The Quest to Solve the Zodiac 340 Cipher

Sam Blake

The University of Melbourne

Success in dealing with unknown ciphers is measured by these 4 things in the order named: perseverance, careful methods of analysis, intuition, luck – Capt. Parker Hitt[1]

[1] Hitt, Capt. Parker, "Manual for the Solution of Military Ciphers", *Army Services Schools Press*, Fort Levenworth, Kansas, 1916

A Brief History of the Zodiac Case

The Zodiac killer

- The Zodiac killer is the pseudonym of an American serial killer who operated from at least the late 1960s to the early 1970s.
- The Zodiac killer murdered five known victims in Northern California.
- The Zodiac killer communicated extensively with law enforcement and the media.
- The Zodiac killer was never caught and is one of the most famous serial killer cold cases in the world.

A Brief History of the Zodiac Case

The Zodiac killer

- The Zodiac killer is the pseudonym of an American serial killer who operated from at least the late 1960s to the early 1970s.
- The Zodiac killer murdered five known victims in Northern California.
- The Zodiac killer communicated extensively with law enforcement and the media.
- The Zodiac killer was never caught and is one of the most famous serial killer cold cases in the world.

A Brief History of the Zodiac Case

The Zodiac killer

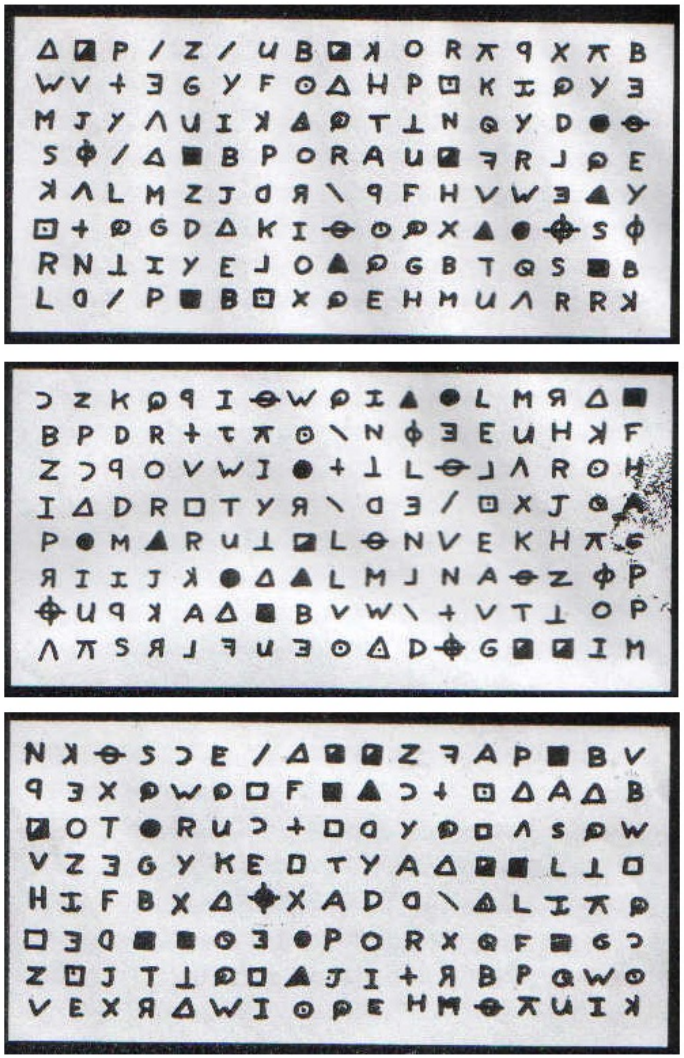
- The Zodiac killer is the pseudonym of an American serial killer who operated from at least the late 1960s to the early 1970s.
- The Zodiac killer murdered five known victims in Northern California.
- The Zodiac killer communicated extensively with law enforcement and the media.
- The Zodiac killer was never caught and is one of the most famous serial killer cold cases in the world.

A Brief History of the Zodiac Case

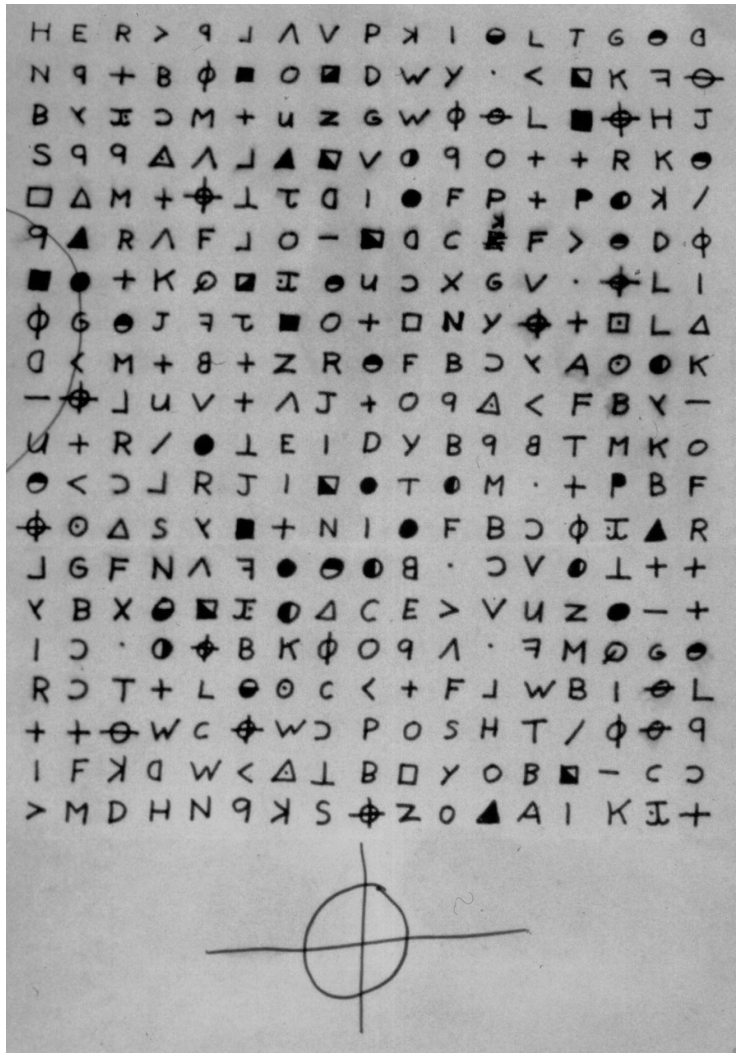
The Zodiac killer

- The Zodiac killer is the pseudonym of an American serial killer who operated from at least the late 1960s to the early 1970s.
- The Zodiac killer murdered five known victims in Northern California.
- The Zodiac killer communicated extensively with law enforcement and the media.
- The Zodiac killer was never caught and is one of the most famous serial killer cold cases in the world.

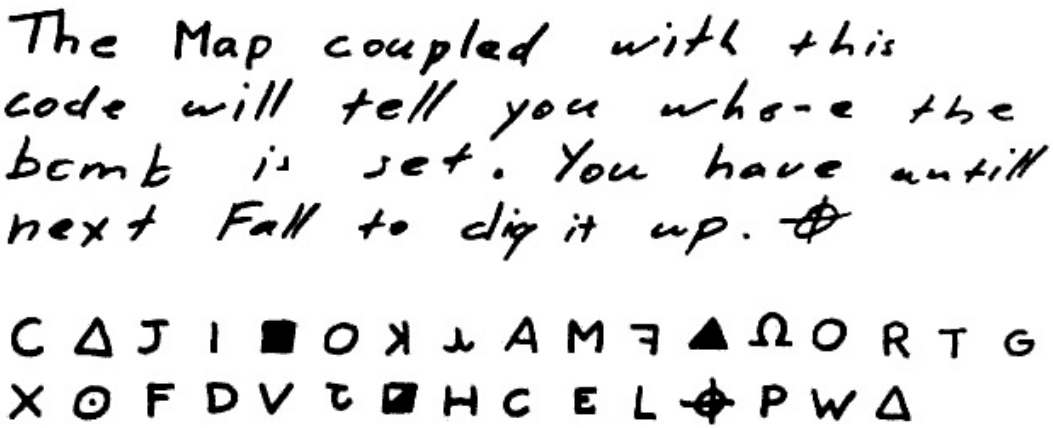
The Z408 Cipher (July 31, 1969)



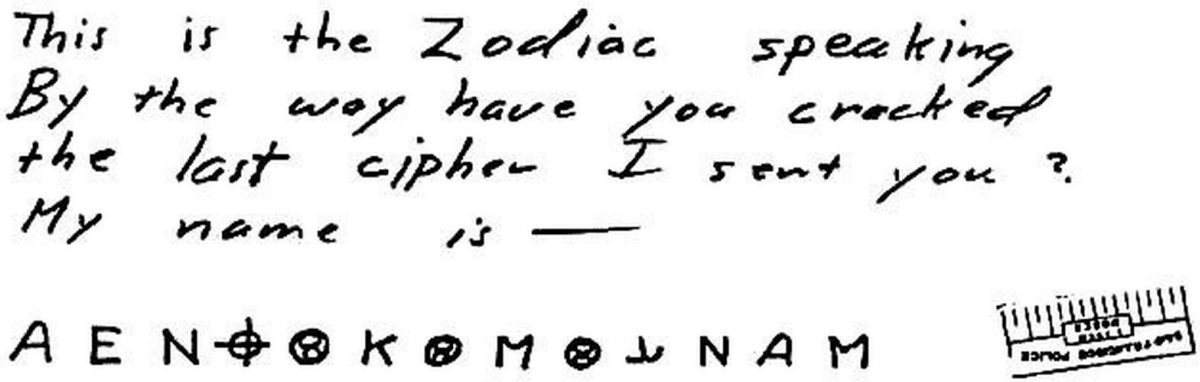
The Z340 Cipher (November 8, 1969)



The Z32 Cipher (April 20, 1970)



The Z13 Cipher (June 26, 1970)



A *simple substitution* replaces each letter in the plaintext with a single letter in the ciphertext. For example

plaintext alphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
ciphertext alphabet:	F	U	V	T	X	I	R	E	H	P	Y	L	A	K	M	Z	G	D	J	W	S	B	Q	O	C	N

Then `"X MARKS THE SPOT"` would be enciphered to `"O AFDYJ WEX JZMW"`.

While there are $26! \approx 2^{88.4}$ different keys, this type of cipher is easily broken using frequency analysis.

A *simple substitution* replaces each letter in the plaintext with a single letter in the ciphertext. For example

plaintext alphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
ciphertext alphabet:	F	U	V	T	X	I	R	E	H	P	Y	L	A	K	M	Z	G	D	J	W	S	B	Q	O	C	N

Then `"X MARKS THE SPOT"` would be enciphered to `"O AFDYJ WEX JZMW"`.

While there are $26! \approx 2^{88.4}$ different keys, this type of cipher is easily broken using frequency analysis.

A *simple substitution* replaces each letter in the plaintext with a single letter in the ciphertext. For example

plaintext alphabet:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
ciphertext alphabet:	F	U	V	T	X	I	R	E	H	P	Y	L	A	K	M	Z	G	D	J	W	S	B	Q	O	C	N

Then `"X MARKS THE SPOT"` would be enciphered to `"O AFDYJ WEX JZMW"`.

While there are $26! \approx 2^{88.4}$ different keys, this type of cipher is easily broken using frequency analysis.

- *Homophonic substitution* attempts to increase the difficulty of frequency analysis attacks by disguising the plaintext letter frequencies.
- The most frequently occurring letters (e – 13.0%, t – 9.1%, a – 8.2%, o – 7.5%, n – 6.7%, $\cdots$) are mapped to multiple cipher symbols.
- As more than 26 characters are required, the Zodiac invented his own symbols including ◪, □, ■, ⟋, △, ⟓, ⍜.

- *Homophonic substitution* attempts to increase the difficulty of frequency analysis attacks by disguising the plaintext letter frequencies.
- The most frequently occurring letters (e – 13.0%, t – 9.1%, a – 8.2%, o – 7.5%, n – 6.7%, $\cdots$) are mapped to multiple cipher symbols.
- As more than 26 characters are required, the Zodiac invented his own symbols including ◪, □, ■, ⟋, △, ↗, ⍜.

- *Homophonic substitution* attempts to increase the difficulty of frequency analysis attacks by disguising the plaintext letter frequencies.
- The most frequently occurring letters (e – 13.0%, t – 9.1%, a – 8.2%, o – 7.5%, n – 6.7%, $\cdots$) are mapped to multiple cipher symbols.
- As more than 26 characters are required, the Zodiac invented his own symbols including ◪, □, ■, ⟋, Δ, ⋊, ⌀.

For example, if the key to encipher E is given by {𝚫, 𝚵, 𝚩, 𝚯}, then

FORCENTURIESKINGSQUE
ENSANDGENERALSHAVERE
LIEDONEFFICIENTCOMMU
NICATIONINORDERTOGOV
ERNTHEIRCOUNTRIESAND
COMMANDTHEIRARMIESAT
THESAMETIMETHEYHAVEA
LLBEENAWAREOFTHECONS
EQUENCESOFTHEIRMESSA
GESFALLINGINTOTHEWRO
NGHANDSREVEALINGPREC
IOUSSECRETSTORIVALNA
TIONSANDBETRAYINGVIT
ALINFORMATIONTOOPPOS
INGFORCESITWASTHETHR
EATOFENEMYINTERCEPTI
ONTHATMOTIVATEDTHEDE
VELOPMENTOFCODESANDC
IPHERSTECHNIQUESFORD
ISGUISINGAMESSAGESOT
HATONLYTHEINTENDEDRE
RECIPIENTCANREADIT

For example, if the key to encipher E is given by {Δ, □, Ɓ, ᘐ}, then

F O R C **E** N T U R I **E** S K I N G S Q U **E**
E N S A N D G **E** N **E** R A L S H A V **E** R **E**
L I **E** D O N **E** F F I C I **E** N T C O M M U
N I C A T I O N I N O R D **E** R T O G O V
E R N T H **E** I R C O U N T R I **E** S A N D
C O M M A N D T H **E** I R A R M I **E** S A T
T H **E** S A M **E** T I M **E** T H **E** Y H A V **E** A
L L B **E** **E** N A W A R **E** O F T H **E** C O N S
E Q U **E** N C **E** S O F T H **E** I R M **E** S S A
G **E** S F A L L I N G I N T O T H **E** W R O
N G H A N D S R **E** V **E** A L I N G P R **E** C
I O U S S **E** C R **E** T S T O R I V A L N A
T I O N S A N D B **E** T R A Y I N G V I T
A L I N F O R M A T I O N T O O P P O S
I N G F O R C **E** S I T W A S T H **E** T H R
E A T O F **E** N **E** M Y I N T **E** R C **E** P T I
O N T H A T M O T I V A T **E** D T H **E** D **E**
V **E** L O P M **E** N T O F C O D **E** S A N D C
I P H **E** R S T **E** C H N I Q U **E** S F O R D
I S G U I S I N G A M **E** S S A G **E** S O T
H A T O N L Y T H **E** I N T **E** N D **E** D R **E**
R **E** C I P I **E** N T C A N R **E** A D I T

For example, if the key to encipher E is given by {Δ, □, Ƀ, ʚ}, then

```
FORCENTURIESKINGSQUE
ENSANDGENERALSHAVERE
LIEDONEFFICIENTCOMMU
NICATIONINORDERTOGOV
ERNTHEIRCOUNTRIESAND
COMMANDTHEIRARMIESAT
THESAMETIMETHEYHAVEA
LLBEENAWAREOFTHECONS
EQUENCESOFTHEIRMESSA
GESFALLINGINTOTHEWRO
NGHANDSREVEALINGPREC
IOUSSECRETSTORIVALNA
TIONSANDBETRAYINGVIT
ALINFORMATIONTOOPPOS
INGFORCESITWASTHETHR
EATOFENEMYINTERCEPTI
ONTHATMOTIVATEDTHEDE
VELOPMENTOFCODESANDC
IPHERSTECHNIQUESFORD
ISGUISINGAMESSAGESOT
HATONLYTHEINTENDEDRE
RECIPIENTCANREADIT
```

```
FORCΔNTURIESKINGSQUE
ENSANDGENERALSHAVERE
LIEDONEFFICIENTCOMMU
NICATIONINORDERTOGOV
ERNTHEIRCOUNTRIESAND
COMMANDTHEIRARMIESAT
THESAMETIMETHEYHAVEA
LLBEENAWAREOFTHECONS
EQUENCESOFTHEIRMESSA
GESFALLINGINTOTHEWRO
NGHANDSREVEALINGPREC
IOUSSECRETSTORIVALNA
TIONSANDBETRAYINGVIT
ALINFORMATIONTOOPPOS
INGFORCESITWASTHETHR
EATOFENEMYINTERCEPTI
ONTHATMOTIVATEDTHEDE
VELOPMENTOFCODESANDC
IPHERSTECHNIQUESFORD
ISGUISINGAMESSAGESOT
HATONLYTHEINTENDEDRE
RECIPIENTCANREADIT
```

For example, if the key to encipher E is given by {Δ, □, Ƀ, ʚ}, then

```
FORCENTURIESKINGSQUE
ENSANDGENERALSHAVERE
LIEDONEFFICIENTCOMMU
NICATIONINORDERTOGOV
ERNTHEIRCOUNTRIESAND
COMMANDTHEIRARMIESAT
THESAMETIMETHEYHAVEA
LLBEENAWAREOFTHECONS
EQUENCESOFTHEIRMESSA
GESFALLINGINTOTHEWRO
NGHANDSREVEALINGPREC
IOUSSECRETSTORIVALNA
TIONSANDBETRAYINGVIT
ALINFORMATIONTOOPPOS
INGFORCESITWASTHETHR
EATOFENEMYINTERCEPTI
ONTHATMOTIVATEDTHEDE
VELOPMENTOFCODESANDC
IPHERSTECHNIQUESFORD
ISGUISINGAMESSAGESOT
HATONLYTHEINTENDEDRE
RECIPIENTCANREADIT
```

```
FORCΔNTURI□SKINGSQUE
ENSANDGENERALSHAVERE
LIEDONEFFICIENTCOMMU
NICATIONINORDERTOGOV
ERNTHEIRCOUNTRIESAND
COMMANDTHEIRARMIESAT
THESAMETIMETHEYHAVEA
LLBEENAWAREOFTHECONS
EQUENCESOFTHEIRMESSA
GESFALLINGINTOTHEWRO
NGHANDSREVEALINGPREC
IOUSSECRETSTORIVALNA
TIONSANDBETRAYINGVIT
ALINFORMATIONTOOPPOS
INGFORCESITWASTHETHR
EATOFENEMYINTERCEPTI
ONTHATMOTIVATEDTHEDE
VELOPMENTOFCODESANDC
IPHERSTECHNIQUESFORD
ISGUISINGAMESSAGESOT
HATONLYTHEINTENDEDRE
RECIPIENTCANREADIT
```

For example, if the key to encipher E is given by {Δ, □, Ɓ, ʚ}, then

FORCENTURIESKINGSQUE
ENSANDGENERALSHAVER E
LIEDONEFFICIENTCOMMU
NICATIONINORDERTOGO V
ERNTHEIRCOUNTRIESAND
COMMANDTHEIRARMIESAT
THESAMETIMETHEYHAVE A
LLBEENAWAREOFTHECONS
EQUENCESOFTHEIRMESSA
GESFALLINGINTOTHEWRO
NGHANDSREVEALINGPREC
IOUSSECRETSTORIVALNA
TIONSANDBETRAYINGVIT
ALINFORMATIONTOOPPOS
INGFORCESITWASTHETHR
EATOFENEMYINTERCEPTI
ONTHATMOTIVATEDTHEDE
VELOPMENTOFCODESAND C
IPHERSTECHNIQUESFORD
ISGUISINGAMESSAGESOT
HATONLYTHEINTENDEDR E
RECIPIENTCANREADIT

FORCΔNTURI□SKINGSQUƁ
ENSANDGENERALSHAVERE
LIEDONEFFICIENTCOMMU
NICATIONINORDERTOGO V
ERNTHEIRCOUNTRIESAND
COMMANDTHEIRARMIESAT
THESAMETIMETHEYHAVE A
LLBEENAWAREOFTHECONS
EQUENCESOFTHEIRMESSA
GESFALLINGINTOTHEWRO
NGHANDSREVEALINGPREC
IOUSSECRETSTORIVALNA
TIONSANDBETRAYINGVIT
ALINFORMATIONTOOPPOS
INGFORCESITWASTHETHR
EATOFENEMYINTERCEPTI
ONTHATMOTIVATEDTHEDE
VELOPMENTOFCODESAND C
IPHERSTECHNIQUESFORD
ISGUISINGAMESSAGESOT
HATONLYTHEINTENDEDRE
RECIPIENTCANREADIT

For example, if the key to encipher E is given by {Δ, □, Ƀ, ᘐ}, then

```
F O R C E N T U R I E S K I N G S Q U E
E N S A N D G E N E R A L S H A V E R E
L I E D O N E F F I C I E N T C O M M U
N I C A T I O N I N O R D E R T O G O V
E R N T H E I R C O U N T R I E S A N D
C O M M A N D T H E I R A R M I E S A T
T H E S A M E T I M E T H E Y H A V E A
L L B E E N A W A R E O F T H E C O N S
E Q U E N C E S O F T H E I R M E S S A
G E S F A L L I N G I N T O T H E W R O
N G H A N D S R E V E A L I N G P R E C
I O U S S E C R E T S T O R I V A L N A
T I O N S A N D B E T R A Y I N G V I T
A L I N F O R M A T I O N T O O P P O S
I N G F O R C E S I T W A S T H E T H R
E A T O F E N E M Y I N T E R C E P T I
O N T H A T M O T I V A T E D T H E D E
V E L O P M E N T O F C O D E S A N D C
I P H E R S T E C H N I Q U E S F O R D
I S G U I S I N G A M E S S A G E S O T
H A T O N L Y T H E I N T E N D E D R E
R E C I P I E N T C A N R E A D I T
```

```
F O R C Δ N T U R I □ S K I N G S Q U Ƀ
ᘐ N S A N D G E N E R A L S H A V E R E
L I E D O N E F F I C I E N T C O M M U
N I C A T I O N I N O R D E R T O G O V
E R N T H E I R C O U N T R I E S A N D
C O M M A N D T H E I R A R M I E S A T
T H E S A M E T I M E T H E Y H A V E A
L L B E E N A W A R E O F T H E C O N S
E Q U E N C E S O F T H E I R M E S S A
G E S F A L L I N G I N T O T H E W R O
N G H A N D S R E V E A L I N G P R E C
I O U S S E C R E T S T O R I V A L N A
T I O N S A N D B E T R A Y I N G V I T
A L I N F O R M A T I O N T O O P P O S
I N G F O R C E S I T W A S T H E T H R
E A T O F E N E M Y I N T E R C E P T I
O N T H A T M O T I V A T E D T H E D E
V E L O P M E N T O F C O D E S A N D C
I P H E R S T E C H N I Q U E S F O R D
I S G U I S I N G A M E S S A G E S O T
H A T O N L Y T H E I N T E N D E D R E
R E C I P I E N T C A N R E A D I T
```

For example, if the key to encipher E is given by {Δ, □, Ƀ, ʘ}, then

F O R C **E** N T U R I **E** S K I N G S Q U **E**
E N S A N D G **E** N **E** R A L S H A V **E** R **E**
L I **E** D O N **E** F F I C I **E** N T C O M M U
N I C A T I O N I N O R D **E** R T O G O V
E R N T H **E** I R C O U N T R I **E** S A N D
C O M M A N D T H **E** I R A R M I **E** S A T
T H **E** S A M **E** T I M **E** T H **E** Y H A V **E** A
L L B **E E** N A W A R **E** O F T H **E** C O N S
E Q U **E** N C **E** S O F T H **E** I R M **E** S S A
G **E** S F A L L I N G I N T O T H **E** W R O
N G H A N D S R **E** V **E** A L I N G P R **E** C
I O U S S **E** C R **E** T S T O R I V A L N A
T I O N S A N D B **E** T R A Y I N G V I T
A L I N F O R M A T I O N T O O P P O S
I N G F O R C **E** S I T W A S T H **E** T H R
E A T O F **E** N **E** M Y I N T **E** R C **E** P T I
O N T H A T M O T I V A T **E** D T H **E** D **E**
V **E** L O P M **E** N T O F C O D **E** S A N D C
I P H **E** R S T **E** C H N I Q U **E** S F O R D
I S G U I S I N G A M **E** S S A G **E** S O T
H A T O N L Y T H **E** I N T **E** N D **E** D R **E**
R **E** C I P I **E** N T C A N R **E** A D I T

F O R C Δ N T U R I □ S K I N G S Q U Ƀ
ʘ N S A N D G Δ N □ R A L S H A V Ƀ R ʘ
L I Δ D O N □ F F I C I Ƀ N T C O M M U
N I C A T I O N I N O R D ʘ R T O G O V
Δ R N T H □ I R C O U N T R I Ƀ S A N D
C O M M A N D T H ʘ I R A R M I Δ S A T
T H □ S A M Ƀ T I M ʘ T H Δ Y H A V □ A
L L B Ƀ ʘ N A W A R Δ O F T H □ C O N S
Ƀ Q U ʘ N C Δ S O F T H □ I R M Ƀ S S A
G ʘ S F A L L I N G I N T O T H Δ W R O
N G H A N D S R □ V Ƀ A L I N G P R ʘ C
I O U S S Δ C R □ T S T O R I V A L N A
T I O N S A N D B Ƀ T R A Y I N G V I T
A L I N F O R M A T I O N T O O P P O S
I N G F O R C ʘ S I T W A S T H Δ T H R
□ A T O F Ƀ N ʘ M Y I N T Δ R C □ P T I
O N T H A T M O T I V A T Ƀ D T H ʘ D Δ
V □ L O P M Ƀ N T O F C O D ʘ S A N D C
I P H Δ R S T □ C H N I Q U Ƀ S F O R D
I S G U I S I N G A M ʘ S S A G Δ S O T
H A T O N L Y T H □ I N T Ƀ N D ʘ D R Δ
R □ C I P I Ƀ N T C A N R ʘ A D I T

A Brief Introduction to Transposition Ciphers

- A transposition cipher is an encryption method where the characters of the plaintext are shifted according to a regular system.
- Mathematically, the transposition is a bijective function.
- For example, a simple transposition cipher is the *columnar transposition*, where the plaintext is written out as in rows and read in columns according to some predetermined order. Given the plaintext:

  ```
  "for centuries kings queens and generals have relied on"
  ```

  We remove the spaces and write it out row–by–row into 12 columns:

  ```
  1  2  3  6  5  4  7  8  9 12 11 10
  ---------------------------------
  f  o  r  c  e  n  t  u  r  i  e  s
  k  i  n  g  s  q  u  e  e  n  s  a
  n  d  g  e  n  e  r  a  l  s  h  a
  v  e  r  e  l  i  e  d  o  n  w  q
  ```

  Then the message is read off in columns in the order specified:

  ```
  fknv oide rngr nqei esnl cgee ture uead relo saaq eshw insn
  ```

A Brief Introduction to Transposition Ciphers

- A transposition cipher is an encryption method where the characters of the plaintext are shifted according to a regular system.
- Mathematically, the transposition is a bijective function.
- For example, a simple transposition cipher is the *columnar transposition*, where the plaintext is written out as in rows and read in columns according to some predetermined order. Given the plaintext:

  `"for centuries kings queens and generals have relied on"`

  We remove the spaces and write it out row–by–row into 12 columns:

```
1  2  3  6  5  4  7  8  9 12 11 10
-------------------------------
f  o  r  c  e  n  t  u  r  i  e  s
k  i  n  g  s  q  u  e  e  n  s  a
n  d  g  e  n  e  r  a  l  s  h  a
v  e  r  e  l  i  e  d  o  n  w  q
```

  Then the message is read off in columns in the order specified:

  `fknv oide rngr nqei esnl cgee ture uead relo saaq eshw insn`

A Brief Introduction to Transposition Ciphers

- A transposition cipher is an encryption method where the characters of the plaintext are shifted according to a regular system.
- Mathematically, the transposition is a bijective function.
- For example, a simple transposition cipher is the *columnar transposition*, where the plaintext is written out as in rows and read in columns according to some predetermined order. Given the plaintext:

```
"for centuries kings queens and generals have relied on"
```

We remove the spaces and write it out row–by–row into 12 columns:

```
 1  2  3  6  5  4  7  8  9 12 11 10
------------------------------------
 f  o  r  c  e  n  t  u  r  i  e  s
 k  i  n  g  s  q  u  e  e  n  s  a
 n  d  g  e  n  e  r  a  l  s  h  a
 v  e  r  e  l  i  e  d  o  n  w  q
```

Then the message is read off in columns in the order specified:

```
fknv oide rngr nqei esnl cgee ture uead relo saaq eshw insn
```

A Brief Introduction to Transposition Ciphers

- A transposition cipher is an encryption method where the characters of the plaintext are shifted according to a regular system.
- Mathematically, the transposition is a bijective function.
- For example, a simple transposition cipher is the *columnar transposition*, where the plaintext is written out as in rows and read in columns according to some predetermined order. Given the plaintext:

  `"for centuries kings queens and generals have relied on"`

  We remove the spaces and write it out row–by–row into 12 columns:

```
1  2  3  6  5  4  7  8  9 12 11 10
------------------------------------
f  o  r  c  e  n  t  u  r  i  e  s
k  i  n  g  s  q  u  e  e  n  s  a
n  d  g  e  n  e  r  a  l  s  h  a
v  e  r  e  l  i  e  d  o  n  w  q
```

  Then the message is read off in columns in the order specified:

  `fknv oide rngr nqei esnl cgee ture uead relo saaq eshw insn`

A Brief Introduction to Transposition Ciphers

- A transposition cipher is an encryption method where the characters of the plaintext are shifted according to a regular system.
- Mathematically, the transposition is a bijective function.
- For example, a simple transposition cipher is the *columnar transposition*, where the plaintext is written out as in rows and read in columns according to some predetermined order. Given the plaintext:

  `"for centuries kings queens and generals have relied on"`

  We remove the spaces and write it out row–by–row into 12 columns:

```
1  2  3  6  5  4  7  8  9 12 11 10
-------------------------------
f  o  r  c  e  n  t  u  r  i  e  s
k  i  n  g  s  q  u  e  e  n  s  a
n  d  g  e  n  e  r  a  l  s  h  a
v  e  r  e  l  i  e  d  o  n  w  q
```

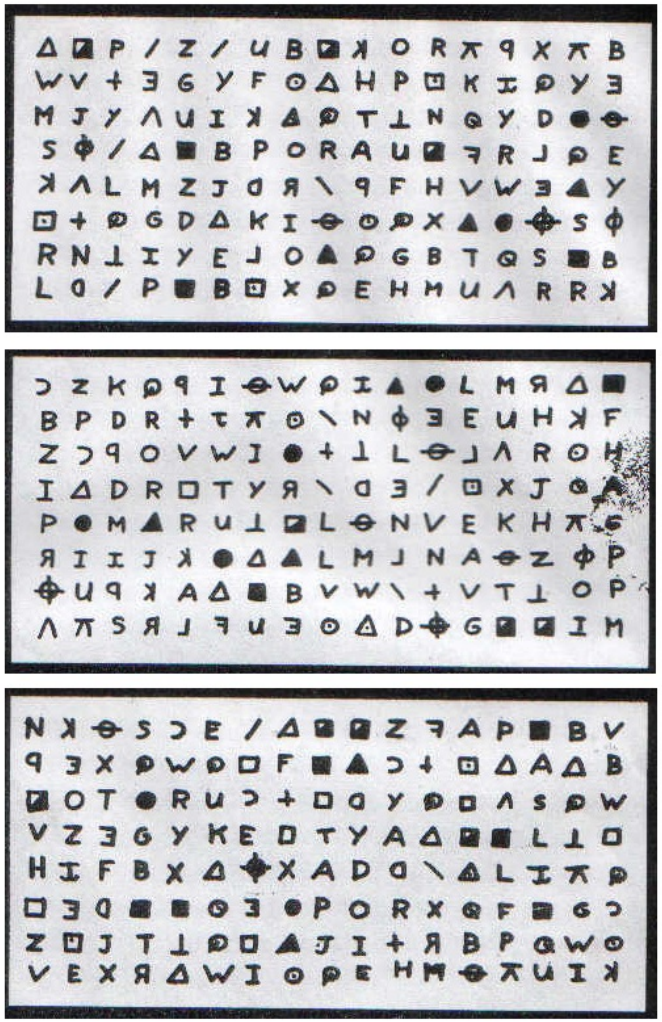
  Then the message is read off in columns in the order specified:

  `fknv oide rngr nqei esnl cgee ture uead relo saaq eshw insn`

The Zodiac's 408 Cipher

History

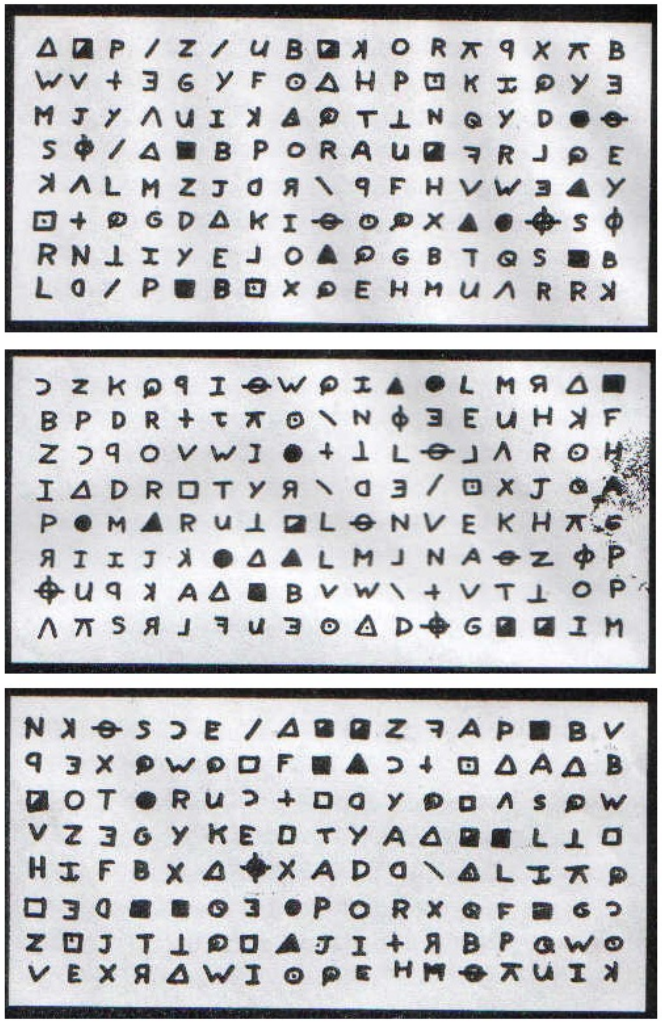
- On July 31, 1969, the Zodiac mailed his first cipher to the press.
- This cipher was mailed in three equally sized segments to the Vallejo Times–Herald, the San Francisco Examiner, and the San Francisco Chronicle.
- The cipher is arranged in a 24×17 grid and contains 408 characters, hence the name: *Z408*.
- The cipher uses 54 distinct symbols.
- The police requested help from the US Navy, FBI, the California Bureau of Investigation, and Donald C.B. Marsh who was the head of the American Cryptogram Association.
- On August 8, 1969, 9 days after the cipher was published, the San Francisco Chronicle received a solution from Donald and Bettye Harden.



The Zodiac's 408 Cipher

History

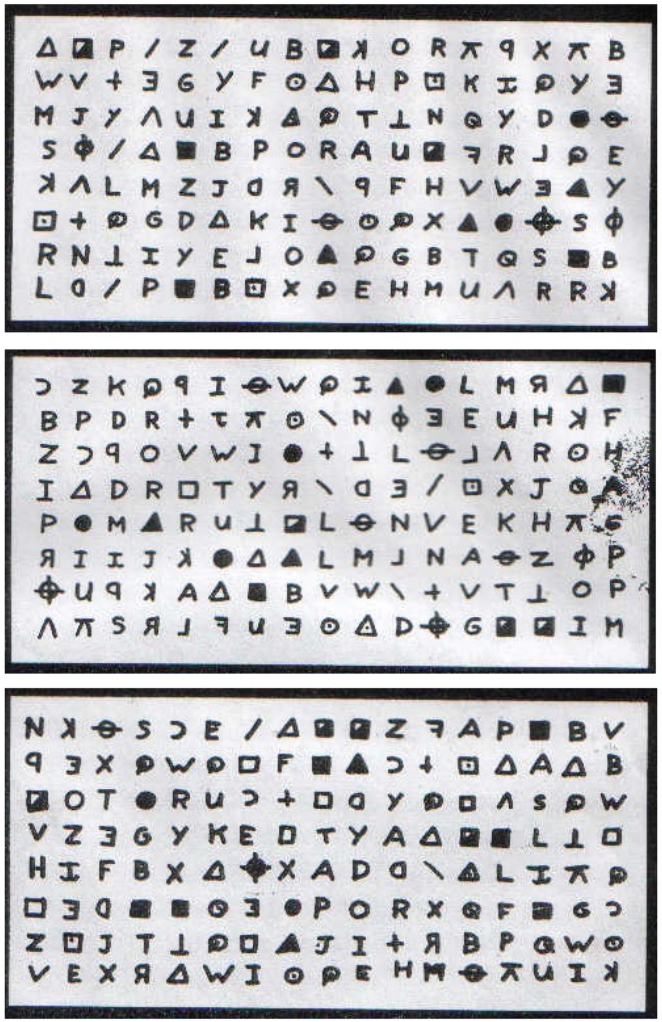
- On July 31, 1969, the Zodiac mailed his first cipher to the press.
- This cipher was mailed in three equally sized segments to the Vallejo Times–Herald, the San Francisco Examiner, and the San Francisco Chronicle.
- The cipher is arranged in a 24×17 grid and contains 408 characters, hence the name: *Z408*.
- The cipher uses 54 distinct symbols.
- The police requested help from the US Navy, FBI, the California Bureau of Investigation, and Donald C.B. Marsh who was the head of the American Cryptogram Association.
- On August 8, 1969, 9 days after the cipher was published, the San Francisco Chronicle received a solution from Donald and Bettye Harden.



The Zodiac's 408 Cipher

History

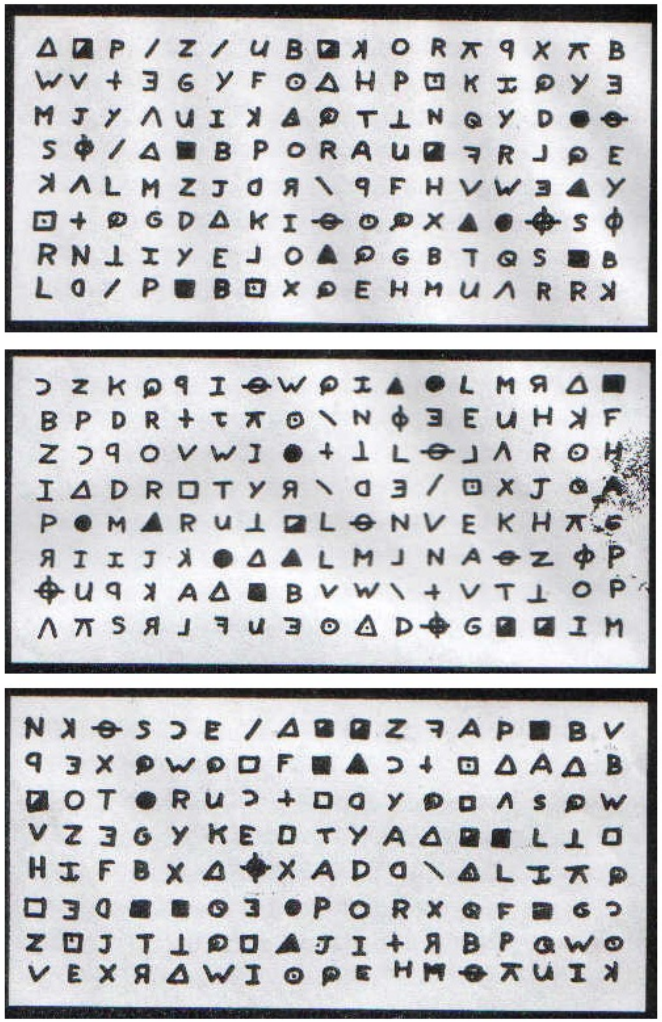
- On July 31, 1969, the Zodiac mailed his first cipher to the press.
- This cipher was mailed in three equally sized segments to the Vallejo Times–Herald, the San Francisco Examiner, and the San Francisco Chronicle.
- The cipher is arranged in a 24×17 grid and contains 408 characters, hence the name: *Z408*.
- The cipher uses 54 distinct symbols.
- The police requested help from the US Navy, FBI, the California Bureau of Investigation, and Donald C.B. Marsh who was the head of the American Cryptogram Association.
- On August 8, 1969, 9 days after the cipher was published, the San Francisco Chronicle received a solution from Donald and Bettye Harden.



The Zodiac's 408 Cipher

History

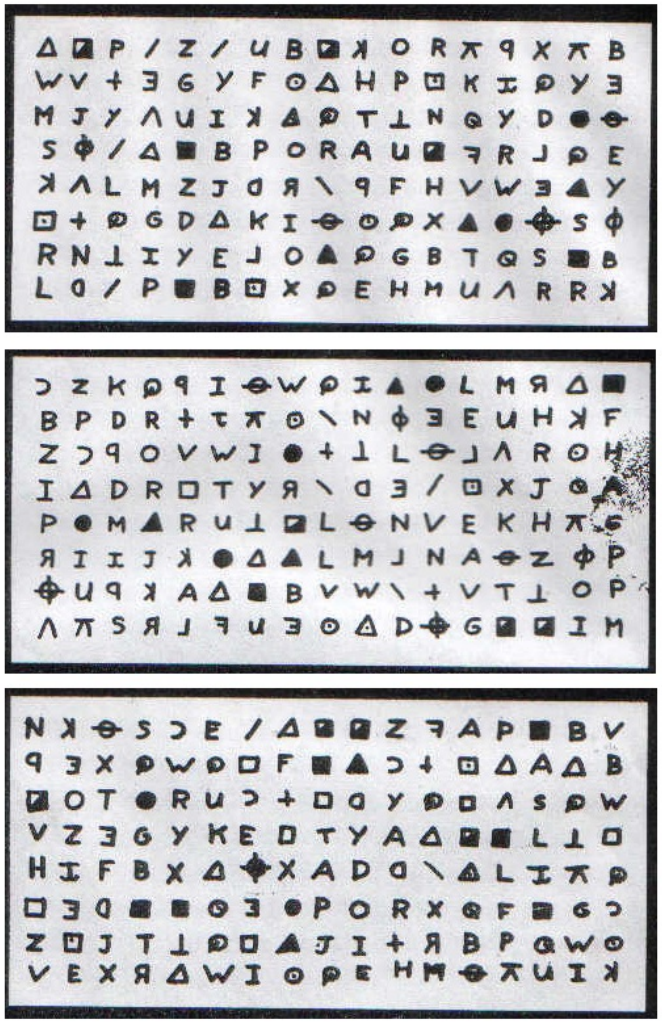
- On July 31, 1969, the Zodiac mailed his first cipher to the press.
- This cipher was mailed in three equally sized segments to the Vallejo Times–Herald, the San Francisco Examiner, and the San Francisco Chronicle.
- The cipher is arranged in a 24×17 grid and contains 408 characters, hence the name: *Z408*.
- The cipher uses 54 distinct symbols.
- The police requested help from the US Navy, FBI, the California Bureau of Investigation, and Donald C.B. Marsh who was the head of the American Cryptogram Association.
- On August 8, 1969, 9 days after the cipher was published, the San Francisco Chronicle received a solution from Donald and Bettye Harden.



The Zodiac's 408 Cipher

History

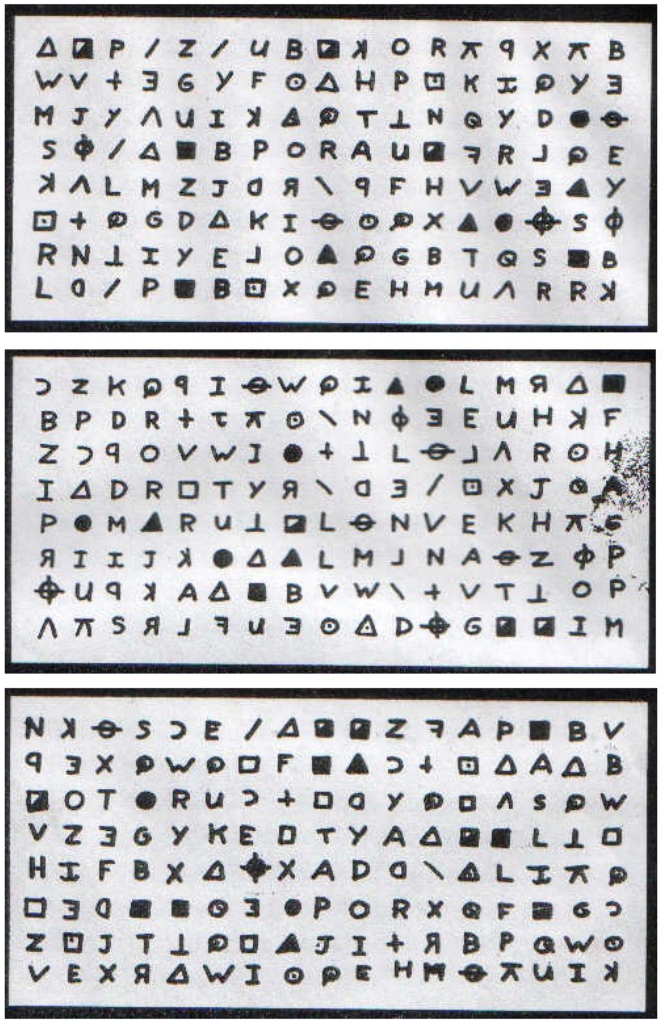
- On July 31, 1969, the Zodiac mailed his first cipher to the press.
- This cipher was mailed in three equally sized segments to the Vallejo Times–Herald, the San Francisco Examiner, and the San Francisco Chronicle.
- The cipher is arranged in a 24×17 grid and contains 408 characters, hence the name: *Z408*.
- The cipher uses 54 distinct symbols.
- The police requested help from the US Navy, FBI, the California Bureau of Investigation, and Donald C.B. Marsh who was the head of the American Cryptogram Association.
- On August 8, 1969, 9 days after the cipher was published, the San Francisco Chronicle received a solution from Donald and Bettye Harden.



The Zodiac's 408 Cipher

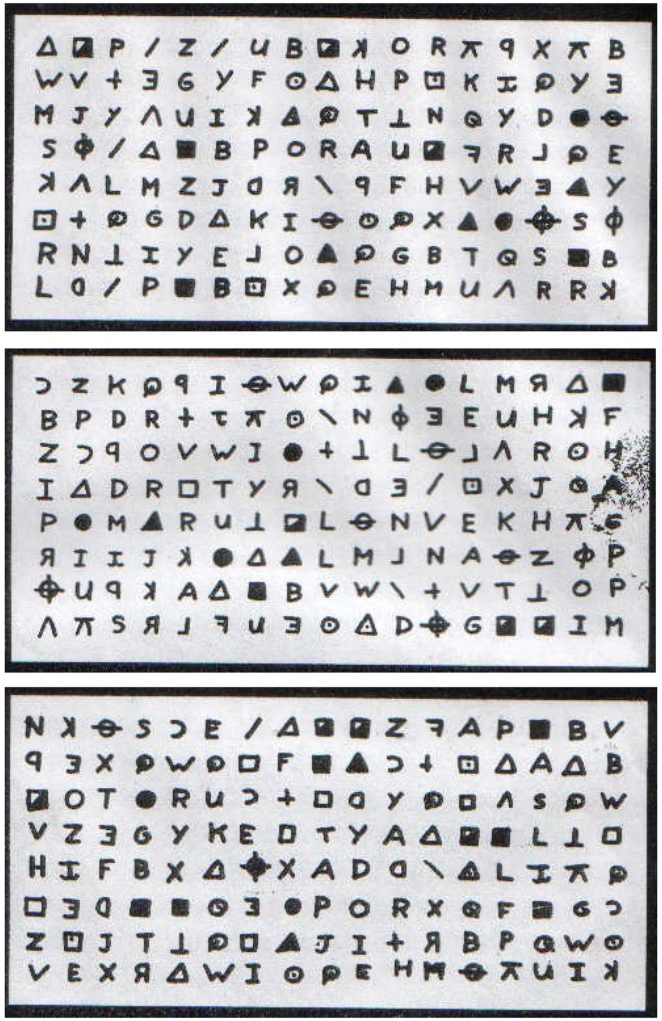
History

- On July 31, 1969, the Zodiac mailed his first cipher to the press.
- This cipher was mailed in three equally sized segments to the Vallejo Times–Herald, the San Francisco Examiner, and the San Francisco Chronicle.
- The cipher is arranged in a 24×17 grid and contains 408 characters, hence the name: *Z408*.
- The cipher uses 54 distinct symbols.
- The police requested help from the US Navy, FBI, the California Bureau of Investigation, and Donald C.B. Marsh who was the head of the American Cryptogram Association.
- On August 8, 1969, 9 days after the cipher was published, the San Francisco Chronicle received a solution from Donald and Bettye Harden.



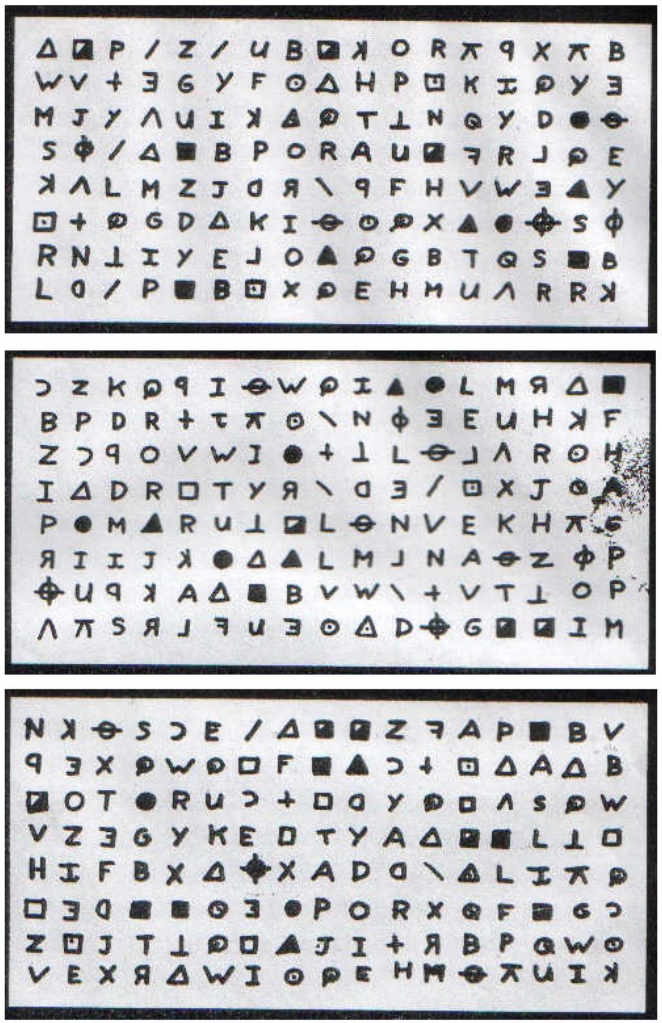
The Hardens' Method

- The Hardens' guessed ◪◪ would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess ◪ → L and ■ → L.
- Then guessed /UBL, /ΔLB, /PLB, /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLIOR → ILIKEKILLING, and so on, and so on ...
- *"Solving the code was trial and error, we tried every combination backwards and forwards"* Bettye Harden.
- After 20 hours of work, the Hardens' had the solution!



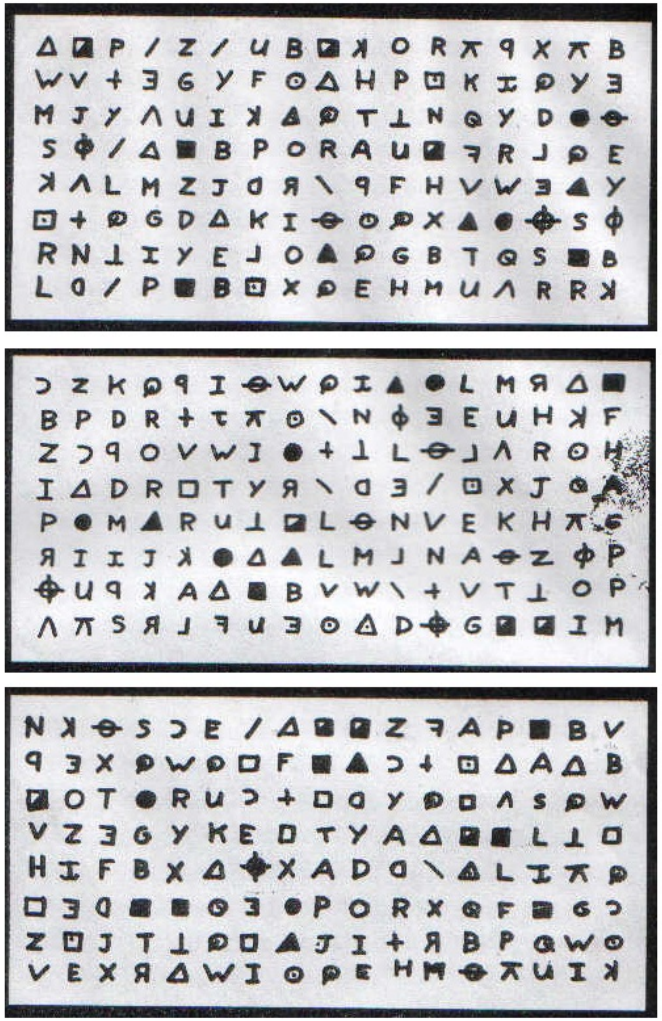
The Hardens' Method

- The Hardens' guessed ◪◪ would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess ◪ → L and ■ → L.
- Then guessed /UBL, /ΔLB, /PLB, /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLKOR → ILIKEKILLING, and so on, and so on ...
- *"Solving the code was trial and error, we tried every combination backwards and forwards"* Bettye Harden.
- After 20 hours of work, the Hardens' had the solution!



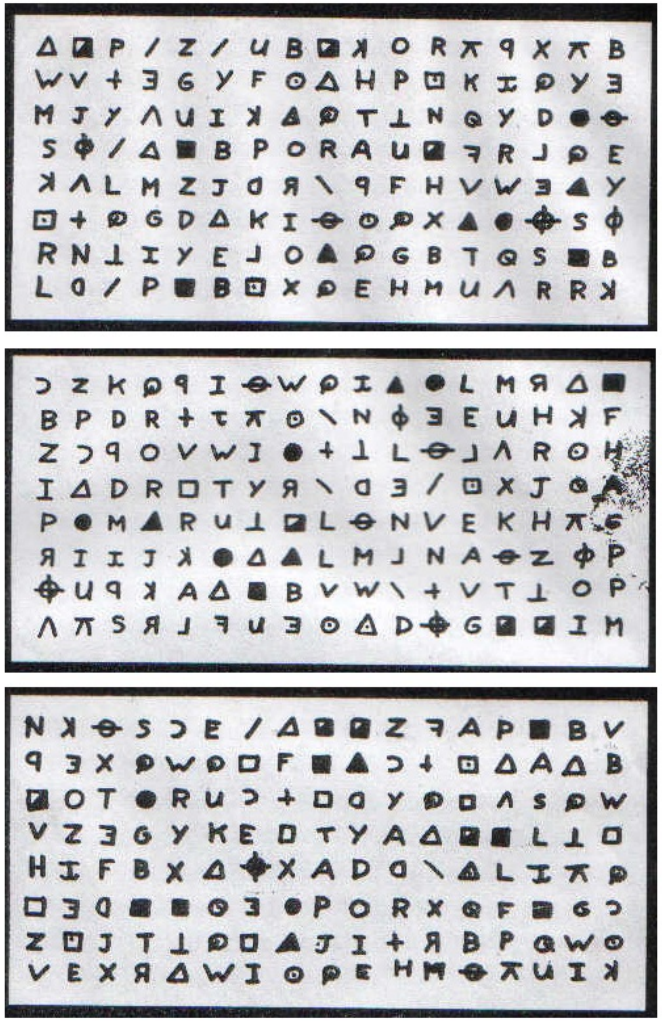
The Hardens' Method

- The Hardens' guessed ◪◪ would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess ◪ → L and ■ → L.
- Then guessed /UBL, /ΔLB, /PLB, /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLKOR → ILIKEKILLING, and so on, and so on ...
- *"Solving the code was trial and error, we tried every combination backwards and forwards"* Bettye Harden.
- After 20 hours of work, the Hardens' had the solution!



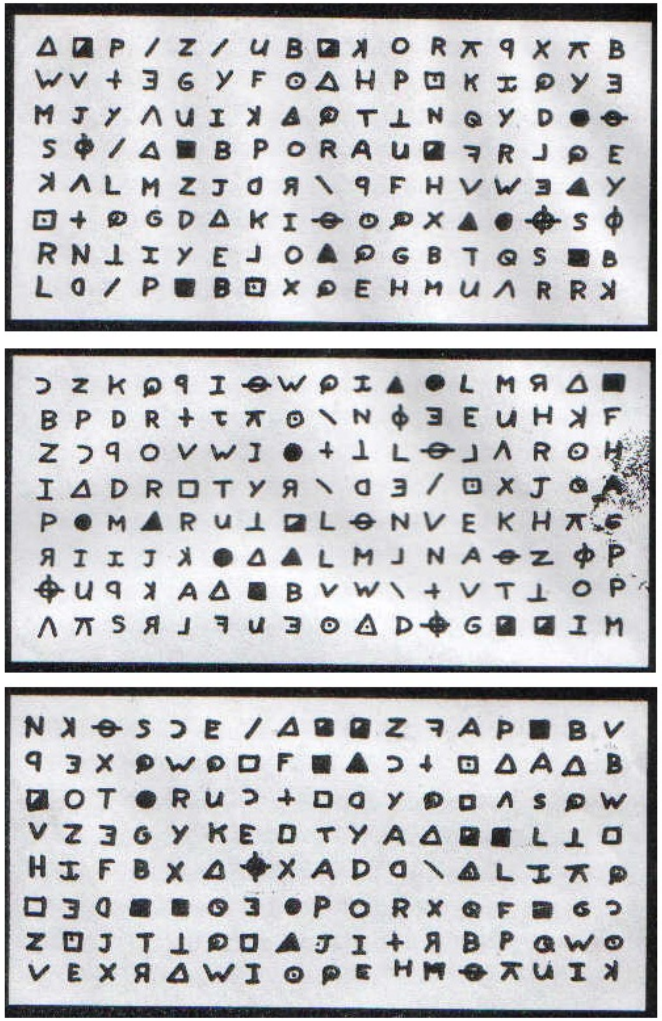
The Hardens' Method

- The Hardens' guessed ◪◪ would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess ◪ → L and ■ → L.
- Then guessed /UBL, /ΔLB, /PLB, /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLKOR → ILIKEKILLING, and so on, and so on ...
- *"Solving the code was trial and error, we tried every combination backwards and forwards"* Bettye Harden.
- After 20 hours of work, the Hardens' had the solution!



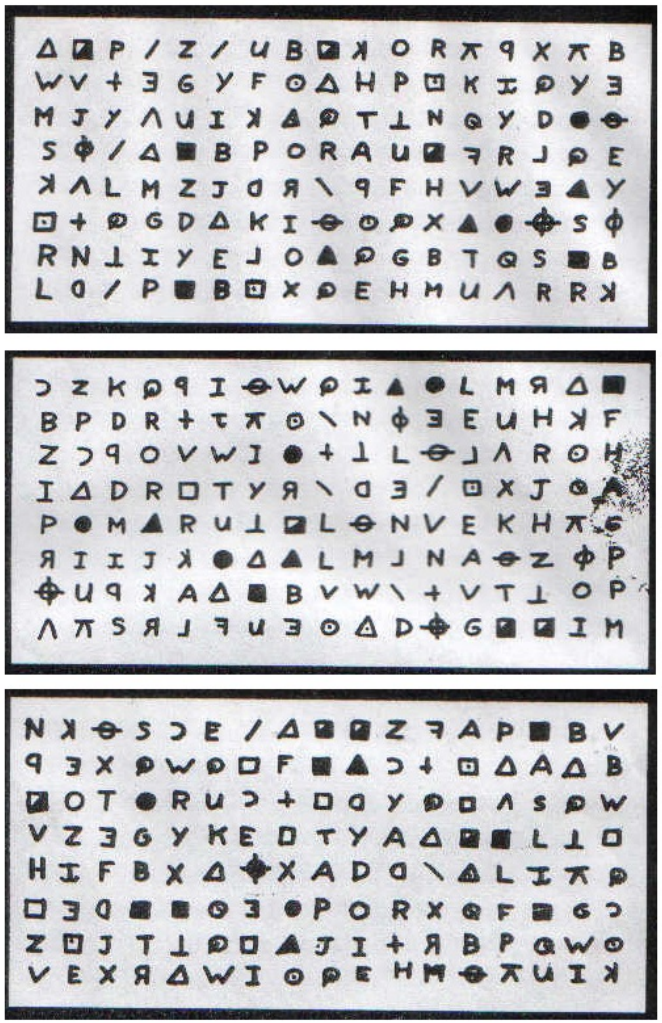
The Hardens' Method

- The Hardens' guessed ◪◪ would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess ◪ → L and ■ → L.
- Then guessed /UBL, /ΔLB, /PLB, /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLXOR → ILIKEKILLING, and so on, and so on ...
- *"Solving the code was trial and error, we tried every combination backwards and forwards"* Bettye Harden.
- After 20 hours of work, the Hardens' had the solution!



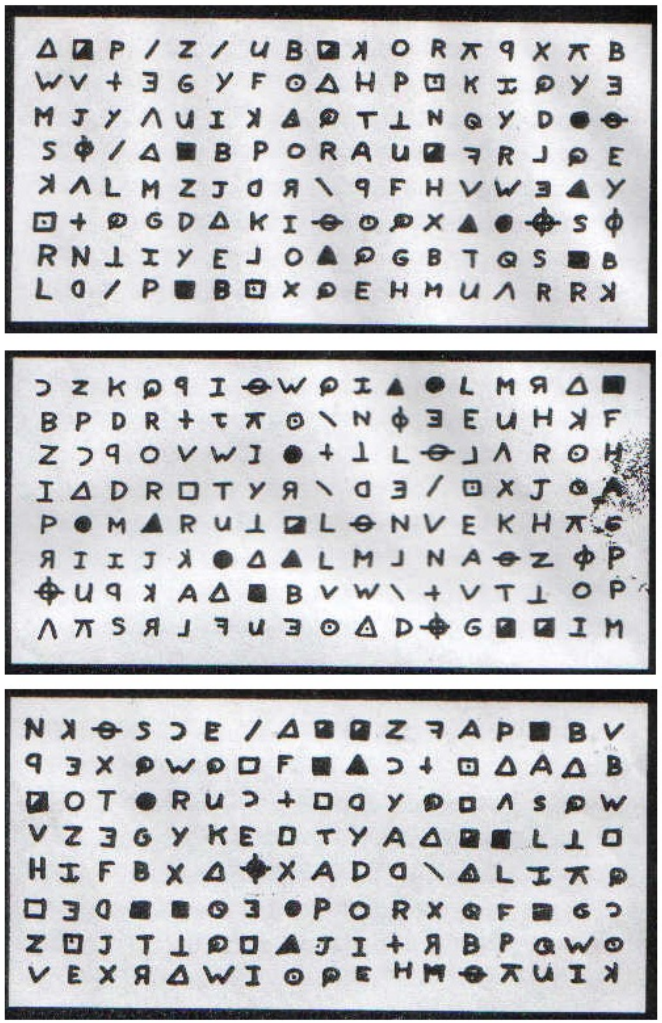
The Hardens' Method

- The Hardens' guessed ◪◪ would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess ◪ → L and ■ → L.
- Then guessed /UBL, /ΔLB, /PLB, /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLXOR → ILIKEKILLING, and so on, and so on ...
- *"Solving the code was trial and error, we tried every combination backwards and forwards"* Bettye Harden.
- After 20 hours of work, the Hardens' had the solution!



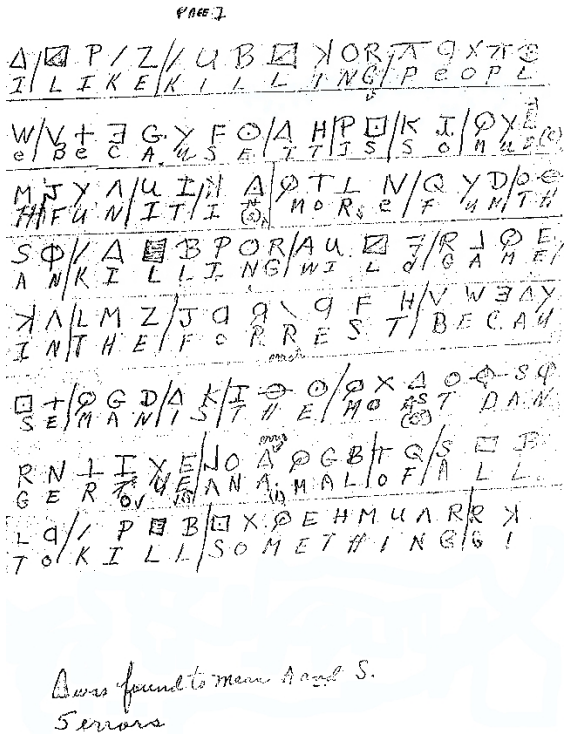
The Hardens' Method

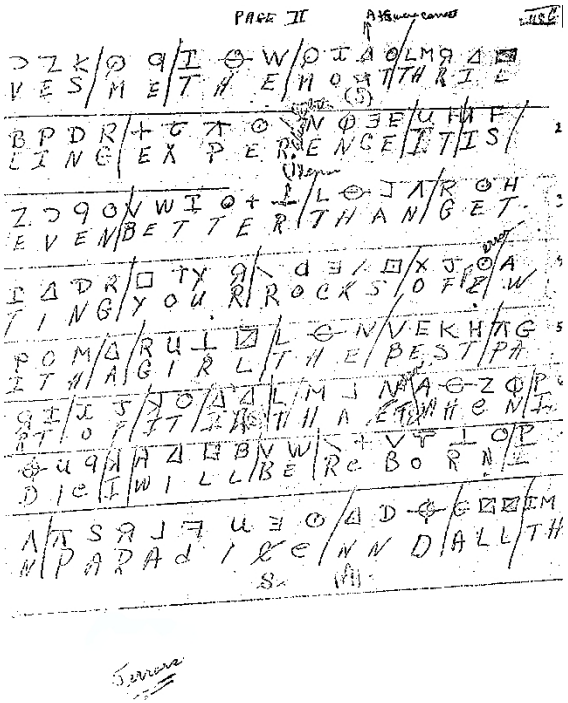
- The Hardens' guessed ◪◪ would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess ◪ → L and ■ → L.
- Then guessed /UBL, /ΔLB, /PLB, /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLKOR → ILIKEKILLING, and so on, and so on ...
- *"Solving the code was trial and error, we tried every combination backwards and forwards"* Bettye Harden.
- After 20 hours of work, the Hardens' had the solution!

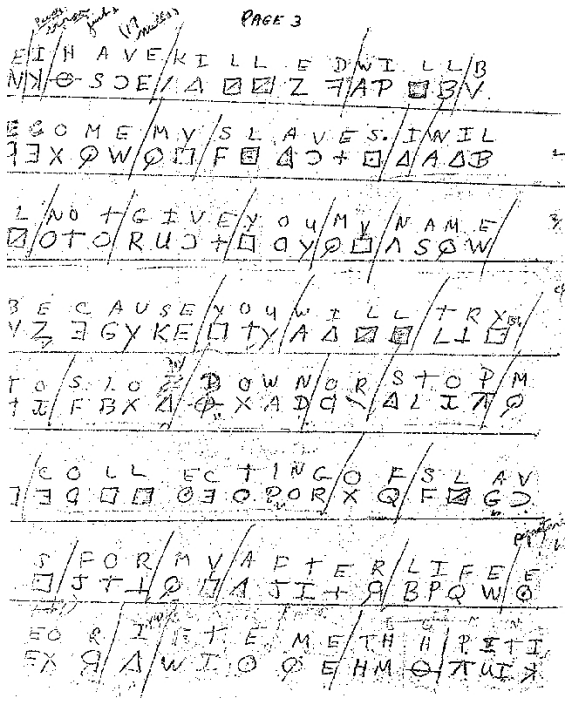


The Zodiac's 408 Cipher

The Hardens' Solution

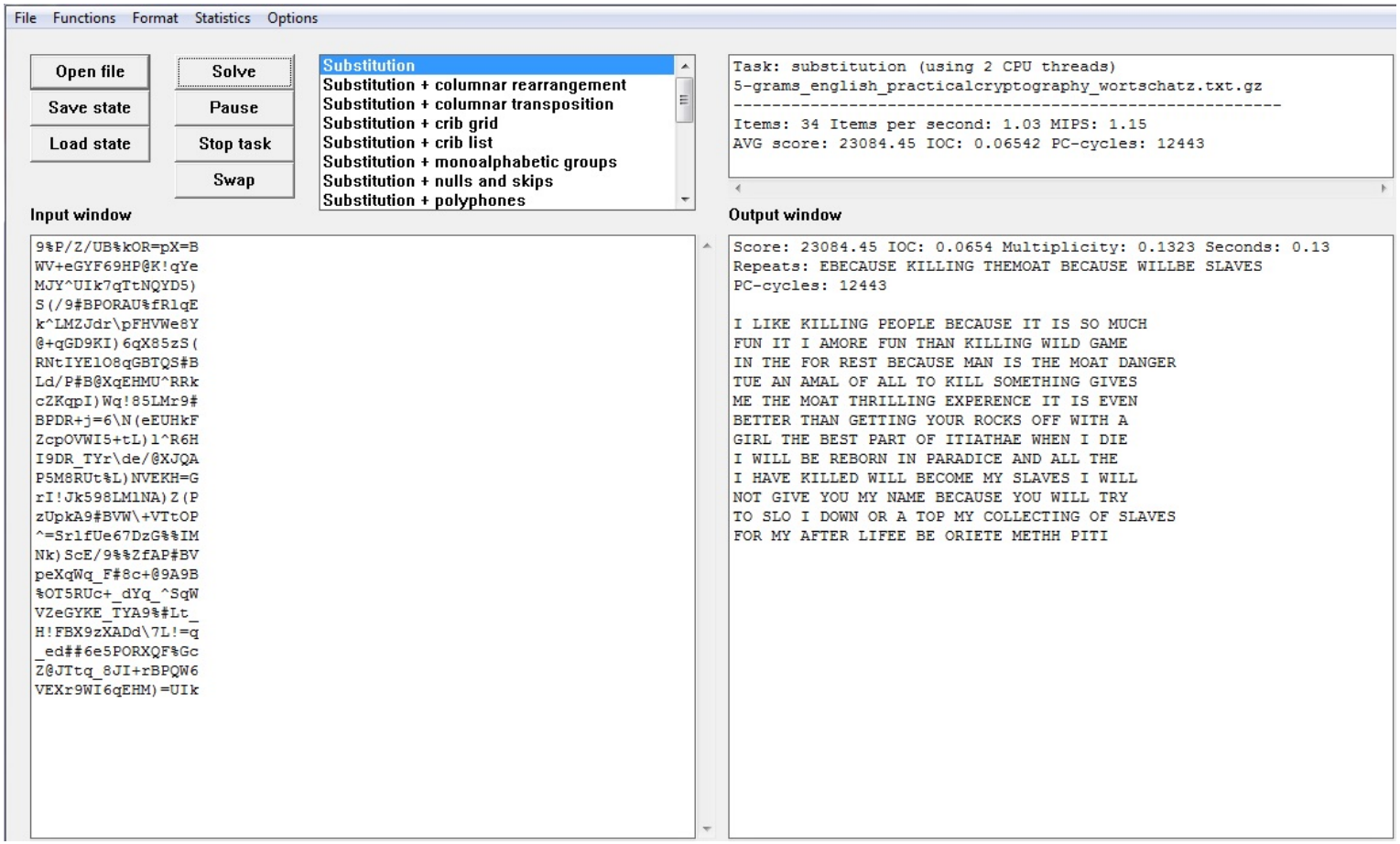






The final 18 characters, EBEORIETEMETHHPITI, appear to be filler.

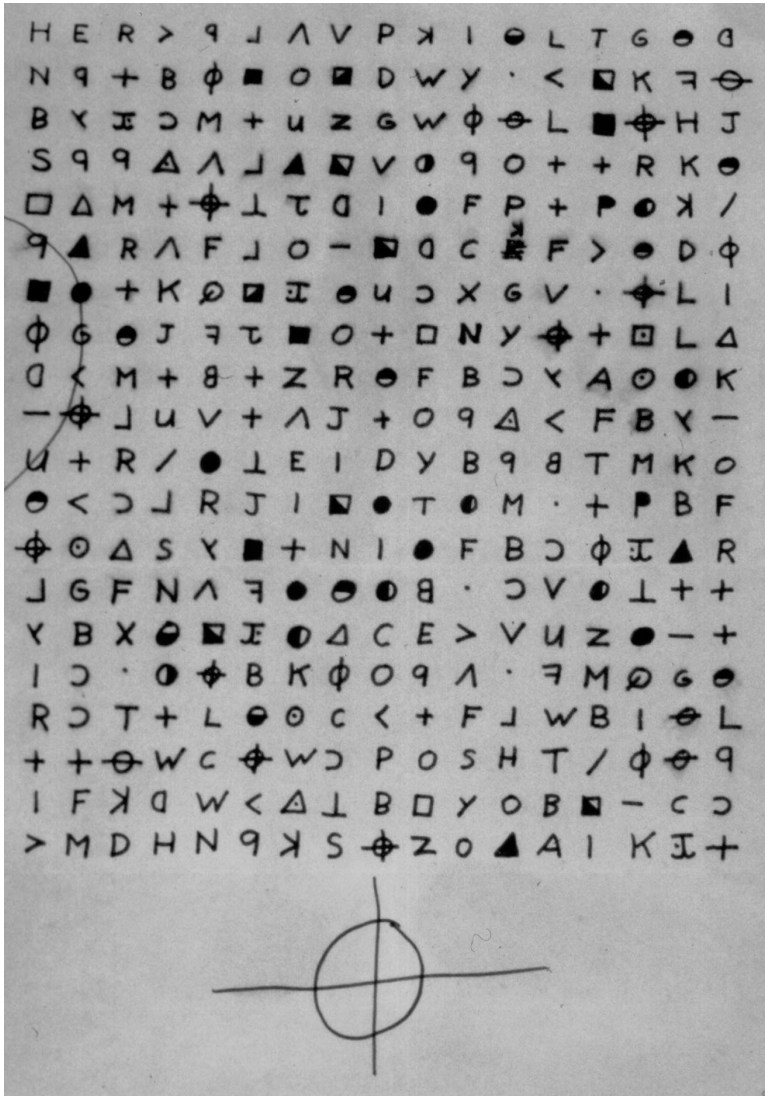
Fast forward half a century and azdecrypt can solve the Z408 cipher in less than a second.



The Zodiac's 340 Cipher

History

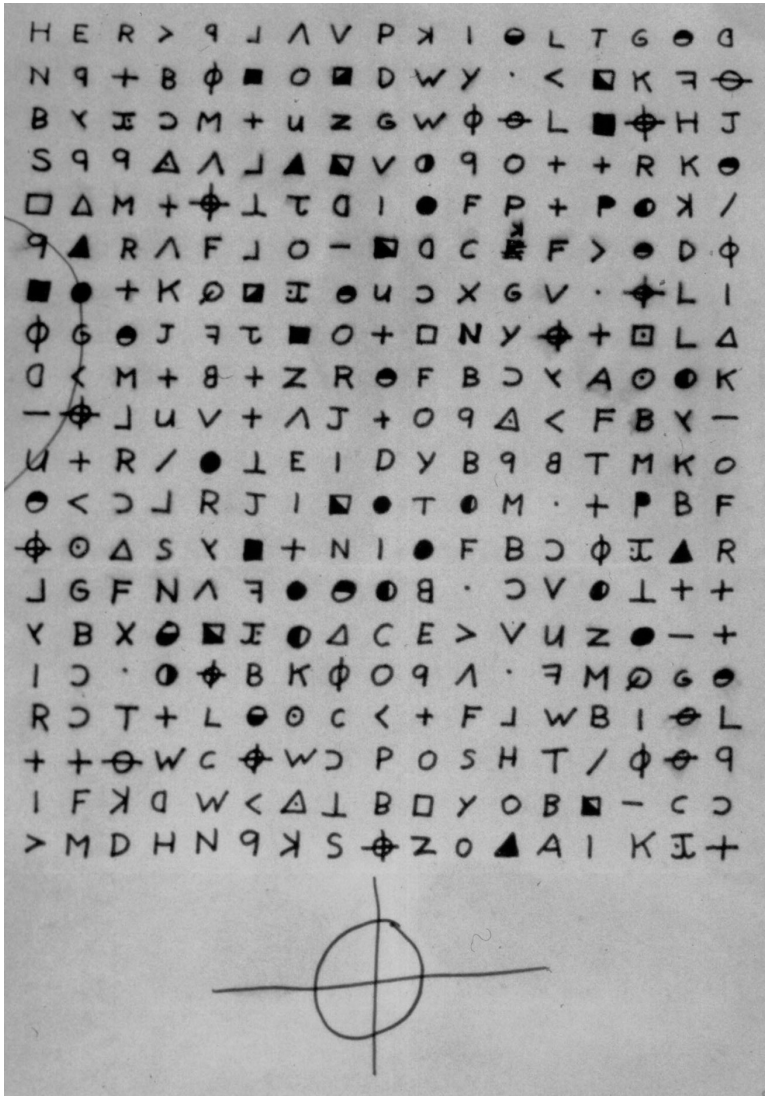
- On November 8, 1969, the Zodiac mailed his second cipher to the San Francisco Chronicle.
- This cipher is arranged in a 20×17 grid and contains 340 characters, hence the name: *Z340*.
- This cipher uses 63 distinct symbols.
- Unlike the Z408, this cipher has survived constant attacks for 50 years.
- Dan Olson (FBI CRRU) said this cipher has been on the FBI's top 10 list of unsolved ciphers for 50 years.



The Zodiac's 340 Cipher

History

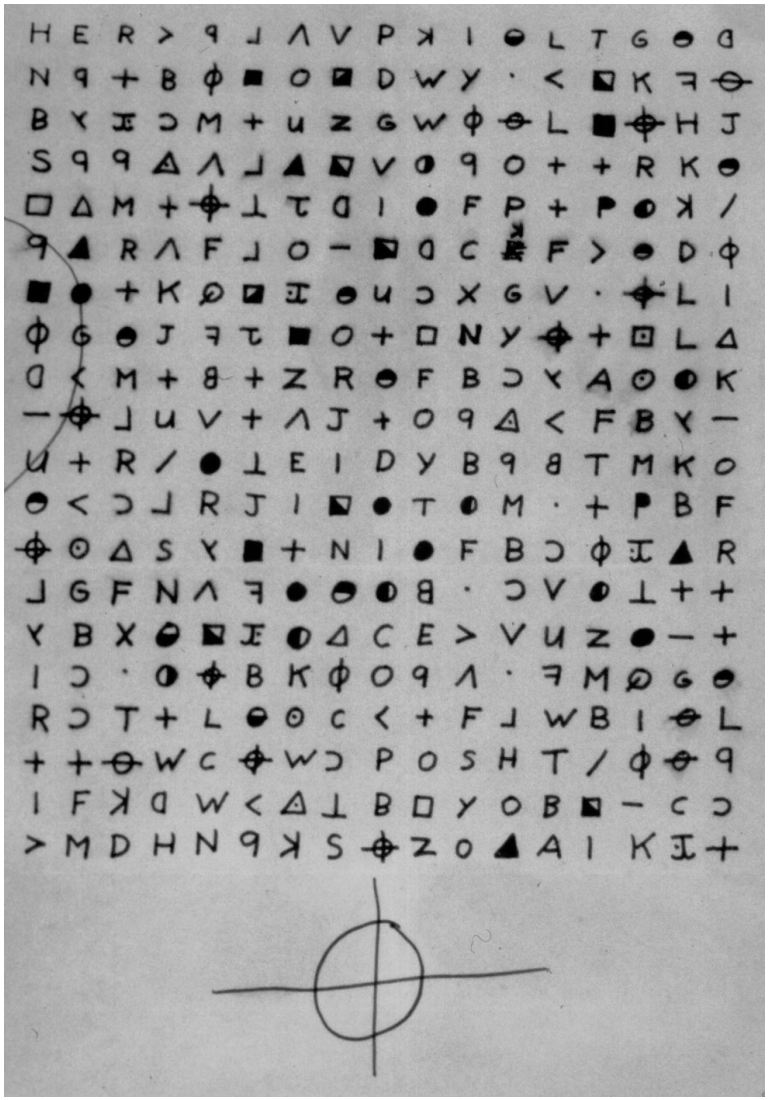
- On November 8, 1969, the Zodiac mailed his second cipher to the San Francisco Chronicle.
- This cipher is arranged in a 20×17 grid and contains 340 characters, hence the name: *Z340*.
- This cipher uses 63 distinct symbols.
- Unlike the Z408, this cipher has survived constant attacks for 50 years.
- Dan Olson (FBI CRRU) said this cipher has been on the FBI's top 10 list of unsolved ciphers for 50 years.



The Zodiac's 340 Cipher

History

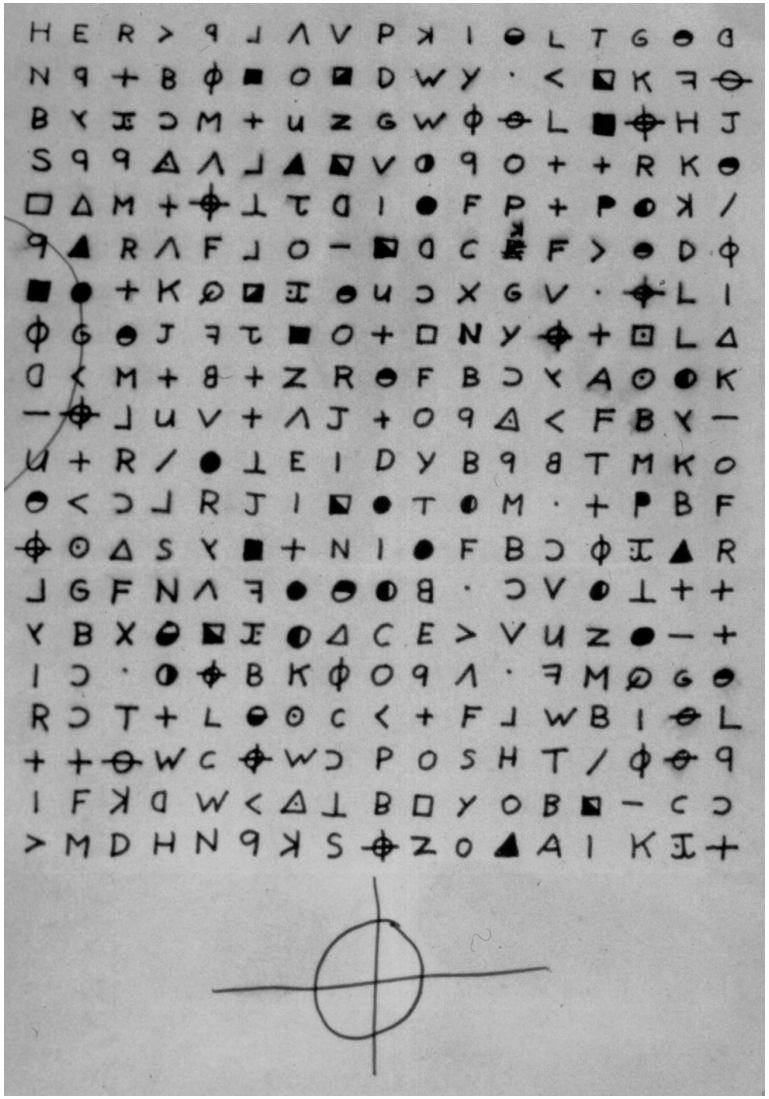
- On November 8, 1969, the Zodiac mailed his second cipher to the San Francisco Chronicle.
- This cipher is arranged in a 20×17 grid and contains 340 characters, hence the name: *Z340*.
- This cipher uses 63 distinct symbols.
- Unlike the Z408, this cipher has survived constant attacks for 50 years.
- Dan Olson (FBI CRRU) said this cipher has been on the FBI's top 10 list of unsolved ciphers for 50 years.



The Zodiac's 340 Cipher

History

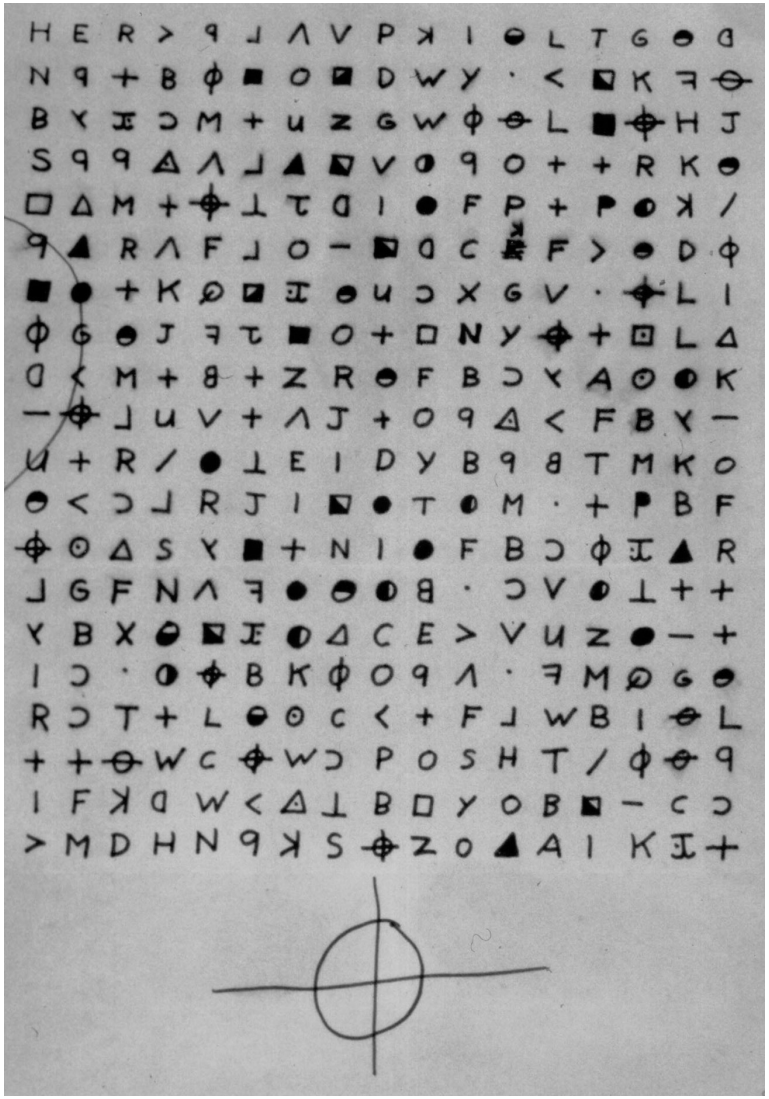
- On November 8, 1969, the Zodiac mailed his second cipher to the San Francisco Chronicle.
- This cipher is arranged in a 20×17 grid and contains 340 characters, hence the name: *Z340*.
- This cipher uses 63 distinct symbols.
- Unlike the Z408, this cipher has survived constant attacks for 50 years.
- Dan Olson (FBI CRRU) said this cipher has been on the FBI's top 10 list of unsolved ciphers for 50 years.



The Zodiac's 340 Cipher

History

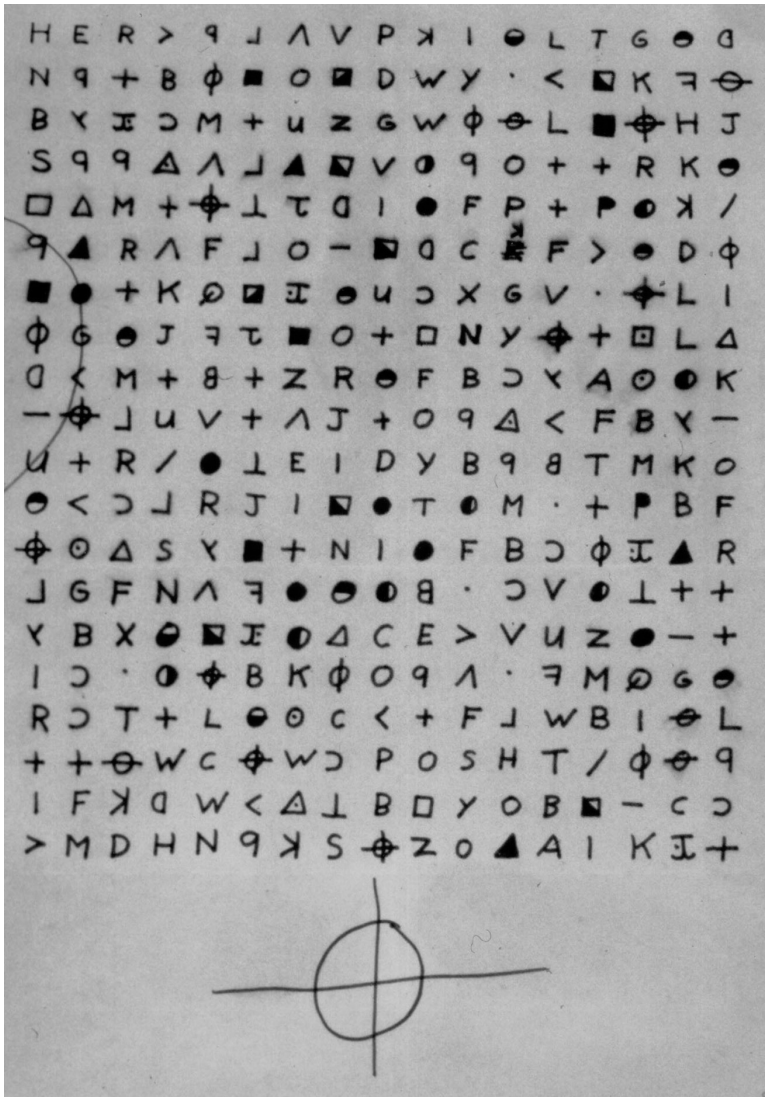
- On November 8, 1969, the Zodiac mailed his second cipher to the San Francisco Chronicle.
- This cipher is arranged in a 20×17 grid and contains 340 characters, hence the name: *Z340*.
- This cipher uses 63 distinct symbols.
- Unlike the Z408, this cipher has survived constant attacks for 50 years.
- Dan Olson (FBI CRRU) said this cipher has been on the FBI's top 10 list of unsolved ciphers for 50 years.



The Zodiac's 340 Cipher

Why do we care?

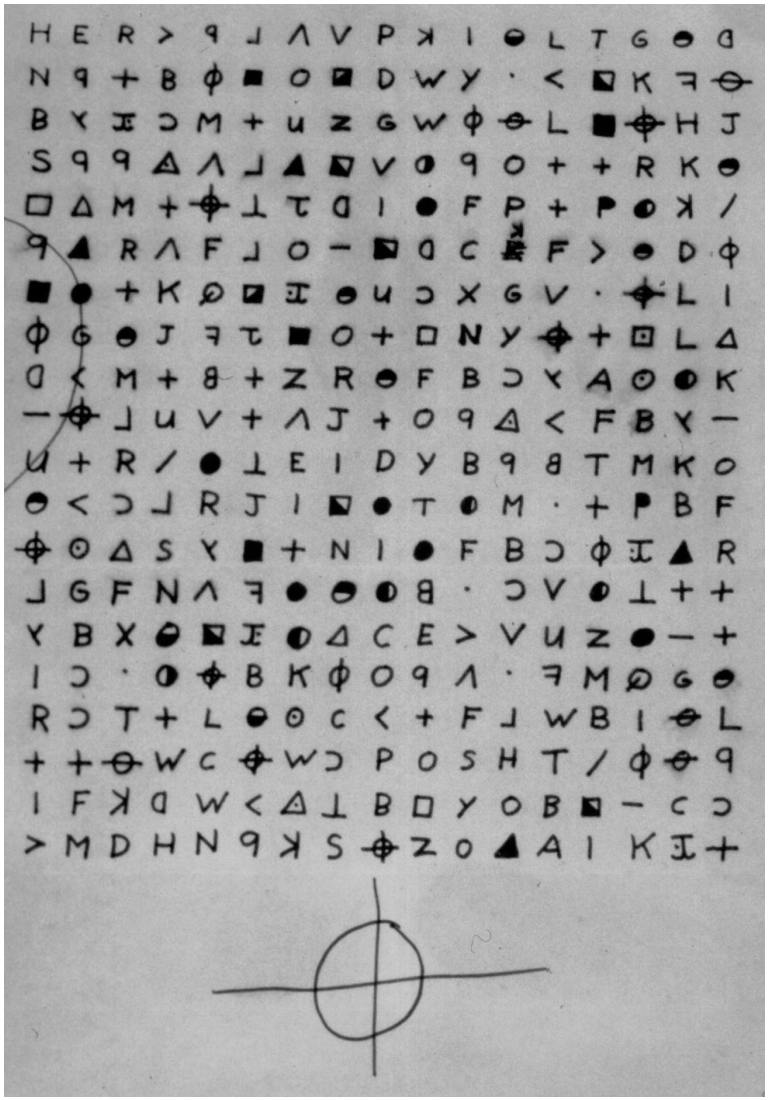
- If the cipher was decoded, its contents would be of interest to investigators.
- The method of construction may also give clues to his education or work background.
- From the point of view of cryptography, the solution to Z340 is considered a grand challenge.
- A large number academic papers have been written on attacks and analysis of the Z340.



The Zodiac's 340 Cipher

Why do we care?

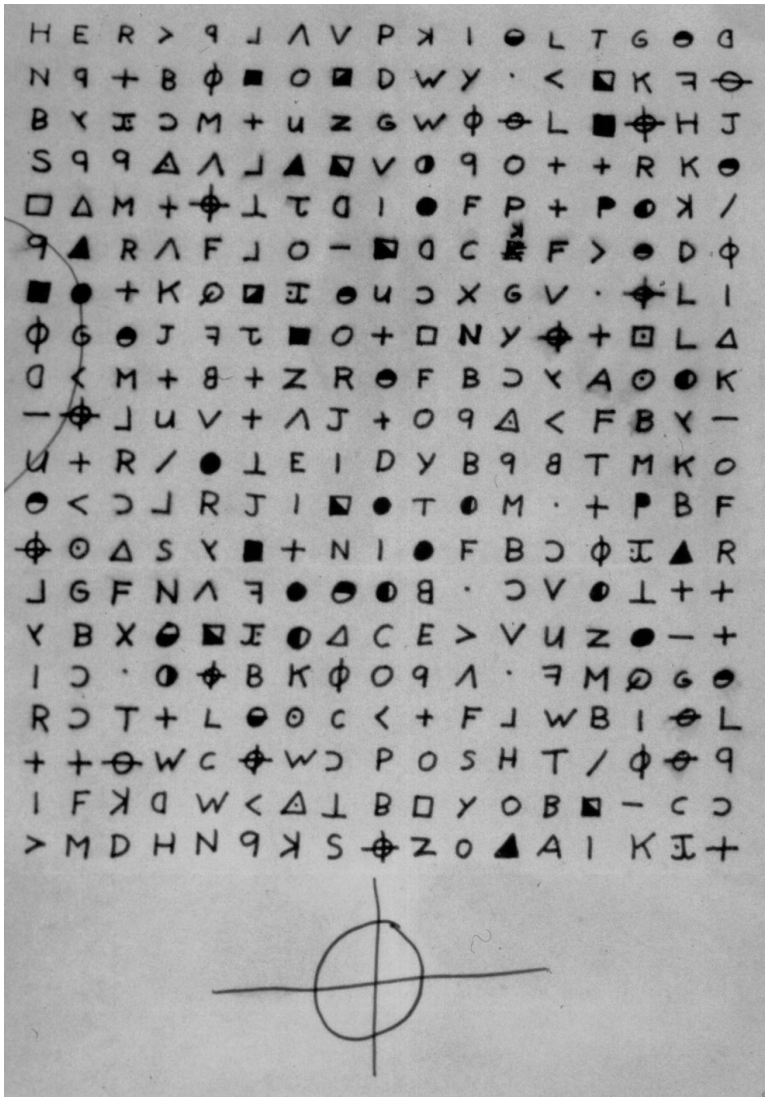
- If the cipher was decoded, its contents would be of interest to investigators.
- The method of construction may also give clues to his education or work background.
- From the point of view of cryptography, the solution to Z340 is considered a grand challenge.
- A large number academic papers have been written on attacks and analysis of the Z340.



The Zodiac's 340 Cipher

Why do we care?

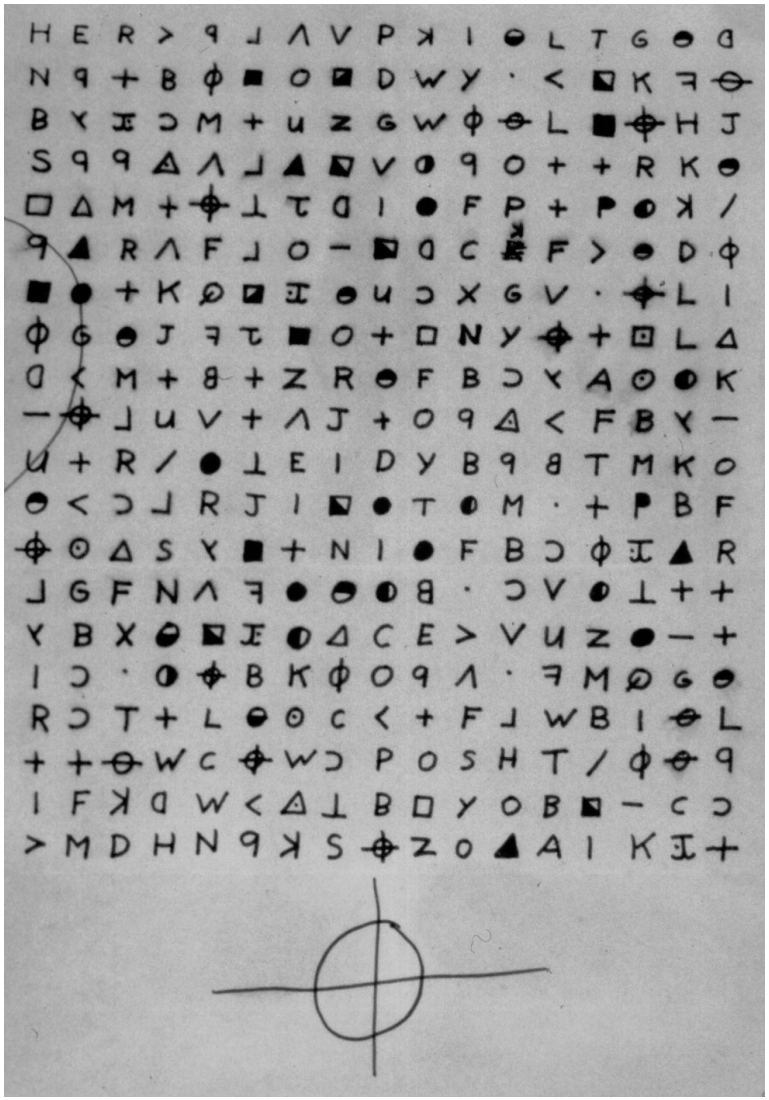
- If the cipher was decoded, its contents would be of interest to investigators.
- The method of construction may also give clues to his education or work background.
- From the point of view of cryptography, the solution to Z340 is considered a grand challenge.
- A large number academic papers have been written on attacks and analysis of the Z340.



The Zodiac's 340 Cipher

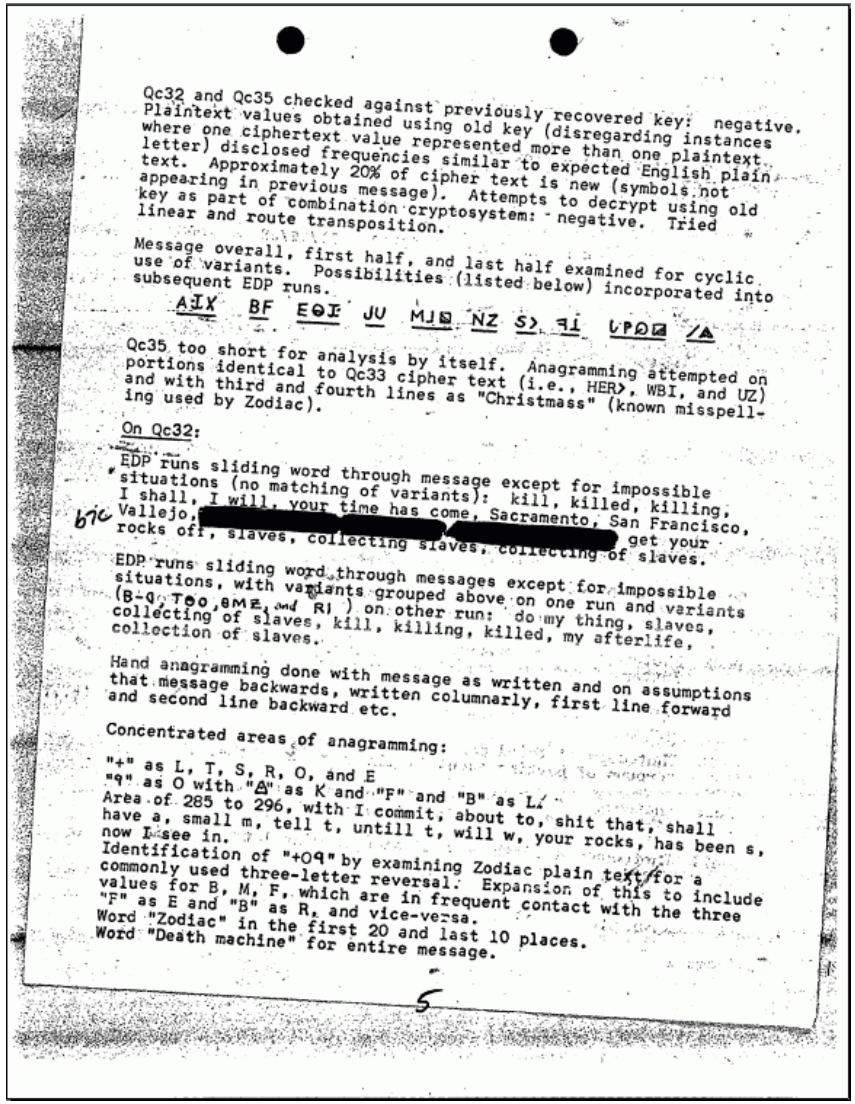
Why do we care?

- If the cipher was decoded, its contents would be of interest to investigators.
- The method of construction may also give clues to his education or work background.
- From the point of view of cryptography, the solution to Z340 is considered a grand challenge.
- A large number academic papers have been written on attacks and analysis of the Z340.



Who has worked on solving Z340 in the past?

- FBI Cryptanalysis and Racketeering Records Unit (CRRU)
- NSA
- CIA
- Many university projects.
- Robert Graysmith's book *Zodiac* talks of computer–based attacks of the Z340 in the 1970s.
- Members of the American Cryptogram Association (ACA), including then president Donald C.B. Marsh.
- Many private citizens including forum users from zodiackillersite.com, zodiackiller.com and zodiackillerfacts.com



Qc32 and Qc35 checked against previously recovered key: negative. Plaintext values obtained using old key (disregarding instances where one ciphertext value represented more than one plaintext letter) disclosed frequencies similar to expected English plain text. Approximately 20% of cipher text is new (symbols not appearing in previous message). Attempts to decrypt using old key as part of combination cryptosystem: negative. Tried linear and route transposition.

Message overall, first half, and last half examined for cyclic use of variants. Possibilities (listed below) incorporated into subsequent EDP runs.

AIX BF EOI JU MJ NZ S> 9i UPO /A

Qc35 too short for analysis by itself. Anagramming attempted on portions identical to Qc33 cipher text (i.e., HER>, WBI, and UZ) and with third and fourth lines as "Christmass" (known misspelling used by Zodiac).

On Qc32:

EDP runs sliding word through message except for impossible situations (no matching of variants): kill, killed, killing, I shall, I will, your time has come, Sacramento, San Francisco, Vallejo, [redacted] get your rocks off, slaves, collecting slaves, collecting of slaves.

EDP runs sliding word through messages except for impossible situations, with variants grouped above on one run and variants (B-9, T∞, ME, and RI) on other run: do my thing, slaves, collecting of slaves, kill, killing, killed, my afterlife, collection of slaves.

Hand anagramming done with message as written and on assumptions that message backwards, written columnarly, first line forward and second line backward etc.

Concentrated areas of anagramming:

"+" as L, T, S, R, O, and E
"9" as O with "Δ" as K and "F" and "B" as L.
Area of 285 to 296, with I commit, about to, shit that, shall have a, small m, tell t, untill t, will w, your rocks, has been s, now I see in.
Identification of "+O9" by examining Zodiac plain text for a commonly used three-letter reversal. Expansion of this to include values for B, M, F, which are in frequent contact with the three "F" as E and "B" as R, and vice-versa.
Word "Zodiac" in the first 20 and last 10 places.
Word "Death machine" for entire message.

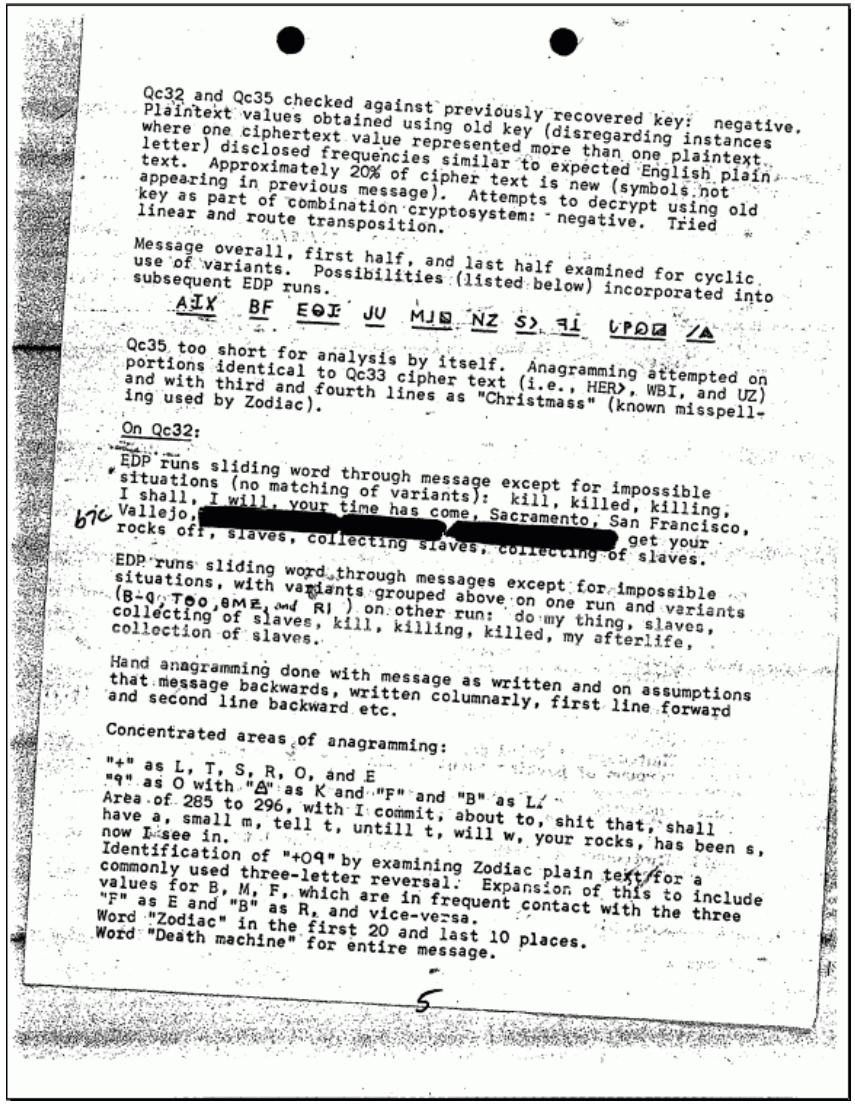
5

The Zodiac's 340 Cipher

Previous efforts to solve Z340

Who has worked on solving Z340 in the past?

- FBI Cryptanalysis and Racketeering Records Unit (CRRU)
- NSA
- CIA
- Many university projects.
- Robert Graysmith's book *Zodiac* talks of computer–based attacks of the Z340 in the 1970s.
- Members of the American Cryptogram Association (ACA), including then president Donald C.B. Marsh.
- Many private citizens including forum users from zodiackillersite.com, zodiackiller.com and zodiackillerfacts.com



Qc32 and Qc35 checked against previously recovered key: negative. Plaintext values obtained using old key (disregarding instances where one ciphertext value represented more than one plaintext letter) disclosed frequencies similar to expected English plain text. Approximately 20% of cipher text is new (symbols not appearing in previous message). Attempts to decrypt using old key as part of combination cryptosystem: negative. Tried linear and route transposition.

Message overall, first half, and last half examined for cyclic use of variants. Possibilities (listed below) incorporated into subsequent EDP runs.

AIX BF EOI JU MJ NZ S> 7i LPO /A

Qc35 too short for analysis by itself. Anagramming attempted on portions identical to Qc33 cipher text (i.e., HER>, WBI, and UZ) and with third and fourth lines as "Christmass" (known misspelling used by Zodiac).

On Qc32:

EDP runs sliding word through message except for impossible situations (no matching of variants): kill, killed, killing, I shall, I will, your time has come, Sacramento, San Francisco, Vallejo, [redacted] get your rocks off, slaves, collecting slaves, collecting of slaves.

EDP runs sliding word through messages except for impossible situations, with variants grouped above on one run and variants collecting of slaves, kill, killing, killed, my afterlife, collection of slaves.

Hand anagramming done with message as written and on assumptions that message backwards, written columnarly, first line forward and second line backward etc.

Concentrated areas of anagramming:

"+" as L, T, S, R, O, and E
"9" as O with "Δ" as K and "F" and "B" as L.
Area of 285 to 296, with I commit, about to, shit that, shall have a, small m, tell t, untill t, will w, your rocks, has been s, now I see in.
Identification of "+O9" by examining Zodiac plain text for a commonly used three-letter reversal. Expansion of this to include values for B, M, F, which are in frequent contact with the three "F" as E and "B" as R, and vice-versa.
Word "Zodiac" in the first 20 and last 10 places.
Word "Death machine" for entire message.

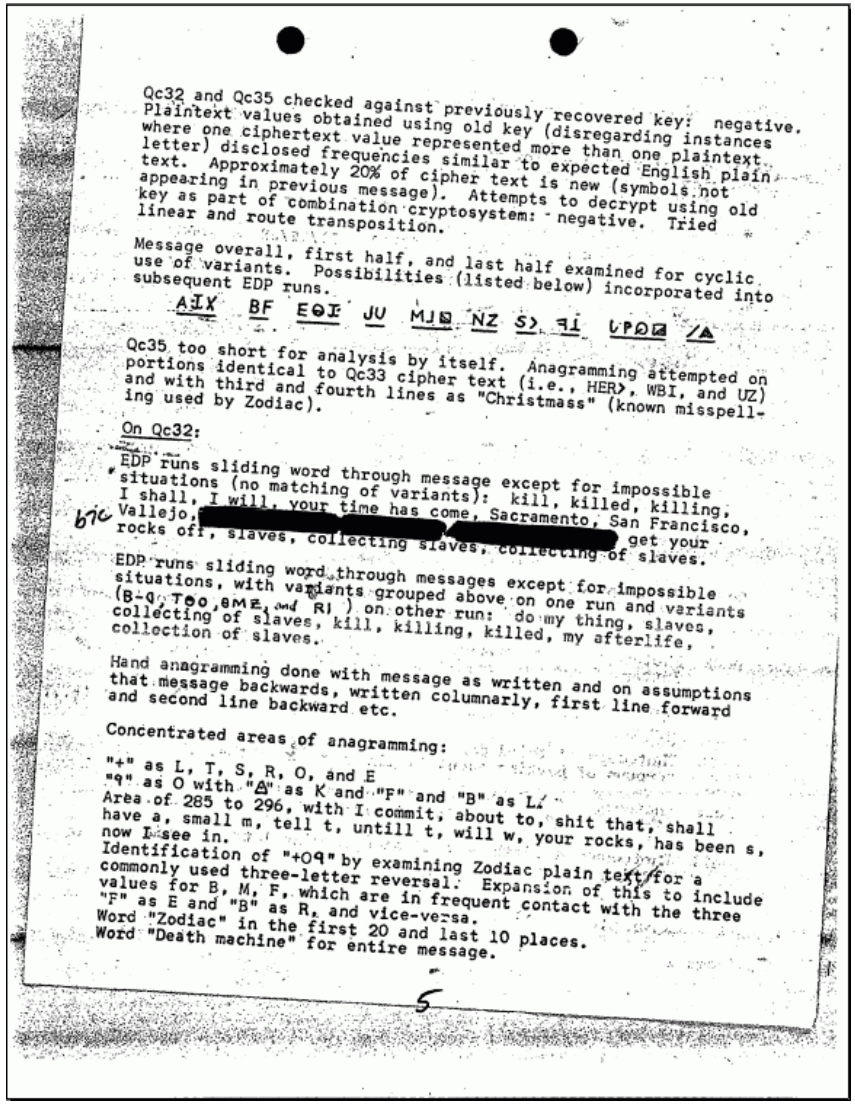
5

The Zodiac's 340 Cipher

Previous efforts to solve Z340

Who has worked on solving Z340 in the past?

- FBI Cryptanalysis and Racketeering Records Unit (CRRU)
- NSA
- CIA
- Many university projects.
- Robert Graysmith's book *Zodiac* talks of computer–based attacks of the Z340 in the 1970s.
- Members of the American Cryptogram Association (ACA), including then president Donald C.B. Marsh.
- Many private citizens including forum users from zodiackillersite.com, zodiackiller.com and zodiackillerfacts.com



Qc32 and Qc35 checked against previously recovered key: negative. Plaintext values obtained using old key (disregarding instances where one ciphertext value represented more than one plaintext letter) disclosed frequencies similar to expected English plain text. Approximately 20% of cipher text is new (symbols not appearing in previous message). Attempts to decrypt using old key as part of combination cryptosystem: negative. Tried linear and route transposition.

Message overall, first half, and last half examined for cyclic use of variants. Possibilities (listed below) incorporated into subsequent EDP runs.

AIX BF EOI JU MJ NZ S> 9i UPO /A

Qc35 too short for analysis by itself. Anagramming attempted on portions identical to Qc33 cipher text (i.e., HER>, WBI, and UZ) and with third and fourth lines as "Christmass" (known misspelling used by Zodiac).

On Qc32:

EDP runs sliding word through message except for impossible situations (no matching of variants): kill, killed, killing, I shall, I will, your time has come, Sacramento, San Francisco, Vallejo, [redacted] get your rocks off, slaves, collecting slaves, collecting of slaves.

EDP runs sliding word through messages except for impossible situations, with variants grouped above on one run and variants (B-9, T∞, ME, and RI) on other run: do my thing, slaves, collecting of slaves, kill, killing, killed, my afterlife, collection of slaves.

Hand anagramming done with message as written and on assumptions that message backwards, written columnarly, first line forward and second line backward etc.

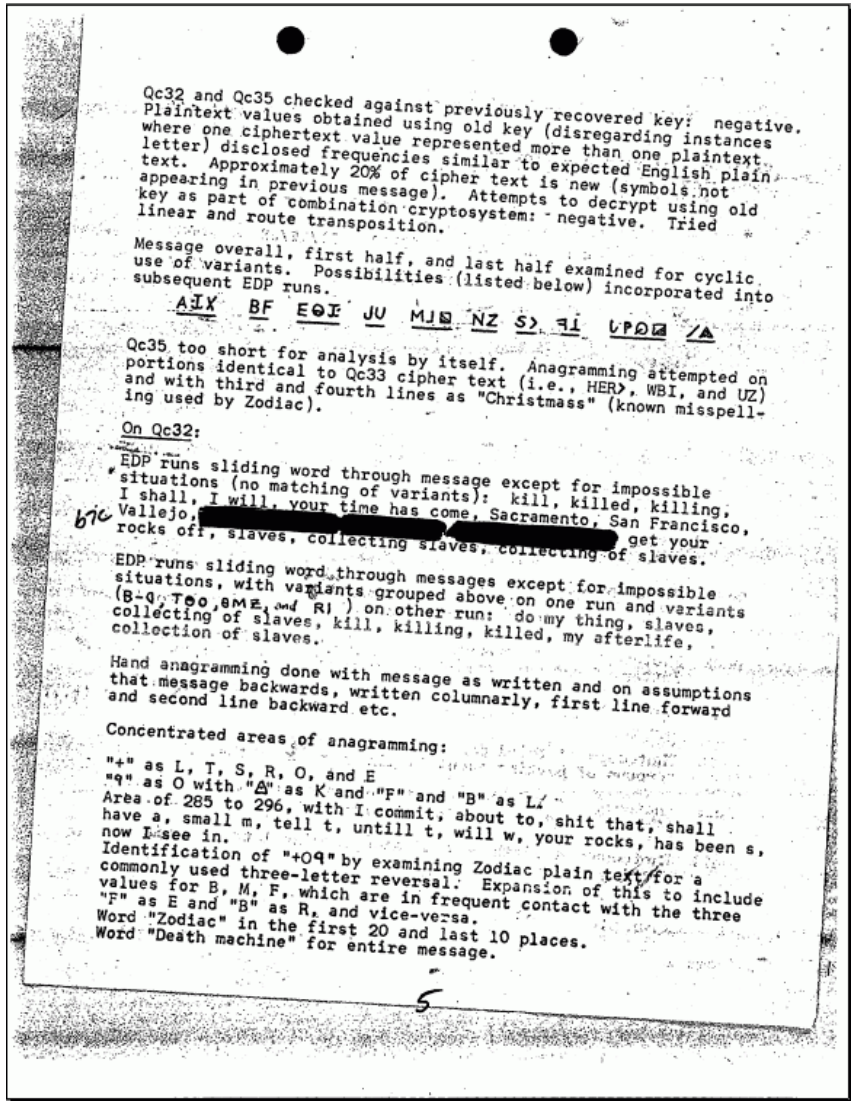
Concentrated areas of anagramming:

"+" as L, T, S, R, O, and E
"9" as O with "Δ" as K and "F" and "B" as L.
Area of 285 to 296, with I commit, about to, shit that, shall have a, small m, tell t, untill t, will w, your rocks, has been s, now I see in.
Identification of "+O9" by examining Zodiac plain text for a commonly used three-letter reversal. Expansion of this to include values for B, M, F, which are in frequent contact with the three "F" as E and "B" as R, and vice-versa.
Word "Zodiac" in the first 20 and last 10 places.
Word "Death machine" for entire message.

5

Who has worked on solving Z340 in the past?

- FBI Cryptanalysis and Racketeering Records Unit (CRRU)
- NSA
- CIA
- Many university projects.
- Robert Graysmith's book *Zodiac* talks of computer–based attacks of the Z340 in the 1970s.
- Members of the American Cryptogram Association (ACA), including then president Donald C.B. Marsh.
- Many private citizens including forum users from zodiackillersite.com, zodiackiller.com and zodiackillerfacts.com



Qc32 and Qc35 checked against previously recovered key: negative. Plaintext values obtained using old key (disregarding instances where one ciphertext value represented more than one plaintext letter) disclosed frequencies similar to expected English plain text. Approximately 20% of cipher text is new (symbols not appearing in previous message). Attempts to decrypt using old key as part of combination cryptosystem: negative. Tried linear and route transposition.

Message overall, first half, and last half examined for cyclic use of variants. Possibilities (listed below) incorporated into subsequent EDP runs.

AIX BF EOI JU MJ NZ S> 9i LPO /A

Qc35 too short for analysis by itself. Anagramming attempted on portions identical to Qc33 cipher text (i.e., HER>, WBI, and UZ) and with third and fourth lines as "Christmass" (known misspelling used by Zodiac).

On Qc32:

EDP runs sliding word through message except for impossible situations (no matching of variants): kill, killed, killing, I shall, I will, your time has come, Sacramento, San Francisco, Vallejo, [redacted] get your rocks off, slaves, collecting slaves, collecting of slaves.

EDP runs sliding word through messages except for impossible situations, with variants grouped above on one run and variants (B-9, T=0, 8=E, and RI) on other run: do my thing, slaves, collecting of slaves, kill, killing, killed, my afterlife, collection of slaves.

Hand anagramming done with message as written and on assumptions that message backwards, written columnarly, first line forward and second line backward etc.

Concentrated areas of anagramming:

"+" as L, T, S, R, O, and E
"9" as O with "Δ" as K and "F" and "B" as L.
Area of 285 to 296, with I commit, about to, shit that, shall have a, small m, tell t, untill t, will w, your rocks, has been s, now I see in.
Identification of "+O9" by examining Zodiac plain text for a commonly used three-letter reversal. Expansion of this to include values for B, M, F, which are in frequent contact with the three "F" as E and "B" as R, and vice-versa.
Word "Zodiac" in the first 20 and last 10 places.
Word "Death machine" for entire message.

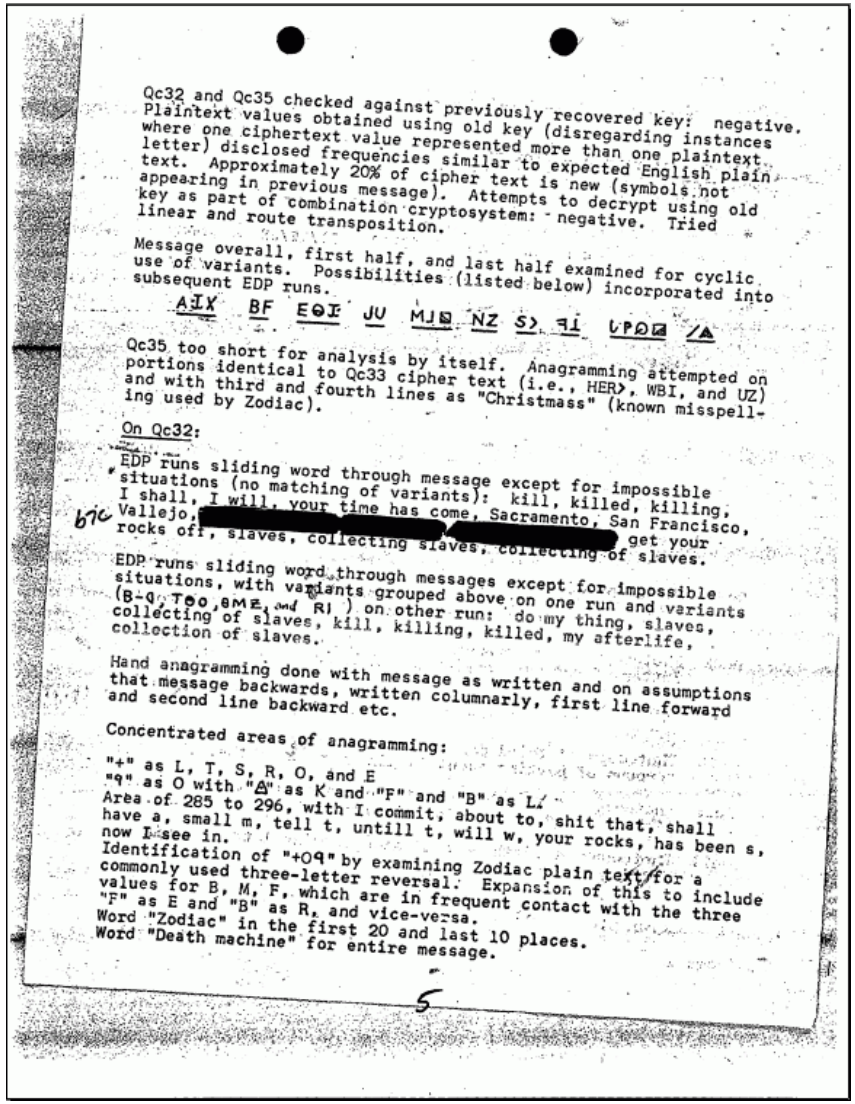
5

The Zodiac's 340 Cipher

Previous efforts to solve Z340

Who has worked on solving Z340 in the past?

- FBI Cryptanalysis and Racketeering Records Unit (CRRU)
- NSA
- CIA
- Many university projects.
- Robert Graysmith's book *Zodiac* talks of computer–based attacks of the Z340 in the 1970s.
- Members of the American Cryptogram Association (ACA), including then president Donald C.B. Marsh.
- Many private citizens including forum users from zodiackillersite.com, zodiackiller.com and zodiackillerfacts.com



Qc32 and Qc35 checked against previously recovered key: negative. Plaintext values obtained using old key (disregarding instances where one ciphertext value represented more than one plaintext letter) disclosed frequencies similar to expected English plain text. Approximately 20% of cipher text is new (symbols not appearing in previous message). Attempts to decrypt using old key as part of combination cryptosystem: negative. Tried linear and route transposition.

Message overall, first half, and last half examined for cyclic use of variants. Possibilities (listed below) incorporated into subsequent EDP runs.

AIX BF EOI JU MJ NZ S> 7i VPO /A

Qc35 too short for analysis by itself. Anagramming attempted on portions identical to Qc33 cipher text (i.e., HER>, WBI, and UZ) and with third and fourth lines as "Christmass" (known misspelling used by Zodiac).

On Qc32:

EDP runs sliding word through message except for impossible situations (no matching of variants): kill, killed, killing, I shall, I will, your time has come, Sacramento, San Francisco, Vallejo, [redacted] get your rocks off, slaves, collecting slaves, collecting of slaves.

EDP runs sliding word through messages except for impossible situations, with variants grouped above on one run and variants (B-Q, T=O, EME, and RI) on other run: do my thing, slaves, collecting of slaves, kill, killing, killed, my afterlife, collection of slaves.

Hand anagramming done with message as written and on assumptions that message backwards, written columnarly, first line forward and second line backward etc.

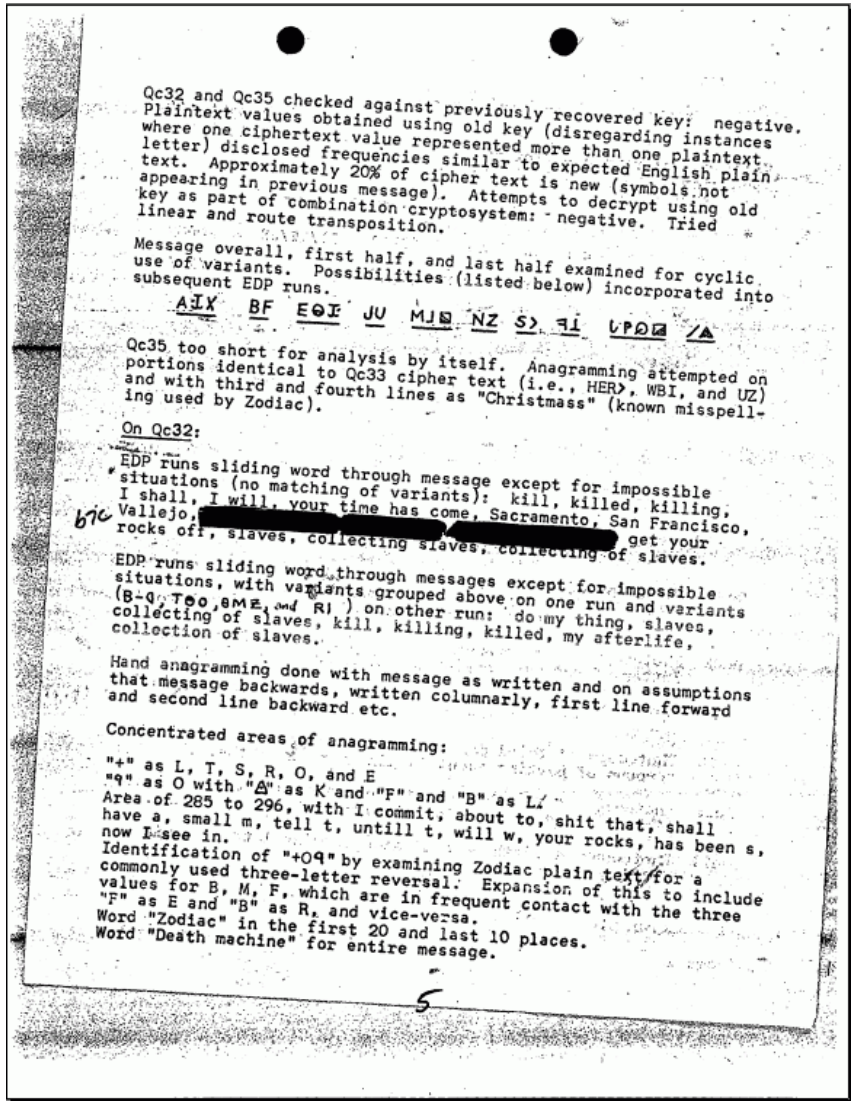
Concentrated areas of anagramming:

"+" as L, T, S, R, O, and E
"9" as O with "Δ" as K and "F" and "B" as L.
Area of 285 to 296, with I commit, about to, shit that, shall have a, small m, tell t, untill t, will w, your rocks, has been s, now I see in.
Identification of "+O9" by examining Zodiac plain text for a commonly used three-letter reversal. Expansion of this to include values for B, M, F, which are in frequent contact with the three "F" as E and "B" as R, and vice-versa.
Word "Zodiac" in the first 20 and last 10 places.
Word "Death machine" for entire message.

5

Who has worked on solving Z340 in the past?

- FBI Cryptanalysis and Racketeering Records Unit (CRRU)
- NSA
- CIA
- Many university projects.
- Robert Graysmith's book *Zodiac* talks of computer–based attacks of the Z340 in the 1970s.
- Members of the American Cryptogram Association (ACA), including then president Donald C.B. Marsh.
- Many private citizens including forum users from zodiackillersite.com, zodiackiller.com and zodiackillerfacts.com



Qc32 and Qc35 checked against previously recovered key: negative. Plaintext values obtained using old key (disregarding instances where one ciphertext value represented more than one plaintext letter) disclosed frequencies similar to expected English plain text. Approximately 20% of cipher text is new (symbols not appearing in previous message). Attempts to decrypt using old key as part of combination cryptosystem: negative. Tried linear and route transposition.

Message overall, first half, and last half examined for cyclic use of variants. Possibilities (listed below) incorporated into subsequent EDP runs.

AIX BF EOI JU MJ NZ S> 9i LPO /A

Qc35 too short for analysis by itself. Anagramming attempted on portions identical to Qc33 cipher text (i.e., HER>, WBI, and UZ) and with third and fourth lines as "Christmass" (known misspelling used by Zodiac).

On Qc32:

EDP runs sliding word through message except for impossible situations (no matching of variants): kill, killed, killing, I shall, I will, your time has come, Sacramento, San Francisco, Vallejo, [redacted] get your rocks off, slaves, collecting slaves, collecting of slaves.

EDP runs sliding word through messages except for impossible situations, with variants grouped above on one run and variants (B-9, T=O, 8=E, and RI) on other run: do my thing, slaves, collecting of slaves, kill, killing, killed, my afterlife, collection of slaves.

Hand anagramming done with message as written and on assumptions that message backwards, written columnarly, first line forward and second line backward etc.

Concentrated areas of anagramming:

"+" as L, T, S, R, O, and E
"9" as O with "Δ" as K and "F" and "B" as L.
Area of 285 to 296, with I commit, about to, shit that, shall have a, small m, tell t, untill t, will w, your rocks, has been s, now I see in.
Identification of "+O9" by examining Zodiac plain text for a commonly used three-letter reversal. Expansion of this to include values for B, M, F, which are in frequent contact with the three "F" as E and "B" as R, and vice-versa.
Word "Zodiac" in the first 20 and last 10 places.
Word "Death machine" for entire message.

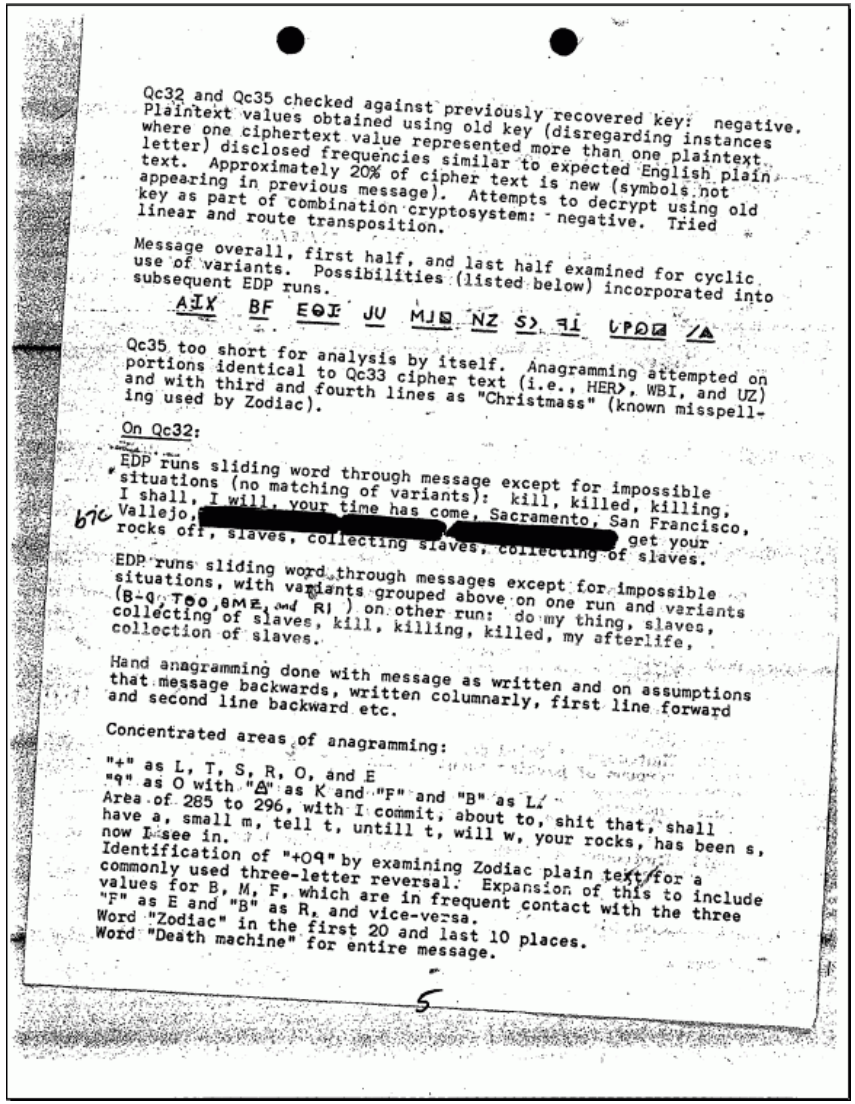
5

The Zodiac's 340 Cipher

Previous efforts to solve Z340

Who has worked on solving Z340 in the past?

- FBI Cryptanalysis and Racketeering Records Unit (CRRU)
- NSA
- CIA
- Many university projects.
- Robert Graysmith's book *Zodiac* talks of computer–based attacks of the Z340 in the 1970s.
- Members of the American Cryptogram Association (ACA), including then president Donald C.B. Marsh.
- Many private citizens including forum users from zodiackillersite.com, zodiackiller.com and zodiackillerfacts.com



Qc32 and Qc35 checked against previously recovered key: negative. Plaintext values obtained using old key (disregarding instances where one ciphertext value represented more than one plaintext letter) disclosed frequencies similar to expected English plain text. Approximately 20% of cipher text is new (symbols not appearing in previous message). Attempts to decrypt using old key as part of combination cryptosystem: negative. Tried linear and route transposition.

Message overall, first half, and last half examined for cyclic use of variants. Possibilities (listed below) incorporated into subsequent EDP runs.

AIX BF EOI JU MJ NZ S> 7i VPO /A

Qc35 too short for analysis by itself. Anagramming attempted on portions identical to Qc33 cipher text (i.e., HER>, WBI, and UZ) and with third and fourth lines as "Christmass" (known misspelling used by Zodiac).

On Qc32:

EDP runs sliding word through message except for impossible situations (no matching of variants): kill, killed, killing, I shall, I will, your time has come, Sacramento, San Francisco, Vallejo, [redacted] get your rocks off, slaves, collecting slaves, collecting of slaves.

EDP runs sliding word through messages except for impossible situations, with variants grouped above on one run and variants (B-Q, T=O, 8=E, and RI) on other run: do my thing, slaves, collecting of slaves, kill, killing, killed, my afterlife, collection of slaves.

Hand anagramming done with message as written and on assumptions that message backwards, written columnarly, first line forward and second line backward etc.

Concentrated areas of anagramming:

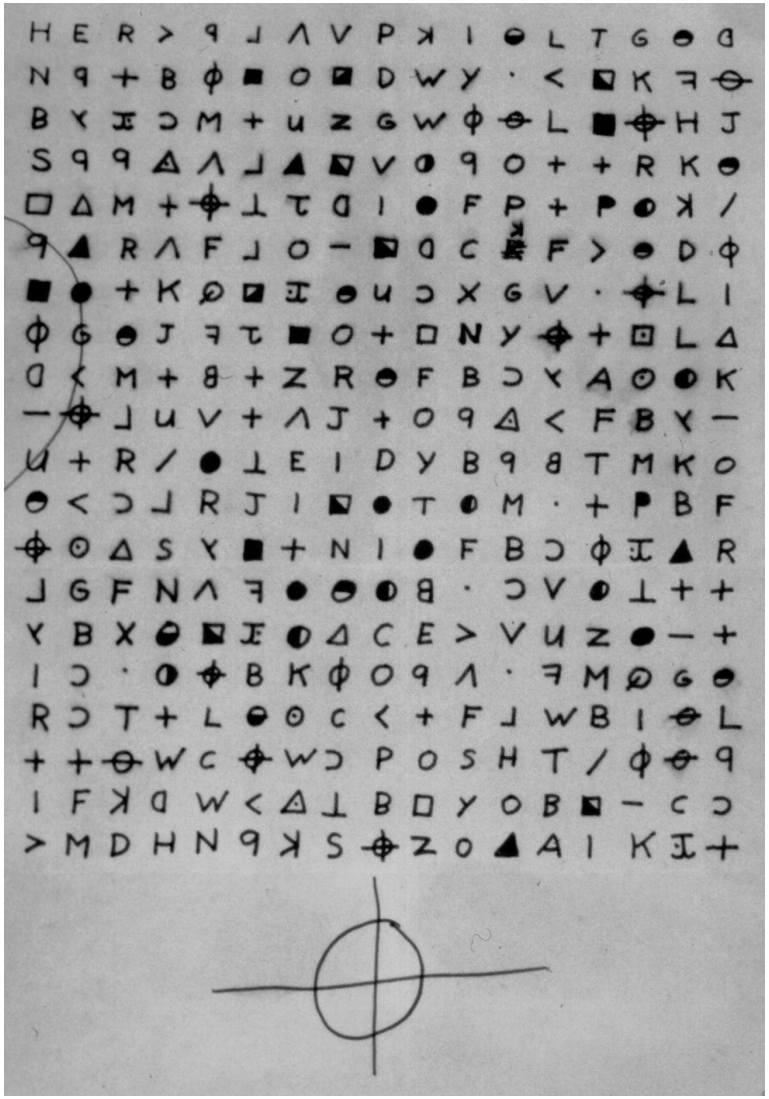
"+" as L, T, S, R, O, and E
"9" as O with "Δ" as K and "F" and "B" as L.
Area of 285 to 296, with I commit, about to, shit that, shall have a, small m, tell t, untill t, will w, your rocks, has been s, now I see in.
Identification of "+O9" by examining Zodiac plain text for a commonly used three-letter reversal. Expansion of this to include values for B, M, F, which are in frequent contact with the three "F" as E and "B" as R, and vice-versa.
Word "Zodiac" in the first 20 and last 10 places.
Word "Death machine" for entire message.

5

The Zodiac's 340 Cipher

Does the cipher contain a message at all?

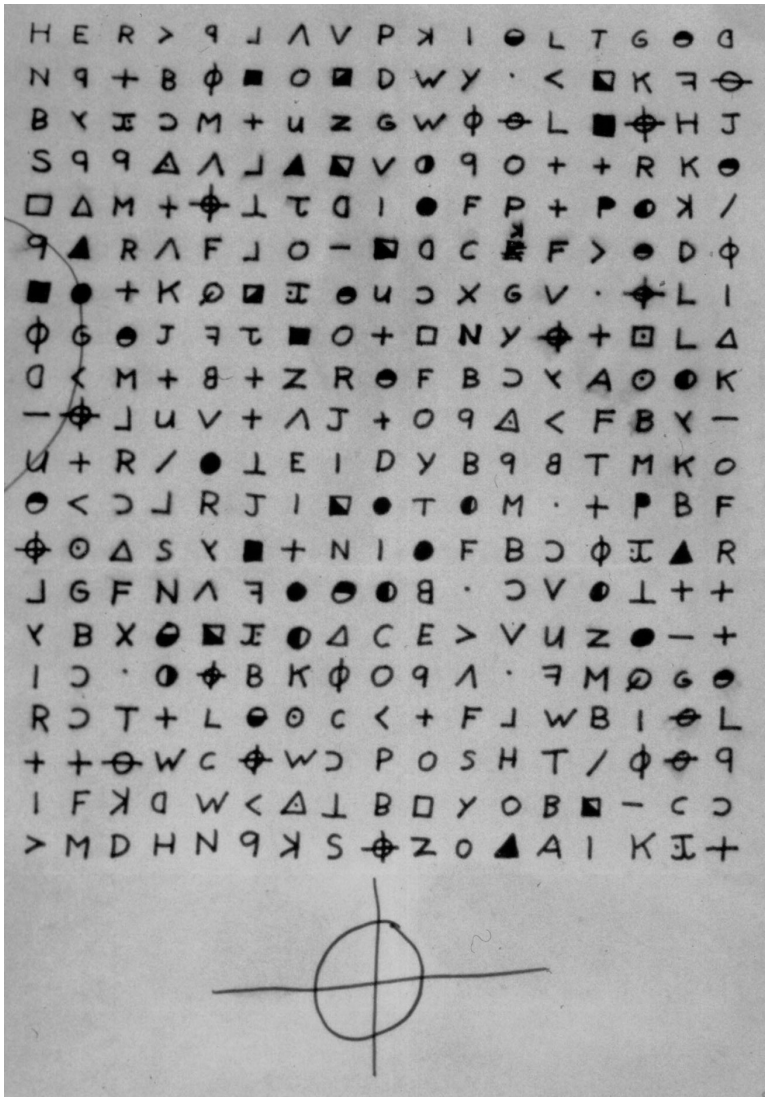
- Perhaps it's just gibberish? Then why did Zodiac correct the ✕?
- It was speculated that this cipher was a ploy to waste law enforcement's time.
- This would explain why it hasn't been solved for 50 years.
- Without a solution, can we distinguish between a genuine cipher and a random assignment of symbols?
- The number of repeating bigrams can indicate a genuine cipher.



The Zodiac's 340 Cipher

Does the cipher contain a message at all?

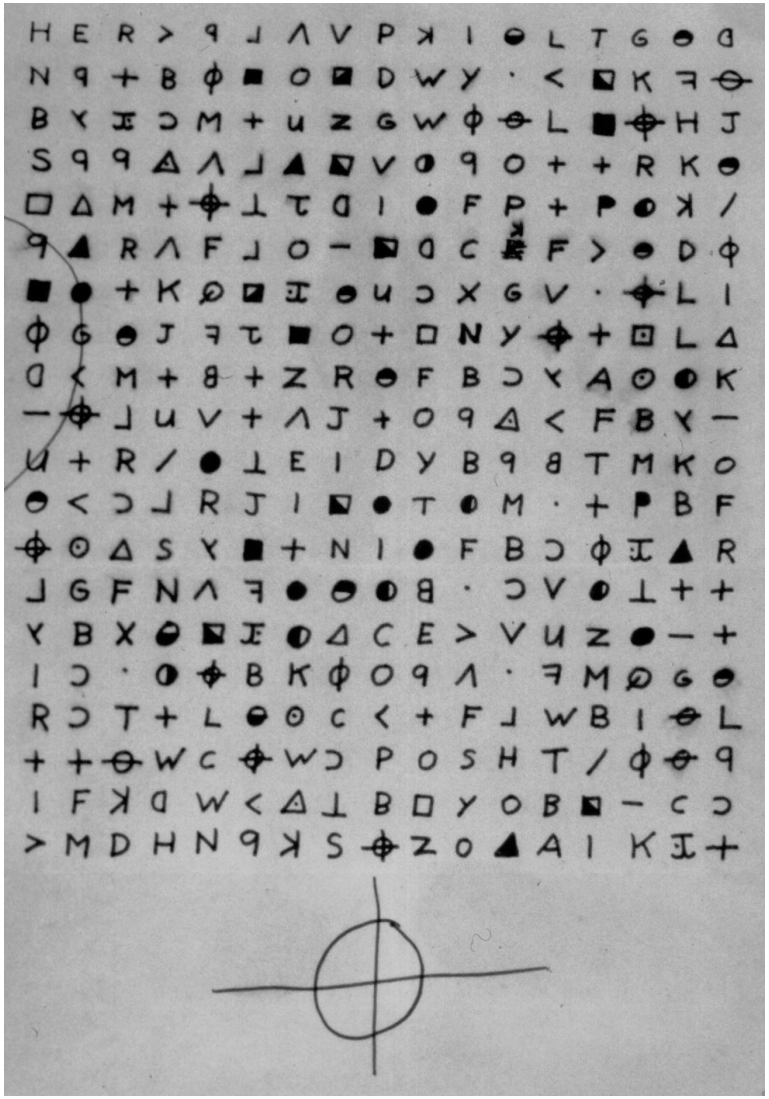
- Perhaps it's just gibberish? Then why did Zodiac correct the ✕?
- It was speculated that this cipher was a ploy to waste law enforcement's time.
- This would explain why it hasn't been solved for 50 years.
- Without a solution, can we distinguish between a genuine cipher and a random assignment of symbols?
- The number of repeating bigrams can indicate a genuine cipher.



The Zodiac's 340 Cipher

Does the cipher contain a message at all?

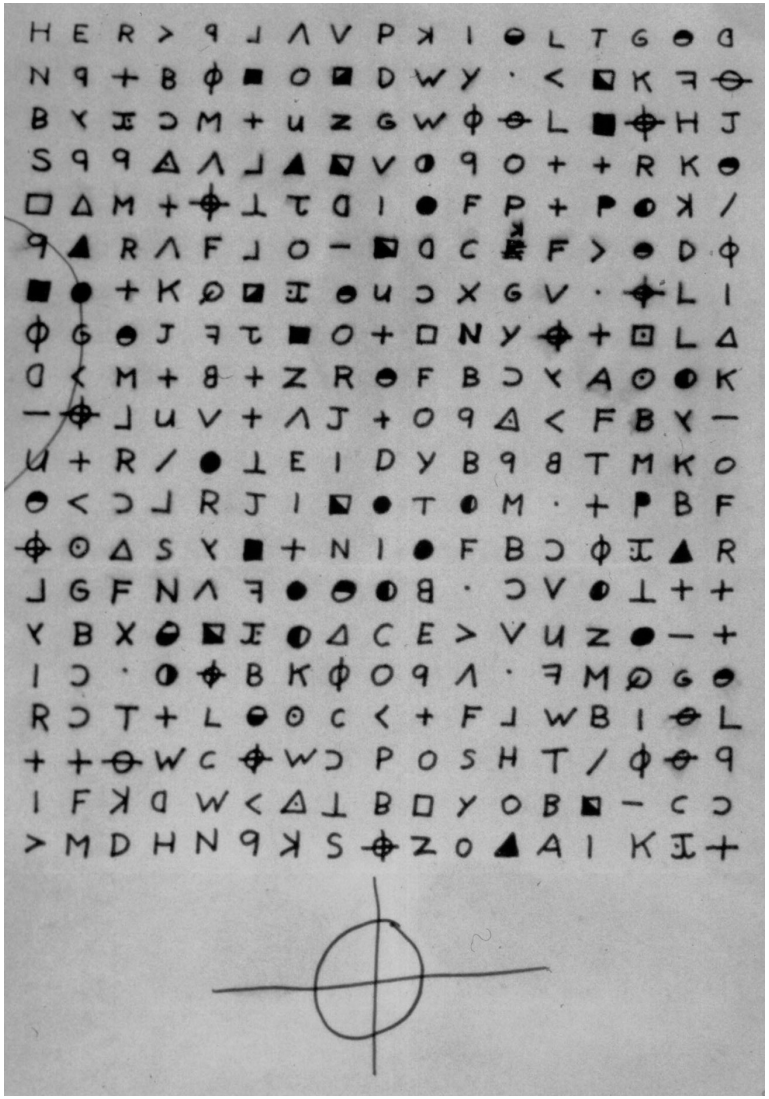
- Perhaps it's just gibberish? Then why did Zodiac correct the ﻫ?
- It was speculated that this cipher was a ploy to waste law enforcement's time.
- This would explain why it hasn't been solved for 50 years.
- Without a solution, can we distinguish between a genuine cipher and a random assignment of symbols?
- The number of repeating bigrams can indicate a genuine cipher.



The Zodiac's 340 Cipher

Does the cipher contain a message at all?

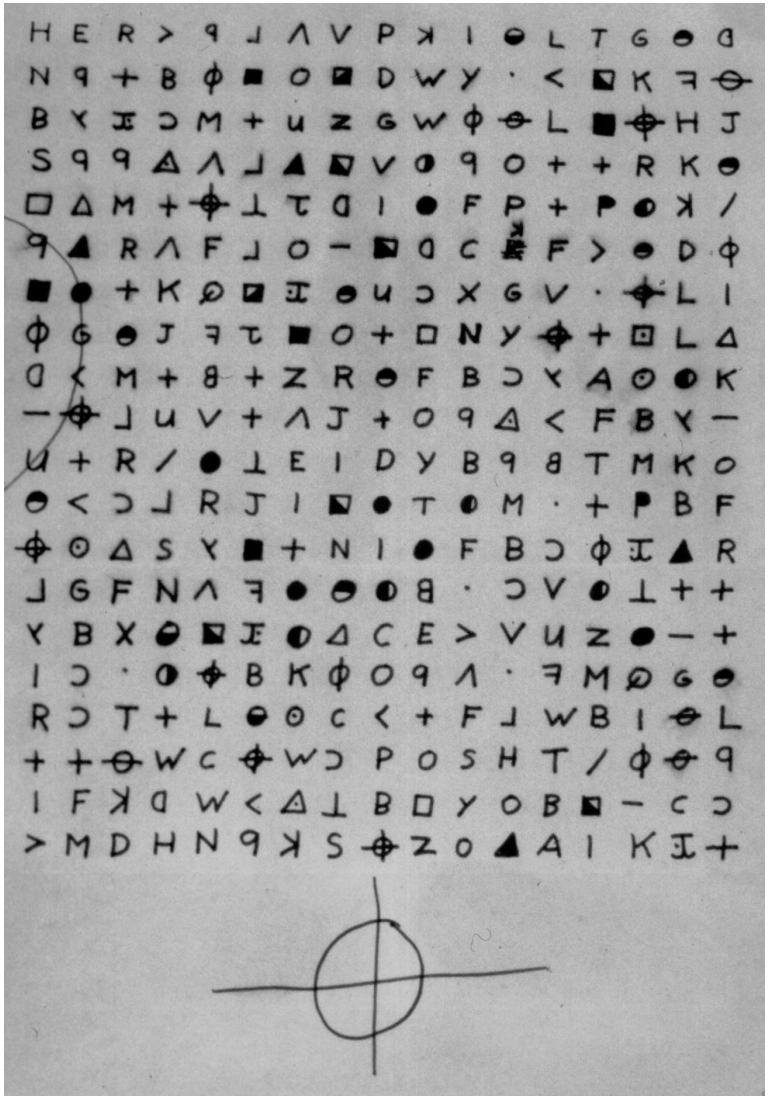
- Perhaps it's just gibberish? Then why did Zodiac correct the ✕?
- It was speculated that this cipher was a ploy to waste law enforcement's time.
- This would explain why it hasn't been solved for 50 years.
- Without a solution, can we distinguish between a genuine cipher and a random assignment of symbols?
- The number of repeating bigrams can indicate a genuine cipher.



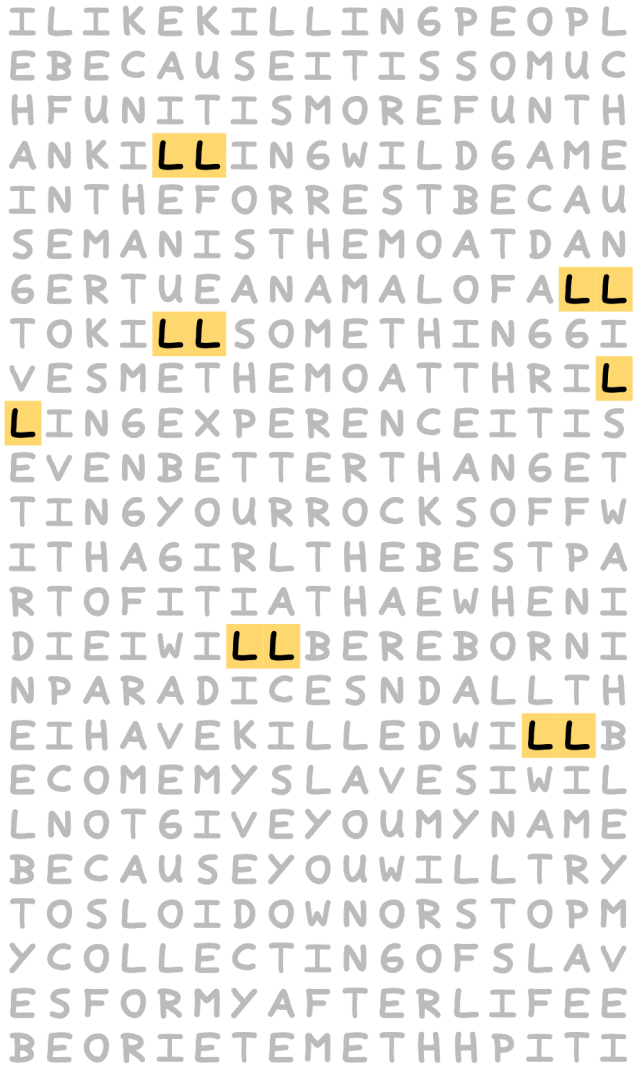
The Zodiac's 340 Cipher

Does the cipher contain a message at all?

- Perhaps it's just gibberish? Then why did Zodiac correct the ✖?
- It was speculated that this cipher was a ploy to waste law enforcement's time.
- This would explain why it hasn't been solved for 50 years.
- Without a solution, can we distinguish between a genuine cipher and a random assignment of symbols?
- The number of repeating bigrams can indicate a genuine cipher.



The most common repeating bigram in the Z408 is ■B, with 6 occurrences.



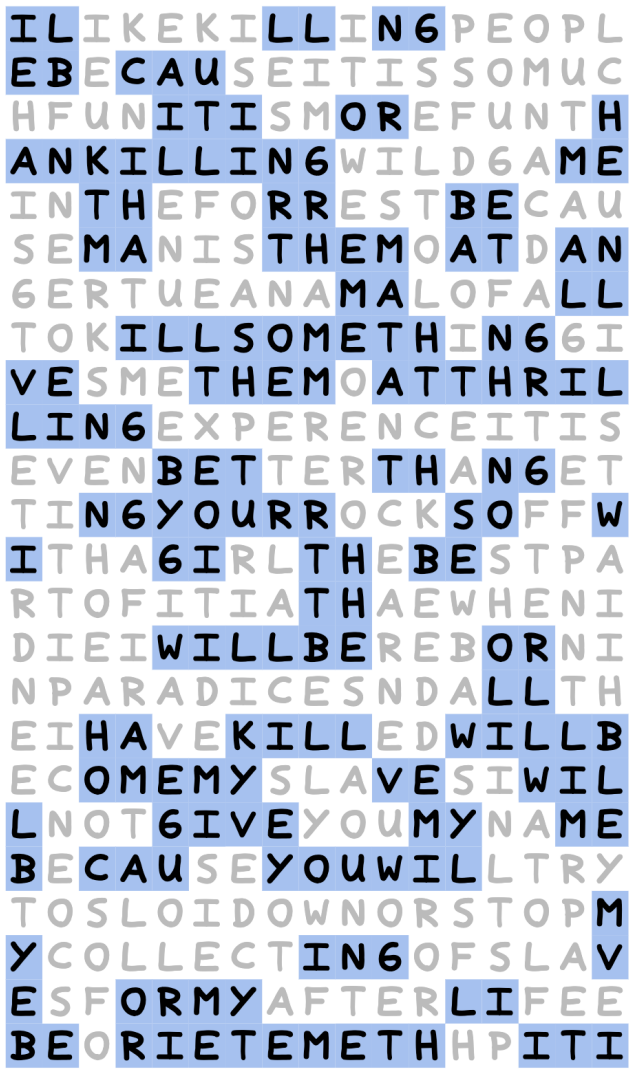
However, by the nature of the encipherment scheme, there are other ways to encode LL.

ILIKEKILLING6PEOPL
EBECAUSEITISSOMUC
HFUNITISMOREFUNTH
ANKILLING6WILD6AME
INTHEFORRESTBECAU
SEMANISTHEMOATDAN
6ERTUEANAMALOFALL
TOKILLSOMETHING6I
VESMETHEMOATTHRIL
LINGEXPERENCEITIS
EVENBETTERTHAN6ET
TING6YOURROCKSOFFW
ITHA6IRLTHEBESTPA
RTOFITIATHAEWHENI
DIEIWILLBEREBORNI
NPARADICESNDALLTH
EIHAVEKILLEDWILLB
ECOMEMYSLAVESIWIL
LNOT6IVEYOUMYNAME
BECAUSEYOUWILLTRY
TOSLOIDOWNORSTOPM
YCOLLECTING6OFSLAV
ESFORMYAFTERLIFEE
BEORIETEMETHHPITI

The second most common repeating bigram is ⍜□, with 4 occurrences.

ILIKEKILLING6PEOPL
EBECAUSEITISSOMUC
HFUNITISMOREFUNTH
ANKILLING6WILD6AME
INTHEFORRESTBECAU
SEMANISTHEMOATDAN
6ERTUEANAMALOFALL
TOKILLSOMETHING6I
VESMETHEMOATTHRIL
LING6EXPERENCEITIS
EVENBETTERTHAN6ET
TING6YOURROCKSOFFW
ITHA6IRLTHEBESTPA
RTOFITIATHAEWHENI
DIEIWILLBEREBORNI
NPARADICESNDALLTH
EIHAVEKILLEDWILLB
ECOMEMYSLAVESIWIL
LNOT6IVEYOUMYNAME
BECAUSEYOUWILLTRY
TOSLOIDOWNORSTOPM
YCOLLECTING6OFSLAV
ESFORMYAFTERLIFEE
BEORIETEMETHHPITI

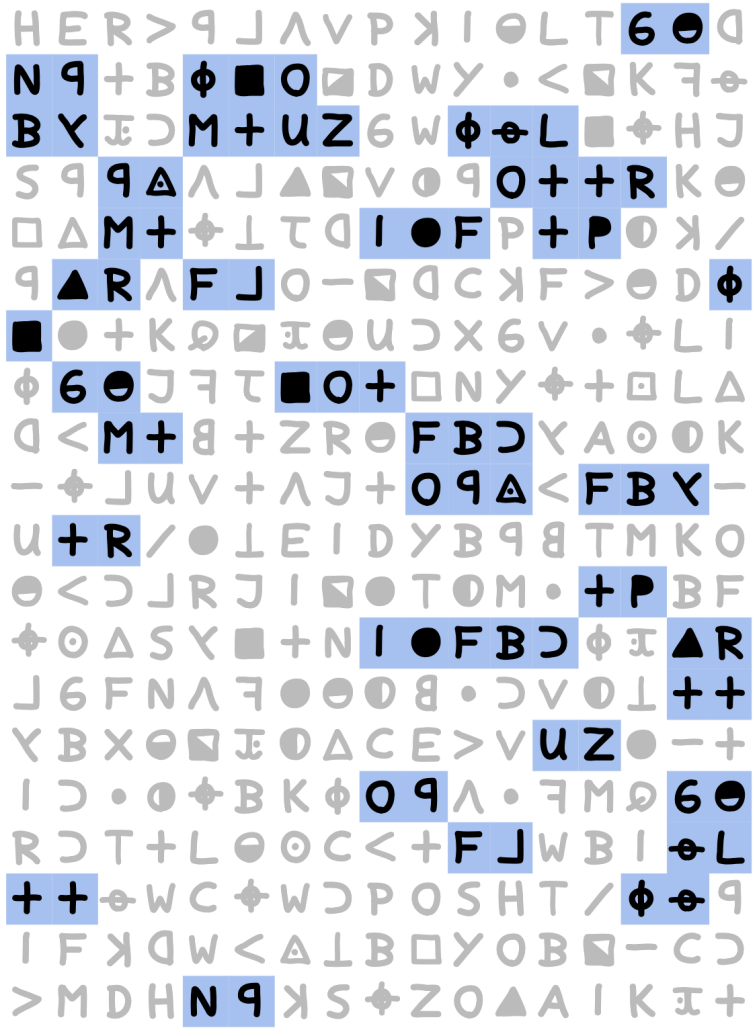
The Z408 has 62 repeating bigrams.



The Zodiac's 340 Cipher

Repeating bigrams

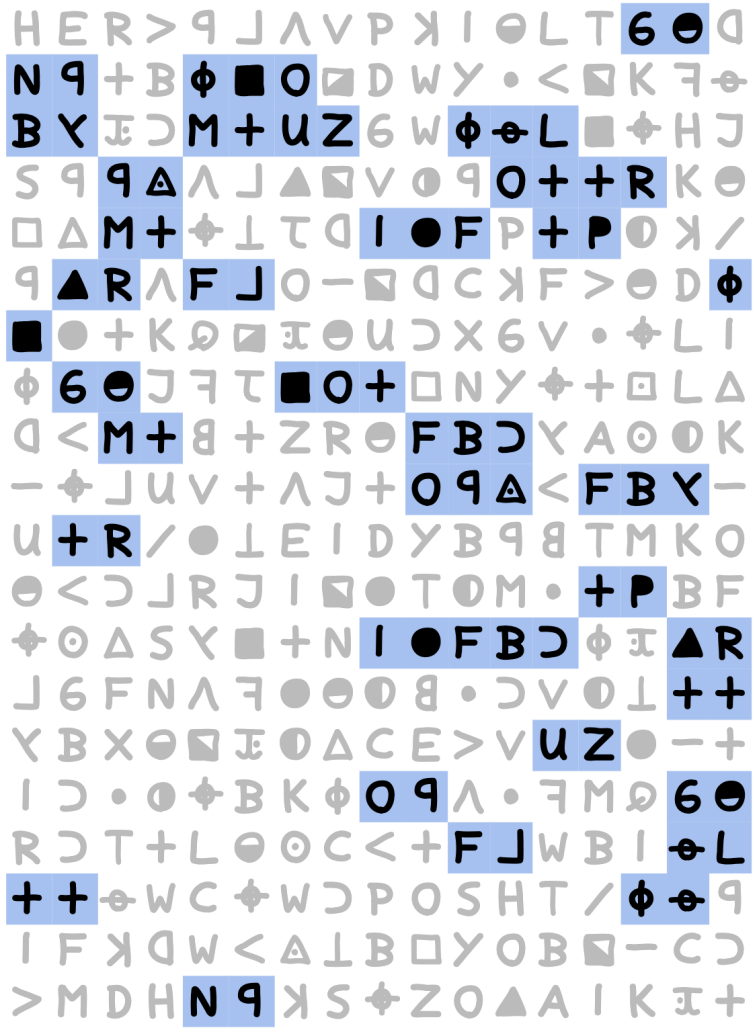
- The Z340 has 25 repeating bigrams. How many bigrams should we expect if the cipher is genuine or not?
- We could compare the number of repeating bigrams of random shuffles of Z340 with randomly generated Z340–like ciphers (Assuming the Z340 is a homophonic substitution cipher like the Z408.).



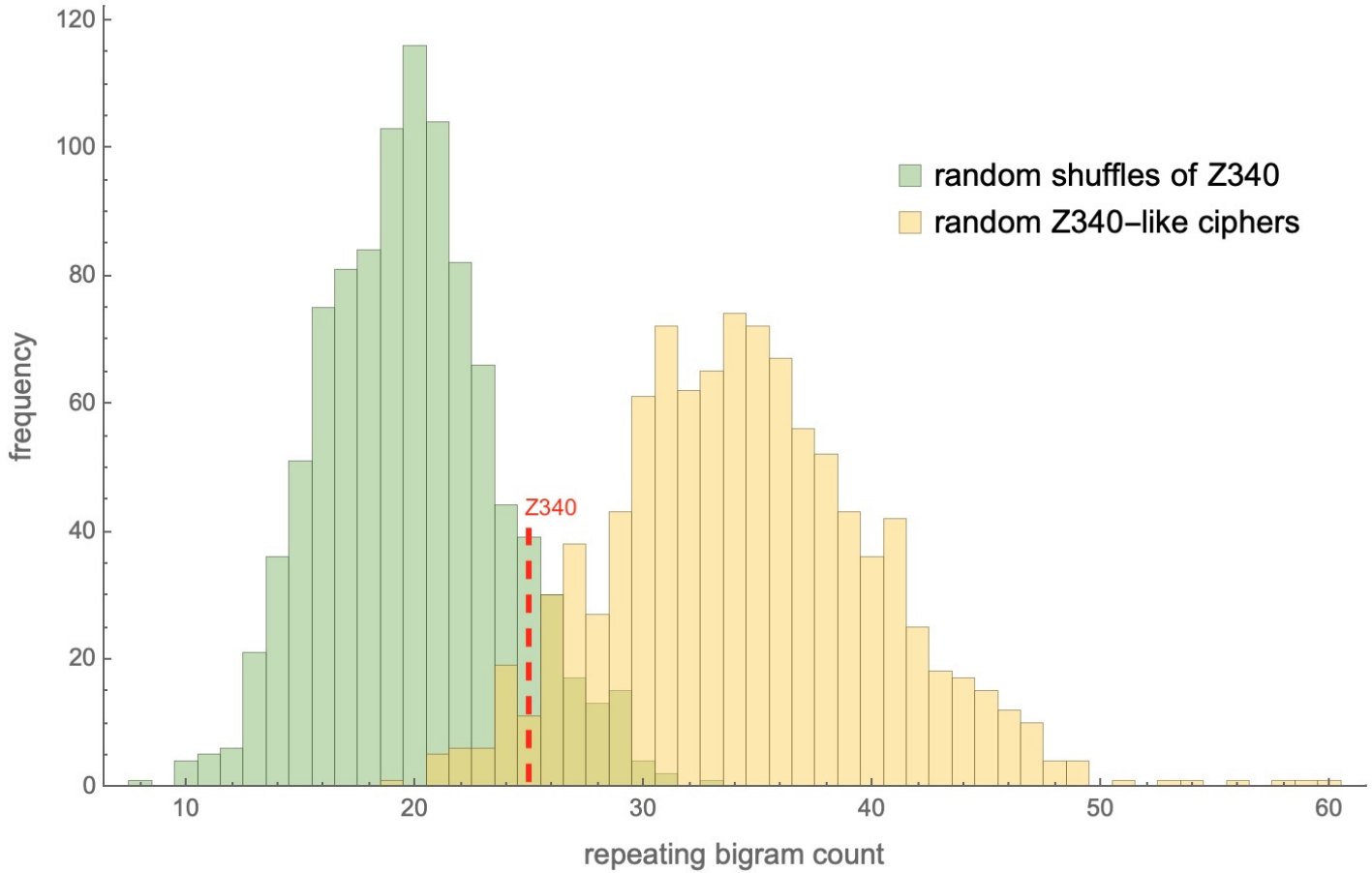
The Zodiac's 340 Cipher

Repeating bigrams

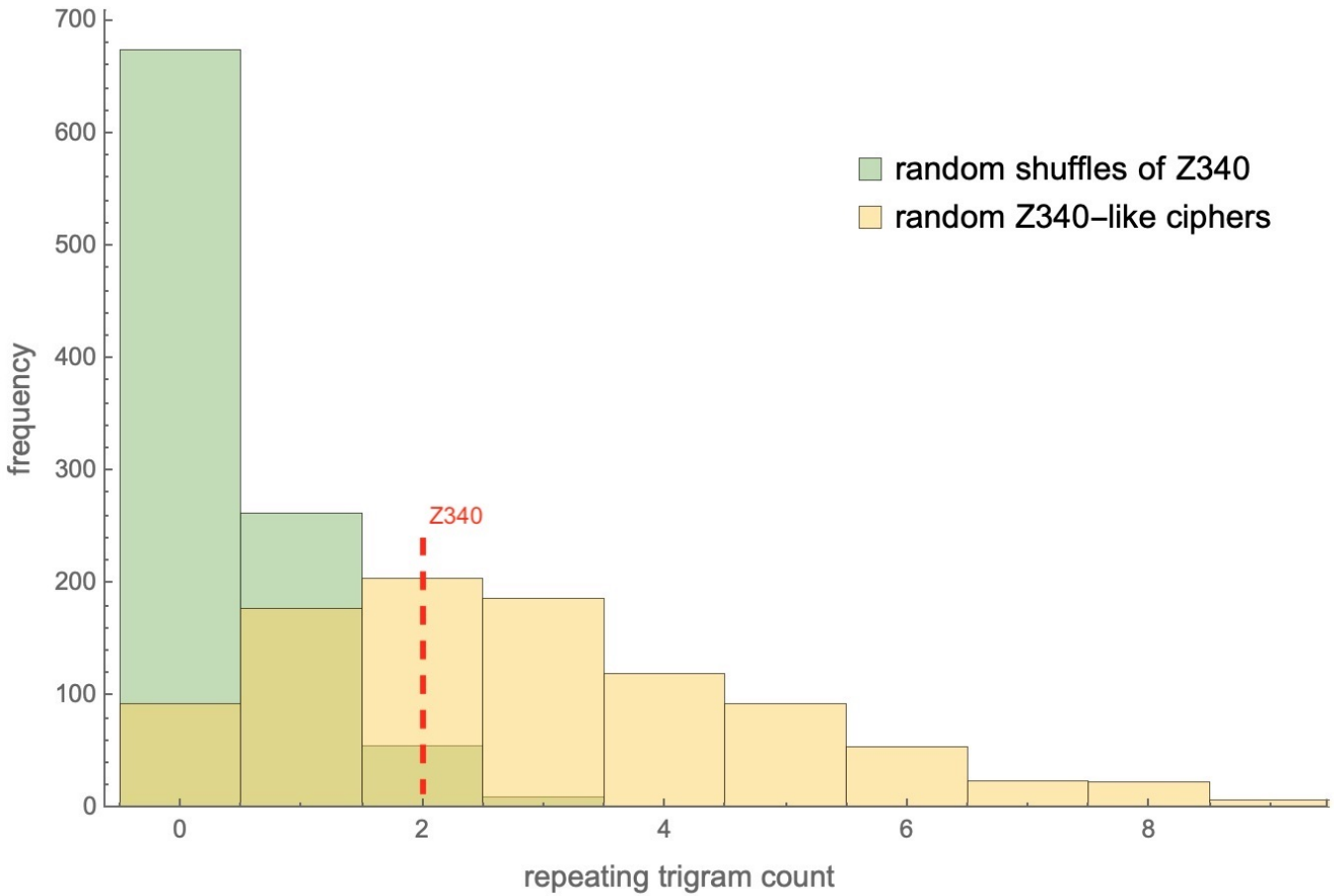
- The Z340 has 25 repeating bigrams. How many bigrams should we expect if the cipher is genuine or not?
- We could compare the number of repeating bigrams of random shuffles of Z340 with randomly generated Z340–like ciphers (Assuming the Z340 is a homophonic substitution cipher like the Z408.).



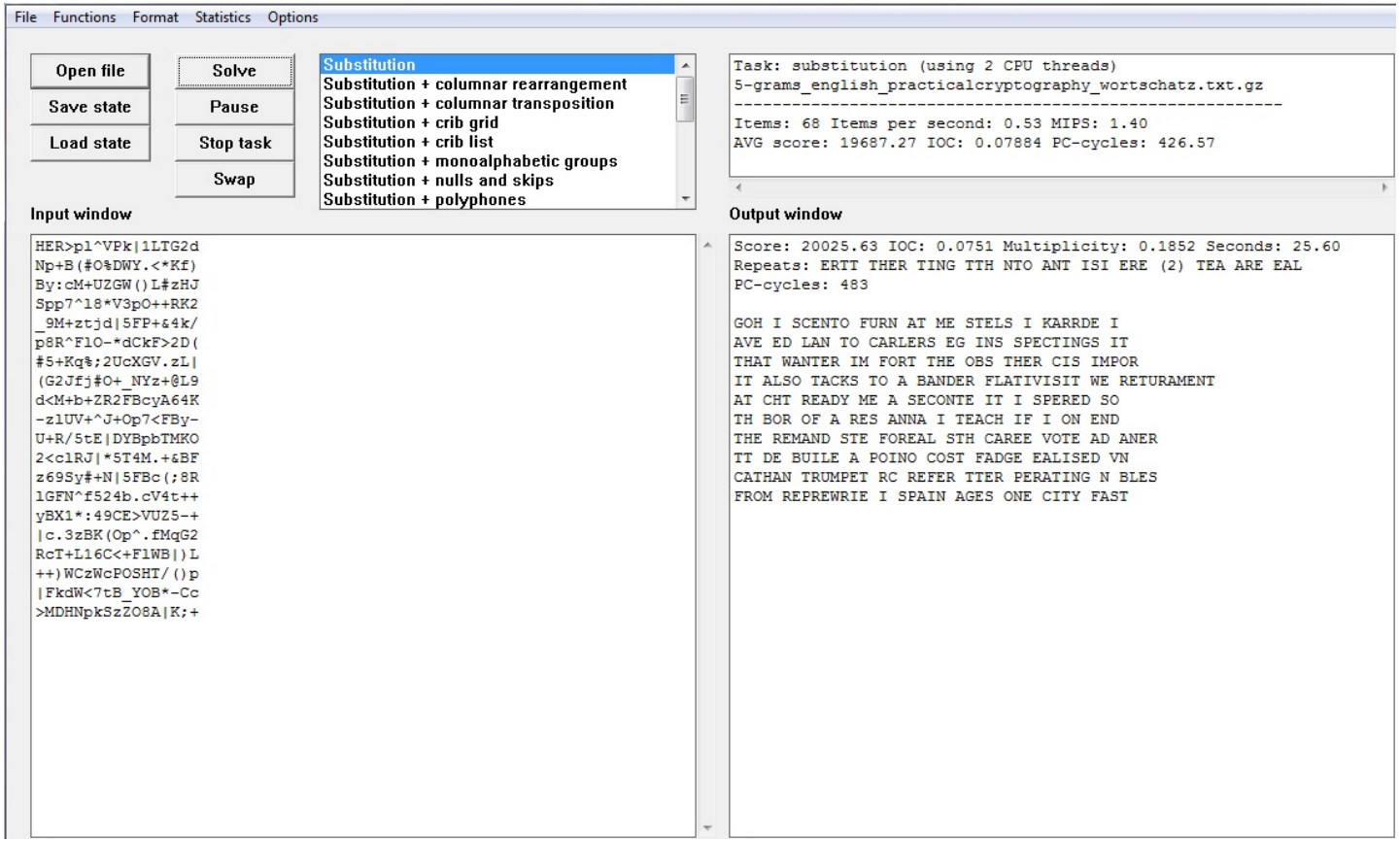
Unfortunately, the results of this experiment were inconclusive. Z340 is 1.33–sigma from the mean of the random shuffles and 1.63–sigma from the mean of the randomly generated Z340–like ciphers.



Rerunning this experiment with repeating trigrams was, once again, inconclusive as the Z340 has 2 repeating trigrams.



Previously we saw how efficiently azdecrypt could solve the Z408. How does it do on the Z340?



- What do we make of `azdecrypt's` failure to solve Z340?
- Experiments indicate that `azdecrypt` can robustly solve homophonic substitution ciphers of the same length and symbol frequency as Z340.
- Perhaps it truly is gibberish, but let's suppose its not.
- Perhaps we are not reading Z340 in the right direction?
- Let's assume Z340 is both a transposition cipher and a substitution cipher?

- What do we make of `azdecrypt's` failure to solve Z340?
- Experiments indicate that `azdecrypt` can robustly solve homophonic substitution ciphers of the same length and symbol frequency as Z340.
- Perhaps it truly is gibberish, but let's suppose its not.
- Perhaps we are not reading Z340 in the right direction?
- Let's assume Z340 is both a transposition cipher and a substitution cipher?

- What do we make of `azdecrypt's` failure to solve Z340?
- Experiments indicate that `azdecrypt` can robustly solve homophonic substitution ciphers of the same length and symbol frequency as Z340.
- Perhaps it truly is gibberish, but let's suppose its not.
- Perhaps we are not reading Z340 in the right direction?
- Let's assume Z340 is both a transposition cipher and a substitution cipher?

- What do we make of `azdecrypt's` failure to solve Z340?
- Experiments indicate that `azdecrypt` can robustly solve homophonic substitution ciphers of the same length and symbol frequency as Z340.
- Perhaps it truly is gibberish, but let's suppose its not.
- Perhaps we are not reading Z340 in the right direction?
- Let's assume Z340 is both a transposition cipher and a substitution cipher?

- What do we make of `azdecrypt's` failure to solve Z340?
- Experiments indicate that `azdecrypt` can robustly solve homophonic substitution ciphers of the same length and symbol frequency as Z340.
- Perhaps it truly is gibberish, but let's suppose its not.
- Perhaps we are not reading Z340 in the right direction?
- Let's assume Z340 is both a transposition cipher and a substitution cipher?

The Zodiac's 340 Cipher

Transposition + substitution?

- In 2018, David Oranchak gave an excellent presentation on the Z340 to the American Cryptogram Association (ACA).
- In this presentation, David investigated the possibility that Z340 was enciphered with both a (homophonic) substitution and a transposition.
- Of particular interest was the (left to right, top to bottom) *period–19* transposition of the cipher, which produced 37 repeating bigrams!
- This observation was independently discovered by a zodiackillersite.com forum user called "daikon" and Jarl van Eycke in 2015.

Re: Things I noticed about Z340

by **daikon** » Wed Aug 05, 2015 1:22 am

Another observation I came across when doing various tests on Z340 has to do with a spike in the bigram IoC at the period of 19 (or step, or distance).
Bigram IoC (index of coincidence) is just another way to measure bigram repeats, but it is more "sensitive" to multiple repeats.
Here's the raw graph:

daikon

Posts: 179
Joined: Thu Jul 02, 2015 7:04 pm

The Zodiac's 340 Cipher

Transposition + substitution?

- In 2018, David Oranchak gave an excellent presentation on the Z340 to the American Cryptogram Association (ACA).
- In this presentation, David investigated the possibility that Z340 was enciphered with both a (homophonic) substitution and a transposition.
- Of particular interest was the (left to right, top to bottom) *period–19* transposition of the cipher, which produced 37 repeating bigrams!
- This observation was independently discovered by a zodiackillersite.com forum user called "daikon" and Jarl van Eycke in 2015.

Re: Things I noticed about Z340

by **daikon** » Wed Aug 05, 2015 1:22 am

Another observation I came across when doing various tests on Z340 has to do with a spike in the bigram IoC at the period of 19 (or step, or distance).
Bigram IoC (index of coincidence) is just another way to measure bigram repeats, but it is more "sensitive" to multiple repeats.
Here's the raw graph:

daikon

Posts: 179
Joined: Thu Jul 02, 2015 7:04 pm

The Zodiac's 340 Cipher

Transposition + substitution?

- In 2018, David Oranchak gave an excellent presentation on the Z340 to the American Cryptogram Association (ACA).
- In this presentation, David investigated the possibility that Z340 was enciphered with both a (homophonic) substitution and a transposition.
- Of particular interest was the (left to right, top to bottom) *period–19* transposition of the cipher, which produced 37 repeating bigrams!
- This observation was independently discovered by a zodiackillersite.com forum user called "daikon" and Jarl van Eycke in 2015.

Re: Things I noticed about Z340

by **daikon** » Wed Aug 05, 2015 1:22 am

Another observation I came across when doing various tests on Z340 has to do with a spike in the bigram IoC at the period of 19 (or step, or distance).
Bigram IoC (index of coincidence) is just another way to measure bigram repeats, but it is more "sensitive" to multiple repeats.
Here's the raw graph:

daikon

Posts: 179
Joined: Thu Jul 02, 2015 7:04 pm

The Zodiac's 340 Cipher

Transposition + substitution?

- In 2018, David Oranchak gave an excellent presentation on the Z340 to the American Cryptogram Association (ACA).
- In this presentation, David investigated the possibility that Z340 was enciphered with both a (homophonic) substitution and a transposition.
- Of particular interest was the (left to right, top to bottom) *period–19* transposition of the cipher, which produced 37 repeating bigrams!
- This observation was independently discovered by a zodiackillersite.com forum user called "daikon" and Jarl van Eycke in 2015.

Re: Things I noticed about Z340

by **daikon** » Wed Aug 05, 2015 1:22 am

Another observation I came across when doing various tests on Z340 has to do with a spike in the bigram IoC at the period of 19 (or step, or distance).
Bigram IoC (index of coincidence) is just another way to measure bigram repeats, but it is more "sensitive" to multiple repeats.
Here's the raw graph:

daikon

Posts: 179
Joined: Thu Jul 02, 2015 7:04 pm

The Zodiac's 340 Cipher

David's period–19 transposition

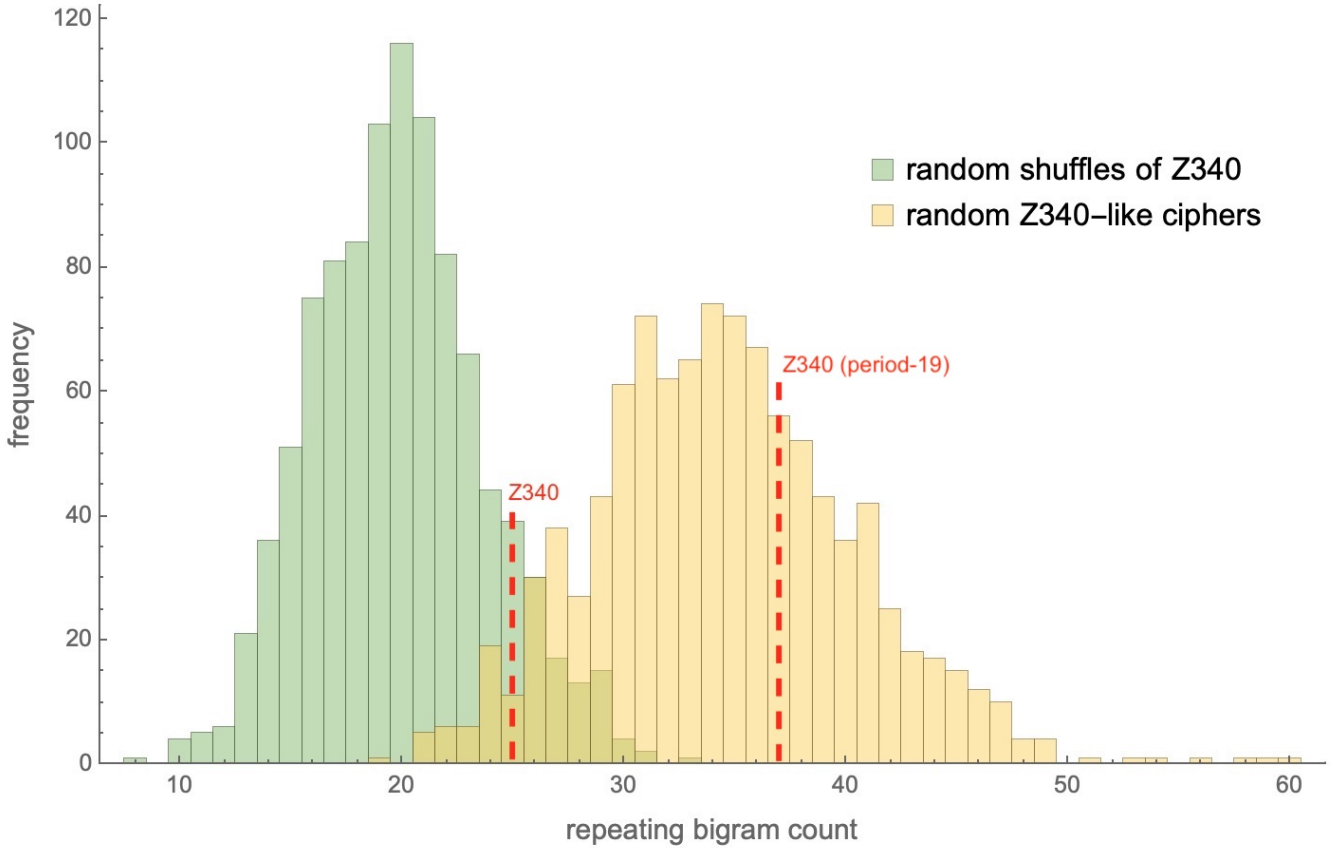
Left–right, top–bottom

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67
68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101
102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118
119	120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135
136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152
153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169
170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186
187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203
204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220
221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237
238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254
255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271
272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288
289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305
306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322
323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339

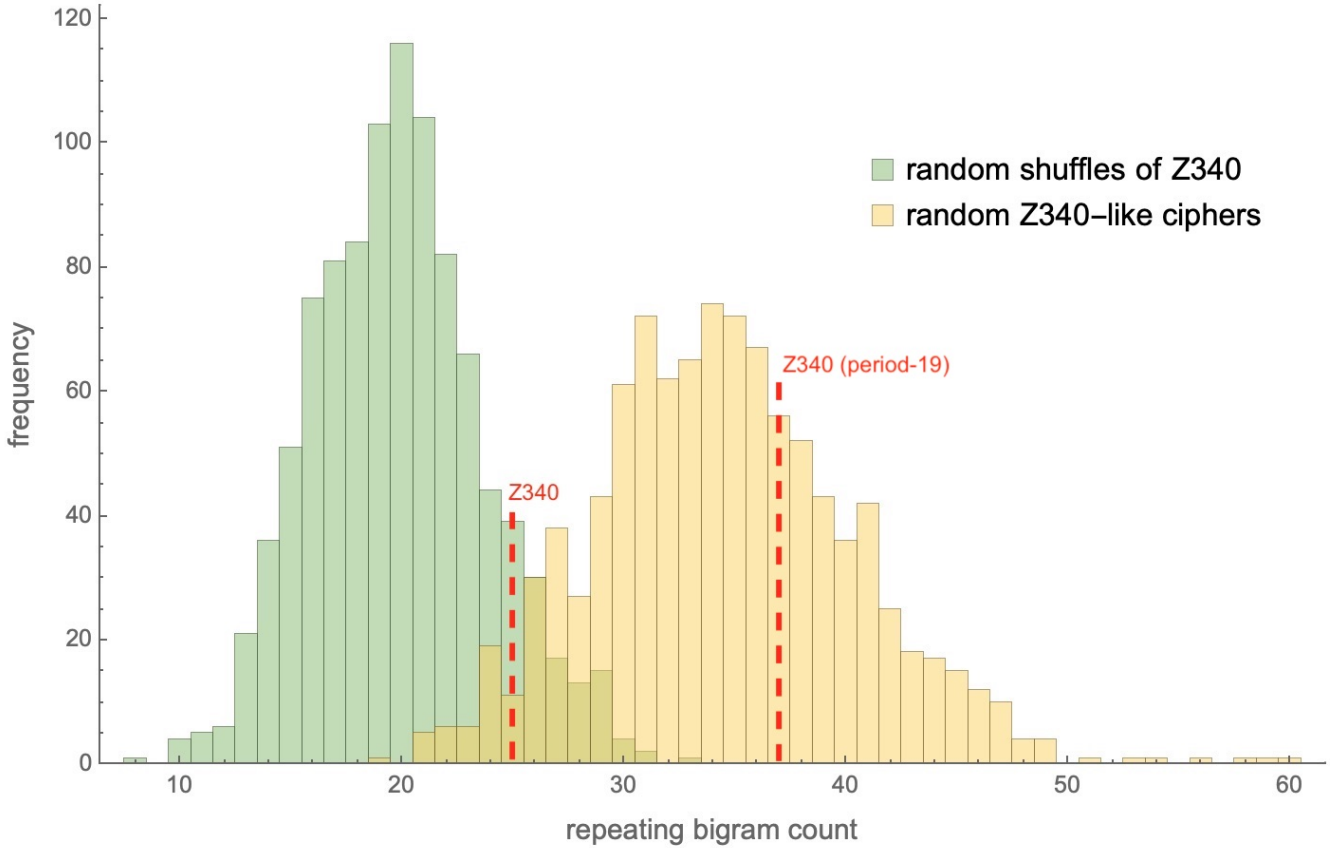
period–19 transposition

0	18	36	54	72	90	108	126	144	162	180	198	216	234	252	270	288
306	324	1	19	37	55	73	91	109	127	145	163	181	199	217	235	253
271	289	307	325	2	20	38	56	74	92	110	128	146	164	182	200	218
236	254	272	290	308	326	3	21	39	57	75	93	111	129	147	165	183
201	219	237	255	273	291	309	327	4	22	40	58	76	94	112	130	148
166	184	202	220	238	256	274	292	310	328	5	23	41	59	77	95	113
131	149	167	185	203	221	239	257	275	293	311	329	6	24	42	60	78
96	114	132	150	168	186	204	222	240	258	276	294	312	330	7	25	43
61	79	97	115	133	151	169	187	205	223	241	259	277	295	313	331	8
26	44	62	80	98	116	134	152	170	188	206	224	242	260	278	296	314
332	9	27	45	63	81	99	117	135	153	171	189	207	225	243	261	279
297	315	333	10	28	46	64	82	100	118	136	154	172	190	208	226	244
262	280	298	316	334	11	29	47	65	83	101	119	137	155	173	191	209
227	245	263	281	299	317	335	12	30	48	66	84	102	120	138	156	174
192	210	228	246	264	282	300	318	336	13	31	49	67	85	103	121	139
157	175	193	211	229	247	265	283	301	319	337	14	32	50	68	86	104
122	140	158	176	194	212	230	248	266	284	302	320	338	15	33	51	69
87	105	123	141	159	177	195	213	231	249	267	285	303	321	339	16	34
52	70	88	106	124	142	160	178	196	214	232	250	268	286	304	322	323
17	35	53	71	89	107	125	143	161	179	197	215	233	251	269	287	305

- The 37 repeating bigrams of the *period–19* transposition is 4.5–sigma from the mean of random shuffles of the Z340.
- This suggests we could be getting closer to the correct reading direction.



- The 37 repeating bigrams of the *period–19* transposition is 4.5–sigma from the mean of random shuffles of the Z340.
- This suggests we could be getting closer to the correct reading direction.



The *period–19* transposition credited to "daikon" & Jarl van Eycke is not a left to right, top to bottom, 19–decimation. When you wrap around vertically the period is only 18.

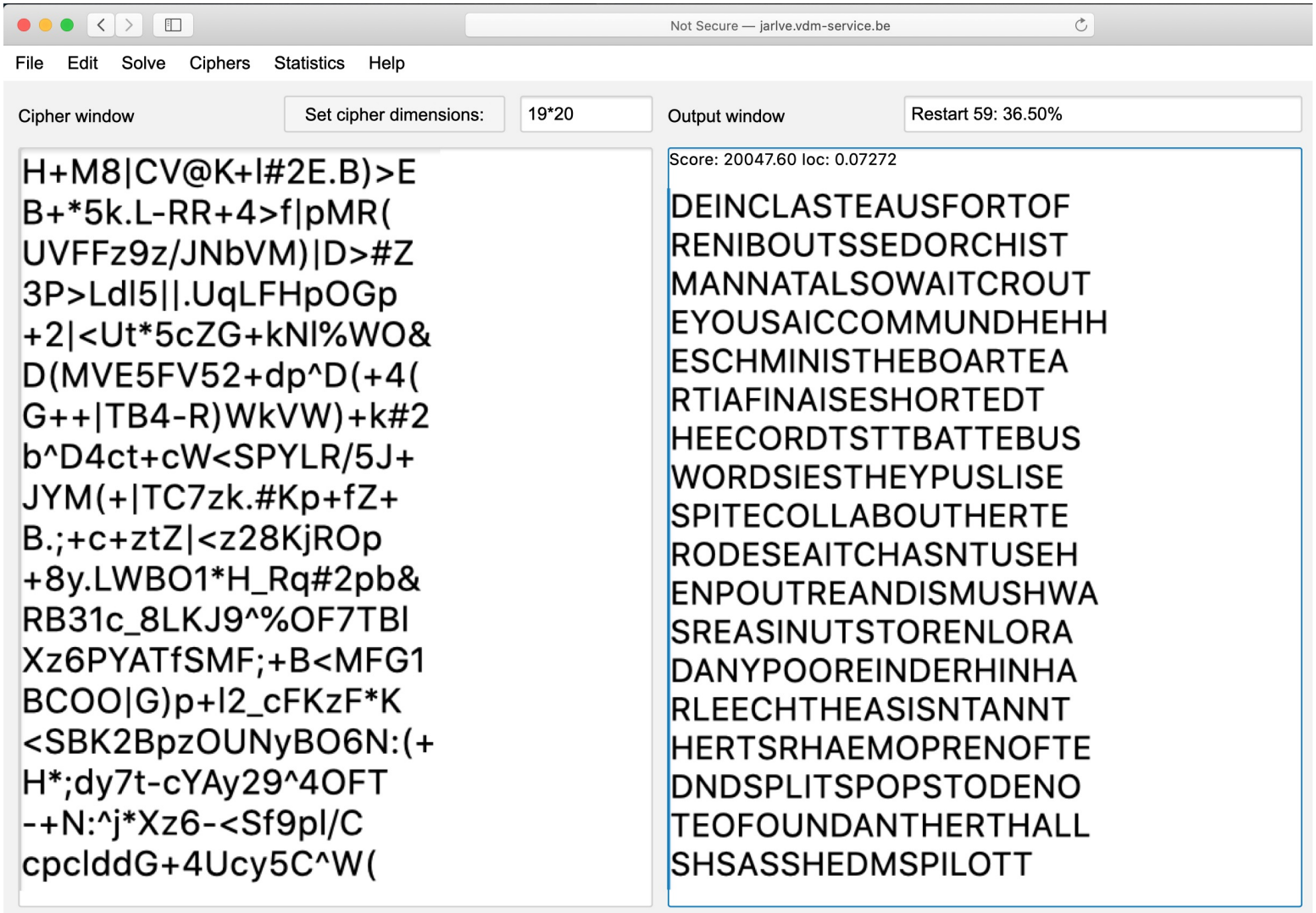
period–19 transposition

0	18	36	54	72	90	108	126	144	162	180	198	216	234	252	270	288
306	324	1	19	37	55	73	91	109	127	145	163	181	199	217	235	253
271	289	307	325	2	20	38	56	74	92	110	128	146	164	182	200	218
236	254	272	290	308	326	3	21	39	57	75	93	111	129	147	165	183
201	219	237	255	273	291	309	327	4	22	40	58	76	94	112	130	148
166	184	202	220	238	256	274	292	310	328	5	23	41	59	77	95	113
131	149	167	185	203	221	239	257	275	293	311	329	6	24	42	60	78
96	114	132	150	168	186	204	222	240	258	276	294	312	330	7	25	43
61	79	97	115	133	151	169	187	205	223	241	259	277	295	313	331	8
26	44	62	80	98	116	134	152	170	188	206	224	242	260	278	296	314
332	9	27	45	63	81	99	117	135	153	171	189	207	225	243	261	279
297	315	333	10	28	46	64	82	100	118	136	154	172	190	208	226	244
262	280	298	316	334	11	29	47	65	83	101	119	137	155	173	191	209
227	245	263	281	299	317	335	12	30	48	66	84	102	120	138	156	174
192	210	228	246	264	282	300	318	336	13	31	49	67	85	103	121	139
157	175	193	211	229	247	265	283	301	319	337	14	32	50	68	86	104
122	140	158	176	194	212	230	248	266	284	302	320	338	15	33	51	69
87	105	123	141	159	177	195	213	231	249	267	285	303	321	339	16	34
52	70	88	106	124	142	160	178	196	214	232	250	268	286	304	322	323
17	35	53	71	89	107	125	143	161	179	197	215	233	251	269	287	305

A (left–right, top–bottom) 19–decimation

0	179	18	197	36	215	54	233	72	251	90	269	108	287	126	305	144
323	162	1	180	19	198	37	216	55	234	73	252	91	270	109	288	127
306	145	324	163	2	181	20	199	38	217	56	235	74	253	92	271	110
289	128	307	146	325	164	3	182	21	200	39	218	57	236	75	254	93
272	111	290	129	308	147	326	165	4	183	22	201	40	219	58	237	76
255	94	273	112	291	130	309	148	327	166	5	184	23	202	41	220	59
238	77	256	95	274	113	292	131	310	149	328	167	6	185	24	203	42
221	60	239	78	257	96	275	114	293	132	311	150	329	168	7	186	25
204	43	222	61	240	79	258	97	276	115	294	133	312	151	330	169	8
187	26	205	44	223	62	241	80	259	98	277	116	295	134	313	152	331
170	9	188	27	206	45	224	63	242	81	260	99	278	117	296	135	314
153	332	171	10	189	28	207	46	225	64	243	82	261	100	279	118	297
136	315	154	333	172	11	190	29	208	47	226	65	244	83	262	101	280
119	298	137	316	155	334	173	12	191	30	209	48	227	66	245	84	263
102	281	120	299	138	317	156	335	174	13	192	31	210	49	228	67	246
85	264	103	282	121	300	139	318	157	336	175	14	193	32	211	50	229
68	247	86	265	104	283	122	301	140	319	158	337	176	15	194	33	212
51	230	69	248	87	266	105	284	123	302	141	320	159	338	177	16	195
34	213	52	231	70	249	88	267	106	285	124	303	142	321	160	339	178
17	196	35	214	53	232	71	250	89	268	107	286	125	304	143	322	161

Have we discovered the correct transposition?



- Although the *period–19* transposition clearly increases the number of repeating bigrams, it's not a very natural way to write out a transposition.
- I thought the transposition used in Z340 may be a doubly periodic, 1,2–decimation.
- Let the i, j entry of the Z340 be given by $s_{i,j}$ and denote the 1,2–decimation with T_i, where

$$T_i = s_{i \bmod 20, 2i \bmod 17}.$$

- While this looks more complicated, geometrically it's just 1–down, 2–right, and wrapping around periodically, both horizontally and vertically.
- The 1,2–decimation transposition follows similar diagonals to the *period–19* transposition.
- The 1,2–decimation also has 37 bigrams.

- Although the *period–19* transposition clearly increases the number of repeating bigrams, it's not a very natural way to write out a transposition.
- I thought the transposition used in Z340 may be a doubly periodic, 1,2–decimation.
- Let the i, j entry of the Z340 be given by $s_{i,j}$ and denote the 1,2–decimation with T_i, where

$$T_i = s_{i \bmod 20, 2i \bmod 17}.$$

- While this looks more complicated, geometrically it's just 1–down, 2–right, and wrapping around periodically, both horizontally and vertically.
- The 1,2–decimation transposition follows similar diagonals to the *period–19* transposition.
- The 1,2–decimation also has 37 bigrams.

- Although the *period–19* transposition clearly increases the number of repeating bigrams, it's not a very natural way to write out a transposition.
- I thought the transposition used in Z340 may be a doubly periodic, 1,2–decimation.
- Let the i, j entry of the Z340 be given by $s_{i,j}$ and denote the 1,2–decimation with T_i, where

$$T_i = s_{i \bmod 20, 2i \bmod 17}.$$

- While this looks more complicated, geometrically it's just 1–down, 2–right, and wrapping around periodically, both horizontally and vertically.
- The 1,2–decimation transposition follows similar diagonals to the *period–19* transposition.
- The 1,2–decimation also has 37 bigrams.

- Although the *period–19* transposition clearly increases the number of repeating bigrams, it's not a very natural way to write out a transposition.
- I thought the transposition used in Z340 may be a doubly periodic, 1,2–decimation.
- Let the i, j entry of the Z340 be given by $s_{i,j}$ and denote the 1,2–decimation with T_i, where

$$T_i = s_{i \bmod 20, 2i \bmod 17}.$$

- While this looks more complicated, geometrically it's just 1–down, 2–right, and wrapping around periodically, both horizontally and vertically.
- The 1,2–decimation transposition follows similar diagonals to the *period–19* transposition.
- The 1,2–decimation also has 37 bigrams.

- Although the *period–19* transposition clearly increases the number of repeating bigrams, it's not a very natural way to write out a transposition.
- I thought the transposition used in Z340 may be a doubly periodic, 1,2–decimation.
- Let the i, j entry of the Z340 be given by $s_{i,j}$ and denote the 1,2–decimation with T_i, where

$$T_i = s_{i \bmod 20, 2i \bmod 17}.$$

- While this looks more complicated, geometrically it's just 1–down, 2–right, and wrapping around periodically, both horizontally and vertically.
- The 1,2–decimation transposition follows similar diagonals to the *period–19* transposition.
- The 1,2–decimation also has 37 bigrams.

- Although the *period–19* transposition clearly increases the number of repeating bigrams, it's not a very natural way to write out a transposition.
- I thought the transposition used in Z340 may be a doubly periodic, 1,2–decimation.
- Let the i, j entry of the Z340 be given by $s_{i,j}$ and denote the 1,2–decimation with T_i, where

$$T_i = s_{i \bmod 20, 2i \bmod 17}.$$

- While this looks more complicated, geometrically it's just 1–down, 2–right, and wrapping around periodically, both horizontally and vertically.
- The 1,2–decimation transposition follows similar diagonals to the *period–19* transposition.
- The 1,2–decimation also has 37 bigrams.

The Zodiac's 340 Cipher

1,2–decimation of Z340

The *period–19* transposition

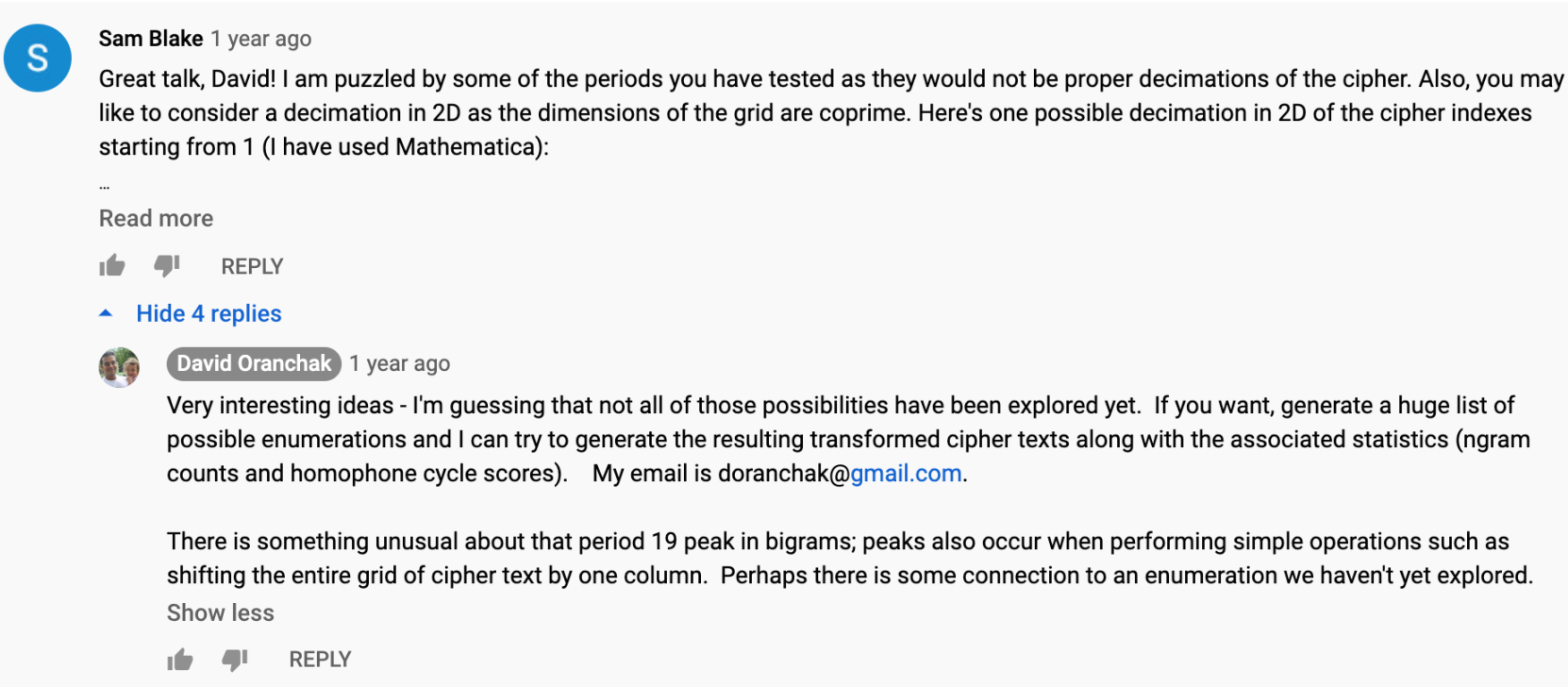
0	18	36	54	72	90	108	126	144	162	180	198	216	234	252	270	288
306	324	1	19	37	55	73	91	109	127	145	163	181	199	217	235	253
271	289	307	325	2	20	38	56	74	92	110	128	146	164	182	200	218
236	254	272	290	308	326	3	21	39	57	75	93	111	129	147	165	183
201	219	237	255	273	291	309	327	4	22	40	58	76	94	112	130	148
166	184	202	220	238	256	274	292	310	328	5	23	41	59	77	95	113
131	149	167	185	203	221	239	257	275	293	311	329	6	24	42	60	78
96	114	132	150	168	186	204	222	240	258	276	294	312	330	7	25	43
61	79	97	115	133	151	169	187	205	223	241	259	277	295	313	331	8
26	44	62	80	98	116	134	152	170	188	206	224	242	260	278	296	314
332	9	27	45	63	81	99	117	135	153	171	189	207	225	243	261	279
297	315	333	10	28	46	64	82	100	118	136	154	172	190	208	226	244
262	280	298	316	334	11	29	47	65	83	101	119	137	155	173	191	209
227	245	263	281	299	317	335	12	30	48	66	84	102	120	138	156	174
192	210	228	246	264	282	300	318	336	13	31	49	67	85	103	121	139
157	175	193	211	229	247	265	283	301	319	337	14	32	50	68	86	104
122	140	158	176	194	212	230	248	266	284	302	320	338	15	33	51	69
87	105	123	141	159	177	195	213	231	249	267	285	303	321	339	16	34
52	70	88	106	124	142	160	178	196	214	232	250	268	286	304	322	323
17	35	53	71	89	107	125	143	161	179	197	215	233	251	269	287	305

A doubly periodic, 1,2–decimation

0	60	120	180	240	300	20	80	140	200	260	320	40	100	160	220	280
221	281	1	61	121	181	241	301	21	81	141	201	261	321	41	101	161
102	162	222	282	2	62	122	182	242	302	22	82	142	202	262	322	42
323	43	103	163	223	283	3	63	123	183	243	303	23	83	143	203	263
204	264	324	44	104	164	224	284	4	64	124	184	244	304	24	84	144
85	145	205	265	325	45	105	165	225	285	5	65	125	185	245	305	25
306	26	86	146	206	266	326	46	106	166	226	286	6	66	126	186	246
187	247	307	27	87	147	207	267	327	47	107	167	227	287	7	67	127
68	128	188	248	308	28	88	148	208	268	328	48	108	168	228	288	8
289	9	69	129	189	249	309	29	89	149	209	269	329	49	109	169	229
170	230	290	10	70	130	190	250	310	30	90	150	210	270	330	50	110
51	111	171	231	291	11	71	131	191	251	311	31	91	151	211	271	331
272	332	52	112	172	232	292	12	72	132	192	252	312	32	92	152	212
153	213	273	333	53	113	173	233	293	13	73	133	193	253	313	33	93
34	94	154	214	274	334	54	114	174	234	294	14	74	134	194	254	314
255	315	35	95	155	215	275	335	55	115	175	235	295	15	75	135	195
136	196	256	316	36	96	156	216	276	336	56	116	176	236	296	16	76
17	77	137	197	257	317	37	97	157	217	277	337	57	117	177	237	297
238	298	18	78	138	198	258	318	38	98	158	218	278	338	58	118	178
119	179	239	299	19	79	139	199	259	319	39	99	159	219	279	339	59

Reaching out to David Oranchak

I thought David may like to know the connection between the *period–19* transposition and a 1,2–decimation transposition of the cipher.



Sam Blake 1 year ago

Great talk, David! I am puzzled by some of the periods you have tested as they would not be proper decimations of the cipher. Also, you may like to consider a decimation in 2D as the dimensions of the grid are coprime. Here's one possible decimation in 2D of the cipher indexes starting from 1 (I have used Mathematica):

...

Read more

REPLY

Hide 4 replies

David Oranchak 1 year ago

Very interesting ideas - I'm guessing that not all of those possibilities have been explored yet. If you want, generate a huge list of possible enumerations and I can try to generate the resulting transformed cipher texts along with the associated statistics (ngram counts and homophone cycle scores). My email is doranchak@gmail.com.

There is something unusual about that period 19 peak in bigrams; peaks also occur when performing simple operations such as shifting the entire grid of cipher text by one column. Perhaps there is some connection to an enumeration we haven't yet explored.

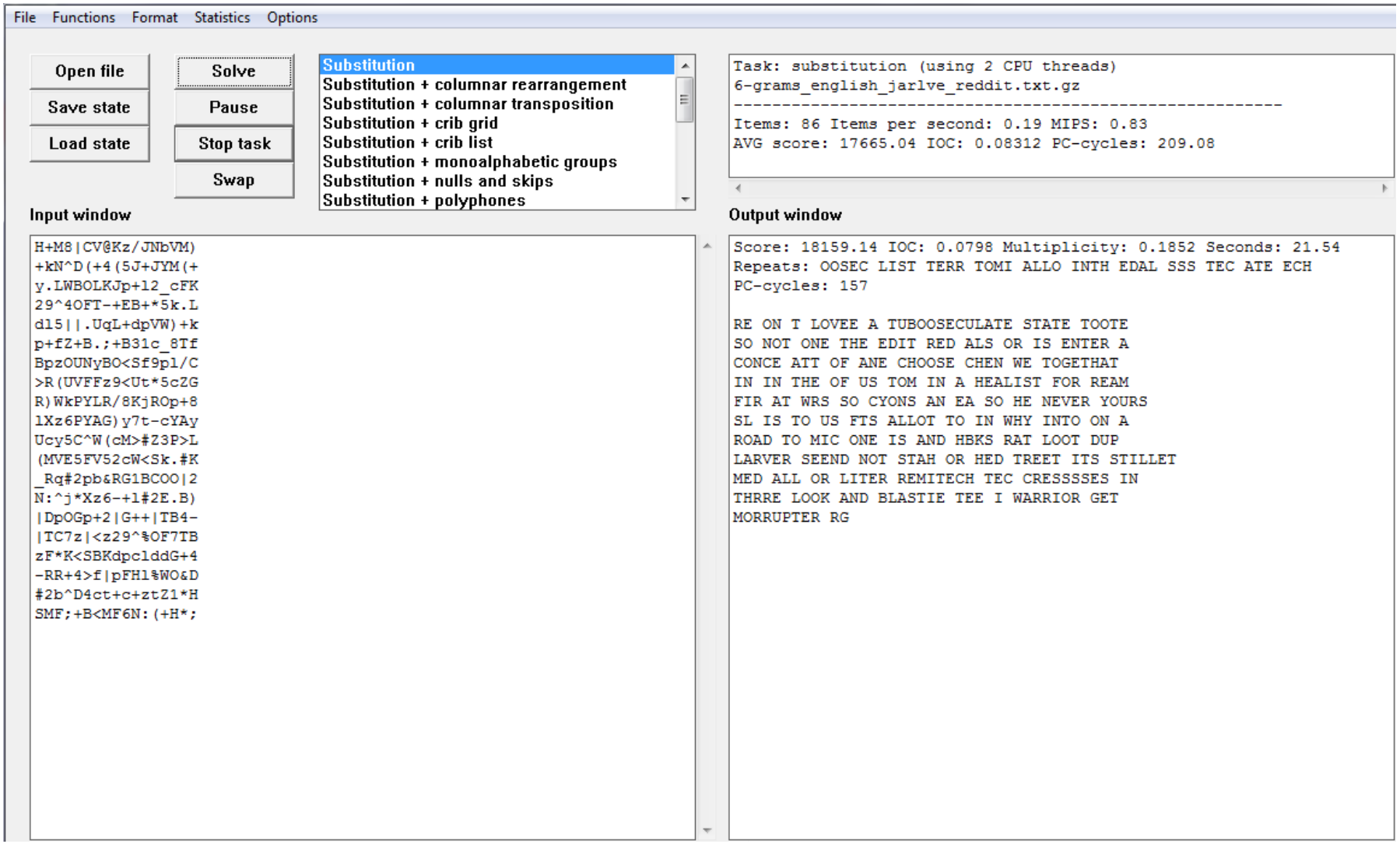
Show less

REPLY

Reaching out to David Oranchak

azdecrypt on the 1,2–decimation transposition of Z340

David and I both tested the 1,2–decimation of Z340 with `azdecrypt` and `zkdecrypto`.



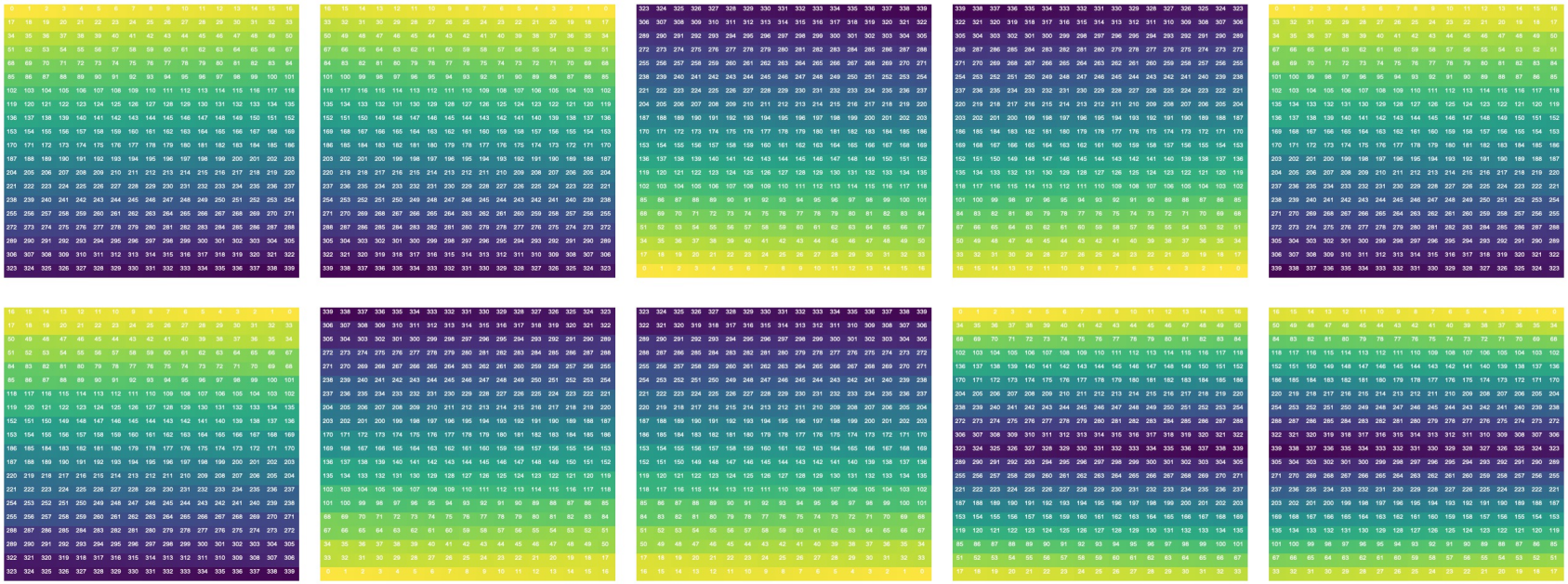
- I was now interested in looking at further transpositions.
- Instead of looking at a handful of selected transpositions, like the 1,2–decimation, my approach was to enumerate all possible transpositions of a given kind.
- We ran these transpositions through `azdecrypt` and `zkdecrypto`.
- The decrypted plaintext of the candidate ciphers were ranked by *score* and analysed for Zodiac–like words.

- I was now interested in looking at further transpositions.
- Instead of looking at a handful of selected transpositions, like the 1,2–decimation, my approach was to enumerate all possible transpositions of a given kind.
- We ran these transpositions through `azdecrypt` and `zkdecrypto`.
- The decrypted plaintext of the candidate ciphers were ranked by *score* and analysed for Zodiac–like words.

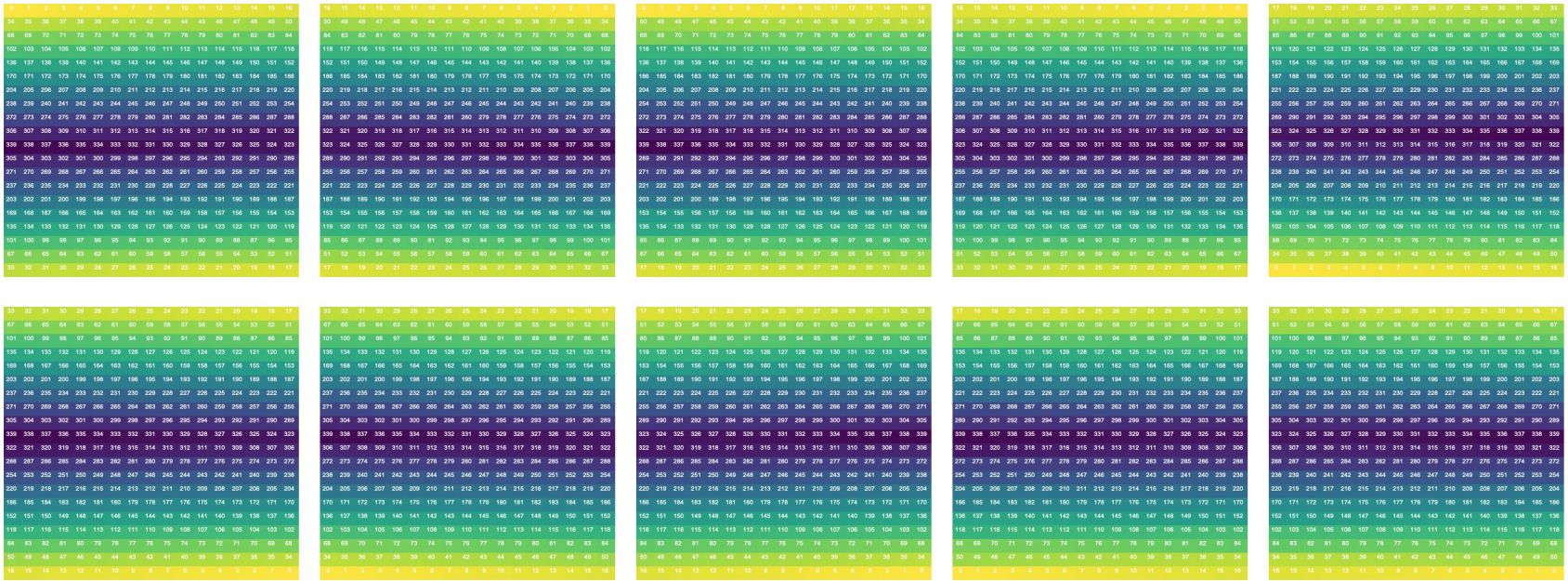
- I was now interested in looking at further transpositions.
- Instead of looking at a handful of selected transpositions, like the 1,2–decimation, my approach was to enumerate all possible transpositions of a given kind.
- We ran these transpositions through `azdecrypt` and `zkdecrypto`.
- The decrypted plaintext of the candidate ciphers were ranked by *score* and analysed for Zodiac–like words.

- I was now interested in looking at further transpositions.
- Instead of looking at a handful of selected transpositions, like the 1,2–decimation, my approach was to enumerate all possible transpositions of a given kind.
- We ran these transpositions through `azdecrypt` and `zkdecrypto`.
- The decrypted plaintext of the candidate ciphers were ranked by *score* and analysed for Zodiac–like words.

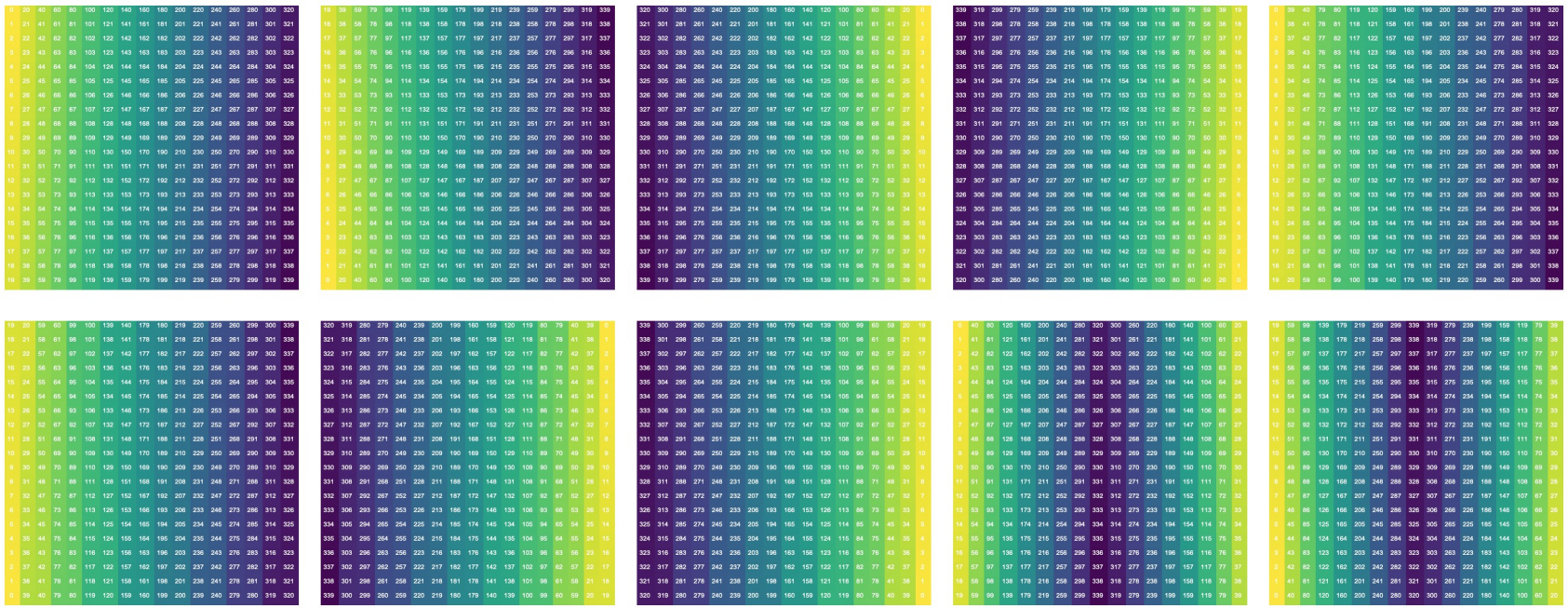
Row–major transpositions



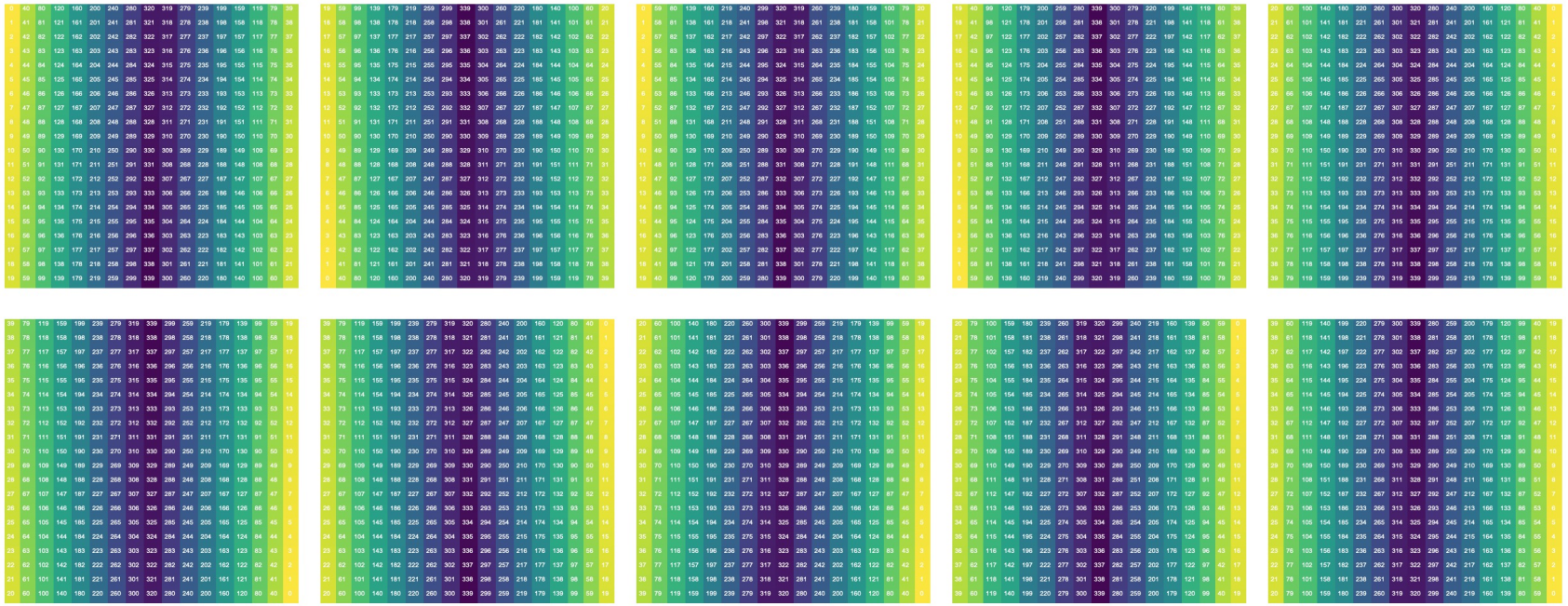
Row–major transpositions cont.



Column–major transpositions



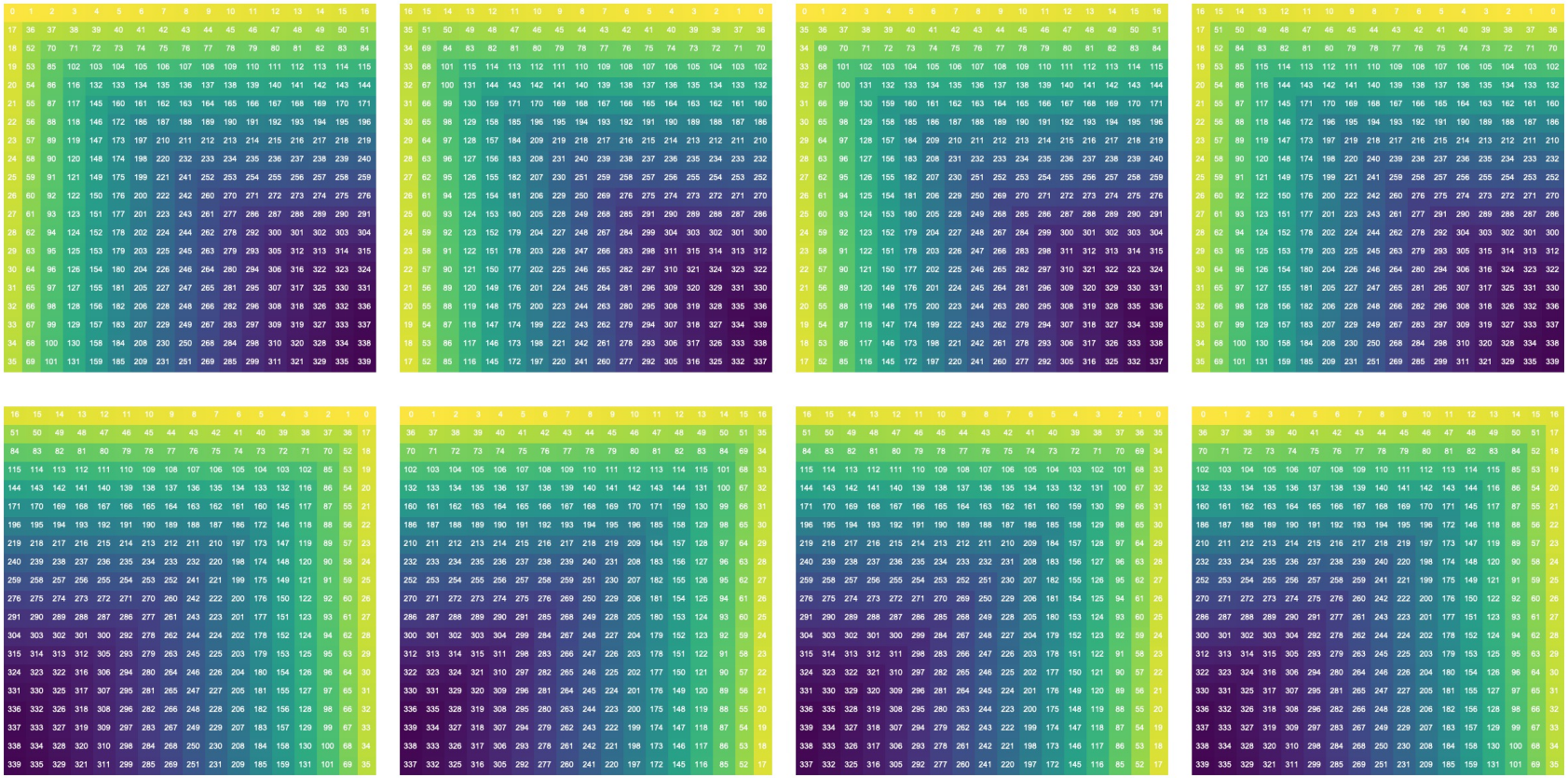
Column–major transpositions cont.



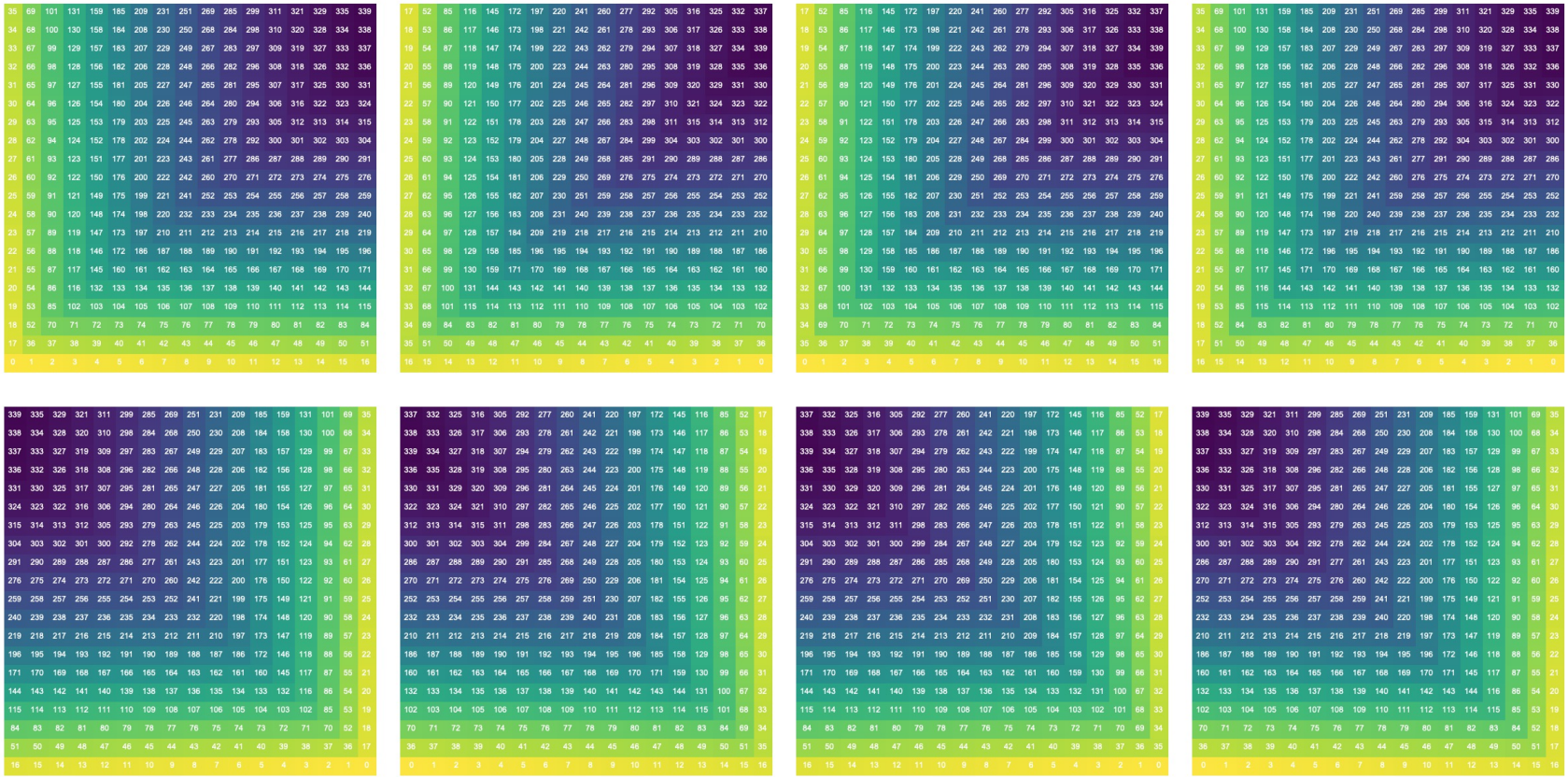
Large–Scale Experiments on the Z340

Enumerating 2D transpositions

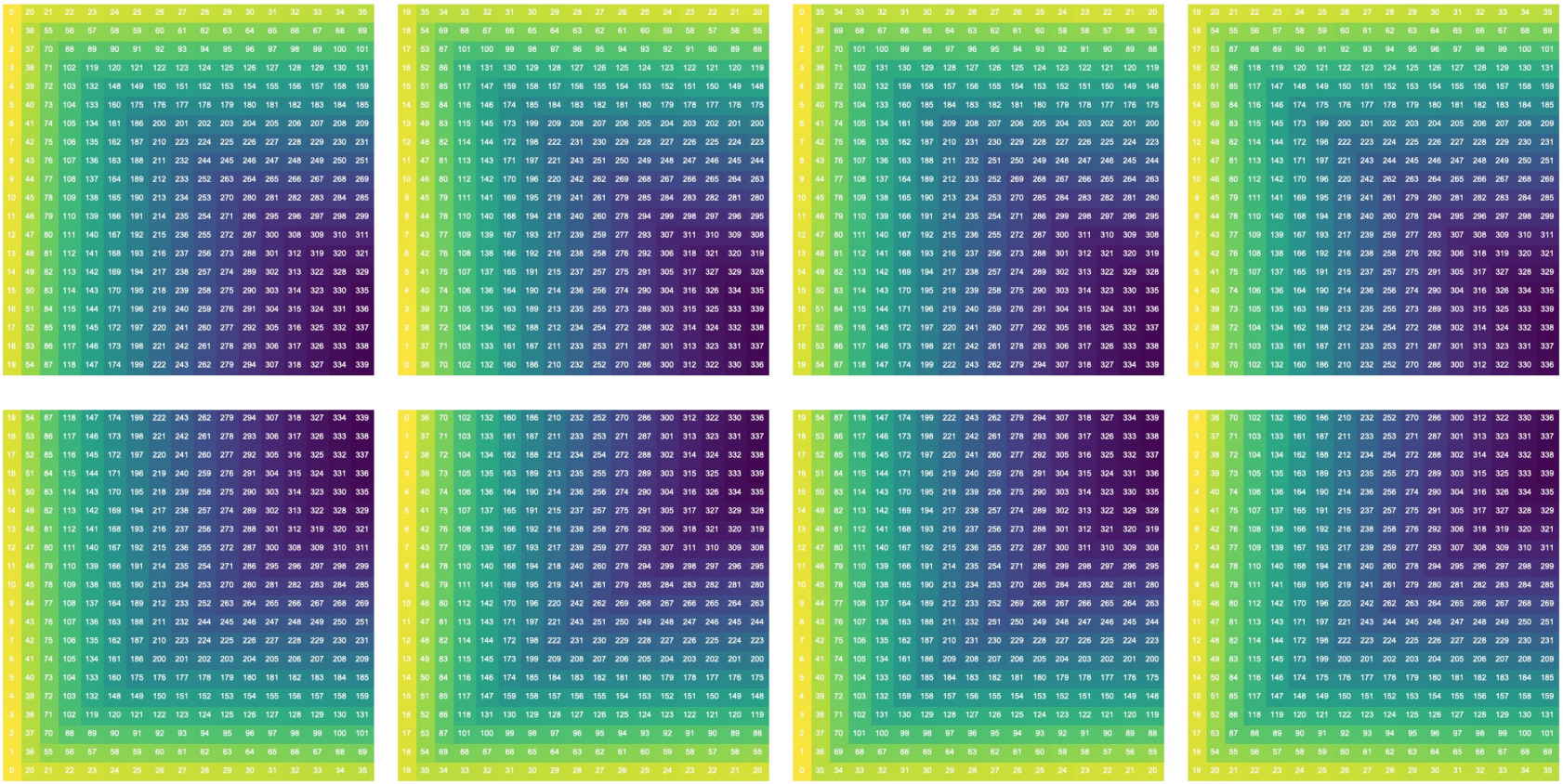
Alternating row–column transpositions



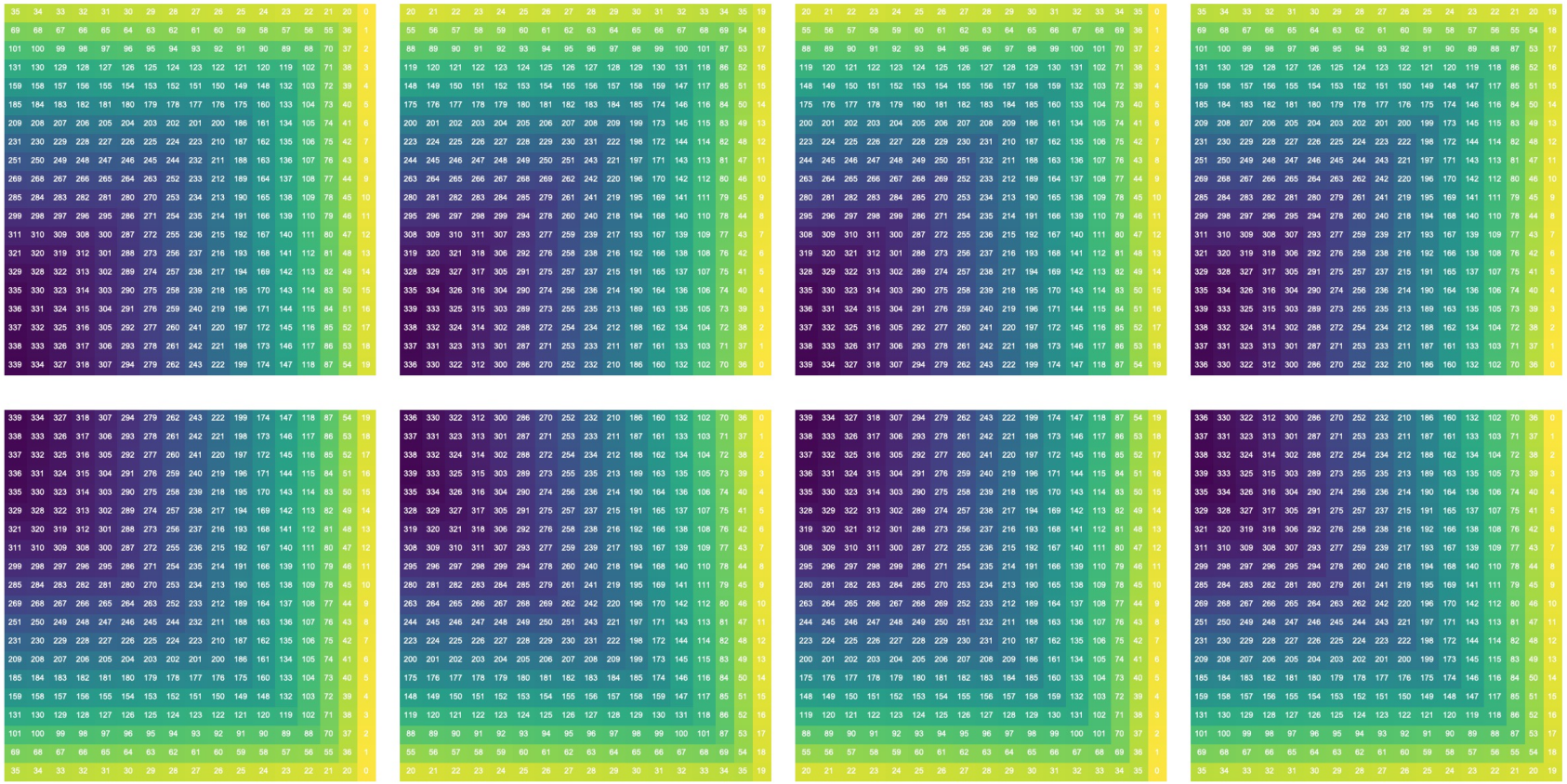
Alternating row–column transpositions cont.



Alternating column–row transpositions



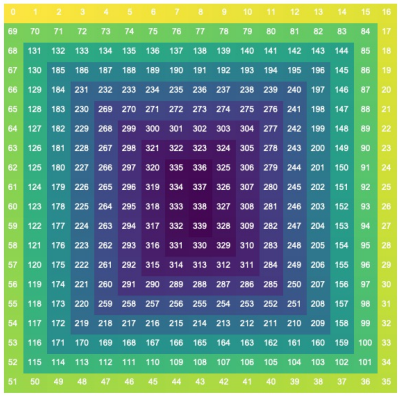
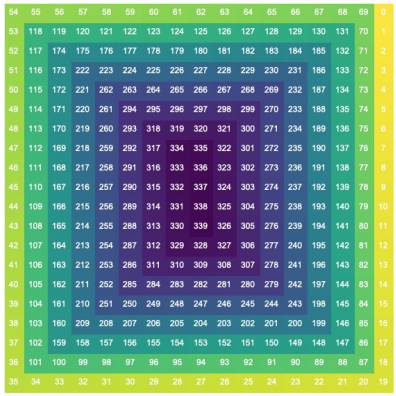
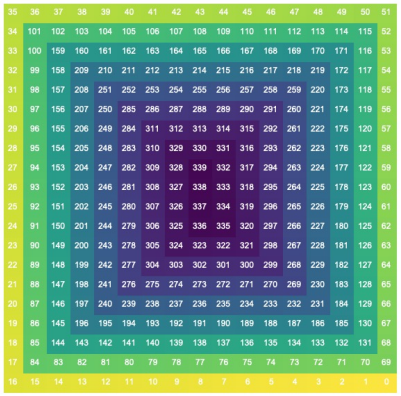
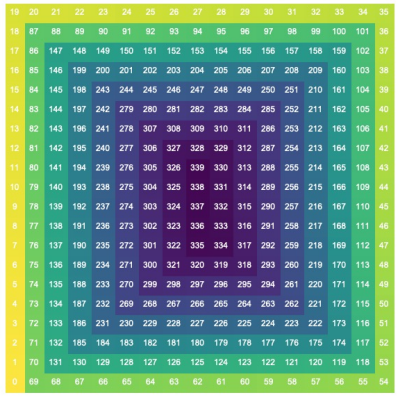
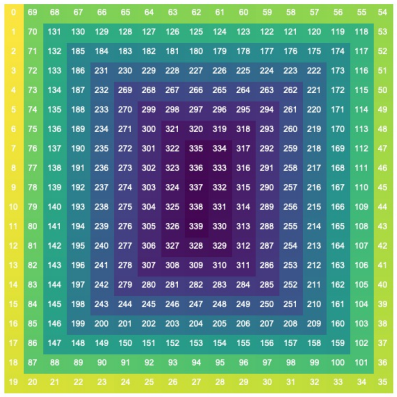
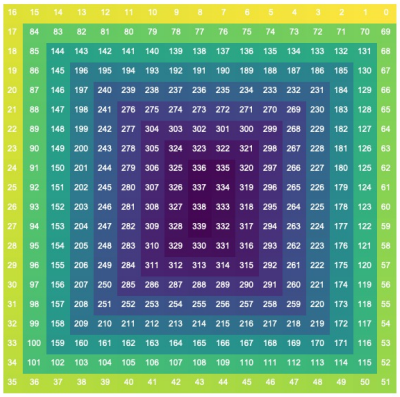
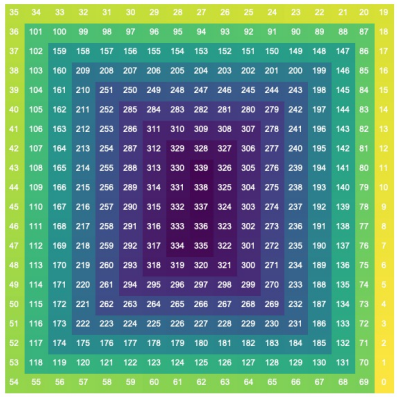
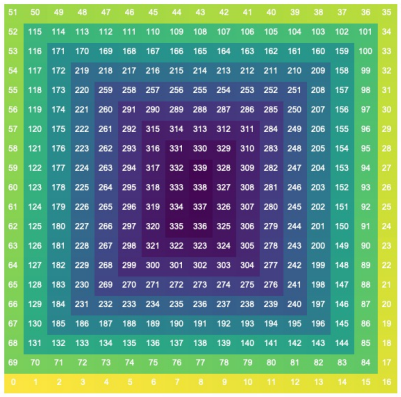
Alternating column–row transpositions cont.



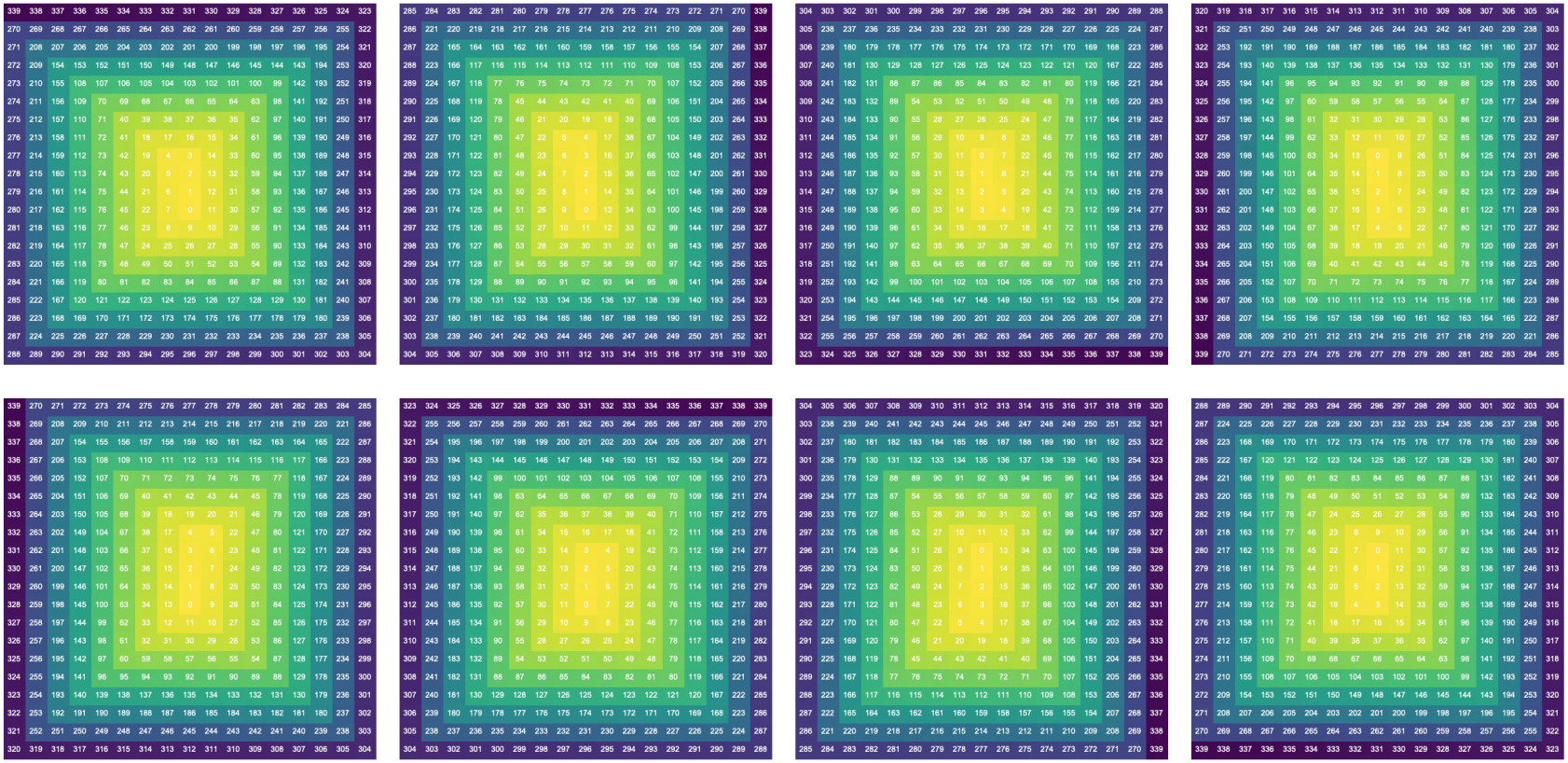
Large–Scale Experiments on the Z340

Enumerating 2D transpositions

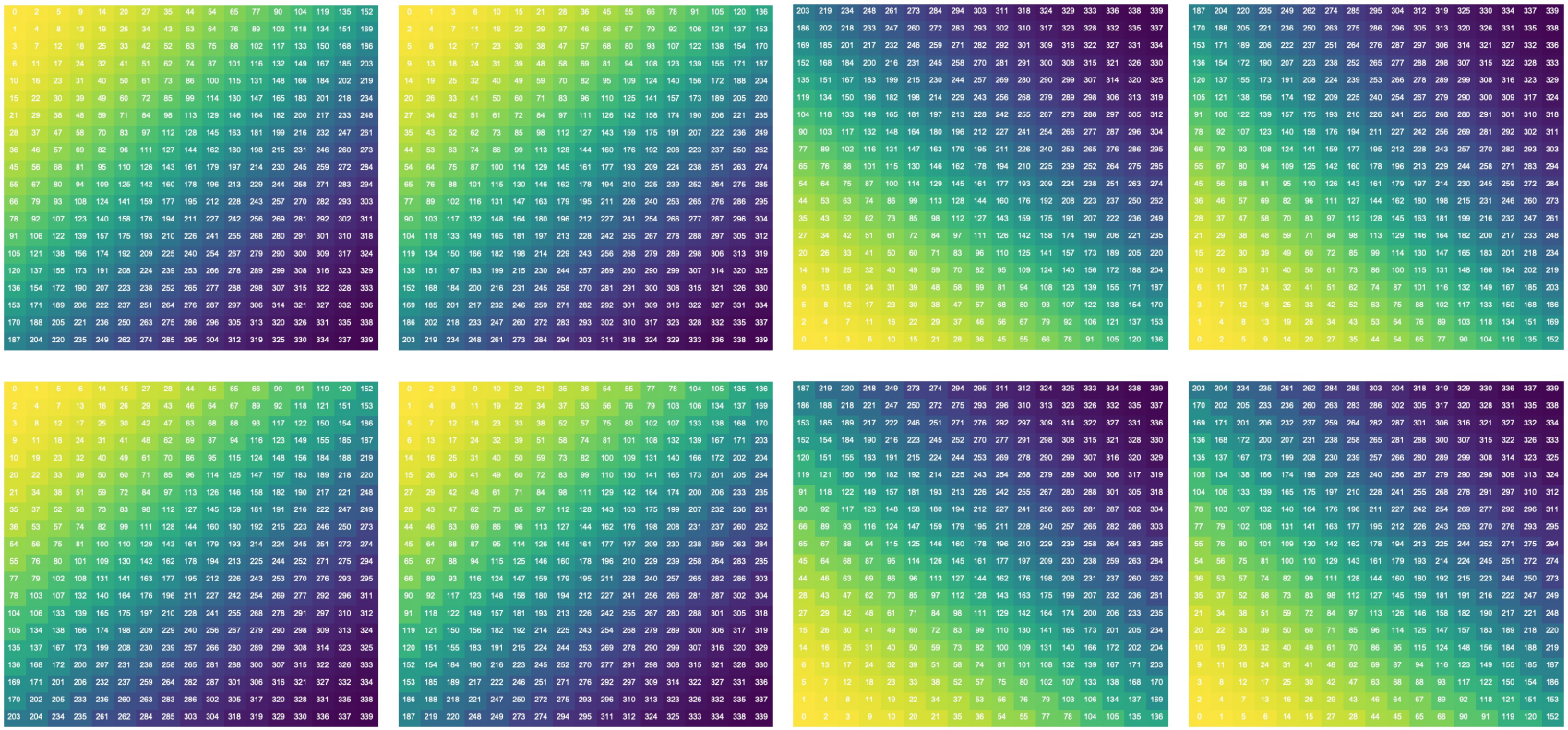
Inward spirals

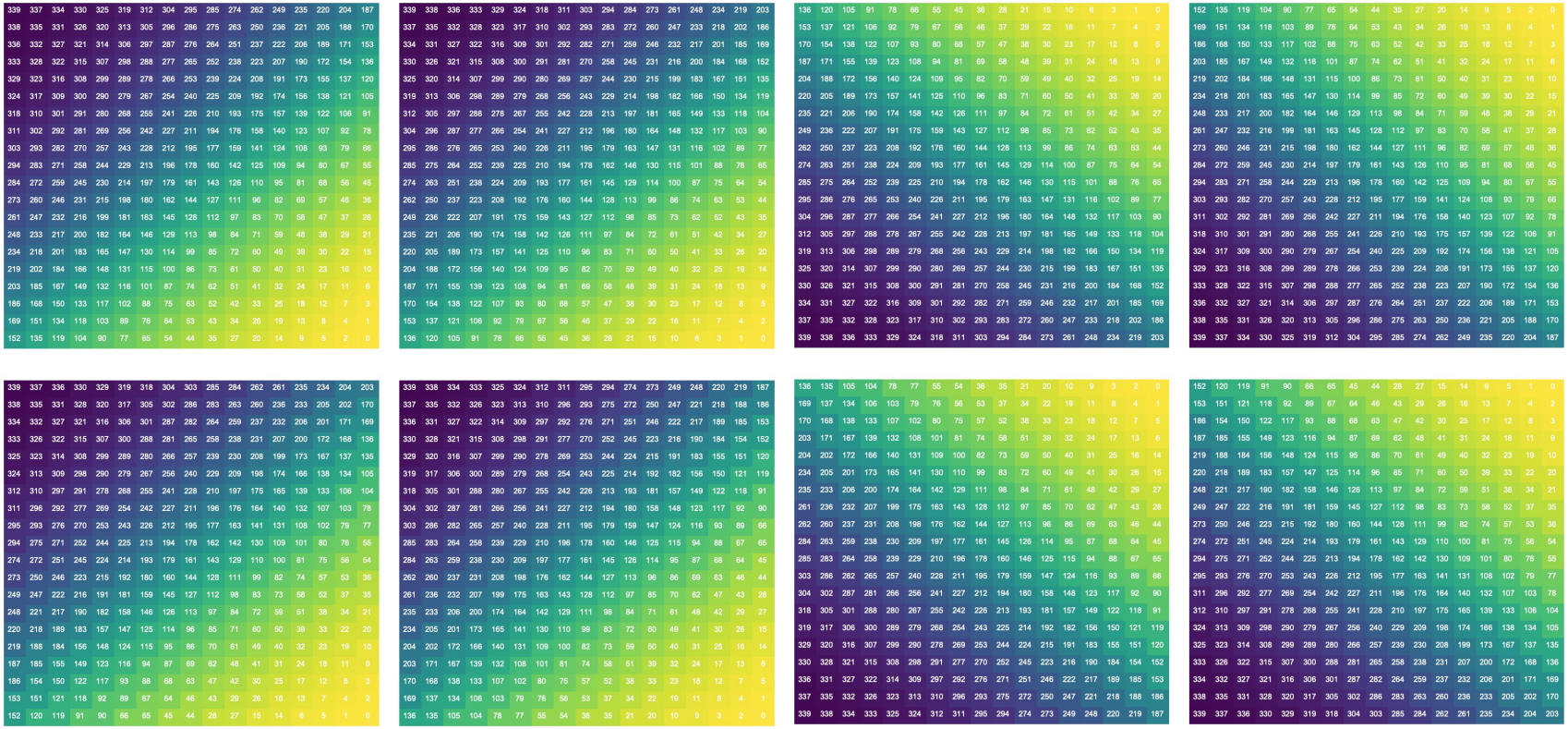
Outward spirals



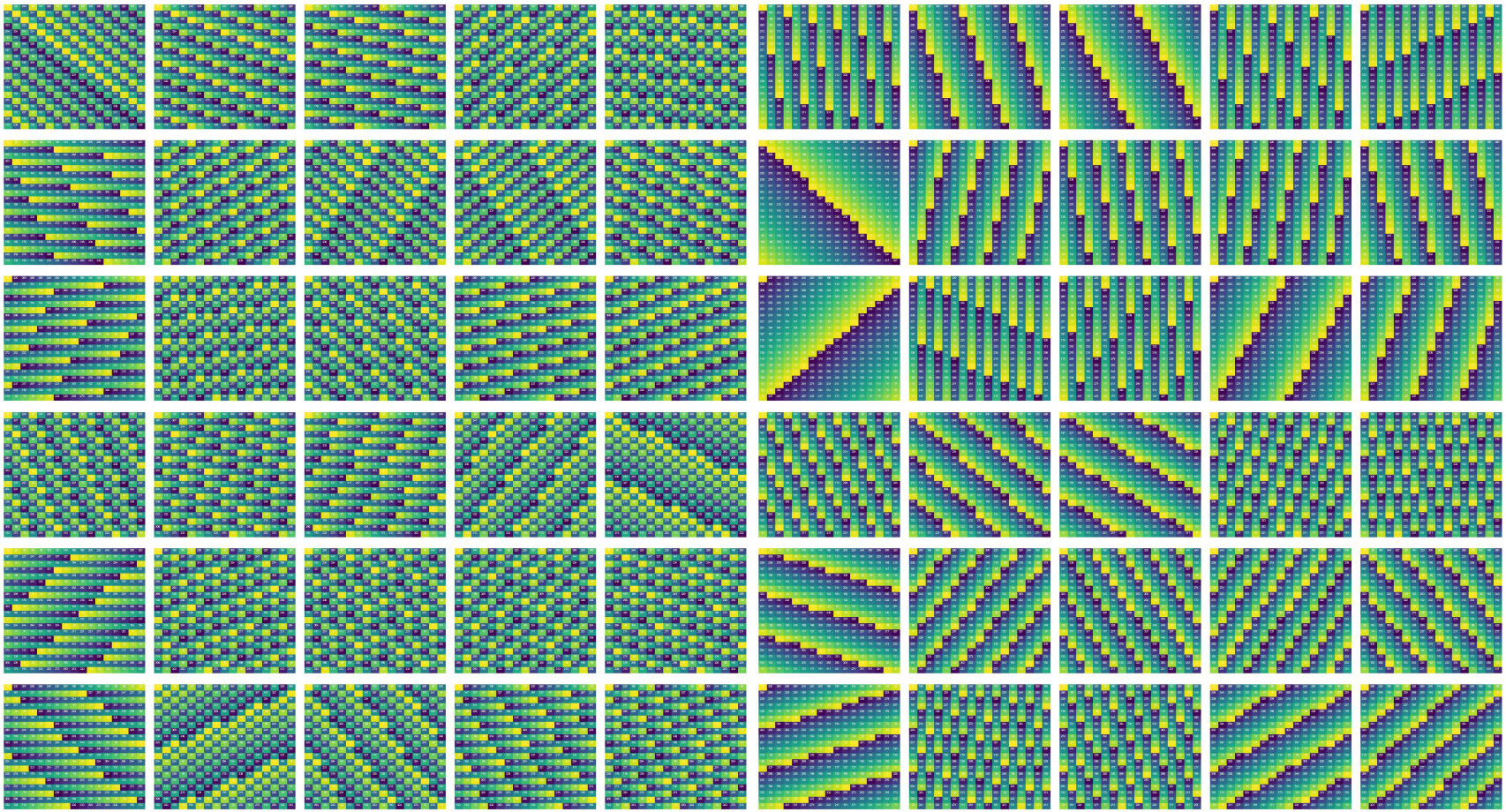
Diagonal transpositions



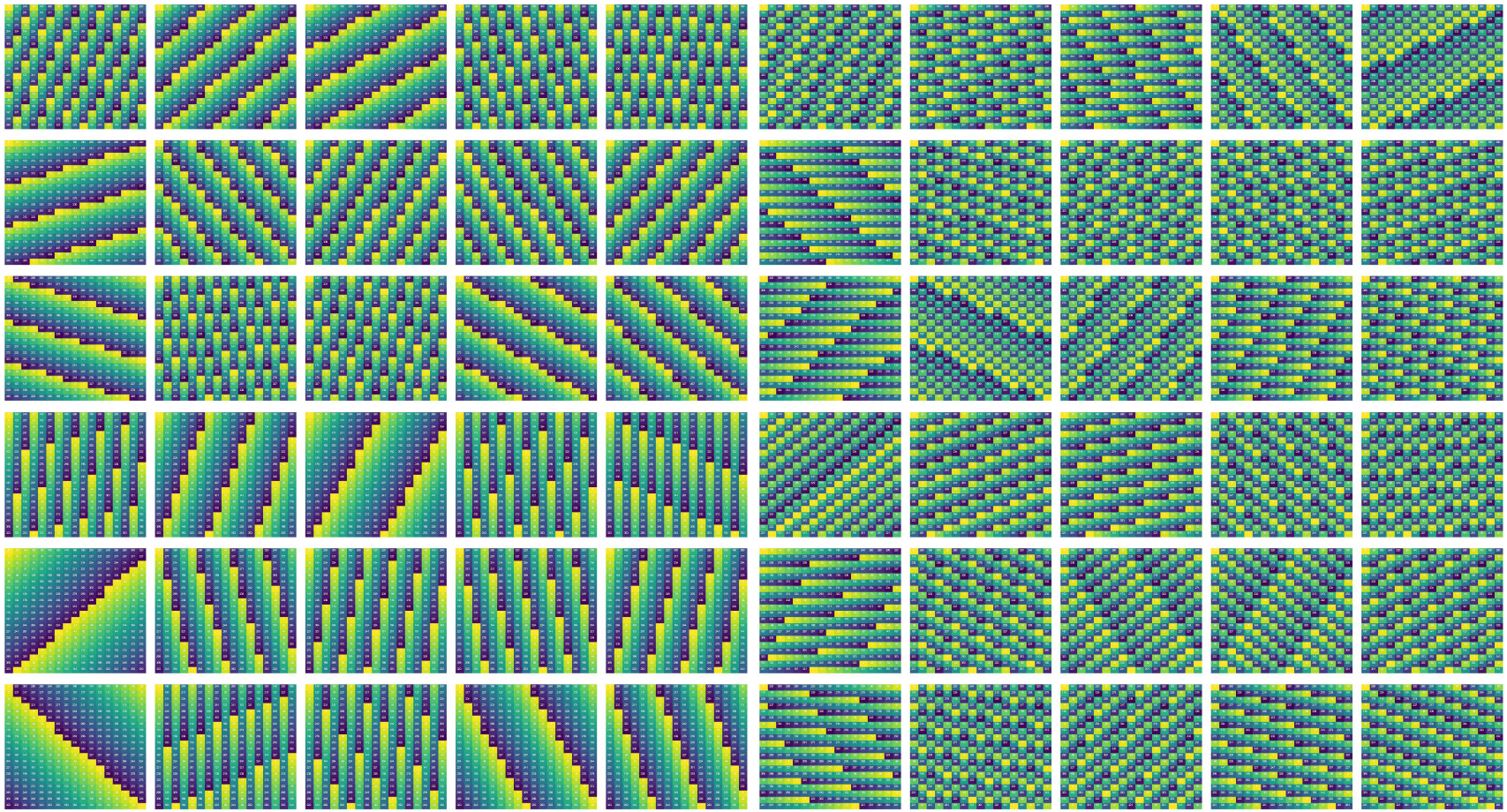
Diagonal transpositions cont.



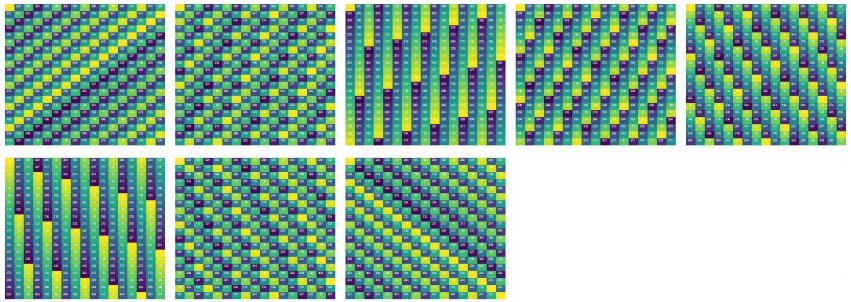
Proper two–dimensional decimations



Proper two–dimensional decimations cont.

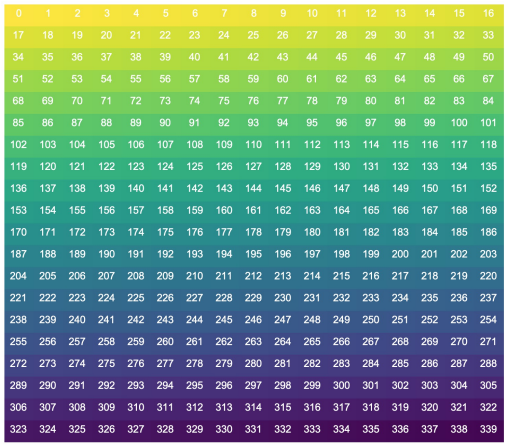


Proper two–dimensional decimations cont.

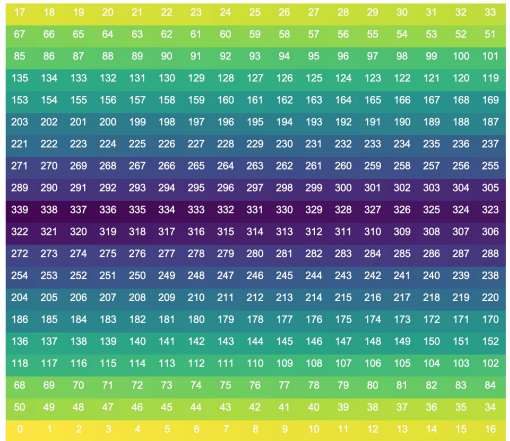


- We tested all row–major, column–major, alternating row–column, alternating column–row, inward spirals, outward spirals, diagonals and proper 2D decimations transpositions.
- This didn't turn up anything that looked like a solution to Z340.
- We then tested all 53 824 pairs of transpositions using `azdecrypt` and `zkdecrypto`. For example

L – R, T – B



L – R, L – R, R – L, R – L, alternating B – T

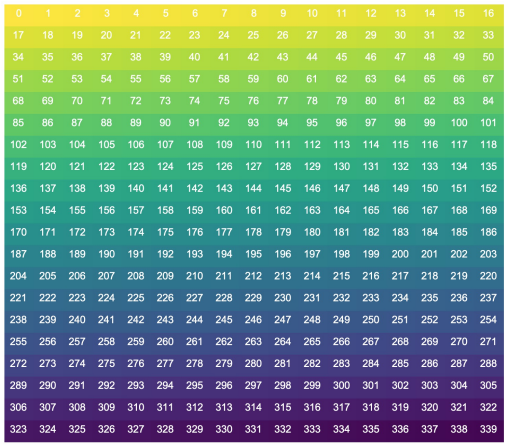


Top left, upper diagonal

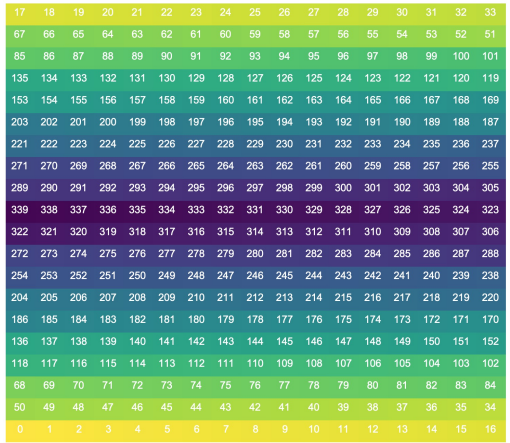
- Once again, this search turned up nothing.

- We tested all row–major, column–major, alternating row–column, alternating column–row, inward spirals, outward spirals, diagonals and proper 2D decimations transpositions.
- This didn't turn up anything that looked like a solution to Z340.
- We then tested all 53 824 pairs of transpositions using `azdecrypt` and `zkdecrypto`. For example

L – R, T – B



L – R, L – R, R – L, R – L, alternating B – T

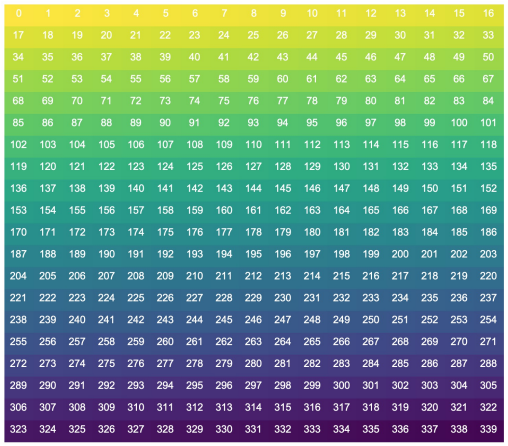


Top left, upper diagonal

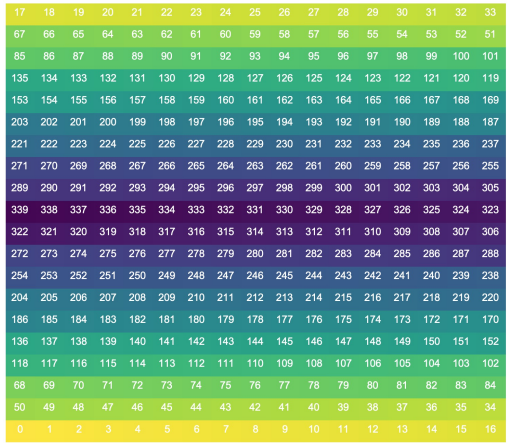
- Once again, this search turned up nothing.

- We tested all row–major, column–major, alternating row–column, alternating column–row, inward spirals, outward spirals, diagonals and proper 2D decimations transpositions.
- This didn't turn up anything that looked like a solution to Z340.
- We then tested all 53 824 pairs of transpositions using `azdecrypt` and `zkdecrypto`. For example

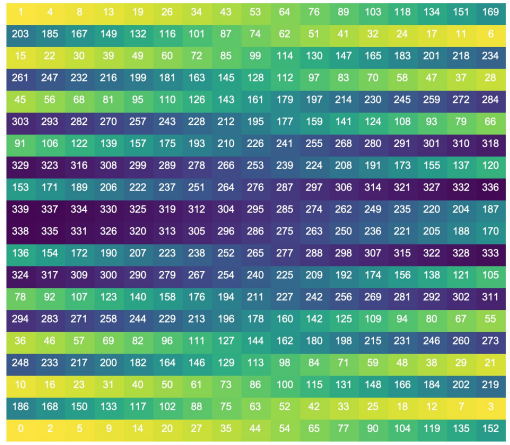
L – R, T – B



L – R, L – R, R – L, R – L, alternating B – T



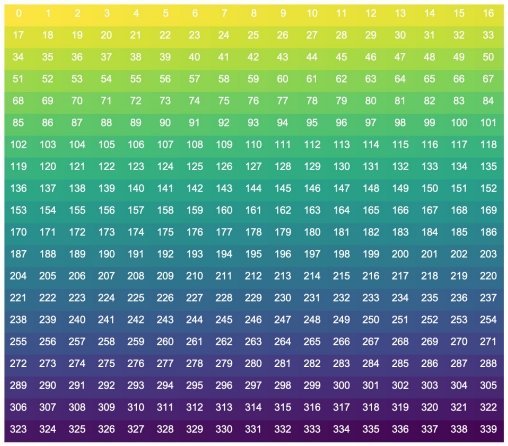
Top left, upper diagonal



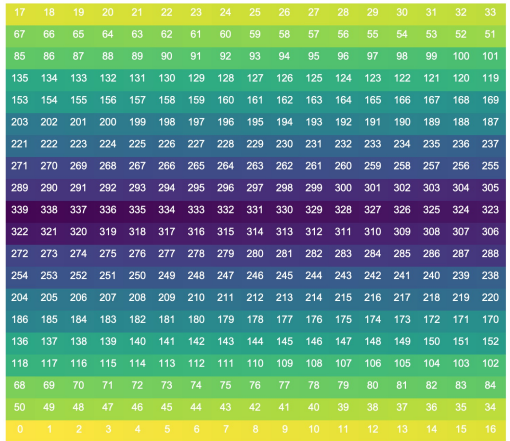
- Once again, this search turned up nothing.

- We tested all row–major, column–major, alternating row–column, alternating column–row, inward spirals, outward spirals, diagonals and proper 2D decimations transpositions.
- This didn't turn up anything that looked like a solution to Z340.
- We then tested all 53 824 pairs of transpositions using `azdecrypt` and `zkdecrypto`. For example

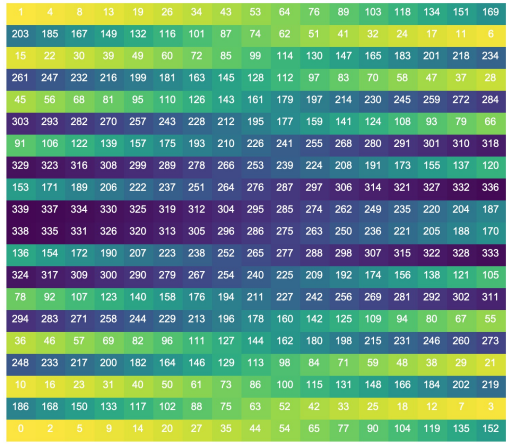
L – R, T – B



L – R, L – R, R – L, R – L, alternating B – T



Top left, upper diagonal



- Once again, this search turned up nothing.

- We then considered testing all 3–tuples of transpositions using `azdecrypt` and `zkdecrypto`.
- However, there are 155 929 364 660 224 such candidates to test.
- Naively checking one a second would take almost 5 million years.
- So we limited our search to proper decimations which seemed reasonable to write out by hand. For example

1,1–decimation

0	120	240	20	140	260	40	160	280	60	180	300	80	200	320	100	220
221	1	121	241	21	141	261	41	161	281	61	181	301	81	201	321	101
102	222	2	122	242	22	142	262	42	162	282	62	182	302	82	202	322
323	103	223	3	123	243	23	143	263	43	163	283	63	183	303	83	203
204	324	104	224	4	124	244	24	144	264	44	164	284	64	184	304	84
85	205	325	105	225	5	125	245	25	145	265	45	165	285	65	185	305
306	86	206	326	106	226	6	126	246	26	146	266	46	166	286	66	186
187	307	87	207	327	107	227	7	127	247	27	147	267	47	167	287	67
68	188	308	88	208	328	108	228	8	128	248	28	148	268	48	168	288
289	69	189	309	89	209	329	109	229	9	129	249	29	149	269	49	169
170	290	70	190	310	90	210	330	110	230	10	130	250	30	150	270	50
51	171	291	71	191	311	91	211	331	111	231	11	131	251	31	151	271
272	52	172	292	72	192	312	92	212	332	112	232	12	132	252	32	152
153	273	53	173	293	73	193	313	93	213	333	113	233	13	133	253	33
34	154	274	54	174	294	74	194	314	94	214	334	114	234	14	134	254
255	35	155	275	55	175	295	75	195	315	95	215	335	115	235	15	135
136	256	36	156	276	56	176	296	76	196	316	96	216	336	116	236	16
17	137	257	37	157	277	57	177	297	77	197	317	97	217	337	117	237
238	18	138	258	38	158	278	58	178	298	78	198	318	98	218	338	118
119	239	19	139	259	39	159	279	59	179	299	79	199	319	99	219	339

13,15–decimation

0	280	220	160	100	40	320	260	200	140	80	20	300	240	180	120	60
17	297	237	177	117	57	337	277	217	157	97	37	317	257	197	137	77
34	314	254	194	134	74	14	294	234	174	114	54	334	274	214	154	94
51	331	271	211	151	91	31	311	251	191	131	71	11	291	231	171	111
68	8	288	228	168	108	48	328	268	208	148	88	28	308	248	188	128
85	25	305	245	185	125	65	5	285	225	165	105	45	325	265	205	145
102	42	322	262	202	142	82	22	302	242	182	122	62	2	282	222	162
119	59	339	279	219	159	99	39	319	259	199	139	79	19	299	239	179
136	76	16	296	236	176	116	56	336	276	216	156	96	36	316	256	196
153	93	33	313	253	193	133	73	13	293	233	173	113	53	333	273	213
170	110	50	330	270	210	150	90	30	310	250	190	130	70	10	290	230
187	127	67	7	287	227	167	107	47	327	267	207	147	87	27	307	247
204	144	84	24	304	244	184	124	64	4	284	224	164	104	44	324	264
221	161	101	41	321	261	201	141	81	21	301	241	181	121	61	1	281
238	178	118	58	338	278	218	158	98	38	318	258	198	138	78	18	298
255	195	135	75	15	295	235	175	115	55	335	275	215	155	95	35	315
272	212	152	92	32	312	252	192	132	72	12	292	232	172	112	52	332
289	229	169	109	49	329	269	209	149	89	29	309	249	189	129	69	9
306	246	186	126	66	6	286	226	166	106	46	326	266	206	146	86	26
323	263	203	143	83	23	303	243	183	123	63	3	283	223	163	103	43

- We further limited the search to candidates with a high bigram count.
- Once again, this search turned up nothing.

- We then considered testing all 3–tuples of transpositions using `azdecrypt` and `zkdecrypto`.
- However, there are 155 929 364 660 224 such candidates to test.
- Naively checking one a second would take almost 5 million years.
- So we limited our search to proper decimations which seemed reasonable to write out by hand. For example

1,1–decimation

0	120	240	20	140	260	40	160	280	60	180	300	80	200	320	100	220
221	1	121	241	21	141	261	41	161	281	61	181	301	81	201	321	101
102	222	2	122	242	22	142	262	42	162	282	62	182	302	82	202	322
323	103	223	3	123	243	23	143	263	43	163	283	63	183	303	83	203
204	324	104	224	4	124	244	24	144	264	44	164	284	64	184	304	84
85	205	325	105	225	5	125	245	25	145	265	45	165	285	65	185	305
306	86	206	326	106	226	6	126	246	26	146	266	46	166	286	66	186
187	307	87	207	327	107	227	7	127	247	27	147	267	47	167	287	67
68	188	308	88	208	328	108	228	8	128	248	28	148	268	48	168	288
289	69	189	309	89	209	329	109	229	9	129	249	29	149	269	49	169
170	290	70	190	310	90	210	330	110	230	10	130	250	30	150	270	50
51	171	291	71	191	311	91	211	331	111	231	11	131	251	31	151	271
272	52	172	292	72	192	312	92	212	332	112	232	12	132	252	32	152
153	273	53	173	293	73	193	313	93	213	333	113	233	13	133	253	33
34	154	274	54	174	294	74	194	314	94	214	334	114	234	14	134	254
255	35	155	275	55	175	295	75	195	315	95	215	335	115	235	15	135
136	256	36	156	276	56	176	296	76	196	316	96	216	336	116	236	16
17	137	257	37	157	277	57	177	297	77	197	317	97	217	337	117	237
238	18	138	258	38	158	278	58	178	298	78	198	318	98	218	338	118
119	239	19	139	259	39	159	279	59	179	299	79	199	319	99	219	339

13,15–decimation

0	280	220	160	100	40	320	260	200	140	80	20	300	240	180	120	60
17	297	237	177	117	57	337	277	217	157	97	37	317	257	197	137	77
34	314	254	194	134	74	14	294	234	174	114	54	334	274	214	154	94
51	331	271	211	151	91	31	311	251	191	131	71	11	291	231	171	111
68	8	288	228	168	108	48	328	268	208	148	88	28	308	248	188	128
85	25	305	245	185	125	65	5	285	225	165	105	45	325	265	205	145
102	42	322	262	202	142	82	22	302	242	182	122	62	2	282	222	162
119	59	339	279	219	159	99	39	319	259	199	139	79	19	299	239	179
136	76	16	296	236	176	116	56	336	276	216	156	96	36	316	256	196
153	93	33	313	253	193	133	73	13	293	233	173	113	53	333	273	213
170	110	50	330	270	210	150	90	30	310	250	190	130	70	10	290	230
187	127	67	7	287	227	167	107	47	327	267	207	147	87	27	307	247
204	144	84	24	304	244	184	124	64	4	284	224	164	104	44	324	264
221	161	101	41	321	261	201	141	81	21	301	241	181	121	61	1	281
238	178	118	58	338	278	218	158	98	38	318	258	198	138	78	18	298
255	195	135	75	15	295	235	175	115	55	335	275	215	155	95	35	315
272	212	152	92	32	312	252	192	132	72	12	292	232	172	112	52	332
289	229	169	109	49	329	269	209	149	89	29	309	249	189	129	69	9
306	246	186	126	66	6	286	226	166	106	46	326	266	206	146	86	26
323	263	203	143	83	23	303	243	183	123	63	3	283	223	163	103	43

- We further limited the search to candidates with a high bigram count.
- Once again, this search turned up nothing.

- We then considered testing all 3–tuples of transpositions using `azdecrypt` and `zkdecrypto`.
- However, there are 155 929 364 660 224 such candidates to test.
- Naively checking one a second would take almost 5 million years.
- So we limited our search to proper decimations which seemed reasonable to write out by hand. For example

1,1–decimation

0	120	240	20	140	260	40	160	280	60	180	300	80	200	320	100	220
221	1	121	241	21	141	261	41	161	281	61	181	301	81	201	321	101
102	222	2	122	242	22	142	262	42	162	282	62	182	302	82	202	322
323	103	223	3	123	243	23	143	263	43	163	283	63	183	303	83	203
204	324	104	224	4	124	244	24	144	264	44	164	284	64	184	304	84
85	205	325	105	225	5	125	245	25	145	265	45	165	285	65	185	305
306	86	206	326	106	226	6	126	246	26	146	266	46	166	286	66	186
187	307	87	207	327	107	227	7	127	247	27	147	267	47	167	287	67
68	188	308	88	208	328	108	228	8	128	248	28	148	268	48	168	288
289	69	189	309	89	209	329	109	229	9	129	249	29	149	269	49	169
170	290	70	190	310	90	210	330	110	230	10	130	250	30	150	270	50
51	171	291	71	191	311	91	211	331	111	231	11	131	251	31	151	271
272	52	172	292	72	192	312	92	212	332	112	232	12	132	252	32	152
153	273	53	173	293	73	193	313	93	213	333	113	233	13	133	253	33
34	154	274	54	174	294	74	194	314	94	214	334	114	234	14	134	254
255	35	155	275	55	175	295	75	195	315	95	215	335	115	235	15	135
136	256	36	156	276	56	176	296	76	196	316	96	216	336	116	236	16
17	137	257	37	157	277	57	177	297	77	197	317	97	217	337	117	237
238	18	138	258	38	158	278	58	178	298	78	198	318	98	218	338	118
119	239	19	139	259	39	159	279	59	179	299	79	199	319	99	219	339

13,15–decimation

0	280	220	160	100	40	320	260	200	140	80	20	300	240	180	120	60
17	297	237	177	117	57	337	277	217	157	97	37	317	257	197	137	77
34	314	254	194	134	74	14	294	234	174	114	54	334	274	214	154	94
51	331	271	211	151	91	31	311	251	191	131	71	11	291	231	171	111
68	8	288	228	168	108	48	328	268	208	148	88	28	308	248	188	128
85	25	305	245	185	125	65	5	285	225	165	105	45	325	265	205	145
102	42	322	262	202	142	82	22	302	242	182	122	62	2	282	222	162
119	59	339	279	219	159	99	39	319	259	199	139	79	19	299	239	179
136	76	16	296	236	176	116	56	336	276	216	156	96	36	316	256	196
153	93	33	313	253	193	133	73	13	293	233	173	113	53	333	273	213
170	110	50	330	270	210	150	90	30	310	250	190	130	70	10	290	230
187	127	67	7	287	227	167	107	47	327	267	207	147	87	27	307	247
204	144	84	24	304	244	184	124	64	4	284	224	164	104	44	324	264
221	161	101	41	321	261	201	141	81	21	301	241	181	121	61	1	281
238	178	118	58	338	278	218	158	98	38	318	258	198	138	78	18	298
255	195	135	75	15	295	235	175	115	55	335	275	215	155	95	35	315
272	212	152	92	32	312	252	192	132	72	12	292	232	172	112	52	332
289	229	169	109	49	329	269	209	149	89	29	309	249	189	129	69	9
306	246	186	126	66	6	286	226	166	106	46	326	266	206	146	86	26
323	263	203	143	83	23	303	243	183	123	63	3	283	223	163	103	43

- We further limited the search to candidates with a high bigram count.
- Once again, this search turned up nothing.

- We then considered testing all 3–tuples of transpositions using `azdecrypt` and `zkdecrypto`.
- However, there are 155 929 364 660 224 such candidates to test.
- Naively checking one a second would take almost 5 million years.
- So we limited our search to proper decimations which seemed reasonable to write out by hand. For example

1,1–decimation

0	120	240	20	140	260	40	160	280	60	180	300	80	200	320	100	220
221	1	121	241	21	141	261	41	161	281	61	181	301	81	201	321	101
102	222	2	122	242	22	142	262	42	162	282	62	182	302	82	202	322
323	103	223	3	123	243	23	143	263	43	163	283	63	183	303	83	203
204	324	104	224	4	124	244	24	144	264	44	164	284	64	184	304	84
85	205	325	105	225	5	125	245	25	145	265	45	165	285	65	185	305
306	86	206	326	106	226	6	126	246	26	146	266	46	166	286	66	186
187	307	87	207	327	107	227	7	127	247	27	147	267	47	167	287	67
68	188	308	88	208	328	108	228	8	128	248	28	148	268	48	168	288
289	69	189	309	89	209	329	109	229	9	129	249	29	149	269	49	169
170	290	70	190	310	90	210	330	110	230	10	130	250	30	150	270	50
51	171	291	71	191	311	91	211	331	111	231	11	131	251	31	151	271
272	52	172	292	72	192	312	92	212	332	112	232	12	132	252	32	152
153	273	53	173	293	73	193	313	93	213	333	113	233	13	133	253	33
34	154	274	54	174	294	74	194	314	94	214	334	114	234	14	134	254
255	35	155	275	55	175	295	75	195	315	95	215	335	115	235	15	135
136	256	36	156	276	56	176	296	76	196	316	96	216	336	116	236	16
17	137	257	37	157	277	57	177	297	77	197	317	97	217	337	117	237
238	18	138	258	38	158	278	58	178	298	78	198	318	98	218	338	118
119	239	19	139	259	39	159	279	59	179	299	79	199	319	99	219	339

13,15–decimation

0	280	220	160	100	40	320	260	200	140	80	20	300	240	180	120	60
17	297	237	177	117	57	337	277	217	157	97	37	317	257	197	137	77
34	314	254	194	134	74	14	294	234	174	114	54	334	274	214	154	94
51	331	271	211	151	91	31	311	251	191	131	71	11	291	231	171	111
68	8	288	228	168	108	48	328	268	208	148	88	28	308	248	188	128
85	25	305	245	185	125	65	5	285	225	165	105	45	325	265	205	145
102	42	322	262	202	142	82	22	302	242	182	122	62	2	282	222	162
119	59	339	279	219	159	99	39	319	259	199	139	79	19	299	239	179
136	76	16	296	236	176	116	56	336	276	216	156	96	36	316	256	196
153	93	33	313	253	193	133	73	13	293	233	173	113	53	333	273	213
170	110	50	330	270	210	150	90	30	310	250	190	130	70	10	290	230
187	127	67	7	287	227	167	107	47	327	267	207	147	87	27	307	247
204	144	84	24	304	244	184	124	64	4	284	224	164	104	44	324	264
221	161	101	41	321	261	201	141	81	21	301	241	181	121	61	1	281
238	178	118	58	338	278	218	158	98	38	318	258	198	138	78	18	298
255	195	135	75	15	295	235	175	115	55	335	275	215	155	95	35	315
272	212	152	92	32	312	252	192	132	72	12	292	232	172	112	52	332
289	229	169	109	49	329	269	209	149	89	29	309	249	189	129	69	9
306	246	186	126	66	6	286	226	166	106	46	326	266	206	146	86	26
323	263	203	143	83	23	303	243	183	123	63	3	283	223	163	103	43

- We further limited the search to candidates with a high bigram count.
- Once again, this search turned up nothing.

- We then considered testing all 3–tuples of transpositions using `azdecrypt` and `zkdecrypto`.
- However, there are 155 929 364 660 224 such candidates to test.
- Naively checking one a second would take almost 5 million years.
- So we limited our search to proper decimations which seemed reasonable to write out by hand. For example

1,1–decimation

0	120	240	20	140	260	40	160	280	60	180	300	80	200	320	100	220
221	1	121	241	21	141	261	41	161	281	61	181	301	81	201	321	101
102	222	2	122	242	22	142	262	42	162	282	62	182	302	82	202	322
323	103	223	3	123	243	23	143	263	43	163	283	63	183	303	83	203
204	324	104	224	4	124	244	24	144	264	44	164	284	64	184	304	84
85	205	325	105	225	5	125	245	25	145	265	45	165	285	65	185	305
306	86	206	326	106	226	6	126	246	26	146	266	46	166	286	66	186
187	307	87	207	327	107	227	7	127	247	27	147	267	47	167	287	67
68	188	308	88	208	328	108	228	8	128	248	28	148	268	48	168	288
289	69	189	309	89	209	329	109	229	9	129	249	29	149	269	49	169
170	290	70	190	310	90	210	330	110	230	10	130	250	30	150	270	50
51	171	291	71	191	311	91	211	331	111	231	11	131	251	31	151	271
272	52	172	292	72	192	312	92	212	332	112	232	12	132	252	32	152
153	273	53	173	293	73	193	313	93	213	333	113	233	13	133	253	33
34	154	274	54	174	294	74	194	314	94	214	334	114	234	14	134	254
255	35	155	275	55	175	295	75	195	315	95	215	335	115	235	15	135
136	256	36	156	276	56	176	296	76	196	316	96	216	336	116	236	16
17	137	257	37	157	277	57	177	297	77	197	317	97	217	337	117	237
238	18	138	258	38	158	278	58	178	298	78	198	318	98	218	338	118
119	239	19	139	259	39	159	279	59	179	299	79	199	319	99	219	339

13,15–decimation

0	280	220	160	100	40	320	260	200	140	80	20	300	240	180	120	60
17	297	237	177	117	57	337	277	217	157	97	37	317	257	197	137	77
34	314	254	194	134	74	14	294	234	174	114	54	334	274	214	154	94
51	331	271	211	151	91	31	311	251	191	131	71	11	291	231	171	111
68	8	288	228	168	108	48	328	268	208	148	88	28	308	248	188	128
85	25	305	245	185	125	65	5	285	225	165	105	45	325	265	205	145
102	42	322	262	202	142	82	22	302	242	182	122	62	2	282	222	162
119	59	339	279	219	159	99	39	319	259	199	139	79	19	299	239	179
136	76	16	296	236	176	116	56	336	276	216	156	96	36	316	256	196
153	93	33	313	253	193	133	73	13	293	233	173	113	53	333	273	213
170	110	50	330	270	210	150	90	30	310	250	190	130	70	10	290	230
187	127	67	7	287	227	167	107	47	327	267	207	147	87	27	307	247
204	144	84	24	304	244	184	124	64	4	284	224	164	104	44	324	264
221	161	101	41	321	261	201	141	81	21	301	241	181	121	61	1	281
238	178	118	58	338	278	218	158	98	38	318	258	198	138	78	18	298
255	195	135	75	15	295	235	175	115	55	335	275	215	155	95	35	315
272	212	152	92	32	312	252	192	132	72	12	292	232	172	112	52	332
289	229	169	109	49	329	269	209	149	89	29	309	249	189	129	69	9
306	246	186	126	66	6	286	226	166	106	46	326	266	206	146	86	26
323	263	203	143	83	23	303	243	183	123	63	3	283	223	163	103	43

- We further limited the search to candidates with a high bigram count.
- Once again, this search turned up nothing.

- We then considered testing all 3–tuples of transpositions using `azdecrypt` and `zkdecrypto`.
- However, there are 155 929 364 660 224 such candidates to test.
- Naively checking one a second would take almost 5 million years.
- So we limited our search to proper decimations which seemed reasonable to write out by hand. For example

1,1–decimation

0	120	240	20	140	260	40	160	280	60	180	300	80	200	320	100	220
221	1	121	241	21	141	261	41	161	281	61	181	301	81	201	321	101
102	222	2	122	242	22	142	262	42	162	282	62	182	302	82	202	322
323	103	223	3	123	243	23	143	263	43	163	283	63	183	303	83	203
204	324	104	224	4	124	244	24	144	264	44	164	284	64	184	304	84
85	205	325	105	225	5	125	245	25	145	265	45	165	285	65	185	305
306	86	206	326	106	226	6	126	246	26	146	266	46	166	286	66	186
187	307	87	207	327	107	227	7	127	247	27	147	267	47	167	287	67
68	188	308	88	208	328	108	228	8	128	248	28	148	268	48	168	288
289	69	189	309	89	209	329	109	229	9	129	249	29	149	269	49	169
170	290	70	190	310	90	210	330	110	230	10	130	250	30	150	270	50
51	171	291	71	191	311	91	211	331	111	231	11	131	251	31	151	271
272	52	172	292	72	192	312	92	212	332	112	232	12	132	252	32	152
153	273	53	173	293	73	193	313	93	213	333	113	233	13	133	253	33
34	154	274	54	174	294	74	194	314	94	214	334	114	234	14	134	254
255	35	155	275	55	175	295	75	195	315	95	215	335	115	235	15	135
136	256	36	156	276	56	176	296	76	196	316	96	216	336	116	236	16
17	137	257	37	157	277	57	177	297	77	197	317	97	217	337	117	237
238	18	138	258	38	158	278	58	178	298	78	198	318	98	218	338	118
119	239	19	139	259	39	159	279	59	179	299	79	199	319	99	219	339

13,15–decimation

0	280	220	160	100	40	320	260	200	140	80	20	300	240	180	120	60
17	297	237	177	117	57	337	277	217	157	97	37	317	257	197	137	77
34	314	254	194	134	74	14	294	234	174	114	54	334	274	214	154	94
51	331	271	211	151	91	31	311	251	191	131	71	11	291	231	171	111
68	8	288	228	168	108	48	328	268	208	148	88	28	308	248	188	128
85	25	305	245	185	125	65	5	285	225	165	105	45	325	265	205	145
102	42	322	262	202	142	82	22	302	242	182	122	62	2	282	222	162
119	59	339	279	219	159	99	39	319	259	199	139	79	19	299	239	179
136	76	16	296	236	176	116	56	336	276	216	156	96	36	316	256	196
153	93	33	313	253	193	133	73	13	293	233	173	113	53	333	273	213
170	110	50	330	270	210	150	90	30	310	250	190	130	70	10	290	230
187	127	67	7	287	227	167	107	47	327	267	207	147	87	27	307	247
204	144	84	24	304	244	184	124	64	4	284	224	164	104	44	324	264
221	161	101	41	321	261	201	141	81	21	301	241	181	121	61	1	281
238	178	118	58	338	278	218	158	98	38	318	258	198	138	78	18	298
255	195	135	75	15	295	235	175	115	55	335	275	215	155	95	35	315
272	212	152	92	32	312	252	192	132	72	12	292	232	172	112	52	332
289	229	169	109	49	329	269	209	149	89	29	309	249	189	129	69	9
306	246	186	126	66	6	286	226	166	106	46	326	266	206	146	86	26
323	263	203	143	83	23	303	243	183	123	63	3	283	223	163	103	43

- We further limited the search to candidates with a high bigram count.
- Once again, this search turned up nothing.

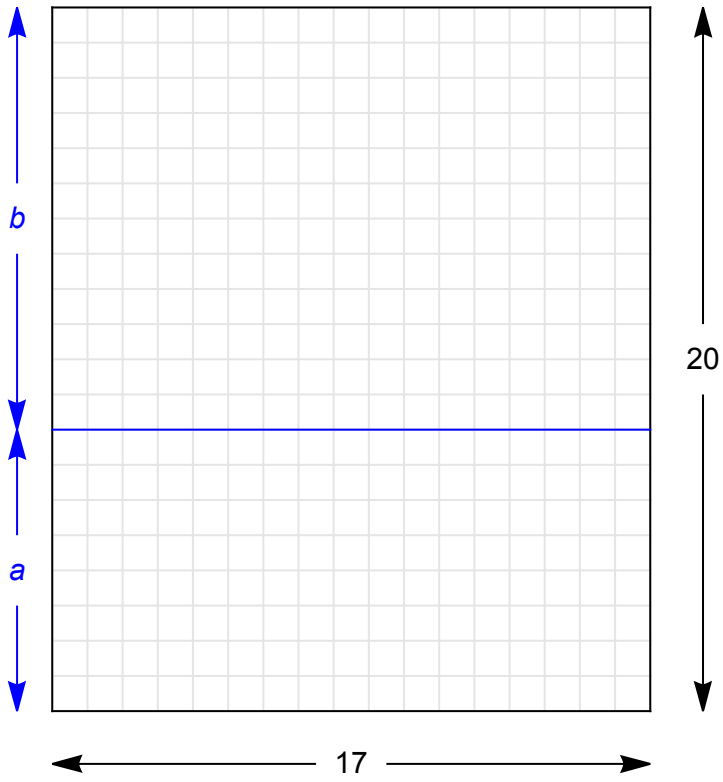
- Our experiments suggested that a composition of a transposition and a homophonic substitution does not solve Z340.
- Perhaps there's another step we are missing?
- We experimented with splitting the cipher into two or more sections prior to applying the transposition.
- For each section of each candidate cipher, we applied all the aforementioned transpositions.
- This would be followed by applying all combinations of all these transpositions to each section of each cipher.

- Our experiments suggested that a composition of a transposition and a homophonic substitution does not solve Z340.
- Perhaps there's another step we are missing?
- We experimented with splitting the cipher into two or more sections prior to applying the transposition.
- For each section of each candidate cipher, we applied all the aforementioned transpositions.
- This would be followed by applying all combinations of all these transpositions to each section of each cipher.

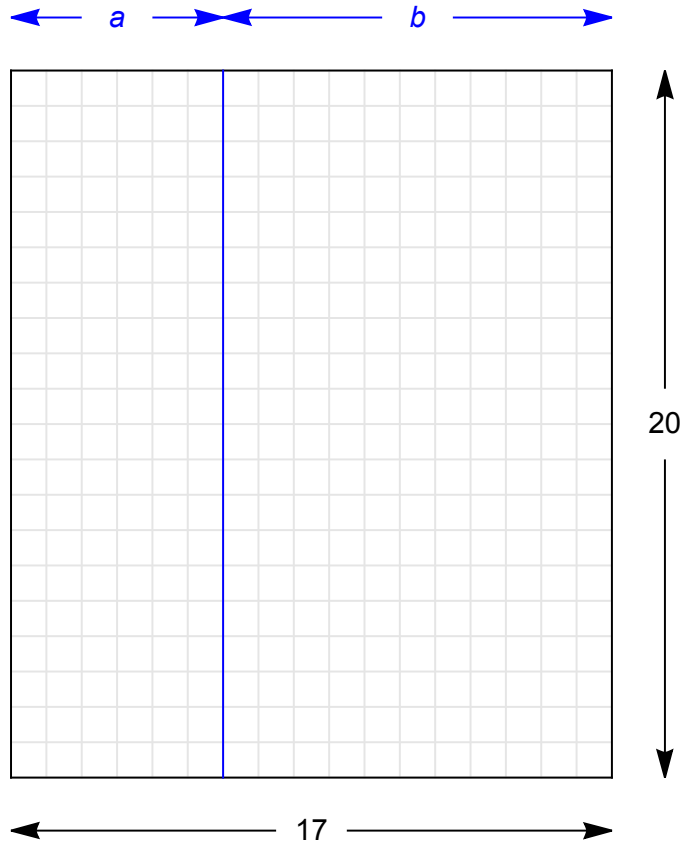
- Our experiments suggested that a composition of a transposition and a homophonic substitution does not solve Z340.
- Perhaps there's another step we are missing?
- We experimented with splitting the cipher into two or more sections prior to applying the transposition.
- For each section of each candidate cipher, we applied all the aforementioned transpositions.
- This would be followed by applying all combinations of all these transpositions to each section of each cipher.

- Our experiments suggested that a composition of a transposition and a homophonic substitution does not solve Z340.
- Perhaps there's another step we are missing?
- We experimented with splitting the cipher into two or more sections prior to applying the transposition.
- For each section of each candidate cipher, we applied all the aforementioned transpositions.
- This would be followed by applying all combinations of all these transpositions to each section of each cipher.

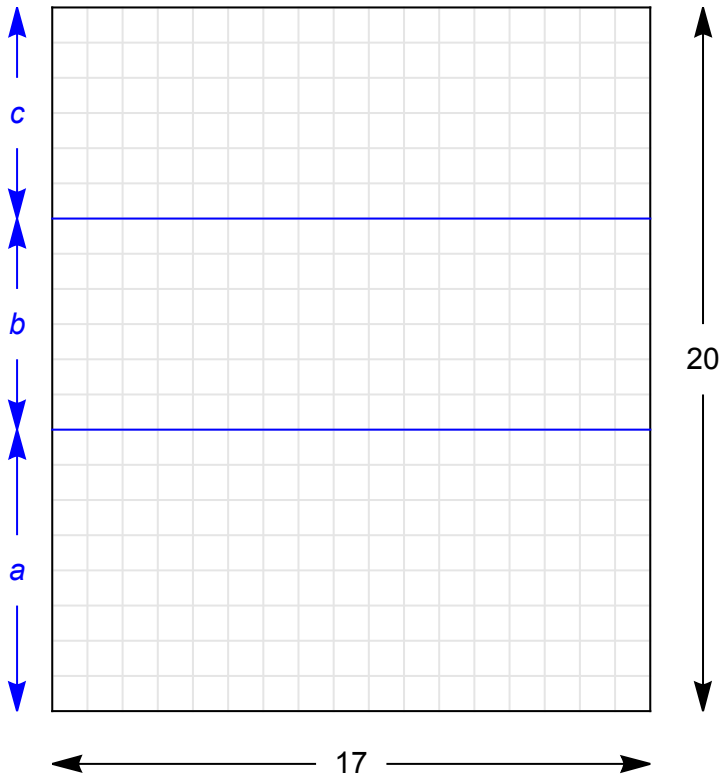
2 vertical sections



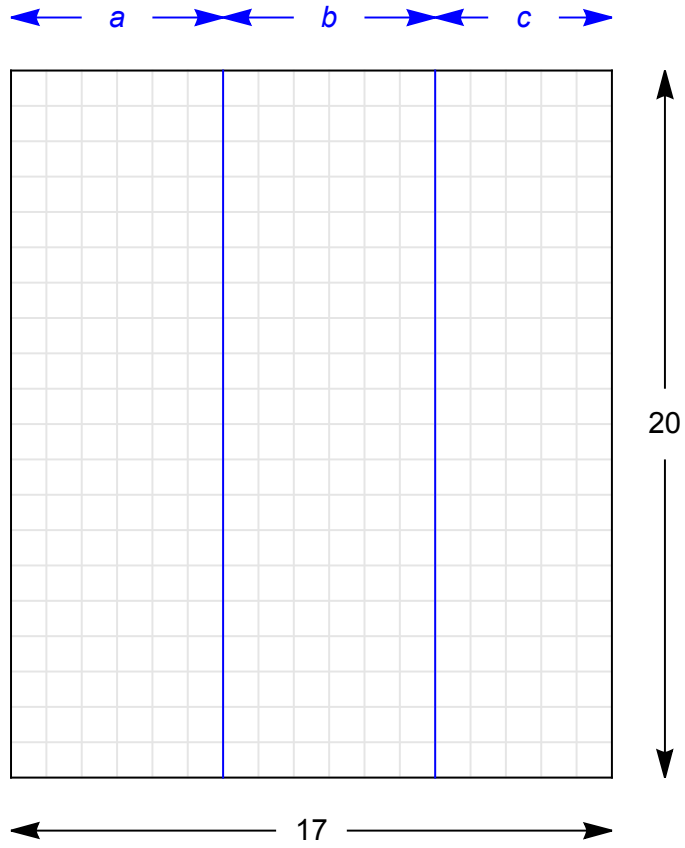
2 horizontal sections



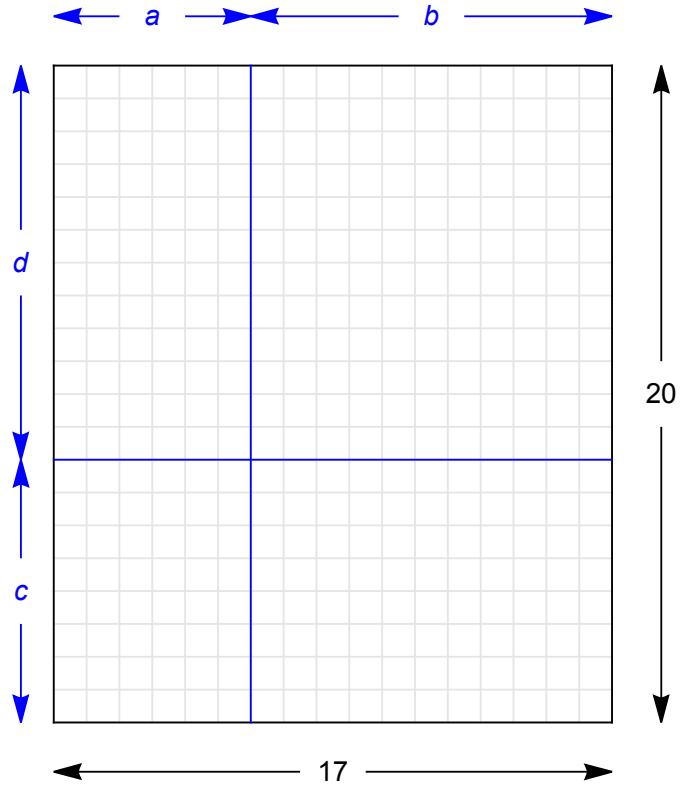
3 vertical sections



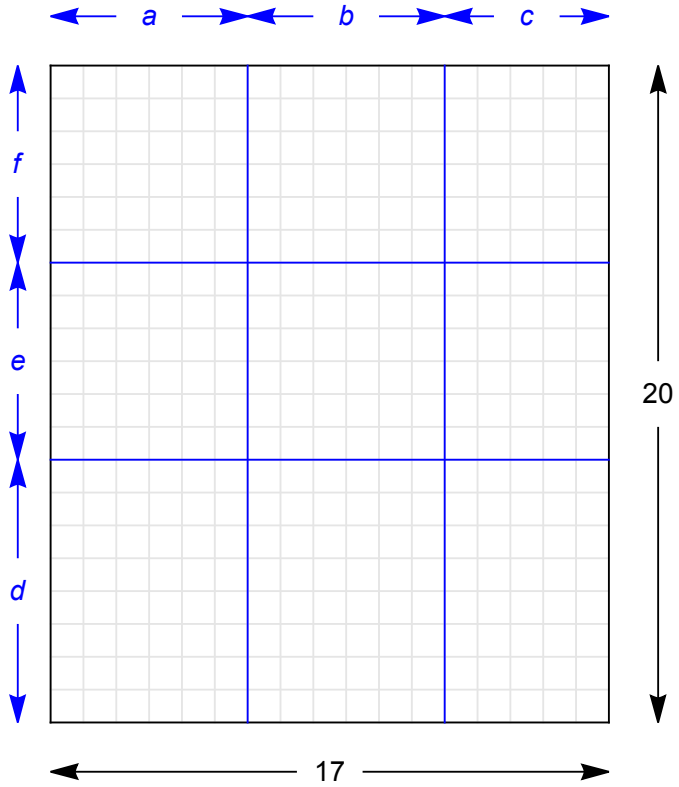
3 horizontal sections



2 horizontal & 2 vertical sections



3 horizontal & 3 vertical sections



Large–Scale Experiments on the Z340

Splitting the cipher + transposition + homophonic substitution

- Given the high bigram count of the 1,2–decimation transposition, we started our search with 2D decimations.
- We started our search with each segment having the same (single) transposition.
- For example, on the right is a split 3 vertical segments of sizes 7, 8 and 5 and a 3,3–decimation.

0	91	63	35	7	98	70	42	14	105	77	49	21	112	84	56	28
68	40	12	103	75	47	19	110	82	54	26	117	89	61	33	5	96
17	108	80	52	24	115	87	59	31	3	94	66	38	10	101	73	45
85	57	29	1	92	64	36	8	99	71	43	15	106	78	50	22	113
34	6	97	69	41	13	104	76	48	20	111	83	55	27	118	90	62
102	74	46	18	109	81	53	25	116	88	60	32	4	95	67	39	11
51	23	114	86	58	30	2	93	65	37	9	100	72	44	16	107	79

119	159	199	239	143	183	223	127	167	207	247	151	191	231	135	175	215
170	210	250	154	194	234	138	178	218	122	162	202	242	146	186	226	130
221	125	165	205	245	149	189	229	133	173	213	253	157	197	237	141	181
136	176	216	120	160	200	240	144	184	224	128	168	208	248	152	192	232
187	227	131	171	211	251	155	195	235	139	179	219	123	163	203	243	147
238	142	182	222	126	166	206	246	150	190	230	134	174	214	254	158	198
153	193	233	137	177	217	121	161	201	241	145	185	225	129	169	209	249
204	244	148	188	228	132	172	212	252	156	196	236	140	180	220	124	164

255	295	335	290	330	285	325	280	320	275	315	270	310	265	305	260	300
272	312	267	307	262	302	257	297	337	292	332	287	327	282	322	277	317
289	329	284	324	279	319	274	314	269	309	264	304	259	299	339	294	334
306	261	301	256	296	336	291	331	286	326	281	321	276	316	271	311	266
323	278	318	273	313	268	308	263	303	258	298	338	293	333	288	328	283

Large–Scale Experiments on the Z340

Splitting the cipher + transposition + homophonic substitution

- Given the high bigram count of the 1,2–decimation transposition, we started our search with 2D decimations.
- We started our search with each segment having the same (single) transposition.
- For example, on the right is a split 3 vertical segments of sizes 7, 8 and 5 and a 3,3–decimation.

0	91	63	35	7	98	70	42	14	105	77	49	21	112	84	56	28
68	40	12	103	75	47	19	110	82	54	26	117	89	61	33	5	96
17	108	80	52	24	115	87	59	31	3	94	66	38	10	101	73	45
85	57	29	1	92	64	36	8	99	71	43	15	106	78	50	22	113
34	6	97	69	41	13	104	76	48	20	111	83	55	27	118	90	62
102	74	46	18	109	81	53	25	116	88	60	32	4	95	67	39	11
51	23	114	86	58	30	2	93	65	37	9	100	72	44	16	107	79

119	159	199	239	143	183	223	127	167	207	247	151	191	231	135	175	215
170	210	250	154	194	234	138	178	218	122	162	202	242	146	186	226	130
221	125	165	205	245	149	189	229	133	173	213	253	157	197	237	141	181
136	176	216	120	160	200	240	144	184	224	128	168	208	248	152	192	232
187	227	131	171	211	251	155	195	235	139	179	219	123	163	203	243	147
238	142	182	222	126	166	206	246	150	190	230	134	174	214	254	158	198
153	193	233	137	177	217	121	161	201	241	145	185	225	129	169	209	249
204	244	148	188	228	132	172	212	252	156	196	236	140	180	220	124	164

255	295	335	290	330	285	325	280	320	275	315	270	310	265	305	260	300
272	312	267	307	262	302	257	297	337	292	332	287	327	282	322	277	317
289	329	284	324	279	319	274	314	269	309	264	304	259	299	339	294	334
306	261	301	256	296	336	291	331	286	326	281	321	276	316	271	311	266
323	278	318	273	313	268	308	263	303	258	298	338	293	333	288	328	283

Large–Scale Experiments on the Z340

Splitting the cipher + transposition + homophonic substitution

- Given the high bigram count of the 1,2–decimation transposition, we started our search with 2D decimations.
- We started our search with each segment having the same (single) transposition.
- For example, on the right is a split 3 vertical segments of sizes 7, 8 and 5 and a 3,3–decimation.

0	91	63	35	7	98	70	42	14	105	77	49	21	112	84	56	28
68	40	12	103	75	47	19	110	82	54	26	117	89	61	33	5	96
17	108	80	52	24	115	87	59	31	3	94	66	38	10	101	73	45
85	57	29	1	92	64	36	8	99	71	43	15	106	78	50	22	113
34	6	97	69	41	13	104	76	48	20	111	83	55	27	118	90	62
102	74	46	18	109	81	53	25	116	88	60	32	4	95	67	39	11
51	23	114	86	58	30	2	93	65	37	9	100	72	44	16	107	79

119	159	199	239	143	183	223	127	167	207	247	151	191	231	135	175	215
170	210	250	154	194	234	138	178	218	122	162	202	242	146	186	226	130
221	125	165	205	245	149	189	229	133	173	213	253	157	197	237	141	181
136	176	216	120	160	200	240	144	184	224	128	168	208	248	152	192	232
187	227	131	171	211	251	155	195	235	139	179	219	123	163	203	243	147
238	142	182	222	126	166	206	246	150	190	230	134	174	214	254	158	198
153	193	233	137	177	217	121	161	201	241	145	185	225	129	169	209	249
204	244	148	188	228	132	172	212	252	156	196	236	140	180	220	124	164

255	295	335	290	330	285	325	280	320	275	315	270	310	265	305	260	300
272	312	267	307	262	302	257	297	337	292	332	287	327	282	322	277	317
289	329	284	324	279	319	274	314	269	309	264	304	259	299	339	294	334
306	261	301	256	296	336	291	331	286	326	281	321	276	316	271	311	266
323	278	318	273	313	268	308	263	303	258	298	338	293	333	288	328	283

Large–Scale Experiments on the Z340

Splitting the cipher + transposition + homophonic substitution

- We ran all proper 2D decimation transpositions for all splits.
- As we had seen so many times, this experiment didn't turn up anything.
- The next search for compositions of multiple transpositions and all combinations of transpositions for all sections would be a significantly larger undertaking.
- So we decided to re-analyse the results from the initial search.

Large–Scale Experiments on the Z340

Splitting the cipher + transposition + homophonic substitution

- We ran all proper 2D decimation transpositions for all splits.
- As we had seen so many times, this experiment didn't turn up anything.
- The next search for compositions of multiple transpositions and all combinations of transpositions for all sections would be a significantly larger undertaking.
- So we decided to re-analyse the results from the initial search.

- We ran all proper 2D decimation transpositions for all splits.
- As we had seen so many times, this experiment didn't turn up anything.
- The next search for compositions of multiple transpositions and all combinations of transpositions for all sections would be a significantly larger undertaking.
- So we decided to re-analyse the results from the initial search.

- We ran all proper 2D decimation transpositions for all splits.
- As we had seen so many times, this experiment didn't turn up anything.
- The next search for compositions of multiple transpositions and all combinations of transpositions for all sections would be a significantly larger undertaking.
- So we decided to re-analyse the results from the initial search.

The Breakthrough

Around 4am on Friday, December 4–th 2020 (AEDST), David found the following result in the sea of noise–like results from `azdecrypt` and `zkdecrypto`. In particular, the phrases `... HOPE YOU ARE ... TRYING TO CATCH ME ... GAS CHAMBER ...` stood out.

Friday, December 4th

David Oranchak 4:04 AM

@Sam Blake ok, this one stood out

length_340_diagonal-variations/vertical_3split_decimations/z340_vertical_3split_decimations_9_9_1_19_2.txt

E**HOPE YOU ARE** HE SING IST TORRA ENN **TRYING**
TO CATCH METH AFTAINT MT ON THE TS **SHOT WHICH**
BRINGS UP ALS IN TABS IT ME NAME OF AR HEED
OR THE GAS CHAMBER BECA ATE IT WILD VENT
ME ROLER A DICE AI I THE VS SHEN BECAUSE
TOO WHA SEEN TIGHT DESERTS WORS ROS ME THERE
EVERYONEED **HE HAS NOTHING THEN THEY** HE ACH
PARADICT IS THEY ALREARE AND NORDER THER
AMEO EARRE AND BECAUITE IS YOT TV HAT MR
NEWE ITLE NEVER IND BAEYN NEIA AT A HOE CDR
PET (edited)

can you describe the steps in that one?

The Breakthrough

- It goes without saying that I was shocked!

- This candidate was split into three vertical sections of lengths 9, 9 and 2.
- The transposition for each section was a 1,2–decimation.

0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144
136	145	1	10	19	28	37	46	55	64	73	82	91	100	109	118	127
119	128	137	146	2	11	20	29	38	47	56	65	74	83	92	101	110
102	111	120	129	138	147	3	12	21	30	39	48	57	66	75	84	93
85	94	103	112	121	130	139	148	4	13	22	31	40	49	58	67	76
68	77	86	95	104	113	122	131	140	149	5	14	23	32	41	50	59
51	60	69	78	87	96	105	114	123	132	141	150	6	15	24	33	42
34	43	52	61	70	79	88	97	106	115	124	133	142	151	7	16	25
17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	8

153	162	171	180	189	198	207	216	225	234	243	252	261	270	279	288	297
289	298	154	163	172	181	190	199	208	217	226	235	244	253	262	271	280
272	281	290	299	155	164	173	182	191	200	209	218	227	236	245	254	263
255	264	273	282	291	300	156	165	174	183	192	201	210	219	228	237	246
238	247	256	265	274	283	292	301	157	166	175	184	193	202	211	220	229
221	230	239	248	257	266	275	284	293	302	158	167	176	185	194	203	212
204	213	222	231	240	249	258	267	276	285	294	303	159	168	177	186	195
187	196	205	214	223	232	241	250	259	268	277	286	295	304	160	169	178
170	179	188	197	206	215	224	233	242	251	260	269	278	287	296	305	161

306	332	324	316	308	334	326	318	310	336	328	320	312	338	330	322	314
323	315	307	333	325	317	309	335	327	319	311	337	329	321	313	339	331

The Breakthrough

- It goes without saying that I was shocked!

Sam Blake 11:26 AM

Holy shit - that one does stand out!

- This candidate was split into three vertical sections of lengths 9, 9 and 2.
- The transposition for each section was a 1,2–decimation.

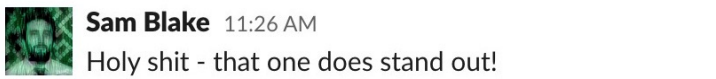
0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144
136	145	1	10	19	28	37	46	55	64	73	82	91	100	109	118	127
119	128	137	146	2	11	20	29	38	47	56	65	74	83	92	101	110
102	111	120	129	138	147	3	12	21	30	39	48	57	66	75	84	93
85	94	103	112	121	130	139	148	4	13	22	31	40	49	58	67	76
68	77	86	95	104	113	122	131	140	149	5	14	23	32	41	50	59
51	60	69	78	87	96	105	114	123	132	141	150	6	15	24	33	42
34	43	52	61	70	79	88	97	106	115	124	133	142	151	7	16	25
17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	8

153	162	171	180	189	198	207	216	225	234	243	252	261	270	279	288	297
289	298	154	163	172	181	190	199	208	217	226	235	244	253	262	271	280
272	281	290	299	155	164	173	182	191	200	209	218	227	236	245	254	263
255	264	273	282	291	300	156	165	174	183	192	201	210	219	228	237	246
238	247	256	265	274	283	292	301	157	166	175	184	193	202	211	220	229
221	230	239	248	257	266	275	284	293	302	158	167	176	185	194	203	212
204	213	222	231	240	249	258	267	276	285	294	303	159	168	177	186	195
187	196	205	214	223	232	241	250	259	268	277	286	295	304	160	169	178
170	179	188	197	206	215	224	233	242	251	260	269	278	287	296	305	161

306	332	324	316	308	334	326	318	310	336	328	320	312	338	330	322	314
323	315	307	333	325	317	309	335	327	319	311	337	329	321	313	339	331

The Breakthrough

- It goes without saying that I was shocked!



- This candidate was split into three vertical sections of lengths 9, 9 and 2.
- The transposition for each section was a 1,2–decimation.

0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144
136	145	1	10	19	28	37	46	55	64	73	82	91	100	109	118	127
119	128	137	146	2	11	20	29	38	47	56	65	74	83	92	101	110
102	111	120	129	138	147	3	12	21	30	39	48	57	66	75	84	93
85	94	103	112	121	130	139	148	4	13	22	31	40	49	58	67	76
68	77	86	95	104	113	122	131	140	149	5	14	23	32	41	50	59
51	60	69	78	87	96	105	114	123	132	141	150	6	15	24	33	42
34	43	52	61	70	79	88	97	106	115	124	133	142	151	7	16	25
17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	8

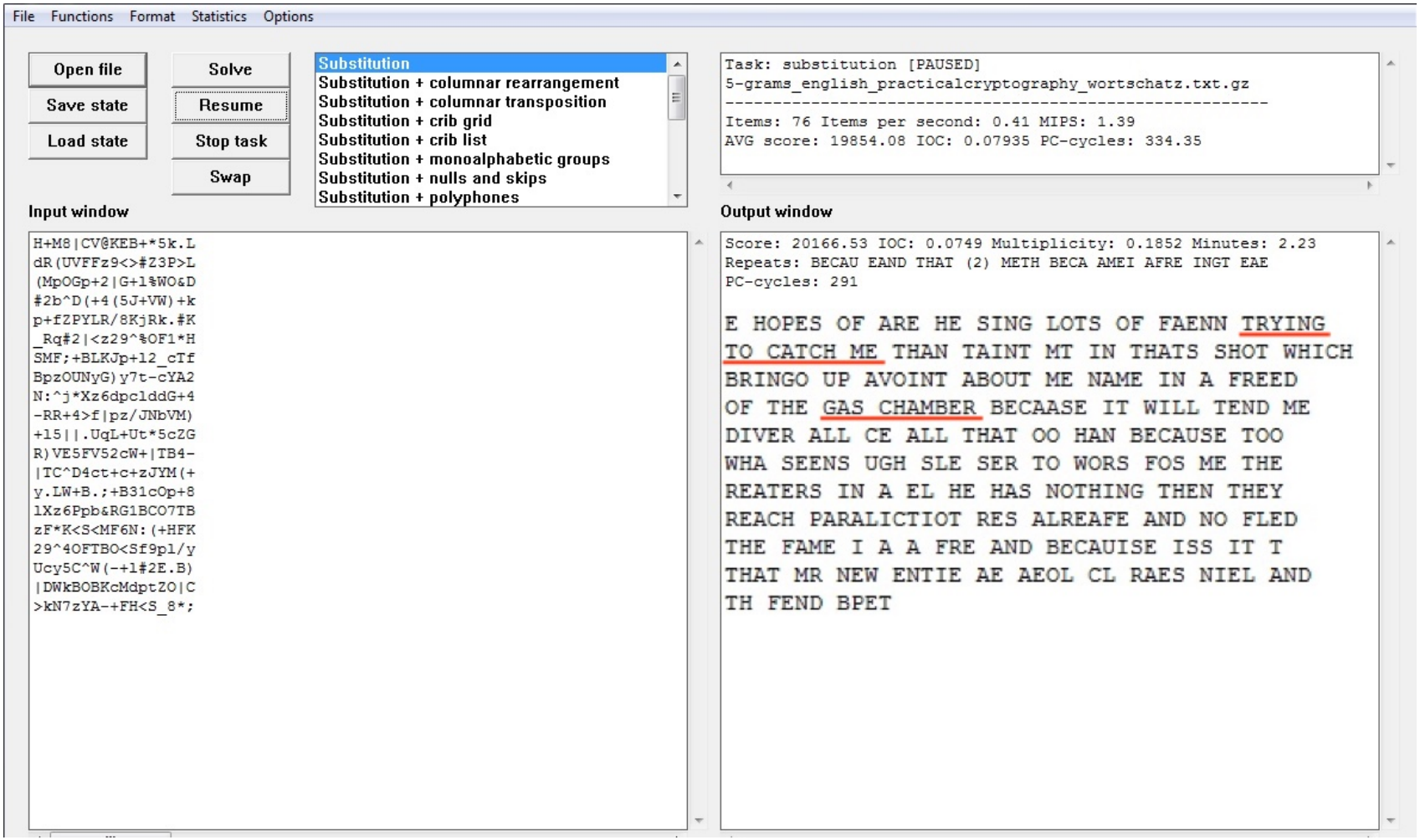
153	162	171	180	189	198	207	216	225	234	243	252	261	270	279	288	297
289	298	154	163	172	181	190	199	208	217	226	235	244	253	262	271	280
272	281	290	299	155	164	173	182	191	200	209	218	227	236	245	254	263
255	264	273	282	291	300	156	165	174	183	192	201	210	219	228	237	246
238	247	256	265	274	283	292	301	157	166	175	184	193	202	211	220	229
221	230	239	248	257	266	275	284	293	302	158	167	176	185	194	203	212
204	213	222	231	240	249	258	267	276	285	294	303	159	168	177	186	195
187	196	205	214	223	232	241	250	259	268	277	286	295	304	160	169	178
170	179	188	197	206	215	224	233	242	251	260	269	278	287	296	305	161

306	332	324	316	308	334	326	318	310	336	328	320	312	338	330	322	314
323	315	307	333	325	317	309	335	327	319	311	337	329	321	313	339	331

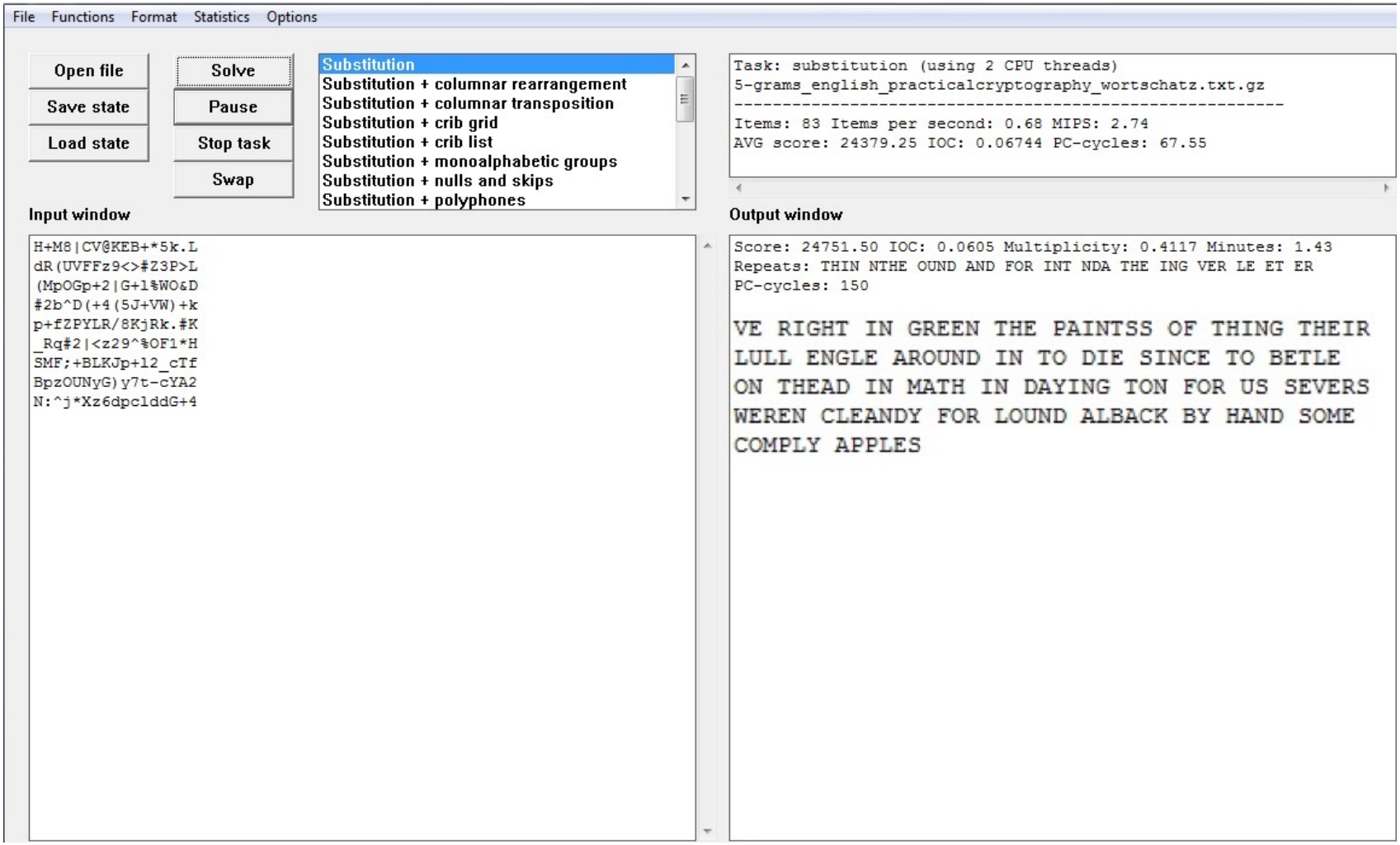
The Breakthrough

Recreating this partial solution with azdecrypt

We can recreate this partial solution with azdecrypt. Again, the terms TRYING TO CATCH ME and GAS CHAMBER appear in my recreation of the partial solution.



Perhaps we can just solve the first lines on its own?



The Breakthrough

Solving the first 9 lines of Z340

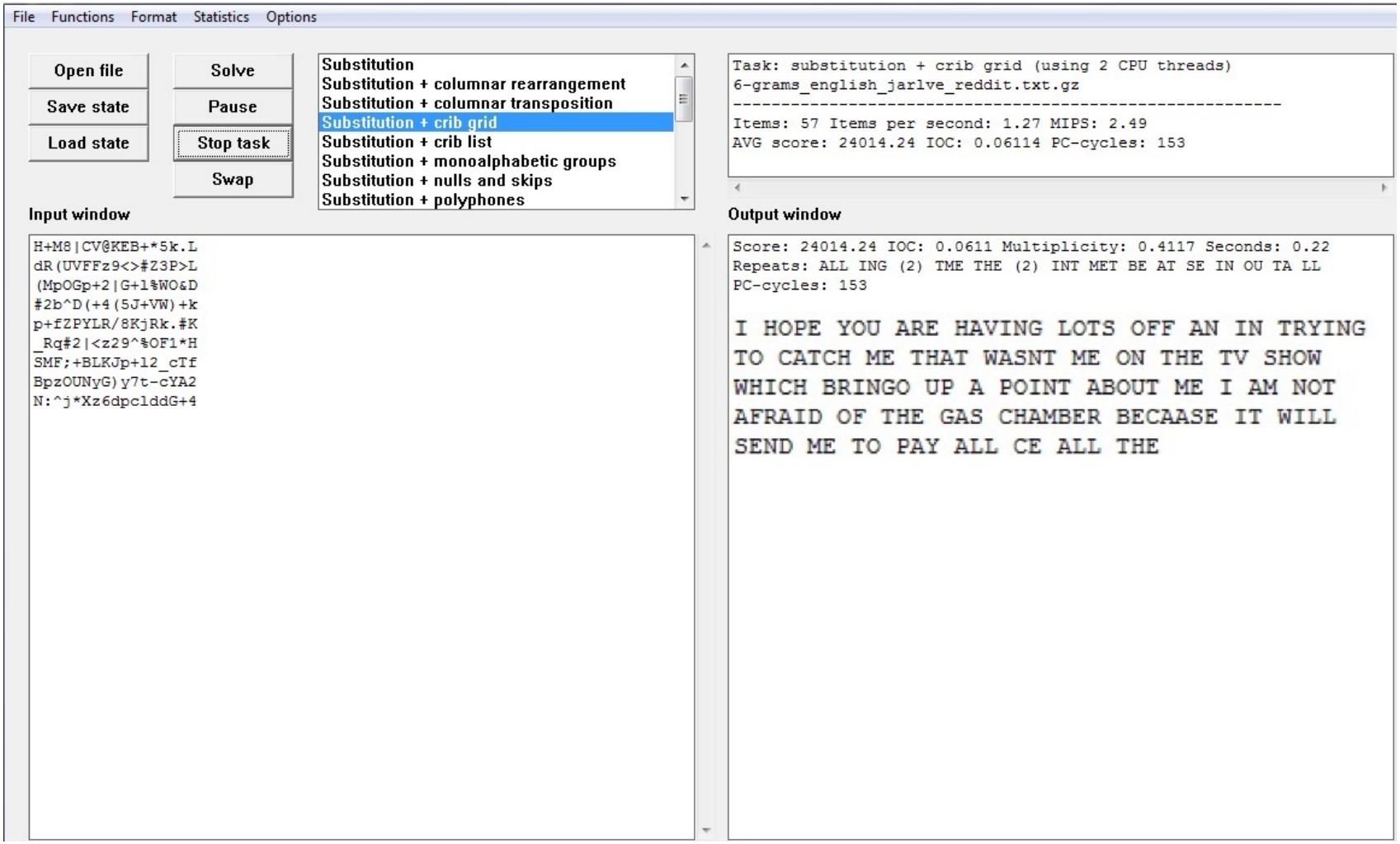
- Using the crib feature of azdecrypt, we can lock in the terms `TRYING TO CATCH ME` and `GAS CHAMBER`
- The remaining terms will be solved with these additional constraints.

The Breakthrough

Solving the first 9 lines of Z340

- Using the crib feature of azdecrypt, we can lock in the terms `TRYING TO CATCH ME` and `GAS CHAMBER`
- The remaining terms will be solved with these additional constraints.

A recreation of the solution for the first 9 lines with `azdecrypt`:



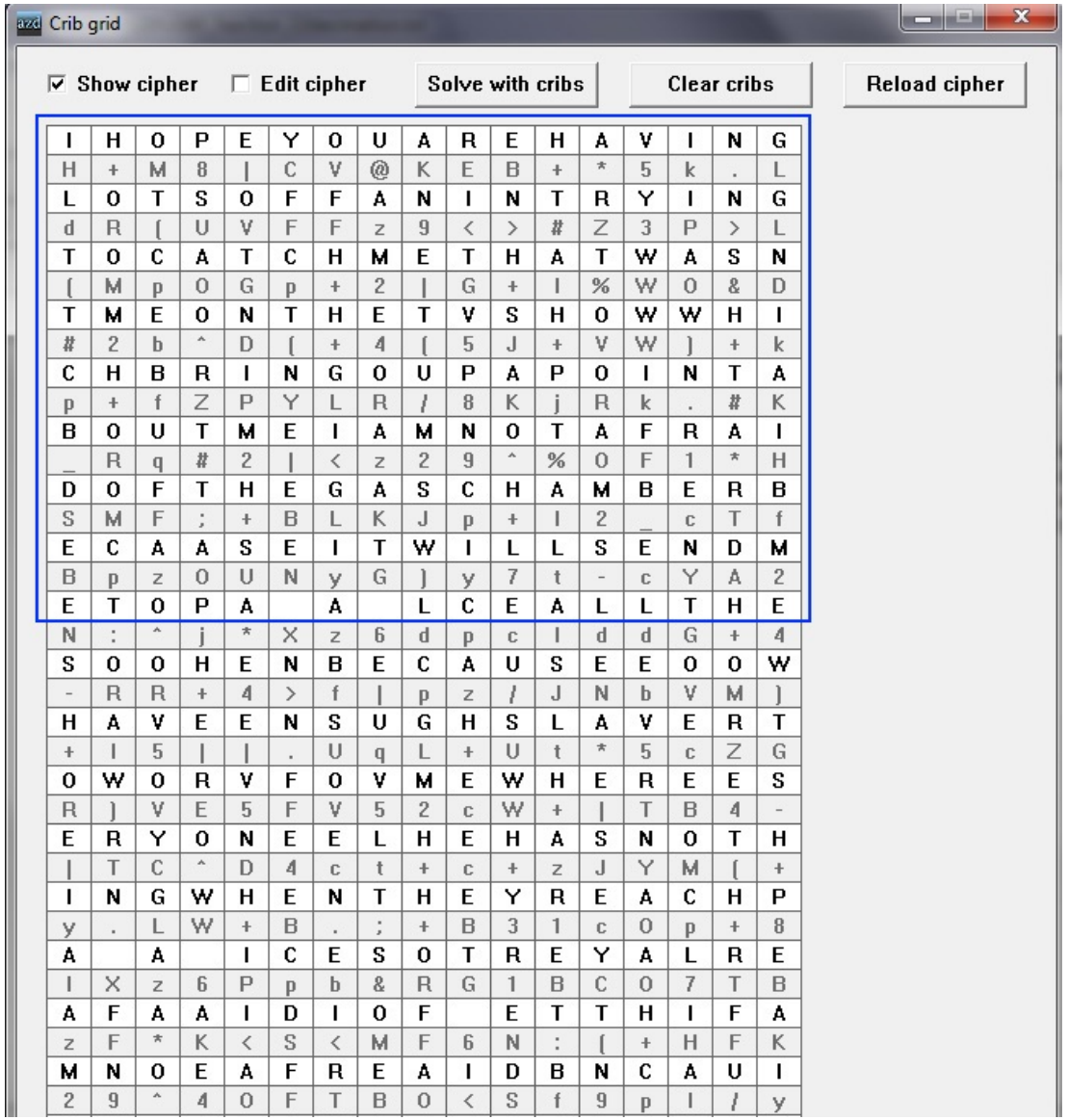
The plaintext we found for the first 9 lines was:

I HOPE YOU ARE HAVING LOTS OF FAN (FUN) IN TRYING TO CATCH
ME THAT WASNT ME ON THE TV SHOW WHICH BRINGO (BRINGS) UP A
POINT ABOUT ME I AM NOT AFRAID OF THE GAS CHAMBER BECAASE
(BECAUSE) IT WILL SEND ME TO PARADLCE (PARADICE) ALL THE

The Breakthrough

Solving the second 9 lines of Z340

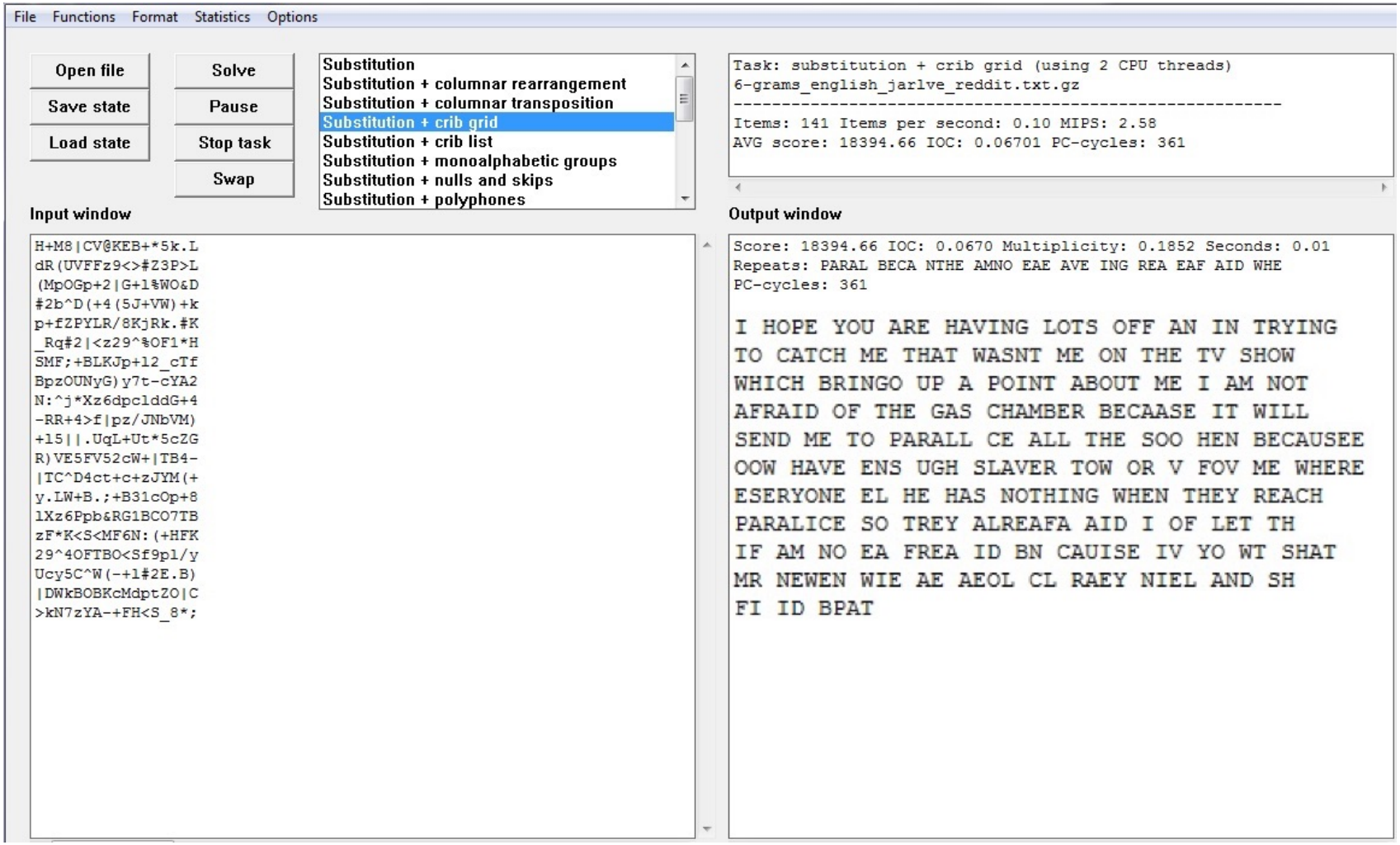
If we crib all the legible text from the first section, does the second section fall out with the same key?



The Breakthrough

Solving the second 9 lines of Z340

Some of it kind of makes sense, but we're not there yet.



At this point David and I contacted Jarl van Eycke, the author of `azdecrypt`. Jarl made the following (amazing) observations, which solved the mystery of the second 9 lines of Z340.

Untransposed, deciphered 2nd section of Z340

S	A	A	S	O	H	O	S	H	A	C	L	I	F	E	I	S
S	H	O	U	V	L	R	E	N	N	E	C	E	R	O	A	A
M	I	E	A	O	S	E	A	V	R	E	O	N	H	S	E	F
A	L	N	D	I	T	H	E	E	V	F	E	E	T	T	P	O
A	T	F	E	O	B	V	M	E	E	N	E	O	E	L	H	H
I	E	R	R	A	T	E	N	Y	R	N	O	S	R	V	S	H
E	E	N	Y	A	E	A	T	A	C	O	N	B	O	U	T	M
O	E	R	H	G	R	L	Y	I	H	F	A	W	E	E	W	G
H	H	W	W	Y	A	W	E	I	A	D	I	R	U	T	W	C

At this point David and I contacted Jarl van Eycke, the author of `azdecrypt`. Jarl made the following (amazing) observations, which solved the mystery of the second 9 lines of Z340.

- The `LIFEIS` plaintext is read left to right.
- The `LIFEIS` plaintext is excluded from the 1,2–decimation transposition and read left to right.
- Numerous spelling mistakes are corrected if `H` on row 6 is moved to the 4th column.
- Apply the 1,2–decimation transposition, skipping (vertically) the positions containing `LIFEIS`.

Untransposed, deciphered 2nd section of Z340

S	A	A	S	O	H	O	S	H	A	C	**L**	**I**	**F**	**E**	**I**	**S**
S	H	O	U	V	L	R	E	N	N	E	C	E	R	O	A	A
M	I	E	A	O	S	E	A	V	R	E	O	N	H	S	E	F
A	L	N	D	I	T	H	E	E	V	F	E	E	T	T	P	O
A	T	F	E	O	B	V	M	E	E	N	E	O	E	L	H	H
I	E	R	**H**	R	A	T	E	N	Y	R	N	O	S	R	V	S
E	E	N	Y	A	E	A	T	A	C	O	N	B	O	U	T	M
O	E	R	H	G	R	L	Y	I	H	F	A	W	E	E	W	G
H	H	W	W	Y	A	W	E	I	A	D	I	R	U	T	W	C

At this point David and I contacted Jarl van Eycke, the author of `azdecrypt`. Jarl made the following (amazing) observations, which solved the mystery of the second 9 lines of Z340.

- The `LIFEIS` plaintext is read left to right.
- The `LIFEIS` plaintext is excluded from the 1,2–decimation transposition and read left to right.
- Numerous spelling mistakes are corrected if `H` on row 6 is moved to the 4th column.
- Apply the 1,2–decimation transposition, skipping (vertically) the positions containing `LIFEIS`.

Untransposed, deciphered 2nd section of Z340

S	A	A	S	O	H	O	S	H	A	C	**L**	**I**	**F**	**E**	**I**	**S**
S	H	O	U	V	L	R	E	N	N	E	C	E	R	O	A	A
M	I	E	A	O	S	E	A	V	R	E	O	N	H	S	E	F
A	L	N	D	I	T	H	E	E	V	F	E	E	T	T	P	O
A	T	F	E	O	B	V	M	E	E	N	E	O	E	L	H	H
I	E	R	**H**	R	A	T	E	N	Y	R	N	O	S	R	V	S
E	E	N	Y	A	E	A	T	A	C	O	N	B	O	U	T	M
O	E	R	H	G	R	L	Y	I	H	F	A	W	E	E	W	G
H	H	W	W	Y	A	W	E	I	A	D	I	R	U	T	W	C

At this point David and I contacted Jarl van Eycke, the author of `azdecrypt`. Jarl made the following (amazing) observations, which solved the mystery of the second 9 lines of Z340.

- The `LIFEIS` plaintext is read left to right.
- The `LIFEIS` plaintext is excluded from the 1,2–decimation transposition and read left to right.
- Numerous spelling mistakes are corrected if `H` on row 6 is moved to the 4th column.
- Apply the 1,2–decimation transposition, skipping (vertically) the positions containing `LIFEIS`.

Untransposed, deciphered 2nd section of Z340

S	A	A	S	O	H	O	S	H	A	C	**L**	**I**	**F**	**E**	**I**	**S**
S	H	O	U	V	L	R	E	N	N	E	C	E	R	O	A	A
M	I	E	A	O	S	E	A	V	R	E	O	N	H	S	E	F
A	L	N	D	I	T	H	E	E	V	F	E	E	T	T	P	O
A	T	F	E	O	B	V	M	E	E	N	E	O	E	L	H	H
I	E	R	**H**	R	A	T	E	N	Y	R	N	O	S	R	V	S
E	E	N	Y	A	E	A	T	A	C	O	N	B	O	U	T	M
O	E	R	H	G	R	L	Y	I	H	F	A	W	E	E	W	G
H	H	W	W	Y	A	W	E	I	A	D	I	R	U	T	W	C

At this point David and I contacted Jarl van Eycke, the author of `azdecrypt`. Jarl made the following (amazing) observations, which solved the mystery of the second 9 lines of Z340.

- The `LIFEIS` plaintext is read left to right.
- The `LIFEIS` plaintext is excluded from the 1,2–decimation transposition and read left to right.
- Numerous spelling mistakes are corrected if `H` on row 6 is moved to the 4th column.
- Apply the 1,2–decimation transposition, skipping (vertically) the positions containing `LIFEIS`.

Untransposed, deciphered 2nd section of Z340

S	A	A	S	O	H	O	S	H	A	C	**L**	**I**	**F**	**E**	**I**	**S**
S	H	O	U	V	L	R	E	N	N	E	C	E	R	O	A	A
M	I	E	A	O	S	E	A	V	R	E	O	N	H	S	E	F
A	L	N	D	I	T	H	E	E	V	F	E	E	T	T	P	O
A	T	F	E	O	B	V	M	E	E	N	E	O	E	L	H	H
I	E	R	**H**	R	A	T	E	N	Y	R	N	O	S	R	V	S
E	E	N	Y	A	E	A	T	A	C	O	N	B	O	U	T	M
O	E	R	H	G	R	L	Y	I	H	F	A	W	E	E	W	G
H	H	W	W	Y	A	W	E	I	A	D	I	R	U	T	W	C

At this point David and I contacted Jarl van Eycke, the author of `azdecrypt`. Jarl made the following (amazing) observations, which solved the mystery of the second 9 lines of Z340.

- The `LIFEIS` plaintext is excluded from the 1,2–decimation transposition and read left to right.
- Numerous spelling mistakes are corrected if `H` on row 6 is moved to the 4th column.
- Apply the 1,2–decimation transposition, skipping (vertically) the positions containing `LIFEIS`.

```
SOO HER BECAUSE E (I) NOW HAVE
ENOUGH SLAVES TO WORV (WORK) FOR ME
WHERE EVERYONE ELSE HAS NOTHING
WHEN THEY REACH PARADICE SO THEY
ARE AFRAID OF DEATH I AM NOT AFRAID
BECAUSE I VNOW (KNOW) THAT MY NEW
LIFE IS
```

Applying our substitution key to the final two (untransposed) lines gives:

EFILWILLEBNAEASYE
NONIECIDARAPDEATH

Including some spaces gives:

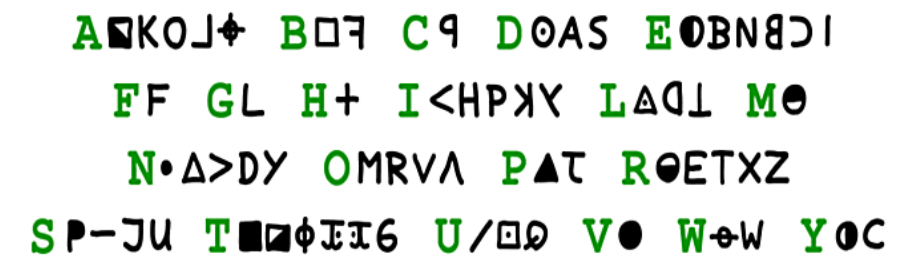
EFIL WILL EB NA EASY ENO NI ECIDARAP DEATH

Then reversing a few words gives:

LIFE WILL BE AN EASY ONE IN PARADICE DEATH

The Z340 Substitution Key and Transposition

The final key and transposition for the Z340.



0	9	18	27	36	45	54	63	72	81	90	99	108	117	126	135	144
136	145	1	10	19	28	37	46	55	64	73	82	91	100	109	118	127
119	128	137	146	2	11	20	29	38	47	56	65	74	83	92	101	110
102	111	120	129	138	147	3	12	21	30	39	48	57	66	75	84	93
85	94	103	112	121	130	139	148	4	13	22	31	40	49	58	67	76
68	77	86	95	104	113	122	131	140	149	5	14	23	32	41	50	59
51	60	69	78	87	96	105	114	123	132	141	150	6	15	24	33	42
34	43	52	61	70	79	88	97	106	115	124	133	142	151	7	16	25
17	26	35	44	53	62	71	80	89	98	107	116	125	134	143	152	8

153	162	171	180	189	198	207	216	225	234	243	300	301	302	303	304	305
284	292	154	163	172	181	190	199	208	217	226	235	244	252	260	268	276
269	277	285	293	155	164	173	182	191	200	209	218	227	236	245	253	261
254	262	270	278	286	294	156	165	174	183	192	201	210	219	228	237	246
238	247	255	263	271	279	287	295	157	166	175	184	193	202	211	220	229
221	230	239	256	264	272	280	288	296	158	167	176	185	194	203	212	248
204	213	222	231	240	249	257	265	273	281	289	297	159	168	177	186	195
187	196	205	214	223	232	241	250	258	266	274	282	290	298	160	169	178
170	179	188	197	206	215	224	233	242	251	259	267	275	283	291	299	161

309	308	307	306	310	311	312	313	315	314	317	316	318	319	320	321	324
323	322	326	325	334	333	332	331	330	329	328	327	335	336	337	338	339

Submitting our Solution to the FBI

David submitted this solution to the FBI CRRU on Saturday, December 5th, 2020.

Z340 has been solved Inbox ×

David Oranchak <doranchak@gmail.com> Sat, Dec 5, 2020, 11:56 PM

to Daniel, Jeanne, Scott, bcc: me

Some friends of mine (Sam Blake and Jarl van Eycke) and I have solved Zodiac's 340 cipher.

We believe this one's the real deal! :)
-Dave

Z340 solution.pdf

FBI Confirmation of our Solution

- We received an unofficial confirmation of our solution later that day.
- The following day our solution was sent from the FBI CRRU to FBI San Francisco.
- The FBI requested we not make our solution public until they had notified victims.
- Sitting on this result for 7 days was hard, but we wanted to respect the FBIs process.

FBI Confirmation of our Solution

- We received an unofficial confirmation of our solution later that day.
- The following day our solution was sent from the FBI CRRU to FBI San Francisco.
- The FBI requested we not make our solution public until they had notified victims.
- Sitting on this result for 7 days was hard, but we wanted to respect the FBIs process.

FBI Confirmation of our Solution

- We received an unofficial confirmation of our solution later that day.
- The following day our solution was sent from the FBI CRRU to FBI San Francisco.
- The FBI requested we not make our solution public until they had notified victims.
- Sitting on this result for 7 days was hard, but we wanted to respect the FBIs process.

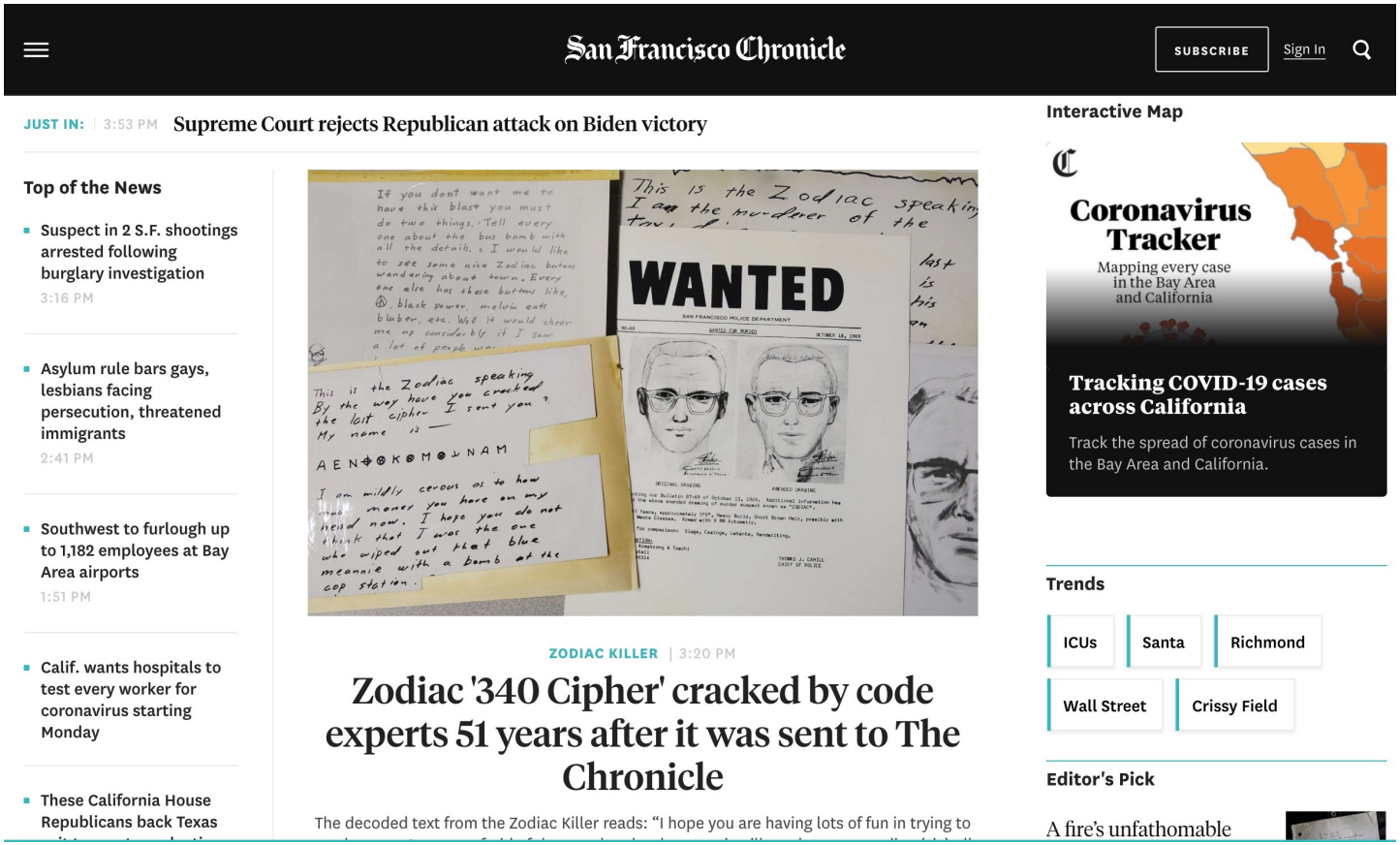
FBI Confirmation of our Solution

- We received an unofficial confirmation of our solution later that day.
- The following day our solution was sent from the FBI CRRU to FBI San Francisco.
- The FBI requested we not make our solution public until they had notified victims.
- Sitting on this result for 7 days was hard, but we wanted to respect the FBIs process.

The International Reaction to the Solution

San Francisco Chronicle

It was a special moment to see our work on the front page of the *San Francisco Chronicle*. Especially as it was covered by long–time Zodiac reporter, Kevin Fagan.



San Francisco Chronicle

SUBSCRIBE Sign In

JUST IN: | 3:53 PM **Supreme Court rejects Republican attack on Biden victory**

Top of the News

- Suspect in 2 S.F. shootings arrested following burglary investigation
  3:16 PM
- Asylum rule bars gays, lesbians facing persecution, threatened immigrants
  2:41 PM
- Southwest to furlough up to 1,182 employees at Bay Area airports
  1:51 PM
- Calif. wants hospitals to test every worker for coronavirus starting Monday
- These California House Republicans back Texas

ZODIAC KILLER | 3:20 PM

Zodiac '340 Cipher' cracked by code experts 51 years after it was sent to The Chronicle

The decoded text from the Zodiac Killer reads: "I hope you are having lots of fun in trying to

Interactive Map

Trends

ICUs | Santa | Richmond | Wall Street | Crissy Field

Editor's Pick

A fire's unfathomable

The International Reaction to the Solution

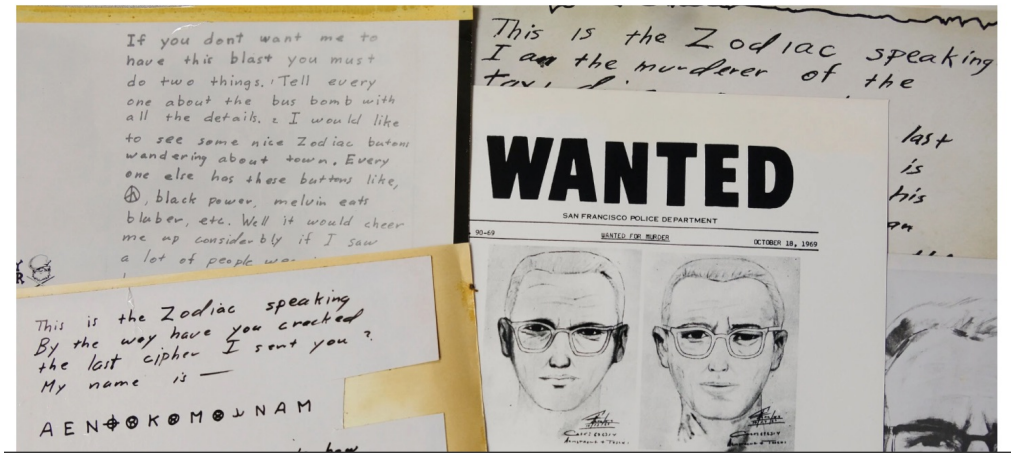
New York Times

We were told to expect a deluge of press, but I honestly had no idea of the attention this would receive.

The New York Times

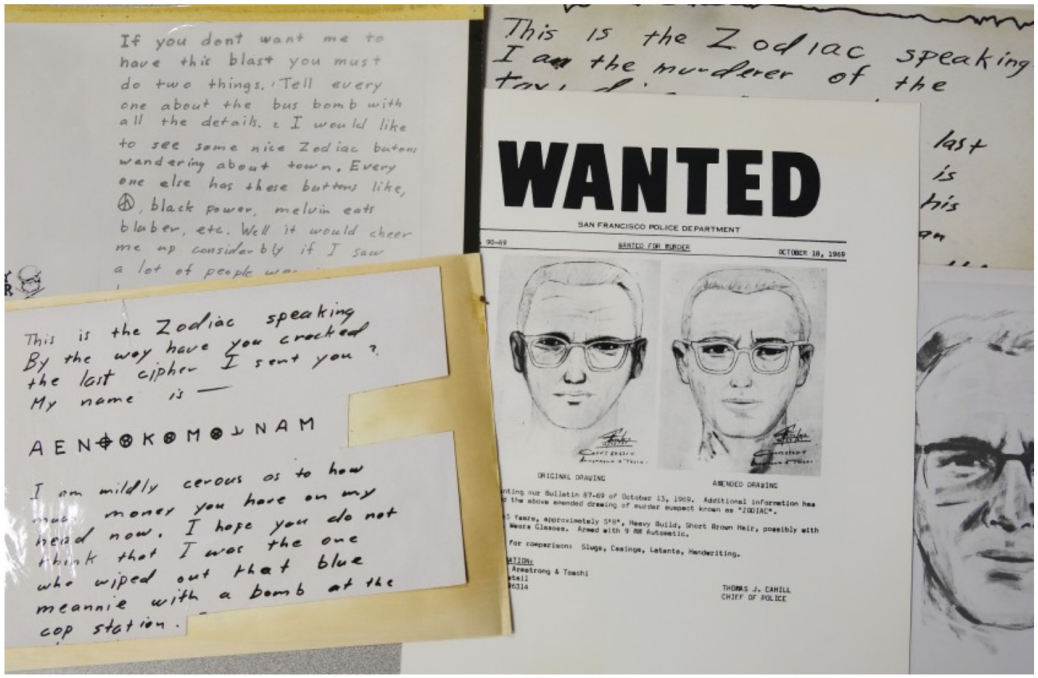
51 Years Later, Coded Message Attributed to Zodiac Killer Has Been Solved, F.B.I. Says

The code had long baffled cryptographers, law enforcement agents and armchair sleuths obsessed with the shadowy killer, who was blamed for five murders in the late 1960s.



Los Angeles Times

Zodiac Killer cipher is solved 51 years after it was sent to newspaper



Amateur sleuths from the U.S., Australia and Belgium teamed up to decipher a coded letter the Zodiac Killer sent to the San Francisco Chronicle in 1969. (Eric Risberg / Associated Press)

By ASSOCIATED PRESS

CORONAVIRUS AND PANDEMIC ›

U.S. angling to secure more of Pfizer's coronavirus vaccine

SoCal cities consider renewed 'hero pay' for grocery store workers amid COVID-19 surge

Joe Biden and Mike Pence will receive COVID-19 vaccine soon

ICU capacity explained

Hundreds of state prison inmates in San Diego County sickened with COVID-19

Cases statewide »

1,699,181	21,887
confirmed	deaths

The International Reaction to the Solution

CNN

CNN US Crime + Justice Energy + Environment Extreme Weather Space + Science Edit

After 51 years, the Zodiac Killer's cipher has been solved by amateur codebreakers

By Leah Asmelash and Cheri Mossburg, CNN

Updated 0049 GMT (0849 HKT) December 12, 2020

(CNN) — More than 50 years after the so-called Zodiac Killer first began terrorizing the streets of Northern California, a code-breaking team is believed to have finally cracked one of the killer's mysterious coded messages sent to the San Francisco Chronicle in 1969.

Dubbed the "340 cipher," the message was unraveled by a trio of code breakers -- David Oranchak, a software developer in Virginia, Jarl Van Eycke, a Belgian computer programmer, and Sam Blake, an Australian mathematician.

Decoding the cipher revealed the following message. It was sent in all capital letters without punctuation and included the misspelling of paradise:

"I hope you are having lots of fun in trying to catch me

That wasn't me on the TV show which brings up a point about me

I am not afraid of the gas chamber because it will send me to paradice all the sooner

NEW YORK POST

NEWS

Zodiac Killer's 1969 cipher 'puzzle' finally solved

By Natalie O'Neill December 11, 2020 | 2:36pm | Updated

A long-unsolved puzzle sent by the Zodiac Killer to

The International Reaction to the Solution

NBC Boston

10 BOSTON LOCAL WEATHER INVESTIGATIONS VIDEOS SPORTS TRAFFIC

ZODIAC KILLER

'I Am Not Afraid of the Gas Chamber': Codebreakers Solve Zodiac Killer Cipher

Federal authorities said they believe the code breakers appear to be on solid ground

Published December 11, 2020 • Updated on December 12, 2020 at 12:48 am

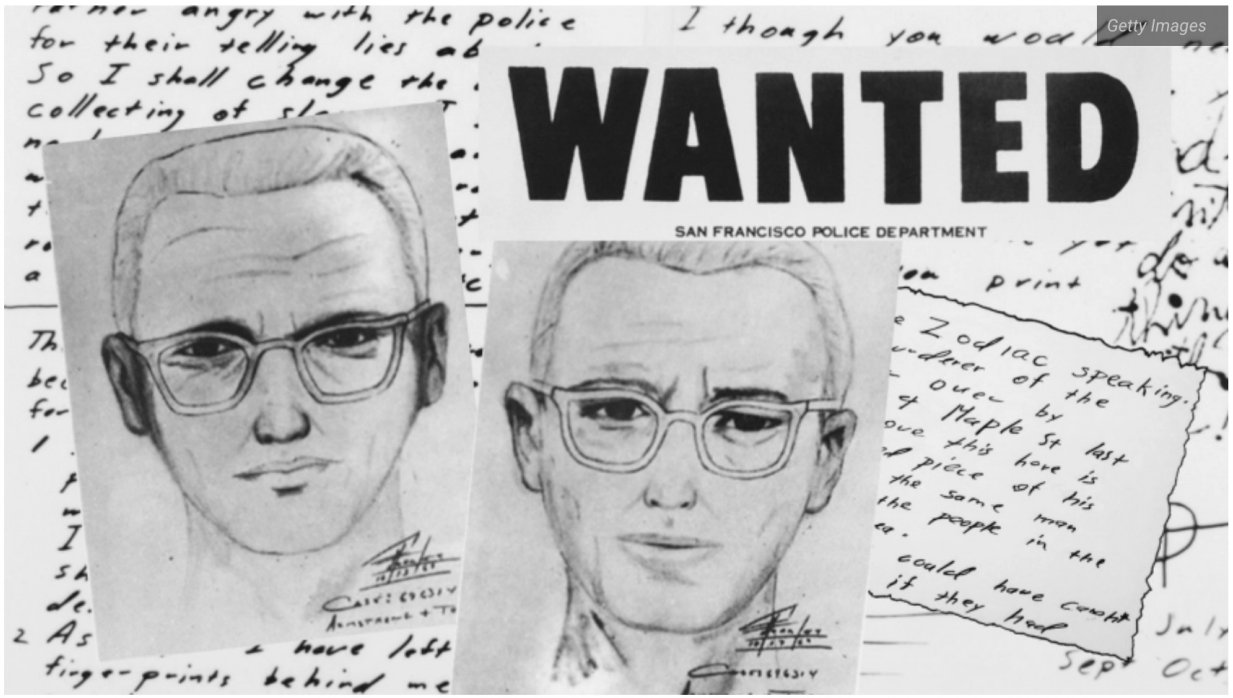


Photo illustration.

The International Reaction to the Solution

USA Today

USA TODAY

COVID-19 RESOURCES
Your questions answered

CORONAVIRUS NUMBERS
Virus numbers by state

HOLIDAY SHOPPING
Deals to your inbox

[News] Sports Entertainment Life Money Tech Travel Opinion

NATION

Zodiac cipher solved 5 decades after serial killer terrorized Northern California

SAN FRANCISCO — A coded letter mailed to a San Francisco newspaper by the Zodiac serial killer in 1969 has been deciphered by a team of amateur sleuths from the United States, Australia and Belgium, the San Francisco Chronicle reported Friday.

The cipher is one of many sent by a killer who referred to himself as Zodiac in letters sent to detectives and the media. The Zodiac terrorized Northern California communities and killed five people in the Bay Area in 1968 and 1969.

According to code-breaking expert David Oranchak, the cipher's text includes: "I hope you are having lots of fun in trying to catch me. ... I am not afraid of the gas chamber because it will send me to paradise all the sooner because I now

This is a file copy of a cryptogram sent to the San Francisco Chronicle in 1969 by the Zodiac Killer. A coded letter mailed to a San Francisco newspaper by the Zodiac serial killer in 1969 has been deciphered by a team of amateur sleuths from the United States, Australia and Belgium, the San Francisco Chronicle reported Friday, Dec. 11, 2020. *San Francisco Chronicle Via AP, File*

Daily Mail AUSTRALIA

News

Home | U.K. | U.S. | News | World News | Sport | TV&Showbiz | Femail | Health | Science | Weather | Video | Travel | DailyMailTV

Royal Family | Covid-19 | US Election | Breaking News | World News | Sydney | Melbourne | Brisbane | New Zealand | Headlines | Wires | Login

'I hope you are having lots of fun trying to catch me': Chilling 1969 cipher written by Zodiac Killer who claimed he murdered 37 people is FINALLY solved 51 years later

- Murderer known as 'Zodiac Killer' was known for sending letters, cards and ciphers to media and police
- Police linked him to five murders and two survivors in the Bay Area between 1965-1969
- But he boasted of at least 37 victims in his cryptic letters or 'ciphers' to the press
- '340 cipher' was sent to San Francisco Chronicle in November 1969 but wasn't deciphered until now
- International team of code-breakers from US, Australia and Belgium worked together to reveal a message that said he 'isn't afraid of the gas chamber'
- Killer refers to his victims as 'slaves' who will 'work' for him when he gets to 'paradise'
- FBI confirmed the cipher had been solved by private citizens
- US cryptographer David Oranchak named the other code-breakers as Australian mathematician Sam Blake and Belgian software developer Jarl Van Eycke

The International Reaction to the Solution

The Sun (UK)

THE SUN, A NEWS UK COMPANY

Sign in

UK Edition | Search

MONEY | DEAR DEIDRE | TECH | TRAVEL | MOTORS | PUZZLES | SUN BINGO | SUN VOUCHERS

All News | UK News | World News | Brexit | Politics | Opinion | Health News

CHILLING NOTE What did the Zodiac Killer's cipher say?

Catriona Graffius
12 Dec 2020, 11:48 | Updated: 12 Dec 2020, 12:38

THE Zodiac Killer's menacing puzzle to a newspaper has finally been cracked decades after the serial murderer claimed to kill 37 people.

The incredibly tough code was one of a number the killer had sent to newspapers across San Francisco. But what did the cipher say? And what did the Zodiac killer do?

The International Reaction to the Solution

ABC (Australia)

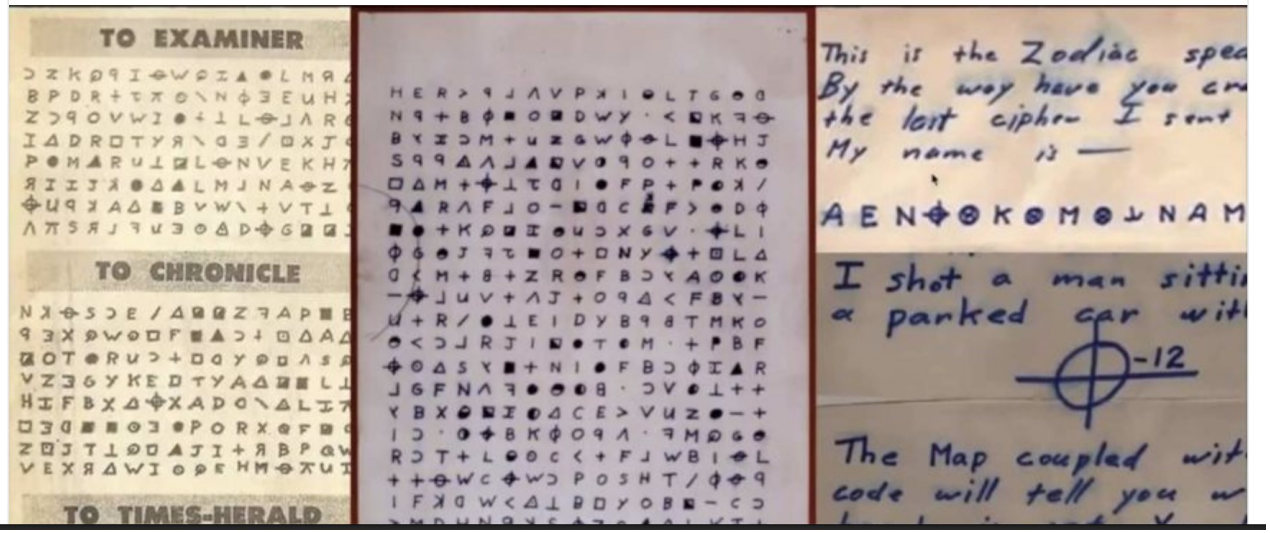
ABC NEWS

Just In | Coronavirus | Watch Live | Politics | World | Business | Analysis | Sport | Science | Health | Arts

Zodiac killer code cracked by Australian mathematician Sam Blake more than 50 years after first murder

By Michael Coggan

Posted 5d ago, updated 2d ago



THE AGE

World North America Crime

Australian mathematician helps crack 'Zodiac' serial killer's coded message

By **Sharon Bernstein**

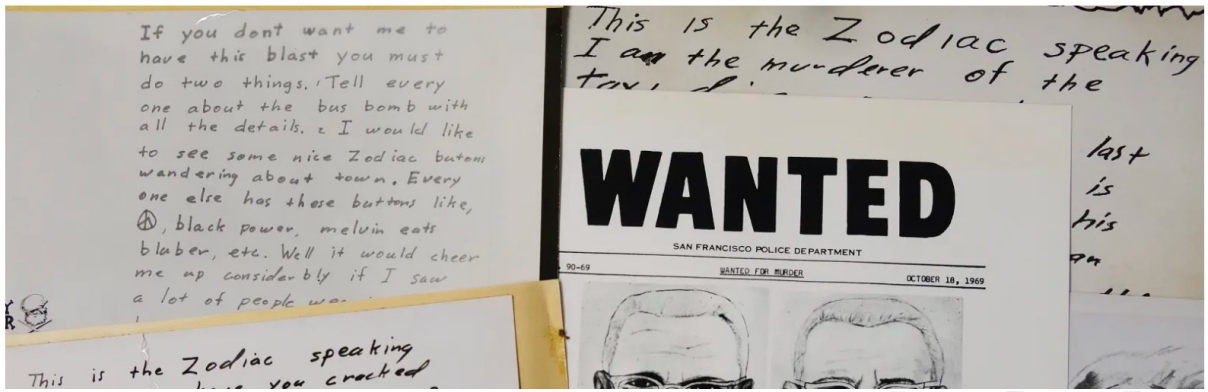
December 12, 2020 — 11.19pm

Save Share A A A

3 View all comments

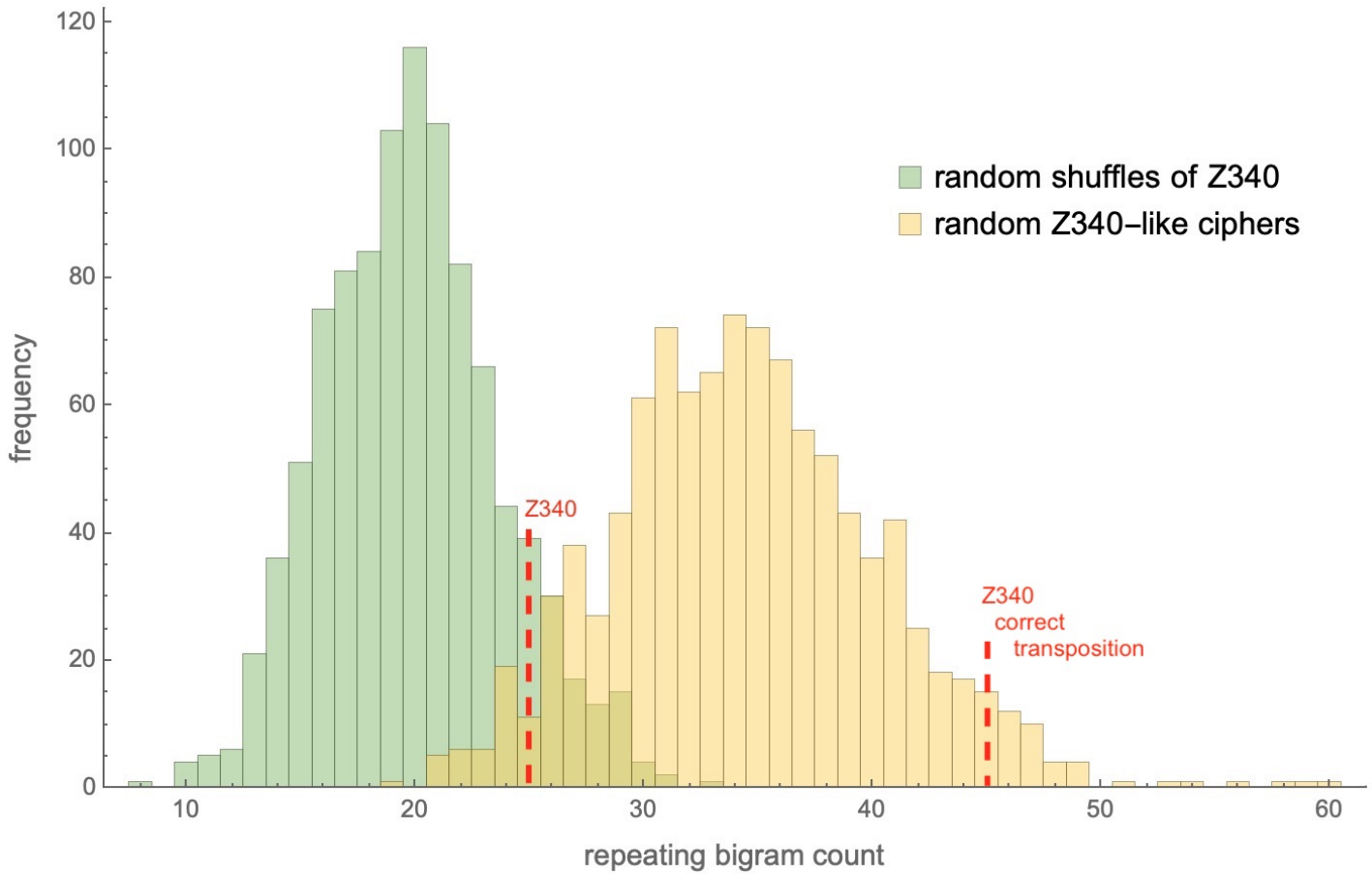
California: A team of volunteer codebreakers, including a Melbourne mathematician, has cracked a mysterious cipher sent more than 50 years ago to a newspaper by the San Francisco serial killer who called himself the Zodiac.

The Zodiac killer – who was never caught – shot or stabbed seven people in the San Francisco Bay Area over the course of about a year in 1968 and 1969, killing all but two of them.



Reflecting on the Correct Transposition of Z340

The correct transposition of Z340 has 45 repeating bigrams (and 5 repeating trigrams). This is 7–sigma from the mean of random shuffles of Z340.



Reflecting on the Difficulty of Z340

- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `... THAT WASNT ME ON THE TV SHOW ...`

  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Reflecting on the Difficulty of Z340

- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `...  THAT WASNT ME ON THE TV SHOW ...`

  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Reflecting on the Difficulty of Z340

- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `... THAT WASNT ME ON THE TV SHOW ...`

  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Reflecting on the Difficulty of Z340

- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `... THAT WASNT ME ON THE TV SHOW ...`

  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Reflecting on the Difficulty of Z340

- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `... THAT WASNT ME ON THE TV SHOW ...`

  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Reflecting on the Difficulty of Z340

- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `... THAT WASNT ME ON THE TV SHOW ...`

  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Reflecting on the Difficulty of Z340

- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `...  THAT WASNT ME ON THE TV SHOW ...`

  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Reflecting on the Difficulty of Z340

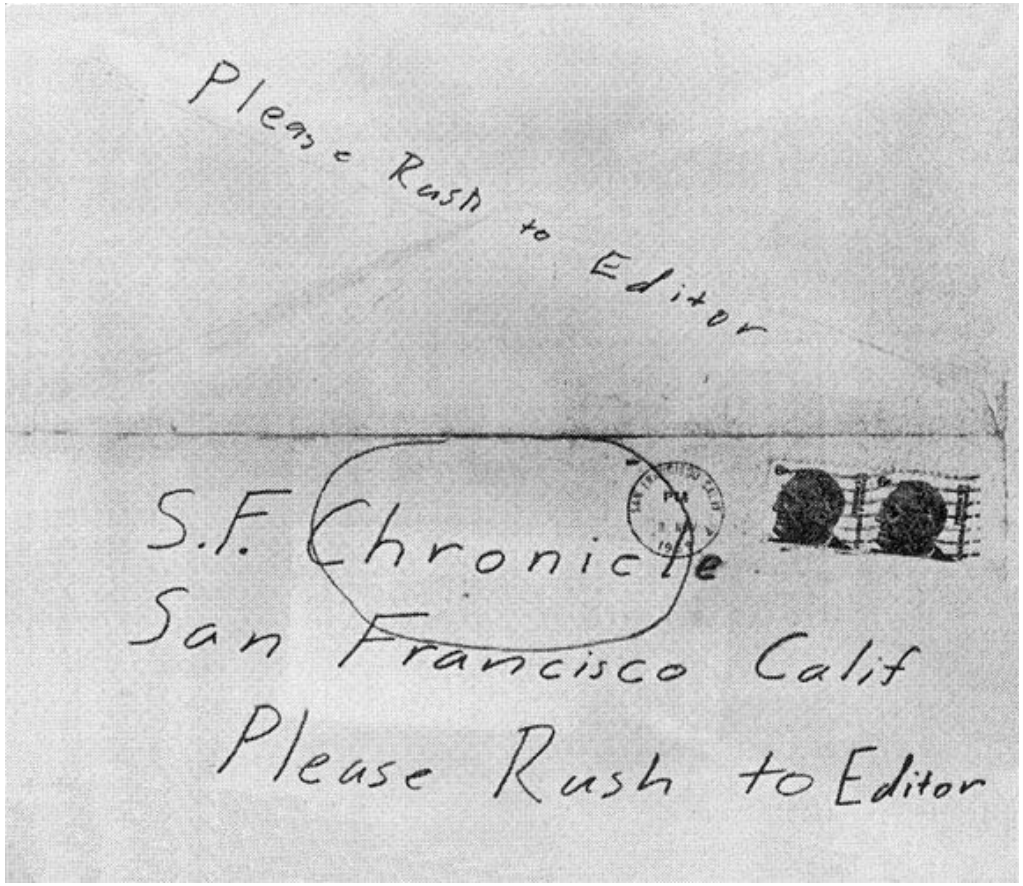
- Z408 was solved within a week.
- Z340 has taken 51 years to solve.
- The computing power required to solve Z340 was unimaginable in 1969.
- Zodiac clearly wanted to make his second cipher more difficult, but how much more difficult?
- The phrase in the cipher

  `...  THAT WASNT ME ON THE TV SHOW ...`

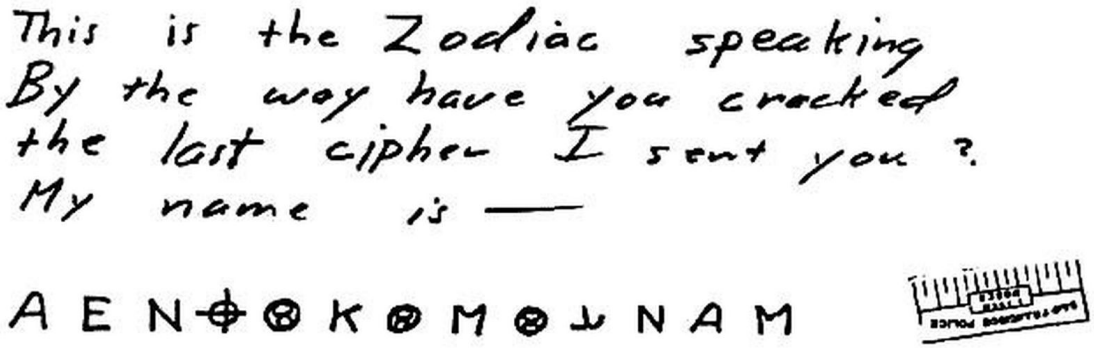
  would indicate he wanted this information known relatively quickly.
- What does the vast increase in difficulty of Z340 say about Zodiac's cryptography skills?
- Was Zodiac only skilled in creating ciphers?
- If he had knowledge of solving such ciphers, should he have known how difficult it would be to solve?

Did Zodiac leave a Hint?

Is the diagonal writing on the back of the envelope used to mail the Z340 a hint to the correct transposition?

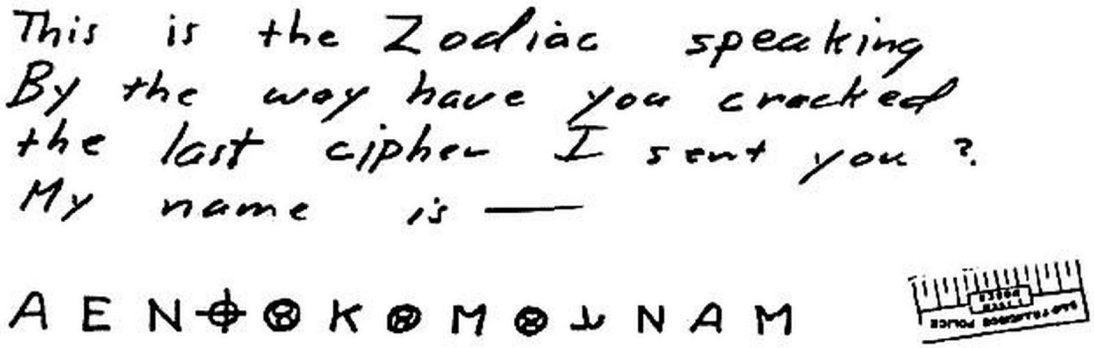


Future Directions



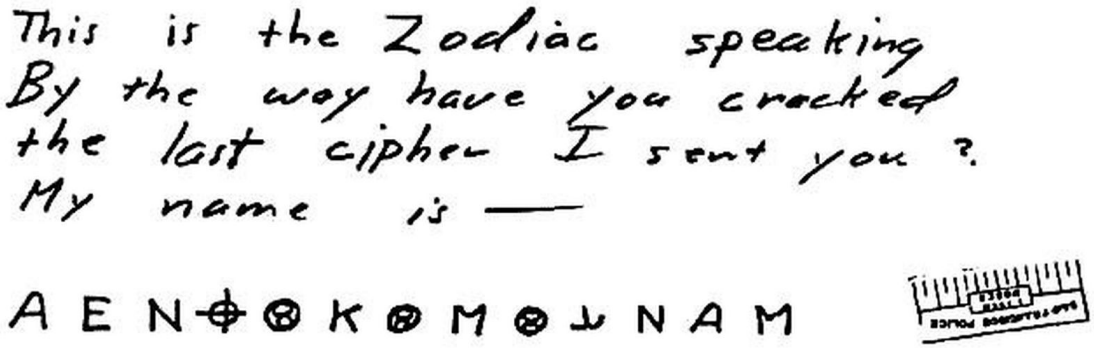
- I would like to write a paper which describes our work solving Z340 and start a project to use deep learning–based approaches to solve all Z340–like ciphers.
- I have a couple of ideas for programmatic attacks of the remaining two Zodiac ciphers which I would like to explore.
- Unfortunately, despite the deluge of international interest in this research outcome, The University of Melbourne is unwilling to financially support this work.
- We have been approached by a number of production companies to create a documentary series on the Zodiac ciphers and our work solving Z340.
- I have been approached by two publishers to write a book on our work.

Future Directions



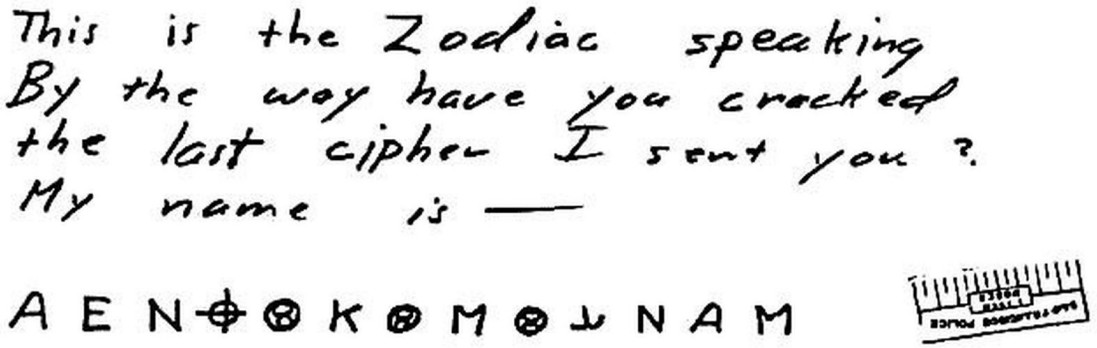
- I would like to write a paper which describes our work solving Z340 and start a project to use deep learning–based approaches to solve all Z340–like ciphers.
- I have a couple of ideas for programmatic attacks of the remaining two Zodiac ciphers which I would like to explore.
- Unfortunately, despite the deluge of international interest in this research outcome, The University of Melbourne is unwilling to financially support this work.
- We have been approached by a number of production companies to create a documentary series on the Zodiac ciphers and our work solving Z340.
- I have been approached by two publishers to write a book on our work.

Future Directions



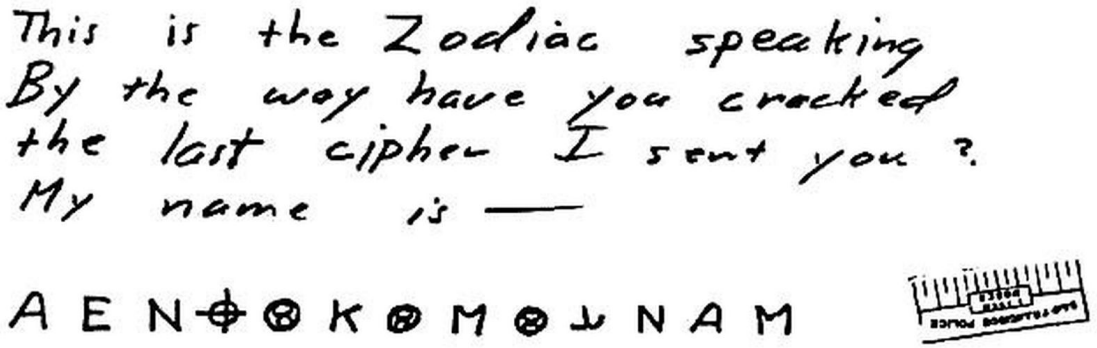
- I would like to write a paper which describes our work solving Z340 and start a project to use deep learning–based approaches to solve all Z340–like ciphers.
- I have a couple of ideas for programmatic attacks of the remaining two Zodiac ciphers which I would like to explore.
- Unfortunately, despite the deluge of international interest in this research outcome, The University of Melbourne is unwilling to financially support this work.
- We have been approached by a number of production companies to create a documentary series on the Zodiac ciphers and our work solving Z340.
- I have been approached by two publishers to write a book on our work.

Future Directions



- I would like to write a paper which describes our work solving Z340 and start a project to use deep learning–based approaches to solve all Z340–like ciphers.
- I have a couple of ideas for programmatic attacks of the remaining two Zodiac ciphers which I would like to explore.
- Unfortunately, despite the deluge of international interest in this research outcome, The University of Melbourne is unwilling to financially support this work.
- We have been approached by a number of production companies to create a documentary series on the Zodiac ciphers and our work solving Z340.
- I have been approached by two publishers to write a book on our work.

Future Directions



- I would like to write a paper which describes our work solving Z340 and start a project to use deep learning–based approaches to solve all Z340–like ciphers.
- I have a couple of ideas for programmatic attacks of the remaining two Zodiac ciphers which I would like to explore.
- Unfortunately, despite the deluge of international interest in this research outcome, The University of Melbourne is unwilling to financially support this work.
- We have been approached by a number of production companies to create a documentary series on the Zodiac ciphers and our work solving Z340.
- I have been approached by two publishers to write a book on our work.

Acknowledgements

- I would have never become involved with solving Z340 without the amazing video series on the Zodiac ciphers by David Oranchak.
- We wouldn't have been able to solve the Z340 without `azdecrypt` by Jarl van Eycke and `zkdecrypto` by Brax Sisco, Wesley Hopper and Michael Eaton.
- The vast efforts to solve the Z340 by the online community on the `zodiackillersite.com`, `zodiackiller.com` and `zodiackillerfacts.com` forums. Much of their work laid the groundwork for our eventual solution.
- I used the University of Melbourne HPC system, *Spartan*, to eliminate many candidate transpositions.
- A special thank you to David Oranchak and Jarl van Eycke.

Acknowledgements

- I would have never become involved with solving Z340 without the amazing video series on the Zodiac ciphers by David Oranchak.
- We wouldn't have been able to solve the Z340 without `azdecrypt` by Jarl van Eycke and `zkdecrypto` by Brax Sisco, Wesley Hopper and Michael Eaton.
- The vast efforts to solve the Z340 by the online community on the `zodiackillersite.com`, `zodiackiller.com` and `zodiackillerfacts.com` forums. Much of their work laid the groundwork for our eventual solution.
- I used the University of Melbourne HPC system, *Spartan*, to eliminate many candidate transpositions.
- A special thank you to David Oranchak and Jarl van Eycke.

Acknowledgements

- I would have never become involved with solving Z340 without the amazing video series on the Zodiac ciphers by David Oranchak.
- We wouldn't have been able to solve the Z340 without `azdecrypt` by Jarl van Eycke and `zkdecrypto` by Brax Sisco, Wesley Hopper and Michael Eaton.
- The vast efforts to solve the Z340 by the online community on the `zodiackillersite.com`, `zodiackiller.com` and `zodiackillerfacts.com` forums. Much of their work laid the groundwork for our eventual solution.
- I used the University of Melbourne HPC system, *Spartan*, to eliminate many candidate transpositions.
- A special thank you to David Oranchak and Jarl van Eycke.

Acknowledgements

- I would have never become involved with solving Z340 without the amazing video series on the Zodiac ciphers by David Oranchak.
- We wouldn't have been able to solve the Z340 without `azdecrypt` by Jarl van Eycke and `zkdecrypto` by Brax Sisco, Wesley Hopper and Michael Eaton.
- The vast efforts to solve the Z340 by the online community on the `zodiackillersite.com`, `zodiackiller.com` and `zodiackillerfacts.com` forums. Much of their work laid the groundwork for our eventual solution.
- I used the University of Melbourne HPC system, *Spartan*, to eliminate many candidate transpositions.
- A special thank you to David Oranchak and Jarl van Eycke.

Acknowledgements

- I would have never become involved with solving Z340 without the amazing video series on the Zodiac ciphers by David Oranchak.
- We wouldn't have been able to solve the Z340 without `azdecrypt` by Jarl van Eycke and `zkdecrypto` by Brax Sisco, Wesley Hopper and Michael Eaton.
- The vast efforts to solve the Z340 by the online community on the `zodiackillersite.com`, `zodiackiller.com` and `zodiackillerfacts.com` forums. Much of their work laid the groundwork for our eventual solution.
- I used the University of Melbourne HPC system, *Spartan*, to eliminate many candidate transpositions.
- A special thank you to David Oranchak and Jarl van Eycke.

Dedication

We would like to dedicate our work that culminated in this solution to the victims of the Zodiac killer, their families and descendants. We hope this is a stepping stone towards finding justice for these people.