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 Hitt¹

¹Hitt, Capt. Parker, "Manual for the Solution of Military Ciphers", Army Services Schools Press, Fort Levenworth, Kansas, 1916 $\Box \rightarrow \langle \Xi \rangle \rightarrow \langle \Xi \rangle \rightarrow \langle \Xi \rangle$

- 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.



< 回 > < 三 > < 三 >

- 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.



くぼう くほう くほう

- 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.



★ ∃ ► < ∃ ►</p>

- 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.



(E)

The Z408 Cipher (July 31, 1969)



The Z340 Cipher (November 8, 1969)



The Z32 Cipher (April 20, 1970)

The Map coupled with this code will tell you whore the bomb is set. You have antik next Fall to dig it up. & C \Delta J I B O X J A M 7 A Q O R T G X O F D V C B H C E L & P W D

The Z13 Cipher (June 26, 1970)

This is the Zodiac speaking By the way have you crecked the last cipher I sent you ? My name is -

AENOOKOMOJNAM



同 ト イヨ ト イヨ ト ヨ うくつ

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

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.

・ 同 ト ・ ヨ ト ・ ヨ ト

э.

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

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.

・ 同 ト ・ ヨ ト ・ ヨ ト

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

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.

(回) (モン・・ モン・

= nav

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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 □ □, □ /, △ ≯, Ø.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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 , D, E, , Δ, λ, Ø.

・ 同 ト ・ ヨ ト ・ ヨ ト

= nav

Homophonic substitution example

For example, if the key to encipher E is given by $\{\Delta, \Box, B, Q\}$, then

FORCENTURIESKINGSQUE ENSANDGENERALSHAVERE I. TEDONEFFICIENTCOMMU NICATIONINORDERTOGOV ERNTHEIRCOUNTRIESAND COMMANDTHEIRARMIESAT THESAMETIMETHEYHAVEA LLBEENAWAREOFTHECONS EQUENCESOFTHEIRMESSA GESFALLINGINTOTHEWRO NGHANDSREVEALTNGPREC IOUSSECRETSTORIVALNA TIONSANDBETRAYINGVIT ALTNEORMATIONTOOPPOS INGFORCESITWASTHETHR EATOFENEMYINTERCEPTI ONTHATMOTIVATEDTHEDE VELOPMENTOFCODESANDC IPHERSTECHNIQUESFORD ISGUISINGAMESSAGESOT HATONLYTHEINTENDEDRE RECTPIENTCANREADIT

< 同 > < 三 > < 三 > 、

Homophonic substitution example

For example, if the key to encipher E is given by $\{\Delta, \Box, B, Q\}$, then

FORCENTURIESKINGSQUE ENSANDGENERALSHAVERE LIEDONEFFICIENTCOMMU NICATIONINORDERTOGOV ERNTHETRCOUNTRTESAND COMMANDTHEIRARMIESAT THESAMETIMETHEYHAVEA LLBEENAWABEOFTHECONS EQUENCESOFTHEIRMESSA GESFALLINGINTOTHEWRO NGHANDSREVEALTNGPREC IOUSSECRETSTORIVALNA TTONSANDBETRAYINGVIT A L T N F O R M A T T O N T O O P P O S INGFORCESITWASTHETHR EATOFENEMYINTERCEPTT ONTHATMOTIVATEDTHEDE VELOPMENTOFCODESANDC IPHERSTECHNIQUE SFORD ISGUISINGAMESSAGESOT HATONLYTHEINTENDEDRE RECTPTENTCANREADIT

く 目 ト く ヨ ト く ヨ ト

Homophonic substitution example

For example, if the key to encipher E is given by $\{\Delta, \Box, B, Q\}$, then

FORC ENTURIESKINGSQUE ENSANDGENERALSHAVERE LIEDONEFFICIENTCOMMU NICATIONINORDERTOGOV ERNTHEIRCOUNTRIESAND COMMANDTHEIRARMIESAT THES A METIMETHEYHAVE A LLBEENAWAREOFTHECONS EQUENCESOFTHEIRMESSA GESFALLINGINTOTHEWRO NGHANDSREVEALTNGPREC IOUSSECRETSTORIVALNA TTONS AND BETRAYINGVIT ALINF ORMATIONTOOPPOS INGFORCESITWASTHETHR EATOFENEMYINTERCEPTI ONTH A TMOTIVATEDTHEDE VELOPMENTOFCODESANDC IPHE R STECHNIQUESFORD ISGUISINGAMESSAGESOT HATONLYTHEINTENDEDRE RECIPIENTCANREADIT

FORCANTURIESKINGSQUE NTCAT LLBEENAWABEOFTHECONS GESEALLINGINTOTHEWRO NGHANDSREVEAL INGPREC IOUS S ECRETSTORIVALNA ALINF ORMATIONTOOPPOS ORCESITWASTHETHR IPHER STECHNIQUESFORD SINGAMESSAGESOT HATONLYTHEINTENDEDRE RECIPIENTCANREADIT

く 目 ト く ヨ ト く ヨ ト

э

Homophonic substitution example

For example, if the key to encipher E is given by $\{\Delta, \Box, B, Q\}$, then

FORCENTURIESKINGSQUE ENSANDGENERALSHAVERE LIEDONEFFICIENTCOMMU NICATIONINORDERTOGOV ERNTHETRCOUNTRTESAND COMMANDTHEIRARMIESAT THESAMETIME THEY HAVE A LLBEENAWARE OF THE CONS EQUENCESOFTHEIRMESSA GESFALLING INTOTHEWRO NGHANDSBEVEALTNGPBEC IOUSSECRETSTORIVALNA TTONSANDBETRAYINGVIT ALINFORMATIONTOOPPOS INGFORCESITWASTHETHR EATOFENEMYINTERCEPTI ONTHATMOTI VATEDTHEDE VELOPMENTOF CODESANDC IPHERSTECHN IQUESFORD ISGUISINGAMESSAGESOT HATONLYTHE INTENDEDRE RECIPIENTCANREADIT

FORCANTURI SKINGSOUE ENSANDGENE BAL NICATIONIN O RDERTOGOV COMMANDTHE I RARMIESAT LLBEENAWARE OF THE CONS GESFALLING INTOTHEWRO NGHANDSBEVEALTNGPBEC IOUSSECRET S TORIVAL ALINFORMATIONTOOPPOS INGFORCESITWASTHETHR VATEDT ISGUISINGA MESSAGESOT HATONLYTHE I NTENDEDRE RECIPIENTC A NREADIT

・ 同 ト ・ ヨ ト ・ ヨ ト

э

For example, if the key to encipher E is given by $\{\Delta, \Box, B, Q\}$, then

FORCENTURIESKINGSOUE ENSANDGENERALSHAVERE LIEDONEFFICIENTCOMMU NICATIONINORDERTOGO V ERNTHETRCOUNTRTESAND COMMANDTHEIRARMIESAT THESAMETIMETHEYHAVE A LLBEENAWABEOFTHECONS EQUENCESOFTHEIRMESSA GESFALLTNGINTOTHEWR O NGHANDSREVEALINGPRE C IOUSSECRETSTORIVALNA TTONSANDBETRAYINGVIT ALINFORMATIONTOOPPO S INGFORCESITWASTHETHR EATOFENEMYINTERCEPTI ONTHATMOTIVATEDTHED E VELOPMENTOFCODESAND C IPHERSTECHNIQUESFORD ISGUISINGAMESSAGESOT HATONI, YTHEINTENDEDRE RECIPIENTCANREADIT

FORCANTURIDSKINGSOUB ENSANDGENERALSHAVERE NICATIONINORDERTOGOV ERNTHETRCOUNTRTESAND COMMANDTHEIRARMIESA LLBEENAWABEOFTHECONS GESFALLINGINTOTHEWR O NGHANDSBEVEALTNGPBEC IOUSSECRETSTORIVALN A L T N F O R M A T I O N T O O P P O S INGFORCESITWASTHETHR TMOTIVATEDTHEDE ISGUISINGAMESSAGESOT HATONLYTHEINTENDEDRE RECIPIENTCANREADIT

Homophonic substitution example

For example, if the key to encipher E is given by $\{\Delta, \Box, B, Q\}$, then

FORCENTURIESKINGSQUE ENSANDGENERALSHAVERE LIEDONEFFICIENTCOMMU NICATIONINORDERTOGOV ERNTHETRCOUNTRIESAND COMMANDTHEIRARMIESAT THESAMETIMETHEYHAVEA L L BEENAWAREOFTHECONS EQUENCESOFTHEIRMESSA 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 T N G P R E C IOUSSECRETSTORIVALNA T TONSANDBE TRAYINGVIT A L TNFORMATTONTOOPPOS INGFORCESITWASTHETHR EATOFENEMYINTERCEPTI O NTHATMOTIVATEDTHEDE V E L O P M E N T O F C O D E S A N D C I PHERSTECHNIQUESFORD ISGUISINGAMESSAGESOT H A T O N L Y T H E T N T E N D E D R E RECTPTENTCANREADIT

F ORCANTURIDSKINGSQUB NSANDGENERALSHAVERE TCATTONTNOBDEBTOGOV E RNTHEIRCOUNTRIESAND L L B E E N A W A R E O F T H E C O N S G E S F A L L T N G T N T O T H E W B O N GHANDSREVEALINGPREC TOUSSECRETSTORTVALNA TONSANDBETRAYINGVIT A LINFORMATIONTOOPPOS **GEORCESTTWASTHETHR** HATMOTIVATEDTHEDE V ELOPMENTOFCODESANDC T SGUTSINGAMESSAGESOT TONLYTHEINTENDEDRE R ECIPIENTCANREADIT

・ 同 ト ・ ヨ ト ・ ヨ ト

э

Homophonic substitution example

For example, if the key to encipher E is given by $\{\Delta, \Box, B, Q\}$, then

FORCENTURIESKINGSQUE ENSANDGENERALSHAVERE LIEDONEFFICIENTCOMMU NICATIONINORDERTOGOV ERNTHETRCOUNTRTESAND COMMANDTHEIRARMIESAT THESAMETIMETHEYHAVEA LLBEENAWABEOFTHECONS EQUENCESOFTHEIRMESSA GESFALLINGINTOTHEWRO NGHANDSREVEALTNGPREC IOUSSECRETSTORIVALNA TTONSANDBETRAYTNGVTT A L T N F O R M A T T O N T O O P P O S INGFORCESITWASTHETHR EATOFENEMYINTERCEPTT ONTHATMOTIVATEDTHEDE VELOPMENTOFCODESANDC IPHERSTECHNIQUE SFORD ISGUISINGAMESSAGESOT HATONLYTHEINTENDEDRE RECTPTENTCANREADIT

FORCANTURI SKINGSOUB ØNSANDG∆N□RALSHAVBRØ Δ D O N \Box F F T C T **B** N T C O M M U ONINORD**P**RTOGOV ▲ R N T H □ T R C O U N T R T **B** S A N D COMMANDTH**Q**IRARMI**D**SAT \Box S A M **B** T I M **Q** T H Δ Y H A V \Box A LLBBON W A R. ΔOF H C B O U O N C A S O F T H D I R M B S S A G ♀ S F A L L I N G I N T O T H △ W R O NGHANDSR**DVB**ALINGPR**9**C I O U S S A C R 🗖 T S T O R R T W A S T H A T H R ORC**P**S **D**AT BNOM NTARC**П**РТТ V Α Τ Β Ο Τ Η **Ο** Ο Δ MOT V T L O P M ΒN OFCOD**9**SANDC IPH∆RST□CHNIQU**B**SFORD INGAM**D**SSAG**D**SOT HATONLYTHDINT**B**ND**9**DR**4** R C C C P T B N T C A N R O A D T T

- 4 同 ト 4 ヨ ト 4 ヨ ト

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		6		4	7		9	12	11	10
f		r		е	n	t	u	r	i	е	
k	i	n			q	u	е	е	n		
n	d	g	е	n	е	r	a.	1		h	
∇	е	r	е	1	i	е	d		n	\overline{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

・ 同 ト ・ ヨ ト ・ ヨ ト

э

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		6		4	7		9	12	11	10
f		r		е	n	t	u	r	i	е	
k	i	n			q	u	е	е	n		
n	d	g	е	n	е	r	a	1		h	
\mathbb{V}	е	r	е	1	i	е	d		n	$\overline{\mathbb{W}}$	

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

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

・ 同 ト ・ ヨ ト ・ ヨ ト

э

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

< 同 > < 回 > < 回 > …

э.

- 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	0	r	с	е	n	t	u	r	i	е	s
k	i	n	g	s	q	u	е	е	n	s	a
n	d	g	е	n	е	r	a	1	s	h	a
v	е	r	е	1	i	е	d	0	n	w	q

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

fknv oide rngr ngei esnl cgee ture uead relo saaq eshw insn

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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	0	r	с	е	n	t	u	r	i	е	s
k	i	n	g	s	q	u	е	е	n	s	a
n	d	g	е	n	е	r	a	1	s	h	а
v	е	r	е	1	i	е	d	0	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

(日本) (日本) (日本) 日本

- On July 31, 1969, the Zodiac mailed his first cipher to the press.



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



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.



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.



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: 7408
- 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.



くロト くぼト くヨト くヨト

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: 7408
- 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 Bettve Harden.



- 4 同 ト - 4 同 ト

The Hardens' Method

The Hardens' guessed a 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 ILIFZKILLXOR \rightarrow 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!



< ロ > < 同 > < 三 > < 三 >

The Hardens' Method

- The Hardens' guessed a 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, /ALB, /PLB, /ALL all decode to KILL.
- Then it follows that ILIFZKILLXOR → 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!



< ロ > < 同 > < 三 > < 三 >

- The Hardens' guessed a would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess $\blacksquare \to L$ and $\blacksquare \to L.$
- Then guessed /UBL, /ALB, /PLB, /ALL all decode to KILL.
- Then it follows that ILIFZKILLXOR → 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!



< ロ > < 同 > < 三 > < 三 >

- The Hardens' guessed a would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess $\blacksquare \to L$ and $\blacksquare \to L.$
- 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!



くロト くぼト くヨト くヨト

- The Hardens' guessed a would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess $\blacksquare \to L$ and $\blacksquare \to L.$
- 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!



くロト くぼト くヨト くヨト
- The Hardens' guessed a would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess $\square \to L$ and $\blacksquare \to L$.
- Then guessed /UBL, /ΔLB, /PLB,
 /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLXOR \rightarrow 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!



< (7) >

(<)</pre>

- The Hardens' guessed a would decrypt to double letters.
- The most common double letters in English is LL.
- The Hardens' made the guess $\blacksquare \to L$ and $\blacksquare \to L.$
- Then guessed /UBL, /ΔLB, /PLB,
 /ΔLL all decode to KILL.
- Then it follows that ILIKZKILLXOR \rightarrow 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!



4 3 5 4 3 5 5

The Zodiac's 408 Cipher

The Hardens' Solution

|--|

ANP/Z/UBEXORA 9XTE W/St Z G & F C/A HP E/K I/P PNORS MFY N/4 I/I A N/Q Y DA SOKABBPORAU PA EI Ø 3/8 1 F TBECAN q Ë RR INTHE/FO 9=18 9 DA 5/F 9 E HO AST 0.0-84 DAN RN-LIXELO APCB/19/SE GERGY HANN ANNALLOFA L La/PBB/2XPEHMUAR La/KILLSO METHINGG Ŀ

Doves found to men A and S. Seriors

OTA 72 K/0 9/2 VES/HE/7 5 L L/n ETA EIN Ä 12 D3/ TAP EIB AP ISOME/MY/SLAVES JAV IL D EVALAND 0 Elot of RUD HO OYD DASPW 0 U d 1 NGI OC AUSE GYKE AABALLE 2 0 M/A/B 41 PI FBX 2 BXADO KALIA $\frac{\partial}{x}$ 13 Elis e 1 TAG OF CTINCO FSLAV - 6 BEREM 5/FOR/MY/A 1 I+ 50 5X RITETEMETHI AAWIO OFHMA Same E

128

PAGE 3

< ロ > < 同 > < 回 > < 回 > < 回 > <

PRES 70

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.

Open file	Solve	Substitution + columnar rearrangement	Task: substitution (using 2 CPU threads)
Save state	Pause	Substitution + columnar transposition	
		Substitution + crib grid	Items: 34 Items per second: 1.03 MIPS: 1.15
Load state	Stop task	Substitution + crib list	AVG score: 23084.45 IOC: 0.06542 PC-cycles: 12443
	Swap	Substitution + nulls and skips	
put window	-	Substitution + polyphones	Output window
P/Z/UB%kOR=	X=B		Score: 23084.45 IOC: 0.0654 Multiplicity: 0.1323 Seconds: 0.1
V+eGYF69HP@K	qYe		Repeats: EBECAUSE KILLING THEMOAT BECAUSE WILLBE SLAVES
JY^UIk7qTtNQ	(D5)		PC-cycles: 12443
(/9#BPORAU%f	RigE		
^LM2Jdr\pFHV	(e8Y		I LIKE KILLING PEOPLE BECAUSE IT IS SO MUCH
+qGD9KI) 6qX8	SzS (FUN IT I AMORE FUN THAN KILLING WILD GAME
ItIYE108qGBT	QS#B		IN THE FOR REST BECAUSE MAN IS THE MOAT DANGER
i/P#B@XqEHMU	RRk		TUE AN AMAL OF ALL TO KILL SOMETHING GIVES
(KqpI)Wq!85L	(r9#		ME THE MOAT THRILLING EXPERENCE IT IS EVEN
PDR+j=6\N(eE)	JHEF		BETTER THAN GETTING YOUR ROCKS OFF WITH A
pOVWIS+tL)1	R6H		GIRL THE BEST PART OF ITIATHAE WHEN I DIE
and Itr/de/6	CUQA		I WILL BE REBORN IN PARADICE AND ALL THE
SMSRUC%L) NVE	CH=G		I HAVE KILLED WILL BECOME MY SLAVES I WILL
I OKSYSLMINA	2(P		NOT GIVE TOU HI NAME DECAUSE TOU WILL THI
UDKA9#DVW\+V	TUP		TO SLO I DOWN OR A TOP HI COLLECTING OF SLAVES
-31110267023	1111		FOR MI WEIER LIFEL DE ORIEIE MEINN FIII
K) SCE/ STRLER	100		
OTEDUct dVg	1A3D		
ZaCVEF TVLOR	U.t.		
LEBYO-YADd) 7	lar		
adffeatpopyo	ThGo		
ATTTA SITAR	20%6		
Xr9WI6gEHM)	UIk		
vquinty			

→ □ → → 三 → → 三 → へへや

- On November 8, 1969, the Zodiac mailed his second cipher to the San Francisco Chronicle.



・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.



- 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.



A 1

(E)

- 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.



(E)

- 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.



-∢∃⇒

• 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.



- 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.



- 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.



- 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.



-∢ ⊒ ▶

- 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

2.25.14		heri.	
10.728 I		•	
他们就			
		-	
Qc32 and Qc35 checked	and and a set of the set		
Plaintext values obtait	against previously	recovered hour	
where one ciphertext	neo using old key (disregarding (-	negative.
letter) disclosed from	alue represented mo	re than one -la	stances
text. Approximately o	sencies similar to	expected Feeld	intext.
appearing in previous	to of cipher text i	s new (auch signal	n plain
key as part of combined	Attempts	to decrupt und	not
linear and route trans	ion cryptosystem: -	Denative Til	ng o1q -
and the second se	osition.	irighterve. Iri	PG
Message overall, first	half is a little in		
use of variants. Possi	lair, and last half	examined for	
subsequent EDP rune	Dilities (listed be	low] (neering	yclic.
ATY PE FAT		and incorporat	ed into
DL FOT	JU MJE NZ SY	AL	
	07	TI UPDE /	 Second and a second and a secon
Qc35 too short for analy	过去,加方大公公司的正式	2011 - P P P P P P P	그녀가는 이것
portions identical to C	als by itself. And	granning atta	in the second second
and with third and found	55 Cipher text (i.e	. HFR WDT	pted on
ing used by Zodiac)	" lines as "Christa	ass" (known ad	ind UZ)
198 October 1		terret inter	sebett=
Un yea2:			
Pho			
, copy runs sliding word th	rough measure		
situations (no matching	of warmessage excep	t for impossibl	
Will, your th	has bas ants/: kill	, killed, killi	na .
bic veriejo,	is nus come, Sacram	ento, San Franc	icon
TOCKS OFF, Slaves, colleg	A REAL PROPERTY AND A REAL	get you	
FDD	and staves, colle	ting of slaves	18 9 18 18 18 18 18 18 18 18 18 18 18 18 18
situate sliding word that	ough messages		• • • • •
(B. a tions, with variants	Grouped abes excep	t for impossib	1a
COLLEGO, BME, M RI)	ph other above on c	ne run and var	Anke
collocating of slaves, kil	1. killing hilling	y thing, slaver	i i i i i i i i i i i i i i i i i i i
staves.	, willed,	my afterlife.	
Hand appearent			
that mongranning done wit	nessage as under	Contraction of the second second	and white the
and roomed Dackwards, w	citten columnariu	n and on assump	tions
the second line backward	tc.	first line forw	ard
Concentrated			
areas of anac	ramming		
Contract of a second		 Statistic 	19
"9" as O with S. R. O. and	E	of the production of	5.051.00
Area of 205 to as K and	"F" and "B" as I	and the stands of the	Service - Contra
have a, small 296, with 1	commit, about +-	aber Children .	and the second
now Lispe in tell t, u	ntill t. will w	enit that, shall	1
Identification of a		ur rocks, has h	een s.
componing wood of "+O4" by	examining Zodine -	C CONTRACTOR OF A	100
values for B three-letter	reversal. Evoluted p	lain text for a	(1994) - 19 B
"F" at E and, M, F, which	re in frequent	on of this to i	nclude
Word "Zodine" as R. and	vice-versa.	tact with the t	hree
Word "Death in the first	20 and last 10 -1-	AN ISSAN	Alexander &
beach machine" for en	tire message	ces.	
	meessage.		10 N. T. 11
	5		
CONTRACTOR AND	he was not a start a start		13
and the second	the second se		
and an extension of the second second	Cartina Lange A Species	Same stand water	Charles and the state of
rener de la constant de la constant	e el Albani - Materi		Street of the

- T

- 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

1999.4	-	3er	
100 A 100	•		
1.402046			
QC32 and Qc35 checked acadeat	a i dan da ara		
Plaintext values obtained using	reviously reco	vered keys	
where one ciphertext value more	old key (disr	egarding ineta	getive,
letter) disclosed frequencies	esented more t	han one plaint	nces
text. Approximately 20% of cia	imilar to expe	cted English n	Late .
appearing in previous messagel	ner text is new	v (symbols not	TO THE PARTY OF
linear part of combination cryp	forwerents to c	ecrypt using	blo
and route transposition.		tive. Tried	
Message overall ci			·*
use of wariants, first half, and	last half	1. C. C. C. S. A.	
subsequent FDD Possibilities	(listed halow)	mined for cycl	ic.
ATV OF	ourow)	incorporated	into
ALL TOP OF ST JU MIS	NZ EL -:	1. F S 182. F 1	
	112 37 41	AL BOAD	
Qc35 too short for analysis	 Qual AS 3 [1] 	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
portions identical to Copp 1	tself. Anagram	mine attents	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
and with third and fourth line	text (i.e., H	(ER), WRT per	2 OD
ing used by Zodiac).	"Christmass"	(known mierro	02)
00.0000		trune myoshe	/11-
<u>00 4635</u>			
EDP Time ald de			
situations filding word through mes	5200 August 6	- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	
I shall, T will	ts), kill in	r impossible	
Lic Vallejo, Vour time has co	me, Sacramonte	iled, killing,	
rocks off, slaves off	and a district	, San Francisc	o, .
Collecting sia	Ves. commenter	get your	
EDP runs sliding word the		or slaves.	
situations, with vamants ugh mest	sages except fo	T-Imposed Lt-	
B-Q, TOO, EME, and BL DO COUPED	above on one r	un and vamined	
collecting of slaves, kill, kills	run: do my th	ing, slaver	16 11 14
contoction of slaves.	g, killed, my	afterlife.	
Hand apparent		the state of the second	
that message hig done with message	as written	1.11.11.11.1	1. 10 10 10 1 10 10 10 10 10 10 10 10 10 1
and second line backwards, written co	lumnarly fim	d on assumptio	ins .
the backward etc.	connerry, firs	t line forward	
Concentrated arous of			
areas or anagramming:		1,000,000	
"+" as L. T. S. P. O	end e doura el	es estrait - es-	
"9" as O with "A" as P and E		numbers	
Area of 285 to 296 with and	"B" as L/		
have a, small m, tell t	about to, shit	that there is	· · · · · · · · · · · · · · · · · · ·
now Lesee in.	will w, your r	ocks, has here	
Identification of "+09" by another	1997 A.	ooka, nas beer	18, 🖉
commonly used three-letter	g Zodiac plain	text/for a	
The start B, M, F, which are in fa	 Expansion o 	f this to incl	unda E
Word Brade B" as R, and viceaver	equent contact	with the thre	- Fi
Word "Deset in the first 20 and 1	5d, 10 - 1	A.C. BRANNIN .	E
beech machine" for entire mes	sage in places.		1997 - M
	auge.		fas
Stellar restriction 5			
A MARKED AND SHOT A CONTRACT OF A CONTRACT O	Contraction of the		/×
and the state of the second second second second	See Lines and the	LEMERAL MERTEN	Constant State
Manager and a superior of the second s	and the second second	Come o restabilita	

- T

- 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

			A		÷ .
				· · ·	
-5.23					
Qc32 and Qc35 checked parts	de la Carlo de				
Plaintext values obtained	st previously	recove	red keyr	Decast	
letterl dichertext value	represented	(disreg	arding in	stances	е.
text. Approximately requenci	es similar to	ore tha	n one pla	intext.	
appearing in previous of	cipher text :	is new	eg Englis	h plain.	
key as part of combination	ge). Attempts	to de	Crypt usi	not not	
intear and route transposit	lon.	negat:	ive. Tri	ed	
Message overall fines have					- C
use of variants. Possibility	and last hal	f exami	ned for		
subsequent EDP runs.	les liisted b	elow) j	ncorpora	ted inte	
AIX BF EOF JU	ALL STATE	1.1	1.1.27	eeo mico	
2014년 - 1915년 1917년 - 19 1917년 - 1917년 - 1917년 1917년 - 1917년 -	NZ 53	41	LPOD >	1.05.00	
Qc35 too short for analysis	maria and and		2.555	- 10 C	
and with identical to Qc33 c	phen tout ()	agram	ing attem	pted on	
ing used by Zadin fourth lin	les as "Cheirt	e., HE	N, WBI,	and UZ)	
(2001ac).	-	- 5 5 6	(known mi	sspell-	
On Qe32:					
EDP Time ald at					
situations (no month through	message exce	nt fer			
I shall, I will, your time ba	riants): kil	1, kill	ed. kills	e	· . •
bre vellejo.	s come, Sacran	mento;	San Franc	isco	
source off, slaves, collecting	STOVES		get you	r	
EDP runs sliding word the	COALC	reting	of slaves	e surda	
situations, with vagiants group	messages exce	pt for.	impossib	10	
collection ema m RI) on ot	her run:	one run	and var	iants	
collection of slaves, kill, ki	lling, killed	my thin	9, slave	s ,	
			corize,		
that magramming done with mes	sace as under		- Andrews	相对的	(k) = 0
and second line backwards, writte	n columnarly	en and	on assump	otions	
Time backward etc.		. ifst	line forv	≉ard	
Concentrated areas of anaoranm					
141 as 1 7 a -	ing:	et es	Softial?		
"9" as O with "A" o, and E		rug ta i	wades.		
Area of 285 to 296, with T	and "B" as Li	(***))) 1	a na sana sa		
have a, small m, tell t, until	it, about to,	shit t	that, tha	11	
Identification of another	t, will w, y	our roo	ks, has	been s.	11
commonly used three lot by exam	ining Zodiac	nlain a	24	14-1-1 C	- 1
values for B, M, F, which and	rsal. Expans	ion of	this to	and other	- 1
Word "Zeddand "B" as R. and vice	n irequent co	ntact w	ith the	three	- 6
Word "Death machine first 20 a	nd last 10 pl		C . Stewart	- A	
for entire	message.	aces.			
	•			2011 - T	1
	6				un fi
	And and a state of the				· 18
The second provide and the second	SANGE LANGER	1.1.1.1	CALL MENT	Electrone Co.	100
BREEDERS A. S. C. C. AND CARDER S.					
					_

- T

- 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

			A		÷ .
				· · ·	
-5.23					
Qc32 and Qc35 checked parts	de la Cara de				
Plaintext values obtained	st previously	recove	red keyr	Decast	
lettonl diphertext value	represented	(disreg	arding in	stances	е.
text. Approximately requenci	es similar to	ore tha	n one pla	intext.	
appearing in previous of	cipher text :	is new	eg Englis	h plain.	
key as part of combination	ge). Attempts	to de	Crypt usi	not not	
intear and route transposit	lon.	negat:	ive. Tri	ed	
Message overall fines have					- C
use of variants. Possibility	and last hal	f exami	ned for		
subsequent EDP runs.	les liisted b	elow) j	ncorpora	ted inte	
AIX BF EOF JU	ALL STATE	1.1	1.1.27	eeo mico	
🗱 소문을 통하는 것을 가지 👘 🖓 이 문지?	NZ 53	41	LPOD >	1.05.00	
Qc35 too short for analysis	maria and and		2.555	the state of the s	
and with identical to Qc33 c	phen tout ()	agram	ing attem	pted on	
ing used by Zadin fourth lin	les as "Cheirt	e., HE	N, WBI,	and UZ)	
(2001ac).	-	- 5 5 6	(known mi	sspell-	
On Qe32:					
EDP Time ald at					
situations (no month through	message exce	nt fee			
I shall, I will, your time ba	riants): kil	1, kill	ed. kills	e	· . •
bre vellejo.	s come, Sacran	mento;	San Franc	isco	
source off, slaves, collecting	STOVES		get you	r	
EDP runs sliding word the	COALC	reting	of slaves	e surda	
situations, with vagiants group	messages exce	pt for.	impossib	10	
collection ema m RI) on ot	her run: da	one run	and var	iants	
collection of slaves, kill, ki	lling, killed	my thin	9, slave	s ,	
			corize,		
that magramming done with mes	sace as under		- Andrews	相对的	(k) = 0
and second line backwards, writte	n columnarly	en and	on assump	otions	
Time backward etc.		. ifst	line forv	≉ard	
Concentrated areas of anaorann					
141 as 1 7 a -	ing:	e trans	Softial?		
"9" as O with "A" o, and E		rug ta i	wades.		
Area of 285 to 296, with T	and "B" as Li	(***))) 1	a na sana sa		
have a, small m, tell t, until	it, about to,	shit t	that, tha	11	24
Identification of another	t, will w, y	our roo	ks, has	been s.	11
commonly used three lot by exam	ining Zodiac	nlain a	24	14-1-1 C	- 1
values for B, M, F, which and	rsal. Expans	ion of	this to	and set	- 1
Word "Zeddand "B" as R. and vice	n irequent co	ntact w	ith the	three	- 6
Word "Death machine first 20 a	nd last 10 pl		C . Stewart	- A	
for entire	message.	aces.			
	•			2011 - T	1
	6				un fi
	And and a state of the				· 18
The second provide and the second	SANGE LANGER	1.1.1.1	CALL MENT	Electrone Co.	100
BREEDERS A. S. C. C. AND CARDER S.					
					_

A B M A B M

- 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

nd d		140°	
			· · ·
Qc32 and Qc35 checked again	t mouleur		
where one sister obtained u	sing old key (d)	overed key:	negative.
letter) disclosed from the second	represented more	regarding ins	tances
text. Approximately 20% of	is similar to exp	ected English	ntext.
key as part previous messac	(e). Attempts to	w (symbols h	ot
linear and route transition of	ryptosystem: - ner	decrypt using	old -
Meesse	on.	interes. iried	5 # 1 21
use of wariants, first half,	and last half		
subsequent EDP runs	ies (listed below	amined for cy	clic.
ALX BE FOT W	And and a second	, incorporate	d into
	IJE NZ S) TI	LPOR ZA	
Qc35 too short for analysis	What was done as it		
portions identical to Oc33 of	y itself. Anagra	mming attemnt	ind all
ing used by Zadd fourth lin	es as "Christman	HER>, WBI, ar	d UZ)
5 Uy 2001ac).		(known miss	pell-
On Qc32;			
EDP runs elide			
situations (no matching word through	message except f	or imposed by	
I shall. I will, your time had	lants): kill, k	illed, killin	
brocks of a slaves	come, sacrament	, San Franci	sco,
For collecting	slaves, collecti	get your	
situations sliding word through	00553000	s exeves.	
(B-q Too and variants grou	ped above on one	or impossible	
collecting of slaves, bill	her run: do my t	hing, slaves	nts
correction of slaves.	lling, killed, my	afterlife.	
Hand anagramming does white		C. Calendaria	hatta sa
that message backwards, written	age as written a	nd on assumet	1000
and second line backward etc.	columnarly, fir	st line forwa	rd
Concentrated areas of			
nagrams	ng: the second of the	Co. S. August 1	
"9" as O with S. R. O. and E	- 문서의 기업을 내용하는 것 같	a program.	
Area of 285 to 296 with and "F"	and "B" as L/		1996 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 -
have a, small m, tell t, untill	it, about to, shi	t that, shall	80 - L
Identification of a second	c, will w, your	rocks, has be	en s.
commonly used three-letton	ining Zodiac plai	n text from .	e
values for B, M, F, which are in	sal. Expansion	of this to in	clude
Word "Zodiac" is as R. and vice-	versa.	t with the th	ree
Word "Death machine" forst 20 ar	d last 10 places	A States	America
intentine for entire	message.		6
	- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1		
Station of the local states	5		
and the second	5		1
	5 Jahr Disserter	er skolente	america and

• = • • = •

- 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

1998 - A		360°	
Qc32 and Qc35 checked acadeat	Acres 1		
Plaintext values obtained using a	lously reco	vered key: n	enative
letterl disclored value represe	nted mone th	egarding inst.	ances
text. Approximately 200 and simi	lar to expen	ted Ecolist	text.
appearing in previous message	text is new	(symbols not	olain.
linear and of combination cryptos	vetopts to c	ecrypt using	old .
and route transposition.	, occas, nega	tive. Tried	- # 1 - 2 ·
Message overall, first half, and i	él incluia		
subsequent Fon. Possibilities (1)	sted half exa	mined for cyc	lic
ATY DE	aced below)	incorporated	into
CHA DE EOF JU MID	12 53 21	ting the second	
0e35 tas -1	= 22, 34	CPDG ZA	
portions identical analysis by itse	lf. Anagram	A State	
and with third and founth to her t	ext (i.e., H	FR> WDT	d on
ing used by Zodiac).	"Christmass"	(known misso	02)
On Qe32:			****
Pho			
situations (inding word through messar			
I shall, I will	t kill kill	impossible	
bic Vallejo, wour time has come.	Sacramento	San Enged	
rocks off, slaves, collecting slaves		get your	:0,
EDP runs sliding word th	. correcting	of slaves.	
situations, with variants using messag	es except fo	T-Imposed L1-	
Collection, emz, and BI) on other mu	ove on one r	un and varian	te
collection of slaves, kill, killing,	killed my	ing, slaves,	
and the second sec	Sec	arteriife,	
that magranning done with message as	and the second	1.	11 10 20 30 30 10
and second line backwards, written colum	narly, fire	on assumptio	ons
and alle backward etc.		tine forward	3 .
Concentrated areas of anagramming:			
"+" as I T P P		scientiat? Ltd.	
"9" as O with "A" as P and E	1000 CQ 10	second et al.	11 C 11
Area of 285 to 296, with I commit	as L/	di tin dan sa	
now Liepe in tell t, untill t, wi	but to, shit	that, shall	1 1
Identification of "+04" but	a w, your r	ocks, has bee	ns,
commonly used three-letter mounting	odiac plain	text for a	C
"F" as F and The F, which are in frem	expansion or	this to inc.	lude
Word "Zodiac" in the R, and vice-versa.	contact	with the thre	ee
Word "Death machine" for and last	10 places.	같은 문화일에서는 이것	i terre de la 🗌
for entire messag	e.		·
sector instruction for the sector of the			1.1
A second strategy of the second strategy o	1 Carnes Sugar	- And Anna - Pitt	TO DE CONTRACTOR
ADDREAM MANAGEMENT ADDREAM STATE AND ADDREAM ADDREAM ADDREAM ADDREAM ADDREAM ADDREAM ADDREAM ADDREAM ADDREAM AD	4-10-2010/02/2013	NATIONAL CONTRACTOR	bubble the cost of the

(E)

- 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 and			
Plaintext values obtained using previous	ly recovered	key: negat	Sec. 1
letterl dichertext value represented	y (disregard	ing instance	cive,
text. Approximately requencies similar	more than o	ne plaintext	
appearing in previous of cipher tex	t is new (es	English plai	in energy. (
key as part of combination and Attemp	pts to decry	of using ald	
linear and route transposition.	n: negative	Tried	
Message overall fine has			
use of wariants, Possibility and last h	alf examiner	for any it.	
subsequent EDP runs.	below) inco	TPOTated in	i i
ALX BE EOF IN MID THE			
	5) AT C. 6	A/ DC	
Qc35 too short for analysis bu de		전 2017년 11년	
and with identical to Qc33 cipher taut	Anagramming	attempted o	2 1
ing used by Zadd fourth lines as "Ches	1.e., HER),	WBI, and UZ	<u>;</u>
2001ac).	(kno	own misspell	÷
Un Qc32;			
EDP runs elide			
situations (no matching word through message ex	cent for in-		
I shall, I will, your time bariants): k	ill, killed.	killin	· · · · ·
Bic veliejo,	ramento, San	Francisco	
staves, collecting slaves, collecting slaves, col	,9	et your	
EDP runs sliding word the	arecting of	slaves.	
situations, with variants grouped area	ccept for im	ossihle	
collection enz, of RI) on other runs	on one run ar	d variants	
collection of slaves, kill, killing, kill	od thing,	slaves,	
	ing arcor		
that anagramming done with message as	ولأرد حرمه درو	a. 1997年1月1日日日	5.898.6.48
and second line hwards, written columnari	tten and on	assumptions	
and backward etc.	// virst lin	e forward	
Concentrated areas of anagramming.			
"4" as I w a		haf"	
"9" as O with "A" o, and E	could be made	tege i de com	
Area of 285 to 296, with and "B" as	L/	i provenské se kontre pasiel. Konsta	
have a, small m, tell t, until) + will	o, shit that	+ shall	1.12
Identification of another to will w.	your rocks,	has been s	
commonly used three lotter by examining Zodia	c plain toke	4.	
values for B, M, F, which are	nsion of thi	s to includ	
Word "Zaddard" B" as R. and vice-versa	contact with	the three	
Word "Death machine first 20 and last 10	alassa (See	Charles and Street	
for entire message.	praces.		
		A 550-1-1	1
			1. 1. 1
5			
5			- 1a
5	saster de	Ander Electron	atan

글 > : < 글 >

• Perhaps it's just gibberish? Then why did Zodiac correct the **X**?

- 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.



- Perhaps it's just gibberish? Then why did Zodiac correct the **X**?
- 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.



- Perhaps it's just gibberish? Then why did Zodiac correct the **X**?
- 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.



- Perhaps it's just gibberish? Then why did Zodiac correct the **X**?
- 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.



(E)

- Perhaps it's just gibberish? Then why did Zodiac correct the **X**?
- 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 **EB**, with 6 occurrences.

 $\Delta \Box P / Z / U B \Box A O R = 9 X = B$ WV+36YF0AHP0KI0Y3 MJYAUIXAØTINQYD●+ S ¢ / A ■ B P O R A U □ ∃ R J Q E XALMZJQ9\9FHVW3▲Y □+06D∆KI+000X▲●+5↓ RNLIYEJOAØ6BTQS L Q / P B D X D E H M U A R R X BPDR+TxO\NØJEUH) ZJ90VWI O+1L+JAROH **ADCXD/ED/RVTDRUT** P●M▲RUL@L+NVEKH×6 **ΥΤΤΙΧΟΔ**ΑΓΗ]ΝΑΦΖΦΡ +U93A∆ ■ B ∨ W \ + ∨ T ⊥ O P AZSAJJUJOAD+600IM $N \rightarrow S \supset E / \Delta \square \square Z \neg A P \square B \vee$ 9 3 X Ø W Ø D F M A O + O A A A B OTORUD+DOYODASOW VZ36YKEDTYAADMLLD HIFBXA + XADONALIZO D 3 0 B B 0 3 0 P 0 R X Q F B 6 3 ZOJTLODAJI+9BPQWO **VEXADVIODEHM** ILIKEKILLINGPEOPL EBECAUSEITISSOMUC **HFUNITISMOREFUNTH** ANKILLINGWILDGAME INTHEFORRESTBECAU SEMANISTHEMOATDAN GERTUEANAMALOFALL TOKILLSOMETHINGGI VESMETHEMOATTHRIL LINGEXPERENCEITIS EVENBETTERTHANGET TINGYOURROCKSOFFW **ITHAGIRLTHEBESTPA** RTOFITIATHAEWHENI DIEIWILLBEREBORNI NPARADICESNDALLTH EIHAVEKILLEDWILLB ECOMEMYSLAVESIWIL LNOTGIVEYOUMYNAME BECAUSEYOUWILLTRY TOSLOIDOWNORSTOPM **YCOLLECTINGOFSLAV** ESFORMYAFTERLIFEE BEORIETEMETHHPITI

ヘロト 人間 とくほ とくほ とうせい

However, by the nature of the encipherment scheme, there are other ways to encode $\ensuremath{\operatorname{LL}}$.

A P / Z / U B A X O R T 9 X T B WV+36YF0AHP0KI0Y3 ΜΙΥΛΟΙΧΑΩΤΙΝΟΥΡΦ S¢∕∆**≣B**PORAU⊠ ∃RJØE XALMZJQ9N9FHVW3AY □+06DAKI+00X▲●+50 RNLIYEJOAØ6BTQS L Q / P B D X D E H M U A R R X BPDR+T×O\N¢3EUH) Z) 9 O V W I O + 1 L + J A R O H IADROTY9\09/0XJQA P ● M ▲ R U ⊥ □ L ↔ N V E K H ≍ 6 +U9XA∆ ■ B ∨ W \ + ∨ T ⊥ O P MINDO + CAOEUFLRZX M $N \rightarrow S \supset E / \Delta \square \square Z = A P \square B V$ OTORUS+DOYODASOW VZ36YKEDTYAAGELID HIFBXA+XADQ\ALIK0 D 3 0 B B 0 3 0 P O R X Q F B 6 3 ZOJTLODAJI+9BPQWO **KIDA** ILIKEKILLINGPEOPL EBECAUSEITISSOMUC **HEUNITISMOREFUNTH** ANKILLINGWILDGAME INTHEFORRESTBECAU SEMANISTHEMOATDAN GERTUEANAMALOFALL TOKILLSOMETHINGGI VESMETHEMOATTHRIL LINGEXPERENCEITIS EVENBETTERTHANGET TINGYOURROCKSOFFW ITHAGIRLTHEBESTPA RTOFITIATHAEWHENI DIEIWILLBEREBORNI NPARADICESNDALLTH EIHAVEKILLEDWILLB ECOMEMYSLAVESIWIL INOTGIVEYOUMYNAME BECAUSEYOUWILLTRY TOSLOIDOWNORSTOPM YCOLLECTINGOF **ESEORMYAETERLT** BEORIETEMETHHP э < = > < = >

The second most common repeating bigram is \mathcal{P} , with 4 occurrences.

 $\Delta \Box P / Z / U B \Box A O R = 9 X = B$ WV+36YF0AHP0KI9Y3 ΜJYΛUIXΔΩΤLNQYD •• 5¢/ABBPORAUG FRJØE XALMZJQ9\9FHVW3▲Y □+960∆KI+000X▲●+50 RNLIYEJO▲96BTQS■B L Q / P B B C X P E H M U A R R X BPDR+TxO\Nø3EUHXF ZJ90VWI0+1L+JAROH A D R D T Y S \ O Z J Q A P ● M ▲ R U L □ L ↔ N V E K H ⊼ 6 + UMINDO+CAOEUFLRZXA N X + S D E / A B B Z T A P B V $\square OT = RU + \Box Q$ VZ36YKEDTYAAGELLD HIFBXA+XADO\ALIKD ■ 3 4 ■ ■ 0 3 ● PORXQF @ 6 3 ZOJTLODAJI+9BPQWO **VEXADVIODEHWerdin**

TLIKEKILLINGPEOPL EBECAUSEITISSOMUC **HFUNITISMOREFUNTH** ANKILLINGWILDGAME INTHEFORRESTBECAU SEMANISTHEMOATDAN GERTUEANAMALOFALL TOKILLSOMETHINGGI VESMETHEMOATTHRIL LINGEXPERENCEITIS EVENBETTERTHANGET TINGYOURROCKSOFFW ITHAGIRLTHEBESTPA RTOFITIATHAEWHENI DIFIWILLBEREBORNI NPARADICESNDALLTH EIHAVEKILLEDWILLB ECOMEMYSLAVESIWIL LNOTGIVEYOUMYNAME BECAUSEYOUWILLTRY TOSLOIDOWNORSTOPM **Y**COLLECTINGOFSLAV ESFORMYAFTERLIFEE BEORIETEMETHHPITI

ヘロト ヘ団ト ヘヨト ヘヨト

3

The Z408 has 62 repeating bigrams.

 $\Delta \square P / Z / U B \square > O R = 9 X = B$ WV+36YF0ΔΗΡΩΚΙΩΥ3 MJYAUIXAQTLNQYD ●● S ¢ / A B B P O R AU A TR J Q E XALMZJOSN9FHVW3AY □ + Ø 6 D △ K I ↔ Ø Ø × ▲ ● ┿ 5 ϕ RNLIYEJOA 🛛 🔓 B TQS 🔳 B LQ/PEBOXQEHMUARRX DZKQ9I + WQI = LM9AI \mathbf{BPDR} + $\mathbf{T} = \mathbf{O} \setminus \mathbf{N} \phi = \mathbf{E} \mathbf{U} H + \mathbf{F}$ $Z \supset 9 \cup V \forall I = + \bot L + J \land R \cup H$ IADRUTYSNUJ CA P • M A R U L @ L + N V E K H × 6 9 D Z & A N L M L A A O K L T I R $+ U 9 \times A \Delta = B \vee W \times + \vee T \perp O P$ N ≍ S Я J ¬ U ∃ O A D + 6 Z Z I M $N \rightarrow S \supset E / \Delta \Box \Box Z = A P \Box B V$ $9 \exists X Q W Q \Box F \equiv A D + \Box A A B$ OT • RUD + D 0 Y 0 D Λ 5 0 W VZ36YKEDTYAAD LLD HIFBXA+XADQ\ALI = 🗩 D 3 0 B B O 3 O P O R X Q F B 6 D Z OJTLODAJI+9 BPQWO KIN×+MH3Q0IWARX3V **IL**IKEKI**LL**INGPEOPL EBECAUSEITISSOMUC HFUNITISMOREFUNTH ANKILLINGWILDGAME INTHEFORRESTBECAU SEMANISTHEMOATDAN GERTUEANAMALOFALL TOKILLSOMETHINGGI VESMETHEMOATTHRIL LINGEXPERENCE EVENBETTERTHANGE TINGYOURROCKSOFFW ITHA6IRLTHEBESTPA RTOFITIATHAEWHENI WTLL BEREBORNT NPARADICESNDALL EKILLEDWILLB EIHAV ECOMENYSLAVESIWIL LNOTGIVEYOUMYNAME BECAUSEYOUWILLTRY TOSLOIDOWNORSTOPM YCOLLECTINGOFSLAV ESFORMYAFTERLIFEE BEORIETEMETHHPITI

く 目 ト く ヨ ト く ヨ ト

- 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.).

 $HER > 9 J \land VP X I \Theta L T G \Theta Q$ N 9 + B ∮ ■ O □ D W Y • < □ K 7 ↔ B Y 3 ⊃ M + U Z 6 W ¢ ↔ L ■ ┿ H J 5994A J A E V 090++R K O $\Box \triangle M + + \bot T \Box I = F P + P \odot 3 /$ $\mathbf{A} \mathbf{R} \wedge \mathbf{F} \mathbf{J} \mathbf{O} - \mathbf{\Box} \mathbf{O} \mathbf{C} \mathbf{A} \mathbf{F} > \mathbf{O} \mathbf{D} \mathbf{\phi}$ ■●+Kり回エ●UつX6V・◆L| $Q < M + B + ZR \ominus FB > YA \odot OK$ - + J U V + A J + O 9 A < F B Y - $U + R / O \perp E \mid D Y B 9 8 T M K O$ e<>JRJIN●TOM•+PBF ♦ ○ △ 5 ¥ ■ + N I ● F B ⊃ ♦ I ▲ R Υ Β Χ Θ 🖬 Ι Ο Δ C Ε > V **U Ζ** 🔍 I Ͻ • @ + B K φ O 9 Λ • ∃ M Ø 6 🔿 R ⊃ T + L ⊖ O C < + F J W B I ↔ L IFXQW<ALBDYOBD-CO > M D H N 9 X S + Z O A A I K I +

< ロ > < 同 > < 回 > < 回 > < 回 > <

3

- 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.).

 $HER > 9 J \land VP X I \Theta L T G \Theta Q$ N 9 + B ∮ ■ O □ D W Y • < □ K 7 ↔ B Y 3 ⊃ M + U Z 6 W ¢ ↔ L ■ ┿ H J 5994A J A E V 090++R K O $\Box \triangle M + + \bot T \Box I = F P + P \odot 3 /$ $\mathbf{A} \mathbf{R} \wedge \mathbf{F} \mathbf{J} \mathbf{O} - \mathbf{\Box} \mathbf{O} \mathbf{C} \mathbf{A} \mathbf{F} > \mathbf{O} \mathbf{D} \mathbf{\phi}$ ■●+Kり回エ●UつX6V・◆L| 6 ⊖ J ¬ T ■ O + □ N Y + □ L Δ ф $0 < M + 8 + ZR \ominus FB > YAOOK$ - + J U V + A J + O 9 A < F B Y - $U + R / O \perp E \mid D Y B 9 8 T M K O$ $\Theta < \Im] R] | \Box \Theta T O M \cdot + P B F$ + ○ △ 5 Y = + N I ● F B ⊃ ∮ I ▲ R Υ Β Χ Θ 🖬 Ι Ο Δ C Ε > V **U Ζ** 🔍 I Ͻ • @ + B K φ O 9 Λ • ∃ M Ø 6 🔿 R ⊃ T + L ⊖ O C < + F J W B I ↔ L IF XQW < ALBOYOBD-CO > M D H N 9 X S + Z O A A I K I +

< 回 > < 三 > < 三 >

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.



< 注入 < 注入

æ

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

Open file	Solve	Substitution		Task: substitution (using 2 CPU threads)			
Save state	Pause	Substitution + columnar transposition		5-grams_english_practicalcryptography_wortschatz.txt.gz			
Jave state	Fause	Substitution + crib grid		Items: 68 Items per second: 0.53 MIPS: 1.40			
Load state	Stop task	Substitution + crib list		AVG score: 19687.27 IOC: 0.07884 PC-cycles: 426.57			
	Swap	Substitution + nulls and skips		() () () () () () () () () ()			
nput window	Substitution + polyphones -			Output window			
ER>p1^VPk 1L1	rg2d		-	Score: 20025.63 IOC: 0.0751 Multiplicity: 0.1852 Seconds: 25.60			
p+B(#O%DWY.<	Kf)			Repeats: ERIT THER TING ITH NTO ANT ISI ERE (2) TEA ARE EAL			
y:cN+UZGW()L4	zHJ			PC-cycles: 483			
pp7^18*V3p0+-	RK2						
9M+ztjd 5FP+	9K/			GOM I SCENTO FURN AT ME STELS I KARRDE I			
Son FIGHTGURF.	-7.1			AVE ED LAN TO CARLERS ES INS SPECIFICS II			
G2.Tf1#O+ NY7	41.9			IT ALSO TACKS TO A BANDED FLATIVISIT WE DETUDAMENT			
M+h+782FBoy	648			AT CHT READY ME & SECONTE IT I SPERED SO			
z1UV+^J+0p7<	Bv-			TH BOR OF A RES ANNA I TEACH IF I ON END			
J+R/StE DYBpb]	INKO			THE REMAND STE FOREAL STH CAREE VOTE AD ANER			
<clrj *5t4m.<="" td=""><td>-6BF</td><td></td><td></td><td>TT DE BUILE A FOINO COST FADGE EALISED VN</td></clrj>	-6BF			TT DE BUILE A FOINO COST FADGE EALISED VN			
69Sy#+N 5FBc	(;8R			CATHAN TRUMPET RC REFER TIER PERATING N BLES			
GFN^f524b.cV	1C++			FROM REPREWRIE I SPAIN AGES ONE CITY FAST			
BX1*:49CE>VU							
c.3zBK(Op^.fl	6qG2						
RoT+L16C<+F1W	31)L						
++) WCzWcPOSHT	()p						
FkdW<7tB_YOB	-Cc						
>MDHNpkSzZOSA	K7+						

◆□ ▶ ◆□ ▶ ◆ 三 ▶ ◆ 三 ▶ ● ○ ○ ○ ○

• 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?

・ 同 ト ・ ヨ ト ・ ヨ ト ・

3

- 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?

3
- 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?

(B) (B)

- 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?

(B) (B)

- 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?

э.

- 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.



ヘロト ヘ戸ト ヘヨト ヘヨト

Re: Things I noticed about Z340 Dby 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:



- 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.



ヘロト ヘ戸ト ヘヨト ヘヨト

Re: Things I noticed about Z340 Dby 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:



- 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.



くぼう くほう くほう

Re: Things I noticed about Z340 Dby 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:



- 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 Dby 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:



< 3 > 4 3 >

Left-right, top-bottom

153																
170																
187																
204																
221																
238																
255											266		268	269		
272								280				284	285	286		288
289	290		292	293	294	295	296		298	299	300		302		304	305
306		308	309									318		320		322
323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339

period-19 transposition

																288
306	324															
	289	307	325	2												
			290	308	326	3										
						309	327									
							292		328	- 5						
									293	311	329					
											294	312	330			
													295		331	8
															296	
332	9															
		333	10													
	280	298	316	334												
				299		335	12									
					282	300		336	13							
						265	283			337	-14					
								266	284	302	320	338	15			
						195		231	249	267	285	303	321	339	16	
												268	286	304	322	323

▲□ ▶ ▲ □ ▶ ▲ □ ▶ ...

- 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.



∃ ► < ∃ ►</p>

э

- 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.



▶ < ∃ >

э

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.

																288
306	324															
271	289	307	325	2												
236			290	308	326	3										
201						309	327									
166							292	310	328	5						
131										311	329					
96											294	312	330			
61													295	313	331	8
26															296	314
332	9															
297	315	333												208		244
262	280	298	316	334											191	
262 227	280 245	298 263	316 281	334 299	11 317	29 335	47 12						155 120		191 156	209 174
262 227 192	280 245 210	298 263 228	316 281 246	334 299 264	11 317 282	29 335 300	47 12 318	65 30 336					155 120 85	173 138 103	191 156 121	209 174 139
262 227 192 157	280 245 210 175	298 263 228 193	316 281 246 211	334 299 264 229	11 317 282 247	29 335 300 265	47 12 318 283	65 30 336 301	83 48 13 319	101 66 31 337			155 120 85 50	173 138 103 68	191 156 121 86	209 174 139 104
262 227 192 157 122	280 245 210 175 140	298 263 228 193 158	316 281 246 211 176	334 299 264 229 194	11 317 282 247 212	29 335 300 265 230	47 12 318 283 248	65 30 336 301 266	83 48 13 319 284	101 66 31 337 302	119 84 49 14 320	137 102 67 32 338	155 120 85 50 15	173 138 103 68 33	191 156 121 86 51	209 174 139 104 69
262 227 192 157 122 87	280 245 210 175 140 105	298 263 228 193 158 123	316 281 246 211 176 141	334 299 264 229 194 159	11 317 282 247 212 177	29 335 300 265 230 195	47 12 318 283 248 213	65 30 336 301 266 231	83 48 13 319 284 249	101 66 31 337 302 267	119 84 49 14 320 285	137 102 67 32 338 303	155 120 85 50 15 321	173 138 103 68 33 339	191 156 121 86 51 16	209 174 139 104 69 34
262 227 192 157 122 87 52	280 245 210 175 140 105 70	298 263 228 193 158 123 88	316 281 246 211 176 141 106	334 299 264 229 194 159 124	11 317 282 247 212 177 142	29 335 300 265 230 195 160	47 12 318 283 248 213 178	65 30 336 301 266 231 196	83 48 13 319 284 249 214	101 66 31 337 302 267 232	119 84 49 14 320 285 250	137 102 67 32 338 303 268	155 120 85 50 15 321 286	173 138 103 69 33 339 304	191 156 121 86 51 16 322	209 174 139 104 69 34 323

period-19 transposition

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



▶ < ∃ >

Have we discovered the correct transposition?

		Not Secure — jarive.vdm-service.be	Ċ
File Edit Solve Ciphers Statistics He	p		
Cipher window Set cipher	limensions: 19*20	Output window	Restart 59: 36.50%
H+M8 CV@K+I#2E.B)> B+*5k.L-RR+4>f pMR(UVFF29z/JNbVM) D># 3P>Ld15 .UqLFHpOGp +2 <ut*5czg+kni%wc D(MVE5FV52+dp^D(+4 G++ TB4-R)WkVW)+ki b^D4ct+cW<spylr 5j<br="">JYM(+ TC7zk.#Kp+fZ+ B.;+c+ztZ <228KjROp +8y.LWBO1*H_Rq#2pb RB31c_8LKJ9^%OF7TE Xz6PYATfSMF;+B<mfg BCO0 G)p+l2_cFKzF*k <5BK2BpzOUNyBO6N H*;dy7t-cYAy29^4OFT -+N:^j*Xz6-<sf9pl c<br="">cpclddG+4Ucy5C^W(</sf9pl></mfg </spylr></ut*5czg+kni%wc 	E Z D& #2 ++ & S1 S1 C C (+	Score: 2004780 loc: 0.07272 DEINCLASTEA RENIBOUTSSE MANNATALSO EYOUSAICCOM ESCHMINISTH RTIAFINAISESI HEECORDTST WORDSIESTHE SPITECOLLABE RODESEAITCH ENPOUTREANI SREASINUTST DANYPOOREIN RLEECHTHEASI HERTSRHAEMI DNDSPLITSPO TEOFOUNDAN SHSASSHEDM	USFORTOF DORCHIST WAITCROUT MMUNDHEHH EBOARTEA HORTEDT TBATTEBUS EYPUSLISE OUTHERTE JASNTUSEH DISMUSHWA ORENLORA HOERHINHA SISNTANNT OPRENOFTE PSTODENO THERTHALL SPILOTT

<回>< E> < E> < E> <

- 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

 $T_i = s_i \mod 20, 2i \mod 17.$

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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

 $T_i = s_i \mod 20, 2i \mod 17$

- 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

 $T_i = s_i \mod 20, 2i \mod 17$.

- 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.

・ロト ・ 一下・ ・ ヨト・

- 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

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

- 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

$$T_i = s_i \mod 20, 2i \mod 17.$$

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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

$$T_i = s_i \mod 20, 2i \mod 17.$$

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

The period-19 transposition

																288
306	324															
271	289	307	325	2												
236			290	308	326	3										
201						309	327									
166							292	310	328	- 5						
131									293	311	329	6				
96											294	312	330			
61													295	313	331	8
															296	314
332	9															
332 297	9 315	27 333	45 10					135 100			189 154	207 172	225 190	243 208	261 226	279 244
332 297 262	9 315 280	27 333 298	45 10 316	63 28 334				135 100 65		171 136 101	189 154 119	207 172 137	225 190 155	243 208 173	261 226 191	279 244 209
332 297 262 227	9 315 280 245	27 333 298 263	45 10 316 281	63 28 334 299	81 46 11 317	99 64 29 335	117 82 47 12	135 100 65 30		171 136 101 66	189 154 119 84	207 172 137 102	225 190 155 120	243 208 173 138	261 226 191 156	279 244 209 174
332 297 262 227 192	9 315 280 245 210	27 333 298 263 228	45 10 316 281 246	63 28 334 299 264	81 46 11 317 282	99 64 29 335 300	117 82 47 12 318	135 100 65 30 336		171 136 101 66 31	189 154 119 84 49	207 172 137 102 67	225 190 155 120 85	243 208 173 138 103	261 226 191 156 121	279 244 209 174 139
332 297 262 227 192 157	9 315 280 245 210 175	27 333 298 263 228 193	45 10 316 281 246 211	63 28 334 299 264 229	81 46 11 317 282 247	99 64 29 335 300 265	117 82 47 12 318 283	135 100 65 30 336 301	153 118 83 48 13 319	171 136 101 66 31 337	189 154 119 84 49 14	207 172 137 102 67 32	225 190 155 120 85 50	243 208 173 138 103 68	261 226 191 156 121 86	279 244 209 174 139 104
332 297 262 227 192 157 122	9 315 280 245 210 175 140	27 333 298 263 228 193 158	45 10 316 281 246 211 176	63 28 334 299 264 229 194	81 46 11 317 282 247 212	99 64 29 335 300 265 230	117 82 47 12 318 283 248	135 100 65 30 336 301 266	153 118 83 48 13 319 284	171 136 101 66 31 337 302	189 154 119 84 49 14 320	207 172 137 102 67 32 338	225 190 155 120 85 50 15	243 208 173 138 103 68 33	261 226 191 156 121 86 51	279 244 209 174 139 104 69
332 297 262 227 192 157 122 87	9 315 280 245 210 175 140 105	27 333 298 263 228 193 158 123	45 10 316 281 246 211 176 141	63 28 334 299 264 229 194 159	81 46 11 317 282 247 212 177	99 64 29 335 300 265 230 195	117 82 47 12 318 283 248 213	135 100 65 30 336 301 266 231	153 118 83 48 13 319 284 249	171 136 101 66 31 337 302 267	189 154 119 84 49 14 320 285	207 172 137 102 67 32 338 303	225 190 155 120 85 50 15 321	243 208 173 138 103 68 33 339	261 226 191 156 121 86 51 16	279 244 209 174 139 104 69 34
332 297 262 227 192 157 122 87 52	9 315 280 245 210 175 140 105 70	27 333 298 263 228 193 158 123 88	45 10 316 281 246 211 176 141 106	63 28 334 299 264 229 194 159 124	81 46 11 317 282 247 212 177 142	99 64 29 335 300 265 230 195 160	117 82 47 12 318 283 248 213 178	135 100 65 30 336 301 266 231 196	153 118 83 48 13 319 284 249 214	171 136 101 66 31 337 302 267 232	189 154 119 84 49 14 320 285 250	207 172 137 102 67 32 338 303 268	225 190 155 120 85 50 15 321 286	243 208 173 138 103 68 33 339 304	261 228 191 156 121 86 51 16 322	279 244 209 174 139 104 69 34 323

A doubly periodic, 1,2-decimation



< 回 > < 三 > < 三 > -

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 () have used Mathematica):

Read more



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



ヘロ ト ヘ 同 ト ヘ 三 ト ー

azdecrypt on the 1,2-decimation transposition of Z340

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

File Functions Format Statistics Options Task: substitution (using 2 CPU threads) Substitution Onen file Solve Substitution + columnar rearrangement 6-grams english jarlve reddit.txt.gz Substitution + columnar transposition Save state Pause Substitution + crib arid Items: 86 Items per second: 0.19 MIPS: 0.83 Load state Stop task Substitution + crib list AVG score: 17665.04 IOC: 0.08312 PC-cycles: 209.08 Substitution + monoalphabetic groups Swap Substitution + nulls and skips Substitution + polyphones Input window Output window H+M8 (CVBKz / JNDVM) Score: 18159.14 IOC: 0.0798 Multiplicity: 0.1852 Seconds: 21.54 +kN^D(+4(5J+JYM(+ Repeats: OOSEC LIST TERR TOMI ALLO INTH EDAL SSS TEC ATE ECH v.LWBOLKJp+12 cFK PC-cycles: 157 29^40FT-+FB+*51 . I. RE ON T LOVEE & TUBOOSECULATE STATE TOOTE d15||.UgL+dpVW)+k p+fZ+B.;+B31c 8Tf SO NOT ONE THE EDIT RED ALS OR IS ENTER A CONCE ATT OF ANE CHOOSE CHEN WE TOGETHAT BpzOUNvBO<Sf9p1/C >R(UVFFz9<Ut*5cZG IN IN THE OF US TOM IN A HEALIST FOR REAM R)WkPYLR/8KiROp+8 FIR AT WRS SO CYONS AN EA SO HE NEVER YOURS SL IS TO US FTS ALLOT TO IN WHY INTO ON A 1Xz6PYAG) v7t-cYAv Ucv5C^W(cM>#Z3P>L ROAD TO MIC ONE IS AND HERS BAT LOOT DUP (MVE5FV52cW<Sk.#K LARVER SEEND NOT STAH OR HED TREET ITS STILLET Rg#2pb&RG1BC00|2 MED ALL OR LITER REMITECH TEC CRESSSES IN N:^j*Xz6-+1#2E.B) THRRE LOOK AND BLASTIE TEE I WARRIOR GET |DpOGp+2|G++|TB4-MORBURTER RG |TC7z|<z29^%OF7TB zF*K<SBKdpclddG+4 -RR+4>f|pFH1%WO&D #2b^D4ct+c+ztZ1*H SMF;+B<MF6N:(+H*; イロト 不得 トイヨト イヨト 3

• 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

э.

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

< 同 > < 回 > < 回 > …

= nav

Row-major transpositions

		KD KH KD KH HP HH	X0 X0 XF X0 X0 X0 XH XO XU XF 10 10 10 10 10 10 10 10 10 10 10	
17 M M 20 21 22 28 24 28 28 27 28 29 20 21 30 30		NH NO DO	X0 X0 X0 X0 X0 X0 X0 X1 X0	
	and was war while was war was war was not be be by be be be-		206 208 200 200 200 200 200 201 201 201 201 201	
		20 20 20 20 20 20 20 20 20 20 20 20 20 2	244 247 246 246 246 240 240 241 241 241 241 241 241 241 241 241	
AN A	and and and and and the line into the line into the line into the line and	PT 275 285 285 285 285 285 285 285 285 285 28	are and the and	AN A
and	ter has not an	and	and	
	THE TAY THE			
			TO DO	
the ter too too two two two two two two two two	ter		per per per per ten	the ter the top two ter
tes tak tak tak ter tak	NOT NOT NOT THE THE THE THE THE THE THE THE THE TH	TO THE TO THE		
				10 17 17 17 17 18 18 19 19 17 19 19 19 10 10 10 10 10 10
107 108 108 100 107 100 100 108 108 107 108 109 201 201 201	201 202 201 202 100 100 107 100 100 100 100 100 100 100	OR C7 OR OR HE HI 10 10 14 14 14 14 14 14 14 10 10 10	10 10 10 10 10 10 10 10 10 10 10 10 10 1	201 202 201 200 100 100 107 100 100 100 100 100 101 100 100
204 205 205 205 206 200 201 201 202 203 205 205 205 205 205 205	and	THE CRI COL		204 206 206 207 208 200 20 20 20 20 20 20 20 20 20 20 20
241 268 268 268 268 268 267 268 269 269 277 269 289 287 288 287 288 287	and	NO WE HE		ANT AND AND AND AND ANY AND ANY
one one and	and			
the line line line line line line line lin	are any set and any set and and and and any set and any set any			(** (** (** (** (** (** (** (** (** (**
11 11 14 15 15 17 17 15 15 16 16 16 16 16 16 16 16 16 16 16 16	THE DIA AND AND AND AND AND AND AND AND AND AN	the last has been been better and we want wat wat had been been been		TE DE
	NO 204 205 205 207 208 208 207 208 204 206 205 207 208 208	THE THE THE THE THE AT ALL ALL ALL ALL ALL ALL ALL ALL ALL		201 204 205 205 207 205 206 206 207 206 206 204 205 205 207 208 208
201 107 108 108 100 101 102 10 10 10 10 10 10 10 10 101 101	\$20 \$21 \$20 \$14 \$14 \$17 \$14 \$15 \$14 \$15 \$15 \$17 \$10 \$20 \$20 \$20 \$20			204 207 204 205 205 21 20 20 20 20 20 20 20 20 20 20 20 20
303 304 308 308 307 308 309 300 308 300 300 308 308 308 307 308 308	200 200 207 200 200 200 202 203 200 200 200 X00 X07 X00 X00 X00 X00		NO 10 10 10 10 10 10 10 10 10 10 10 10 10	204 204 207 204 204 204 205 200 200 201 200 200 207 201 201 201 201
		NO N		
	NN NF NN NN 100 101 102 103 104 105 106 107 108 100 10 10 10	NO NO DI		
	501 504 501 501 501 500 304 304 307 306 306 304 300 307 308 309			
	10 10 1N 10 1N 17 1N 17 10 10 10 10 10 10 10 10 10 10 10 10	348 347 368 361 364 363 361 361 361 361 378 378 378 378 378 378 378	10 10 10 10 10 10 10 10 10 10 11 10 10 1	
	211 211 241 244 247 246 246 244 245 242 247 240 249 248 247 248 248	AND	OR OF OR OR HE	10 10 10 10 10 10 10 10 10 10 10 10 10 1
at an at an an an at at at an at at at at an at an	the test test test test test test test t	and		144 144 144 146 146 147 140 149 149 147 148 147 148 148 148 149 149 149
the text the text the text text text tex	and	are any are		
the tail tail tail tail tail tail tail tail	and			
the test the two two two two two two two two test test test test	and and and the two	ter ten		
the tax tax tax tax tax tax tax and	THE TTO THE THE THE THE TTO THE THE THE THE THE THE THE THE			22 23 20 20 20 20 27 20 20 20 20 20 20 20 20 20 20 20 20 20
	ten ten tet ten ten ten ten ten ten ten		NO X8 X0 X8 X7 X8 X8 10 10 10 10 10 10 10 10 10 10	208 208 207 208 208 208 208 208 208 208 208 208 208
ALL THE	the term the term we had not been not been not been not been not	10 10 10 10 10 10 10 10 10 10 10 10 10 1	340 350 3H 310 350 3H 361 3H 3H 3H 3H 3H 501 501 501 501 504 505	201 204 205 205 204 200 206 207 206 206 206 206 206 206 201 201 201
280 246 246 247 246 246 246 20 20 24 20 388 388 307 388 388 384		THE CELE CELE CELE CELE CELE CELE CELE CE	248 248 247 248 249 240 241 240 240 241 241 241 241 241 241 241 241	271 270 240 248 247 246 248 244 240 240 241 241 241 248 247 246 241
201 208 208 208 208 208 207 208 209 200 201 20 20 20 20 20 20 20			204 200 200 204 205 206 207 208 208 201 201 201 201 201 201 201 201 201	217 206 206 208 200 209 209 209 209 209 207 208 207 208 201 201 201
He				24 24 24 25 26 26 26 26 26 26 26 26 26 26 26 26 26
245 245 247 248 240 240 247 242 245 246 246 246 247 247				
the list list list list list list list list				
22 21 20 No				
213 224 225 226 227 228 229 220 27 22 20 2N 2N 2N 2N 2N 2N				

イロン イロン イヨン イヨン

Row-major transpositions cont.

				10 10 10 10 10 10 17 10 10 10 10 10 10 10 10 10 10 10 10 10
AND AND THE AND	AN AN AT AN AT AN AN AN AT	211 222 200 200 207 208 205 201 201 202 201 201 201 201 207 201 201	AN AN AT AN	244 244 245 241 242 245 246 245 245 247 248 247 241 241 247 247 241
AT 25 25 25 25 25 25 25 25 25 25 25 25 25	AT 100 AD	AT 200 AT 200 AT 200 AT 200 AT 200 AT 200 AT 201 AT 201 AT 201 AT	are and and and and are are and any are any are any any are any	
	FT M M M M M M M M M M M M M M M M M M M			
the time was not the time time time time time time time tim	the the test the test the test test test	the table of tables and tak and tables and tables and tables and tables	the the the the the the can be be be be be the the the the the	THE TAK
			TO DE	
27 27 30 30 30 30 30 30 30 30 30 30 30 30 30	211 215 308 308 307 308 305 304 305 305 301 308 308 308 307 308	286 286 287 286 280 380 381 382 383 384 385 388 387 388 388 291 291	271 275 286 286 287 286 286 284 280 281 281 281 288 287 286 281	100 100 107 100 100 101 102 100 100 100 100 107 100 100 170 171
NO 300 300 300 301 301 300 300 307 300 301 301 308 300 300 300	100 XM XXX XXX XXX XXX XXX XXX XXX XXX XX	240 240 241 240 240 244 246 246 247 248 248 248 251 251 251 251 254 255	288 286 281 282 280 284 286 286 287 288 288 281 201 201 203 204 201	101 104 102 102 104 100 206 206 207 206 206 206 200 201 201 201
		100 104 106 106 107 XM XM XM XM XM 100 100 104 104 104 104	104 104 107 106 106 108 100 100 107 108 108 107 108 108 108 108	143 144 145 146 147 146 146 150 159 150 150 150 150 150 150 150 150
NO 20 AD DO		NO 104 100 PO PR PO PR PK PN PO PO PO PH IN NO NO NO NO	NA NY NO DE DE DT DE DE DE DE DE DE DE DE NE NE NE NE NE	
	and the site and			
the the the the ball ball ball ball ball ball ball bal	the time and	the life life life life has been been been been been been been life life	the test test test the test test test te	the life and left the life the life and life and life and and and and and
TO DO	De De De Di. De De Le Li	DO DO DO DA DA DO	Do Do Do Do Do Do Lo	
		140 140 144 140 140 141 140 119 119 119 119 119 119 119 119 119	100 100 100 100 100 100 100 100 100 100	THE
TO THE HE H	THE TOP THE THE HE H	TEL TEL TO THE THE THE THE THE THE THE THE THE TEL TEL TEL TEL	THE TOP THE	10 101 100 140 140 147 140 140 144 140 140 141 140 04 031 031 04
THE TO THE THE THE TO TO THE THE NOT TO THE TOP TOP TOP TOP TOP		THE TY THE THE THE TO TO THE		102 102 104 105 108 107 108 109 10 17 10 10 11 11 11 11 11 11
	M M 20 70 70 70 70 70 70 70 70 70 80 81 80 80 80 80	N N N N N N N N N N N N N N N N N N N		AL A

Column-major transpositions



・ロ・ ・ 四・ ・ ヨ・ ・ ヨ・ ・

Column-major transpositions cont.



Alternating row-column transpositions



Sam Blake The Quest to Solve the Zodiac 340 Cipher

イロト イロト イヨト イヨト

æ

Alternating row-column transpositions cont.

35 48 131 131 158 165 200 231 261 268 265 290 211 321 328 335 330	17 82 86 118 545 172 107 220 241 260 277 202 305 314 325 332 337	17 52 55 196 145 172 197 230 241 260 277 292 305 396 325 332 337	36 58 531 531 558 565 200 231 261 268 265 290 311 321 329 335 330
34 88 100 130 158 164 208 200 200 288 264 288 313 320 528 334 338	18 53 56 117 546 173 196 221 542 241 279 260 517 306 517 306 533 336	18 50 66 117 148 175 188 221 242 261 276 283 306 217 228 333 308	24 88 930 930 958 984 208 200 200 288 284 288 518 320 528 354 338
<u>35 87 98 99 197 985 207 229 249 297 285 207 808 319 827 335 337</u>	13 54 87 515 547 174 999 222 243 262 279 264 567 518 327 534 335	18 54 27 118 147 174 199 222 243 262 279 294 207 318 227 334 338	15 57 56 59 157 555 267 228 245 267 265 267 858 319 527 355 337
27 66 66 700 106 162 206 229 240 266 262 266 208 210 228 232 236	27 55 56 118 118 148 178 200 223 344 263 280 295 308 319 338 335 336	20 55 68 119 148 175 228 223 244 263 260 296 208 219 228 235 336	22 56 56 556 556 556 562 226 228 248 256 256 256 256 258 218 228 232 236
21 55 57 ST 155 564 285 227 247 255 264 285 307 217 525 350 301	21 56 59 123 149 176 201 224 245 264 291 296 309 329 329 531 355	21 55 50 120 140 576 201 224 245 254 241 296 300 520 229 330 301	14 85 87 927 156 984 285 227 247 285 284 286 307 317 328 334 330
20 64 18 108 184 180 204 228 266 284 280 284 308 318 322 323 324	22 817 80 121 180 177 202 228 348 268 282 297 310 321 334 323 322	22 87 80 121 180 177 202 238 248 268 262 287 210 321 322 303 324	20 64 66 758 756 760 200 228 246 264 280 264 308 376 376 320 323 327
20 83 86 535 553 179 203 225 245 283 279 283 565 512 513 514 515	22 56 51 122 101 176 200 226 347 266 293 206 211 515 314 513 312	23 58 54 122 155 176 20 225 247 256 265 298 311 212 313 314 515	20 40 46 525 550 570 225 225 245 280 279 285 556 515 514 513 512
25 82 84 124 152 178 282 224 244 282 278 282 300 301 302 303 384	24 88 82 123 182 179 204 227 248 247 284 299 304 303 362 301 300	24 88 82 123 112 179 294 227 248 267 264 299 200 321 302 303 304	28 82 84 524 152 179 262 224 244 262 279 262 304 305 302 301 300
27 81 80 100 101 177 201 222 243 271 277 286 277 286 299 299 291	25 00 00 10 100 100 100 205 200 340 200 205 201 200 200 200 200 207 200	22 00 90 10 10 100 225 239 249 259 259 259 251 257 258 259 259 251	27 81 80 120 151 177 21 220 240 281 277 21 209 209 209 207 206
25 45 87 177 188 178 280 272 342 248 273 271 277 273 274 278 274	21 41 44 124 194 191 206 229 293 299 279 275 271 273 277 277 277	24 45 46 128 144 141 228 229 240 248 270 271 272 273 275 275 278	24 46 40 42 40 114 200 222 342 240 218 276 214 213 277 211 270
20 09 01 101 100 110 100 221 241 250 250 254 255 250 257 250 259	27 52 55 10 10 10 10 10 20 20 20 20 20 20 20 20 20 20 20 20 20	27 42 45 128 128 139 142 207 200 201 202 203 204 205 204 207 208 209	20 29 21 221 249 113 199 221 241 229 229 211 259 255 254 255 254 250 252
24 14 10 120 144 174 184 220 232 233 234 235 236 237 238 230 240	21 43 84 127 946 143 204 231 343 230 238 237 236 335 234 233 232	24 43 96 127 198 183 208 231 232 233 234 298 236 237 238 239 242	24 14 16 120 144 174 184 220 240 298 214 227 296 205 204 203 202
22 87 89 119 167 112 187 213 211 212 213 214 215 216 217 218 219	20 44 87 128 127 184 208 218 218 217 218 215 214 213 212 211 210	27 64 87 128 107 184 228 210 211 212 213 214 215 218 217 218 218	20 87 88 118 167 112 187 218 218 217 218 218 210 214 213 212 211 210
20 94 84 118 146 172 146 197 948 148 920 141 122 955 134 925 146	AN AT AN 128 198 198 198 198 198 198 199 199 199 19	10 AC 04 120 158 105 156 177 188 150 150 121 152 153 154 155 156	22 54 58 103 104 172 196 196 196 193 192 191 198 990 198 197 196
		11 AN AN 120 110 100 101 101 101 101 100 100 100	
	10 47 100 111 144 147 142 141 143 115 118 117 116 116 116 119 112	10 42 100 101 102 103 104 105 104 102 106 108 109 40 141 142 145 144	20 M M 100 M 101 M 102 M 100 100 100 107 108 105 104 105 101 102
1 47 78 78 79 79 79 79 78 78 79 78 78 48 49 40 48 49	N 10 M 41 82 81 41 40 70 70 77 76 15 74 71 72 71 70	N 44 10 10 10 10 10 10 15 10 17 10 10 10 11 10 10 10	
238 235 229 221 311 299 295 295 291 221 208 185 188 131 821 88 21	317 332 308 314 306 290 277 280 381 200 187 172 148 118 86 80 17	337 330 338 316 308 382 277 360 341 328 187 172 348 196 48 10 17	208 201 229 221 211 208 201 201 201 221 208 101 100 101 101 101 100
208 205 229 221 311 209 206 209 201 221 209 105 199 131 101 00 20 309 304 329 220 210 209 204 209 200 220 209 104 159 130 130 100 00 24	337 332 328 314 306 393 277 396 341 220 187 172 148 114 88 49 17 399 320 306 377 306 323 378 241 342 231 198 173 146 177 46 37 198	207 202 228 276 268 282 277 280 241 228 187 172 148 196 48 12 17 286 203 201 271 268 270 271 271 262 271 262 712 196 171 168 23 19	338 335 329 321 311 299 285 289 201 221 209 186 198 131 181 49 20 208 234 234 231 222 212 209 204 208 220 220 228 184 158 130 180 49 24
238 336 329 327 311 398 386 389 381 231 309 188 189 31 31 38 38 328 324 328 320 376 228 284 398 20 226 329 394 138 130 188 49 327 333 327 339 309 309 307 388 397 388 397 388 197 388 197 388 399 49 47 31	207 202 208 316 206 202 217 266 241 220 107 112 Met 118 46 49 17 208 233 206 517 206 209 219 241 542 251 198 173 546 117 66 23 15 208 336 377 318 307 248 279 244 279 362 262 252 188 TK 647 118 67 54 15	207 202 228 376 206 208 202 277 200 241 220 107 172 146 176 86 62 17 230 233 228 371 208 263 271 266 242 221 156 172 146 151 86 62 15 230 234 257 356 256 259 262 241 252 169 174 147 148 457 14 15	238 238 229 221 211 219 209 208 209 211 221 209 108 109 101 101 00 20 238 234 228 220 276 209 204 238 220 226 209 104 159 150 160 60 24 257 333 207 339 308 207 248 207 248 202 207 105 10 00 100 10 20 10
100 305 509 327 371 309 306 309 371 371 309 409 100 101 40 40 100 324 507 507 507 509 304 504 500 500 500 507 404 100 100 400 50 107 503 507 511 500 507 508 507 504 507 508 107 508 107 10 107 507 507 507 507 507 507 507 507 507 5	257 328 258 344 366 262 277 366 261 327 360 187 172 568 198 46 2 17 268 329 366 572 366 263 378 374 364 124 367 187 167 168 17 66 33 19 268 353 377 38 377 394 377 394 379 372 384 222 198 175 167 118 77 16 77	217 202 208 214 206 242 277 240 241 229 1147 172 448 154 48 20 17 226 233 248 21 268 249 244 245 241 247 156 173 48 151 18 238 254 257 258 257 244 278 252 252 258 151 157 158 25 141 15 258 255 257 257 258 257 258 257 252 244 257 252 248 151 151 154 159 8 15 259 253 258 257 259 255 255 255 245 242 252 256 151 151 151 155 25	338 338 328 327 311 388 288 288 281 201 328 88 188 18 18 18 18 18 18 18 18 18 18 1
308 208 201 211 201 201 304 108 101 101 101 001 308 304 202 202 204 204 200 202 201 201 200	337 342 346 346 347 346 347 346 148 148 148 149 111 383 326 57 366 367 367 347 348 347 347 348	XI7 XX2 XX3 XX3 <th>XXX XXX XXX</th>	XXX
X00 X00 X01 X00 X00 X01 X01 <th>307 202 204 206 202 277 206 241 201 117 146 118 86 107 208 303 305 207 306 307 301 301 302 101 101 302 101 301 302 301 301 302 101 301 302 301 301 302 301 301 302 301 301 302 301</th> <th>XI7 XI0 XI0<th>Jam Jam <thjam< th=""> <thjam< th=""> <thjam< th=""></thjam<></thjam<></thjam<></th></th>	307 202 204 206 202 277 206 241 201 117 146 118 86 107 208 303 305 207 306 307 301 301 302 101 101 302 101 301 302 301 301 302 101 301 302 301 301 302 301 301 302 301 301 302 301	XI7 XI0 XI0 <th>Jam Jam <thjam< th=""> <thjam< th=""> <thjam< th=""></thjam<></thjam<></thjam<></th>	Jam Jam <thjam< th=""> <thjam< th=""> <thjam< th=""></thjam<></thjam<></thjam<>
Max Max <thmax< th=""> <thmax< th=""> <thmax< th=""></thmax<></thmax<></thmax<>	317 320 324 345 346 217 346 325 346 118 43 45 321 323 325 57 36 321 31 34 21 166 176 46	317 320 326 346 346 377 360 371 370 371 <th>Jam Jam Jam</th>	Jam
	O D <thd< th=""> <thd< th=""> <thd< th=""> <thd< th=""></thd<></thd<></thd<></thd<>	Mode Mode <th< th=""><th></th></th<>	
			Mai

イロト イヨト イヨト イヨト

Alternating column-row transpositions



イロト イヨト イヨト イヨト

Alternating column-row transpositions cont.

	20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 19	20 21 22 23 24 25 26 27 28 29 20 21 22 33 24 35 0	38 34 33 32 31 30 29 28 27 28 25 24 23 22 21 20 19
eo eo a7 os es e4 a3 o2 e7 e0 50 58 57 50 55 56 1	55 56 57 58 59 60 81 62 63 64 85 58 67 68 69 54 18	05 50 57 58 59 60 81 62 63 64 85 68 67 68 69 50 1	08 68 E7 66 65 64 E3 62 61 60 59 56 57 56 55 54 16
107 100 96 98 97 96 95 94 90 82 91 90 89 86 73 37 3	88 80 80 91 02 85 84 95 96 87 88 98 100 101 87 85 17	AN AD BD 91 02 65 84 96 96 67 86 98 500 121 78 87 2	101 100 80 84 07 85 85 84 03 62 81 80 88 88 87 83 17
131 130 128 138 137 136 128 131 133 132 131 138 188 187 13	118 120 121 122 123 124 128 128 127 128 128 130 131 118 88 12 14	118 120 121 122 123 124 128 129 127 138 129 130 131 162 17 28 3	131 130 128 128 127 138 128 124 123 122 121 128 118 118 18 12 14
109 199 197 198 195 194 193 192 191 190 149 148 192 189 72 29 4	148 149 150 151 152 153 154 155 156 157 158 158 147 117 85 51 15	148 149 150 151 152 153 154 155 158 157 158 158 152 150 72 59 4	109 100 137 158 155 154 153 152 151 150 149 148 147 117 85 84 15
985 184 183 192 181 180 178 178 177 176 178 183 133 184 73 43 1	175 176 177 178 179 180 181 152 180 184 185 174 145 116 84 80 14	175 176 177 178 179 180 181 182 183 184 185 150 153 164 73 40 5	105 164 183 152 101 100 170 178 177 175 176 174 148 115 54 50 14
209 208 207 208 209 204 203 202 201 200 188 181 134 105 14 41 4	200 201 202 203 204 208 204 207 208 209 189 173 148 118 83 48 13	200 201 202 203 204 205 204 207 208 209 184 181 134 105 14 41 4	209 208 207 208 209 204 203 202 201 200 199 172 148 118 80 49 13
221 220 228 227 227 228 228 229 220 270 197 192 195 198 19 42 1	222 224 225 228 227 228 229 228 231 222 188 172 184 114 82 48 11	220 224 225 228 227 228 229 229 221 221 210 187 182 125 126 13 42 1	231 230 229 239 237 239 225 234 233 232 199 172 144 114 82 48 11
217 200 248 247 246 245 244 232 211 188 193 198 197 78 43 4	244 245 246 247 248 249 250 251 243 221 197 171 143 113 81 47 11	244 245 246 247 248 249 250 251 232 211 186 193 136 197 79 43 4	251 250 240 248 247 245 245 244 243 221 197 171 143 113 81 47 11
200 208 207 208 205 204 203 202 233 212 100 104 137 106 177 44 1	263 264 265 256 267 268 269 262 242 220 186 173 142 112 83 46 10	263 264 265 256 267 266 269 252 233 212 160 164 137 106 177 44	269 265 267 256 265 264 263 262 262 220 186 172 162 112 86 46 10
205 204 202 201 200 272 253 254 213 100 105 108 109 10 45 10	200 201 202 200 200 200 200 201 201 200 100 1	200 201 202 203 204 205 270 203 204 213 100 105 108 109 10 45 10	205 204 203 202 201 202 279 201 201 212 100 100 101 101 10 45 1
200 200 207 200 205 200 271 254 235 214 121 100 100 100 70 40 11	205 206 207 208 209 204 278 209 240 210 104 108 140 110 11 44 5	295 296 297 298 299 290 271 254 235 214 191 198 139 110 79 49 11	209 209 207 208 205 204 279 208 249 219 104 109 149 109 70 44 1
211 210 338 338 300 287 272 258 236 215 182 187 140 111 88 47 12	808 909 310 311 807 283 277 259 239 217 183 197 139 169 77 43 7	308 309 310 311 300 287 272 358 238 215 182 187 143 111 88 47 12	211 210 300 308 307 205 277 298 239 217 183 197 539 509 77 43 7
221 220 318 312 301 288 273 314 227 216 180 188 181 112 81 48 11	219 220 221 218 209 282 279 258 238 279 182 188 138 109 19 42 4	219 200 221 212 201 200 272 200 227 230 10 100 101 112 01 10	201 200 219 218 208 282 279 238 238 238 150 160 138 208 78 42 4
209 200 202 213 202 209 274 257 250 217 104 109 142 113 02 49 14	209 209 207 217 205 201 275 257 217 215 101 105 127 107 125 41 5	229 229 222 213 222 289 274 257 238 217 114 119 142 113 82 43 14	229 239 237 27 255 281 275 257 237 215 191 195 137 197 75 41 5
335 330 323 314 303 280 279 258 230 216 185 173 443 114 83 80 15	335 334 326 314 304 200 274 256 236 214 190 154 536 106 174 40 4	335 330 323 314 303 290 276 298 239 216 195 178 143 114 83 80 15	335 334 336 314 334 290 274 296 236 214 190 194 336 306 74 40 4
201 221 224 213 204 291 279 218 242 279 191 171 344 173 44 11	200 201 201 201 202 200 272 200 201 201 100 100 100 100 100 10	228 227 224 219 204 291 279 289 242 279 189 177 144 178 46 11 14	219 223 229 219 220 209 272 299 273 199 110 110 129 72 29 2
217 222 225 219 205 282 277 298 241 220 187 172 145 198 45 52 17	230 232 234 214 202 200 272 254 234 212 100 102 134 104 172 20 2	227 222 225 214 205 282 277 298 241 220 187 172 145 119 85 82 17	220 222 224 214 202 200 272 254 234 212 100 102 104 104 12 20 2
335 335 334 317 306 283 274 261 242 221 136 173 545 117 66 53 14	327 331 323 313 301 307 271 253 233 211 147 151 533 565 71 37 1	338 333 336 317 338 285 276 281 242 221 186 177 548 117 86 53 18	27 29 29 29 29 29 27 27 29 29 21 17 19 19 29 29 29 21 17 19
220 224 227 218 227 284 279 282 243 222 189 114 147 118 87 84 19	238 230 222 212 200 286 270 282 232 210 186 182 182 182 18 26 0	338 334 327 318 327 284 279 282 243 222 188 174 147 118 87 84 13	238 230 222 312 200 286 270 282 232 210 188 182 122 122 72 28 0
339 334 327 318 307 284 279 262 243 222 189 174 547 518 87 54 59	236 330 322 312 300 286 270 352 232 210 186 183 132 162 73 36 0	339 334 327 318 307 284 279 283 343 222 189 174 547 118 87 54 19	236 230 222 312 200 286 270 252 232 210 186 182 132 162 78 26 0
229 234 227 218 267 284 279 262 243 222 189 174 547 198 87 54 1 336 333 526 317 306 285 276 261 342 221 198 173 546 117 66 15 16	00 00 00 000 000 000 000 000 000 000 0	338 334 327 318 307 384 276 382 343 222 188 174 547 118 87 54 19 338 333 305 307 347 348 283 276 281 342 221 186 173 548 117 56 53 16	336 330 332 512 300 386 270 252 232 270 186 182 132 162 17 36 0 37 311 23 162 17 31 26 31 31 31 31 31 31 31 31 31 31 31 31 31
239 334 327 318 307 244 279 342 343 343 222 146 174 547 138 47 44 13 336 333 326 317 306 263 278 261 342 221 156 173 546 137 68 53 337 332 328 314 305 282 277 368 341 220 187 172 145 136 68 18 17	256 500 522 512 500 246 276 252 220 116 198 198 122 192 19 26 0 317 311 323 193 301 247 271 253 233 211 197 191 133 196 17 17 336 332 334 314 332 298 272 394 234 212 198 192 134 194 172 39 2	238 254 227 218 257 264 279 262 243 222 188 TN 547 198 87 26 16 17 358 355 356 177 356 255 276 261 342 221 186 173 546 117 54 55 16 357 352 358 374 355 282 277 366 341 220 157 172 146 115 58 18 17	308 300 302 512 500 200 270 502 232 210 196 196 132 162 17 166 10 307 311 323 513 107 207 271 253 253 211 107 191 153 950 71 27 308 332 304 704 302 308 273 364 234 212 198 192 314 304 305 72 308 2
200 201 207 244 240 242 241 241 241 141 <td>226 200 202 217 200 246 270 252 222 270 146 146 142 132 152 15 16 15 15 15 15 15 15 15 15 15 15 15 15 15</td> <td>320 334 327 348 278 343 322 180 174 587 588 57 300 335 307 167 306 207 201 201 180 177 366 367</td> <td>300 302 312 300 300 300 202 312 311</td>	226 200 202 217 200 246 270 252 222 270 146 146 142 132 152 15 16 15 15 15 15 15 15 15 15 15 15 15 15 15	320 334 327 348 278 343 322 180 174 587 588 57 300 335 307 167 306 207 201 201 180 177 366 367	300 302 312 300 300 300 202 312 311
200 201 <td>300 301 302 303 302 303 302 303 304 302 302 304 302 304 302 303 303 303 304 304 302 304 302 304 302 304 302 304 302 304 303 303 303 304<td>30 34 32 704 367 244 274 362 240 214 116 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 468 467 116 467 468 467 116 467 468 467 116 467 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468</td><td>30 302 312 303 304 207 303 303 904 80 207 301 901 801 70 901 701</td></td>	300 301 302 303 302 303 302 303 304 302 302 304 302 304 302 303 303 303 304 304 302 304 302 304 302 304 302 304 302 304 303 303 303 304 <td>30 34 32 704 367 244 274 362 240 214 116 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 468 467 116 467 468 467 116 467 468 467 116 467 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468</td> <td>30 302 312 303 304 207 303 303 904 80 207 301 901 801 70 901 701</td>	30 34 32 704 367 244 274 362 240 214 116 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 116 467 468 467 116 467 468 467 116 467 468 467 116 467 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468 467 116 468	30 302 312 303 304 207 303 303 904 80 207 301 901 801 70 901 701
200 204 207 207 207 208 207 208 207 208 <td>300 302 302 303 304 302 322 324 304 324<td>320 321 320 240 240 240 240 241 241 241 141<td>310 302 322 320 300 300 300 320 320 320 320 321</td></td></td>	300 302 302 303 304 302 322 324 304 324 <td>320 321 320 240 240 240 240 241 241 241 141<td>310 302 322 320 300 300 300 320 320 320 320 321</td></td>	320 321 320 240 240 240 240 241 241 241 141 <td>310 302 322 320 300 300 300 320 320 320 320 321</td>	310 302 322 320 300 300 300 320 320 320 320 321
30 30 30 70 <th70< th=""> 70 70 70<!--</td--><td>Max Dots Dir <thdir< td="" th<=""><td>300 300<td>100 100</td></td></thdir<></td></th70<>	Max Dots Dir Dir <thdir< td="" th<=""><td>300 300<td>100 100</td></td></thdir<>	300 300 <td>100 100</td>	100 100
Jose Male Jose Male <t< td=""><td>10 00 10<</td><td>10 10<</td><td>Main Main <th< td=""></th<></td></t<>	10 00 10<	10 10<	Main Main <th< td=""></th<>
310 310 <td>Mai Mai Mai<td>100 100<td>Me Dot <thdot< th=""> Dot <thdo< th=""> <thdo< th=""> <thdo< th=""></thdo<></thdo<></thdo<></thdot<></td></td></td>	Mai Mai <td>100 100<td>Me Dot <thdot< th=""> Dot <thdo< th=""> <thdo< th=""> <thdo< th=""></thdo<></thdo<></thdo<></thdot<></td></td>	100 100 <td>Me Dot <thdot< th=""> Dot <thdo< th=""> <thdo< th=""> <thdo< th=""></thdo<></thdo<></thdo<></thdot<></td>	Me Dot Dot <thdot< th=""> Dot <thdo< th=""> <thdo< th=""> <thdo< th=""></thdo<></thdo<></thdo<></thdot<>
	Max Max <td>10 10<</td> <td>Mai Mai Pai Mai Mai</td>	10 10<	Mai Mai Pai Mai
Mode Mode <th< td=""><td></td><td></td><td></td></th<>			

◆□ ▶ ◆□ ▶ ◆ 三 ▶ ◆ 三 ▶ ● ○ ○ ○ ○

Large–Scale Experiments on the Z340

Enumerating 2D transpositions

Inward spirals



イロト イヨト イヨト イヨト

æ

Large–Scale Experiments on the Z340

Enumerating 2D transpositions

Outward spirals

338 338 337 338 335 334 333 332 337 330 328 328 327 328 328 324 323	285 284 283 282 281 280 219 278 277 278 275 274 273 272 271 270 238	204 203 202 201 200 200 200 200 200 200 200 201 201	320 210 218 217 216 318 214 213 312 211 312 309 308 307 308 308 304
278 269 268 267 266 265 264 263 262 261 263 256 257 266 255 322	205 221 220 219 218 217 218 215 214 213 212 211 210 209 298 209 308	585 259 207 236 255 234 255 202 231 259 228 225 227 226 225 224 2 67	521 212 251 251 251 240 240 247 246 245 246 244 243 242 241 240 230 258 503
271 208 207 208 205 204 203 202 201 200 100 100 107 108 105 256 221	202 222 165 164 162 161 160 158 158 157 156 155 154 227 268 237	200 229 160 179 178 177 176 175 174 172 177 177 189 168 222 200	322 253 152 181 190 188 188 187 186 185 184 183 182 181 180 237 263
272 280 154 153 152 151 150 149 148 147 148 145 144 143 154 253 320	266 222 966 117 196 115 114 113 112 111 110 108 188 153 296 267 336	367 240 181 130 128 127 126 125 124 123 122 121 120 167 222 285	322 284 105 142 139 138 137 138 138 134 133 132 131 132 179 238 381
273 210 155 138 107 138 105 154 133 102 131 130 99 142 135 252 218	209 224 967 118 27 18 28 24 19 22 11 28 987 152 226 206 205	208 241 182 121 88 87 86 85 64 83 82 61 86 119 156 221 264	224 255 124 141 96 26 54 93 82 51 90 88 68 129 126 255 265
274 211 134 128 12 48 48 47 44 45 44 43 54 141 152 251 218	290 228 148 118 78 48 44 43 42 41 40 48 126 181 204 248 234	309 342 163 132 68 84 63 52 61 53 48 44 78 118 165 220 263	328 296 199 142 87 48 89 54 87 56 59 54 87 128 177 234 299
275 212 157 110 71 44 30 30 37 36 36 42 57 44 141 253 57	264 228 969 122 79 45 21 20 19 96 39 58 185 150 293 264 535	510 243 154 135 98 95 28 27 26 25 24 47 78 117 154 218 262	538 257 126 143 26 51 32 51 36 29 28 53 66 127 5% 259 286
278 213 138 111 12 41 18 17 16 15 34 81 96 139 190 249 276	212 227 130 121 10 47 22 5 4 17 38 47 154 149 222 243 232	211 244 185 134 21 24 22 15 2 8 23 44 77 158 383 278 281	327 238 197 168 99 62 33 12 11 10 27 52 65 128 175 232 287
277 214 159 112 73 42 19 4 3 14 30 60 95 138 180 248 318	200 229 171 122 81 45 22 6 3 96 27 66 183 145 291 262 331	312 245 168 135 82 87 30 11 0 7 22 45 78 116 162 217 280	229 210 199 145 100 53 24 13 6 9 25 11 54 125 174 231 296
278 215 900 113 14 40 20 5 2 13 22 59 94 137 166 247 274	254 229 572 529 52 49 24 7 2 55 36 55 552 547 220 261 230	213 245 187 136 20 26 21 12 1 8 21 44 75 154 26 279	529 260 199 146 101 54 35 14 1 8 25 50 60 124 175 200 285
279 226 361 316 25 46 21 8 1 12 21 88 80 126 187 268 213	205 220 173 124 83 80 28 8 1 14 35 64 101 146 199 260 229	314 247 188 137 84 88 32 13 2 8 20 43 F4 113 180 218 278	338 241 200 147 162 48 26 18 2 7 24 48 42 122 172 229 244
280 217 952 115 25 46 22 7 6 11 20 57 92 126 96 245 212	296 291 574 525 64 57 28 9 8 59 34 53 56 58 589 529	315 243 199 135 95 80 30 14 3 4 19 42 73 112 159 214 277	501 282 201 148 905 56 37 16 3 6 27 46 51 122 171 229 285
287 278 763 776 77 48 23 8 9 70 29 86 97 734 785 244 277	297 222 175 128 88 82 27 10 11 12 23 82 89 144 187 238 227	276 269 190 139 96 61 34 19 19 17 16 41 72 111 196 213 275	202 243 202 148 104 67 28 17 4 5 22 47 60 121 170 227 280
252 219 56 117 35 47 24 25 26 27 28 55 50 133 56 243 310	296 201 526 127 86 55 28 29 30 31 32 51 56 143 196 217 526	917 250 191 140 97 42 38 34 37 34 30 40 71 110 97 212 275	333 284 253 156 955 58 20 18 18 20 21 45 79 128 169 225 291
200 220 905 118 79 48 49 00 51 52 53 54 69 132 165 542 209	279 224 377 128 17 54 55 50 57 58 59 61 17 542 116 250 235	218 251 132 141 98 83 64 85 66 67 88 69 78 159 156 211 214	204 215 204 151 100 88 40 41 42 43 44 45 18 118 168 225 280
284 221 346 118 80 81 82 83 84 85 86 87 88 131 982 241 328	200 228 178 129 88 88 88 81 82 83 84 88 86 81 32	318 212 193 142 88 180 101 132 163 194 188 196 137 168 155 216 275	338 266 255 152 157 78 71 72 73 36 78 78 77 118 167 226 265
285 222 107 128 121 122 123 124 125 126 127 128 129 138 141 240 207	81 28 59 59 50 51 51 51 50 54 55 58 57 58 50 50 50 50 50	320 253 134 145 144 145 145 147 148 148 149 150 151 152 153 154 259 272	506 247 206 153 108 108 110 111 112 115 114 115 115 117 166 223 286
218 223 168 169 130 171 172 173 174 175 178 177 178 179 160 239 208	202 227 180 181 182 183 184 185 188 187 188 189 180 191 182 223 222	221 254 185 186 187 188 189 200 201 202 283 204 205 206 207 238 271	237 288 207 154 155 156 157 158 159 160 161 162 163 164 165 222 287
287 224 225 228 227 228 229 230 231 232 230 234 235 238 237 238 388	805 298 280 241 242 240 244 245 248 247 248 240 250 251 252 821	322 255 256 267 258 260 260 261 262 263 264 265 268 267 268 269 270	338 280 255 298 210 211 212 213 214 215 218 217 215 219 220 221 286
218 289 290 291 282 290 284 285 298 287 298 289 300 301 352 300 304	204 205 206 207 208 209 218 211 212 213 214 215 216 217 218 219 222	323 234 325 336 327 328 229 330 331 332 333 334 336 336 337 338 339	200 200 211 272 273 214 275 279 277 278 279 280 281 282 283 284 285
500 200 217 272 273 274 275 279 277 278 279 280 281 282 283 284 285	NO 204 NO 205 NO 207 NO 208 NO 201 202 205 204 205 206 207 206 208	384 805 386 367 808 389 393 511 312 513 514 315 516 317 518 518 325	288 286 290 291 282 290 284 295 298 287 298 286 900 901 982 900 994
200 200 217 222 235 234 235 237 238 237 238 239 286 281 282 283 284 285 288 289 208 288 235 237 235 237 238 238 238 237 238 238 238	825 524 525 528 527 528 528 528 526 526 527 522 525 524 525 526 527 528 528 528 527 528 528 528 527 528 528 528 527 528 528 528 527 528 528 528 527 528 528 528 527 528 528 528 527 528 528 528 527 528 528 528 528 528 528 528 528 528 528	204 205 208 207 208 209 200 201 212 213 214 215 214 217 218 219 200 202 228 228 249 240 241 242 243 244 245 248 247 248 240 251 252 257	200 200 200 201 202 200 204 205 206 201 200 206 200 200 200 200 200 200 200 200
500 200 217 222 215 214 205 215 217 218 217 208 219 200 201 200 200 200 200 200 300 200 200 217 212 213 210 210 210 210 210 210 210 200 221 200 300 207 154 105 156 157 157 156 158 100 150 152 152 156 156 152 22 20	215 5A 305 5A 307 5A 5A 307 5A 5A 5A 306 5A 307 3A 34 34 35 5A 35 3A 30 5A 30 222 3A 24 32 3A 34 34 34 34 34 34 34 34 34 34 34 34 34	944 305 308 307 308 948 310 544 312 513 544 315 548 317 518 318 320 328 328 329 346 345 343 348 348 348 348 348 348 348 328 328 328 328 328 329 327 588 44 55 487 542 487 544 55 486 557 588 549 158 441 52 23 322	200 200 200 201 202 202 200 204 205 200 201 200 205 200 201 202 200 204 200 201 202 200 201 201 201 201 201 201
300 201 <td>355 544 355 568 357 368 508 500 101 301 303 304 308 301 301 303 303 303 303 301 301 303 303 301 301 301 301 303 303 301 301 303 303 301 301 303 303 301 301 303 303 301 301 303 303 301 301 303 303 301 301 301 303 301<td>304 305 306 307 508 307 508 307 208<td>368 369 201 352 202 204 205 206 201 202 200 204 205 206 201 202 200 204 200 204 200 201 202 201 203 201 203 201 201 201 204 201</td></td></td>	355 544 355 568 357 368 508 500 101 301 303 304 308 301 301 303 303 303 303 301 301 303 303 301 301 301 301 303 303 301 301 303 303 301 301 303 303 301 301 303 303 301 301 303 303 301 301 303 303 301 301 301 303 301 <td>304 305 306 307 508 307 508 307 208<td>368 369 201 352 202 204 205 206 201 202 200 204 205 206 201 202 200 204 200 204 200 201 202 201 203 201 203 201 201 201 204 201</td></td>	304 305 306 307 508 307 508 307 208 <td>368 369 201 352 202 204 205 206 201 202 200 204 205 206 201 202 200 204 200 204 200 201 202 201 203 201 203 201 201 201 204 201</td>	368 369 201 352 202 204 205 206 201 202 200 204 205 206 201 202 200 204 200 204 200 201 202 201 203 201 203 201 201 201 204 201
300 200 210 210 210 210 210 210 210 210 210 211 <td>100 NM 105 NM 100</td> <td>Me SM SM<</td> <td>201 201</td>	100 NM 105 NM 100	Me SM SM<	201 201
Max Max <td>bit bit bit<td>M4 M5 M6 M6 M6 M6 M6 M6 M6 M6 M7 M7<</td><td>AM AM AM<</td></td>	bit bit <td>M4 M5 M6 M6 M6 M6 M6 M6 M6 M6 M7 M7<</td> <td>AM AM AM<</td>	M4 M5 M6 M6 M6 M6 M6 M6 M6 M6 M7 M7<	AM AM<
	Dia Dia <thdia< th=""> <thdia< th=""> <thdia< th=""></thdia<></thdia<></thdia<>		Image: Second

Sam Blake The Quest to Solve the Zodiac 340 Cipher

イロン イロン イヨン イヨン

æ –

Large-Scale Experiments on the Z340

Enumerating 2D transpositions

Diagonal transpositions



Sam Blake The Quest to Solve the Zodiac 340 Cipher

イロト イヨト イヨト イヨト

э
Diagonal transpositions cont.



Sam Blake The Quest to Solve the Zodiac 340 Cipher

イロト イヨト イヨト イヨト

э

Proper two-dimensional decimations

		////		
	1		//	
		$\geq >$		

Sam Blake

◆□▶ ◆□▶ ◆ ミ ▶ ◆ ミ ▶ ● ○ ○ ○ ○

Proper two-dimensional decimations cont.



回とくほとくほと

э

Proper two-dimensional decimations cont.



▲□ ▶ ▲ □ ▶ ▲ □ ▶ …

∃ 990

Compositions of transformations

- 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



Once again, this search turned up nothing.

< ロ > < 同 > < 回 > < 回 > .

э

Compositions of transformations

- 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 53824 pairs of transpositions using azdecrypt and zkdecrypto. For example



Once again, this search turned up nothing.

< ロ > < 同 > < 回 > < 回 > .

э

Large–Scale Experiments on the Z340 Compositions of transformations

- 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 53824 pairs of transpositions using azdecrypt and zkdecrypto. For example



・ 同 ト ・ ヨ ト ・ ヨ ト

Compositions of transformations

- 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 53824 pairs of transpositions using azdecrypt and zkdecrypto. For example



• Once again, this search turned up nothing.

く 目 ト く ヨ ト く ヨ ト

Compositions of transformations

- 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



• We further limited the search to candidates with a high bigram count.

Once again, this search turned up nothing

・ 同 ト ・ ヨ ト ・ ヨ ト

Compositions of transformations

- 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



• We further limited the search to candidates with a high bigram count.

Once again, this search turned up nothing

・ 同 ト ・ ヨ ト ・ ヨ ト

Compositions of transformations

- 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



• We further limited the search to candidates with a high bigram count.

• Once again, this search turned up nothing

(E)

Compositions of transformations

- 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



We further limited the search to candidates with a high bigram count.

Once again, this search turned up nothing

13,15-decimation

(E)

Compositions of transformations

- 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



• We further limited the search to candidates with a high bigram count.

Once again, this search turned up nothing

13,15-decimation

< 3 > < 3 > <

Compositions of transformations

- 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



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

13,15-decimation

▶ ∢ ∃ ▶

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

• 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

▲□ ▶ ▲ □ ▶ ▲ □ ▶ □ ● ● ● ● ●



◆□▶ ◆□▶ ◆ ミ ▶ ◆ ミ ▶ ● ○ ○ ○ ○

Splitting the cipher + transposition + homophonic substitution



Sam Blake The Quest to Solve the Zodiac 340 Cipher

◆□▶ ◆□▶ ◆ ミ ▶ ◆ ミ ▶ ● ○ ○ ○ ○

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.

	91	63	35		98	70	42	-14	105	77	49	21	112	84	56	28
68			103	75			110	82			117	89				96
	108	80			115					94				101		45
85	57	29	1	92	64	36	8	99	71		15	106	78	50	22	113
		97	69			104	76			111	83			118	90	62
102	74			109	81			116	88				95			11
51	23	114	86	58	30	2	93	65	37	9	100	72	44	16	107	79
	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	206	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		129	169	209	249
204	244	148	188	228	132			252	156	196	236	140	180		124	164
	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

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

	91	63	35		98	70	42	-14	105	77	49	21	112	84	56	28
68			103	75			110	82			117	89				96
	108	80			115					94				101		45
85	57	29	1	92	64	36	8	99	71		15	106	78	50	22	113
		97	69			104	76			111	83			118	90	62
102	74			109	81			116	88				95			11
51	23	114	86	58	30	2	93	65	37	9	100	72	44	16	107	79
	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		252	156	196	236	140	180		124	164
																_
	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
											_					

- 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.

	91	63	35		98	70	42		105	77	49	21	112	84	56	28
68			103	75			110	82			117	89				96
	108	80			115					94				101		45
85	57	29	1	92	64	36	8	99	71		15	106	78	50	22	113
		97	69			104	76			111	83			118	90	62
102	74			109	81			116	88				95			11
							93									79
	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		252	156	196	236	140	180		124	164
	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

* E * * E *

• 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

= nav

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.



通 ト イ ヨ ト イ ヨ ト ー

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.

														126	135	144
136	145															
	128	137	146	2												
			129	138	147											
					130	139	148									
								140	149	5						
									132	141	150					
											133	142	151	7		
												125		143	152	

						207	216	225	234	243	252	261	270	279	288	297
289	298													262		280
	281	290	299	155												263
			282	291	300	156										
					283	292	301	157								
					266		284	293	302	158						
						258	267	276	285	294	303					
									268		286	295	304	160		
				206		224	233	242	251	260	269	278	287	296	305	161

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

▶ < Ξ >

э

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.

				36	45	54	63	72	81	90	99	108	117	126	135	144
136	145															
	128	137	146													
			129	138	147											
					130	139	148									
								140	149	5						
									132	141	150					
											133	142	151	7		
												125		143	152	
						207	216	225	234	243	252	261	270	279	288	297

									234		252	261		2/9	288	297
289	298															280
		290	299													
	264		282		300	156										
					283	292	301									
			248		266		284	293	302	158						
									285	294	303					
									268		286	295	304	160		
				206		224	233	242	251	260	269	278	287	296	305	

	332		334		336		338		
		333		335		337		339	

▶ < ∃ >

• 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.

				36	45	54	63	72	81	90	99	108	117	126	135	144
136	145															
	128	137	146													
			129	138	147											
					130	139	148									
								140	149	5						
										141	150					
											133	142	151			
												125		143	152	
								225	234	243	252	261	270	279	288	297

											202				200	
289	298															280
		290	299													
			282	291	300											
			265		283	292	301									
					266		284	293	302	158						
						258	267	276	285	294	303					
									268		286	295	304	160		
										260	269	278	287	296	305	

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

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.

File Functions Forr	mat Statistics Opti	ions		
Open file Save state Load state	Solve Resume Stop task Swap	Substitution Substitution + columnar rearrangement Substitution + columnar transposition Substitution + crib list Substitution + crib list Substitution + mole and skips Substitution + nulls and skips	* III *	Task: substitution (FAUSED) 5-gramm_english_practicalcryptography_mortschetz.txt.gz Ttems: 76 tems per second 0.41 MTFS: 1.39 AVG soore: 19854.08 IOC: 0.07935 PC-cycles: 334.35
H-MGI (CVBECH GR (CVFEP2) <- 42 (hpCOGP-2] (-14) (- 452b C) (-4 (-53-V p-f_2) (-14) (-4 (-53-V p-f_2) (-14) (-4 (-53-V p-f_2) (-14) (-4 (-53-V p-f_2) (-14)	4k.L MOAD MOAD NI + K K.HK - CTL - CTL		A A .	Some: 20166.33 DOC: 0.0749 Moltsplicity: 0.3852 Minutest: 2.23 Repears: REAL EAD THAT (2) METR BECA ANEL AFRE HANT EAN PC-cycles: 201 E HOPES OF ARE HE SING LOTS OF FAENN <u>TRYING</u> <u>TO CATCH ME</u> THAN TAINT MT IN THATS SHOT WHICH BRINGO UP AVOINT ABOUT ME NAME IN A FREED OF THE <u>GAS CHAMBER</u> BECAASE IT WILL TEND ME DIVER ALL CE ALL THAT OO HAN BECAUSE TOO WHA SEENS UGH SLE SER TO WORS FOS ME THE REATERS IN A EL HE HAS NOTHING THEN THEY REACH PARALICITOT RES ALREAFE AND NO FLED THE FAME IA A FRE AND BECAUSE IS IT T THAT MR NEW ENTIE AE AEOL CL RAES NIEL AND IH FEND BFET

= nar

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

File Functions Forn	nat Statistics Opt	ions		
Open file	Solve	Substitution Substitution + columnar rearrangement	•	Task: substitution (using 2 CPU threads) 5-grams_english_practicalcryptography_wortschatz.txt.gz
Save state	Pause	Substitution + columnar transposition Substitution + crib grid	1	Items: 83 Items per second: 0.68 MIPS: 2.74
Load state	Stop task	Substitution + crib list Substitution + monoalphabetic groups		AVG score: 24379.25 IOC: 0.06744 PC-cycles: 67.55
	Swap	Substitution + nulls and skips	-	4
Input window		Substitution + polyphones		Output window
H:40[CV8EB+ 46[CVFF9<42]CH2 (NpC0p+2]CH2 (NpC0p+2]CH2 (NpC0p+2]CH2 NpC0p+2]CH2 NpC0p+2	5k.L MODD MODD X.K.K.K.K.K.K.K.K.K.K.K.K.K.K.K.K.K.K.K		~	Score: 24751.50 IOC: 0.0003 Multiplicity: 0.4117 Munutes: 1.43 Repears: THIN INTE COUND AND FOR INT NAM THE ING VER LE FE ER FC-eycles: 150 VE RIGHT IN GREEN THE PAINTSS OF THING THEIR LULL ENGLE AROUND IN TO DIE SINCE TO BETLE ON THEAD IN MATH IN DAYING TON FOR US SEVERS WERERN CLEANDY FOR LOUND ALBACK BY HAND SOME COMPLY APPLES

▲ □ ▶ ▲ 三 ▶ ▲ 三 ▶ →

- 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.

7 Show cipher 🔲 Edit cipher				r	Solve with cribs						Clea	r cril	os	Reload cipher			
-	н	0 P		E	Y	0	U	A	R	E	н					G	
Н	+	м	8		С	٧	@	K	E	В	+	*	5	k		L	
		Т		0						N	Т	R	Y	1	Ν	G	
d	R	[U	V	F	F	Z	9	<	>	22	Z	3	Р	>	L	
Г	0	С	Α	Т	С	н	м	E	Т	н	Α			Α			
(M	р	0	G	р	+	2	1	G	+	1	%	W	0	8	D	
Г	м				Т	н		Т		S	н	0			н		
2	2	b	^	D	1	+	4	1	5	J	+	٧	W		+	k	
С	н		R	1		G			Ρ	Α					Т	Α	
p_	+	f	Z	Р	Y	L	R	1	8	K	j	R	k		#	K	
В			T	м	E			м				A					
_	R	q	22	2		<	z	2	9	^	%	0	F	1	*	Н	
	0			н	E	G	Α	S	С	н	Α	м	В	E	R		
S	м	F	;	+	В	L	K	J	р	+	1	2	_	С	Т	f	
E	С		A				Т						E			м	
B	р	Z	0	U	N	У	G)	У	7	t	-	С	Y	A	2	
_									С	E	A			T	н		
N	1 :	^	l i	*	X	Z	6	d	р	C		d	d	G	+	4	

回 とくほとくほとう

æ

- 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.

✓ Show cipher				S	olve	with	crib	в		Clea	r cril	os	Reload cipher																				
_	H O P		Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	Р	E	Y	0	U	A	R	E	н					G	
Н	+	м	8		С	٧	@	K	E	В	+	*	5	k		L																	
		Т		0						N	Т	R	Y	Т	Ν	G																	
d	R	[U	V	F	F	Z	9	<	>	22	Z	3	Р	>	L																	
Т	0	С	Α	Т	С	н	м	E	Т	н	Α			Α																			
(M	р	0	G	р	+	2	1	G	+	1	%	W	0	8	D																	
Т	м				Т	н		Т		S	н	0			н																		
#	2	b	^	D	(+	4	(5	J	+	٧	W)	+	k																	
С	н		R	1		G			Р	A					Т	Α																	
р	+	f	Z	Р	Y	L	R	1	8	K	j	R	k		#	K																	
в			T	м	E			м				A																					
_	R	q	22	2		<	z	2	9	^	%	0	F	1	*	Н																	
	0			н	E	G	Α	S	С	н	Α	м	В	E	R																		
S	м	F	;	+	В	L	K	J	р	+	1	2	_	С	Т	f																	
E	С		A	_			Т						E			м																	
В	р	Z	0	U	N	У	G)	У	7	t	-	С	Y	A	2																	
									C	E	A			T	н																		
N	:	^	j	*	X	Z	6	d	p	C		d	d	G	+	4																	

E > < E > ...

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

File Functions Form	nat Statistics Opt	ions		
Open file Save state	Solve	Substitution Substitution + columnar rearrangement Substitution + columnar transposition	A H	Task: substitution + crib grid (using 2 CPU threads) 6-grams_english_jarlve_reddit.txt.gz
Load state	Stop task	Substitution + crib grid Substitution + crib list Substitution + monoalphabetic groups		Items: 57 Items per second: 1.27 MIPS: 2.49 AVG score: 24014.24 IOC: 0.06114 PC-cycles: 153
	Swap	Substitution + nulls and skips Substitution + polyphones	-	۰ ۱
dR (UVFFz9<>#2 (MpOGp+2 G+1% #2b^D(+4(5J+V p+f2PYLR/8KjR _Rq#2 <z29^%0 SMF;+BLKJp+12</z29^%0 	3P>L W06D W)+k k.#K F1*H cTf			Repease: ALL ING (2) THE THE (2) INT MET BE AT SE IN OU TA LL PC-cycles: 153 I HOPE YOU ARE HAVING LOTS OFF AN IN TRYING TO CATCH ME THAT WASNT ME ON THE TV SHOW
BpzOUNyG)y7t- N:^j*Xz6dpcld	cYA2 dG+4			WHICH BRINGO UP A POINT ABOUT ME I AM NOT AFRAID OF THE GAS CHAMBER BECAASE IT WILL SEND ME TO PAY ALL CE ALL THE
			-	

イロン イロン イヨン イヨン

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

4 3 4 3 4 3 4

Crib	grid																×
⊽ s	how	ciph	er		Edit o	iphe:	r	S	olve	with	crib	5		Clea	r crit	os	Reload cipher
	н	0	Р	E	Y	0	U	Α	R	E	н	Α	۷	Т	N	G	
Н	+	М	8	1	C	V	@	K	E	В	+	*	5	k		L	
L	0	Т	S	0	F	F	A	N	1	N	Т	R	Y	1	N	G	
d	R	1	U	٧	F	F	z	9	<	>	#	Z	3	Р	>	L	
T	0	C	A	Т	С	н	м	E	Т	н	Α	Т	w	Α	S	Ν	
1	М	р	0	G	р	+	2	1	G	+	1	%	W	0	8	D	
T	м	Ē	0	N	Ť	н	E	Ť	٧	S	н	0	w	w	н	1	
22	2	b	^	D	ſ	+	4	ſ	5	J	+	V	W	1	+	k	
C	н	в	R	1	Ň	G	0	Ù	Р	Α	Р	0	1	N	Т	Α	
р	+	f	Z	Р	Y	L	R	1	8	K	i	R	k		#	K	
B	0	U	т	м	E	1	A	M	N	0	Ť	A	F	R	A	1	
	R	q	#	2	1	<	z	2	9	^	%	0	F	1	*	Н	
D	0	F	Т	н	Ē	G	Α	S	С	н	Α	м	в	Е	R	в	
S	м	F	:	+	В	L	K	J	D	+	1	2		С	Т	f	
E	С	Α	A	S	E	1	т	w	î.	L	L	S	E	N	D	м	
В	D	Z	0	U	N	v	G	1	v	7	t	-	с	Y	A	2	
E	T	0	Р	A		Á		Ĺ	ć	E	A	L	L	Т	н	E	
N	:	^	i	*	X	z	6	d	D	С	1	d	d	G	+	4	-
S	0	0	Ĥ	E	N	в	E	С	A	υ	S	E	E	0	0	w	
	B	B	+	4	>	f	-	D	Z	1	J	N	b	V	M	1	
н	A	٧	E	E	N	S	Ú	G	н	S	L	A	٧	E	B	Ť	
+	1	5	1	1		U	a	L	+	U	t	*	5	С	Z	G	
0	w	0	R	v	F	0	v	м	E	w	н	E	R	E	E	S	
B	1	V	E	5	F	V	5	2	С	W	+	1	Т	В	4	-	
E	Ŕ	Y	0	N	E	E	L	н	E	н	A	s	N	0	т	н	
	Т	С	^	D	4	С	t	+	С	+	z	J	Y	М	ſ	+	
1	N	G	w	н	E	N	Т	н	E	Y	R	E	Α	С	Ĥ	Р	
y		L	W	+	В		;	+	В	3	1	С	0	р	+	8	
Á		Α		1	С	E	S	0	Т	R	E	Y	Α	L	R	E	
1	X	z	6	P	D	b	8	R	G	1	В	C	0	7	T	В	
A	F	A	A	1	D	T	0	F		E	T	T	н	1	F	A	
Z	F	*	K	<	S	<	M	F	6	N	:	ſ	+	H	F	K	
M	N	0	E	A	F	R	E	A	1	D	В	Ň	С	A	υ	1	
2	q	^	4	0	F	Т	B	0	1	S	f	9	n		1	v	

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



イロト イポト イヨト イヨト

Untransposed, deciphered 2nd section of Z340



通 ト イ ヨ ト イ ヨ ト -

- 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



< 回 > < 回 > < 回 >

- 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	А	А	s	0	Н	0	s	н	А	С	L	I	F	Е	I	s
s	Н	0	U	٧	L	R	Е	Ν	Ν	Е	С	Е	R	0	А	А
М	Т	Е	А	0	s	Е	А	٧	R	Е	0	Ν	н	s	Е	F
А	L	Ν	D	T	т	н	Е	Е	٧	F	Е	Е	т	т	Р	0
А	Т	F	Е	0	в	۷	М	Е	Е	Ν	Е	0	Е	L	Н	Н
I.	Е	R	Н	R	А	Т	Е	Ν	Y	R	Ν	0	s	R	۷	s
Е	Е	Ν	Y	А	Е	Α	Т	А	С	0	Ν	В	0	U	Т	М
0	Е	R	Н	G	R	L	Y	T	Н	F	А	W	Е	Е	W	G
н	Н	w	w	Y	Α	w	Е	T	Α	D	T	R	U	Т	w	С

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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	А	Α	s	0	н	0	s	н	Α	С	L	I	F	Е	T	s
s	Н	0	U	٧	L	R	Е	Ν	Ν	Е	С	Е	R	0	А	А
М	Т	Е	А	0	s	Е	А	٧	R	Е	0	Ν	н	s	Е	F
А	L	Ν	D	T	Т	Н	Е	Е	٧	F	Е	Е	т	Т	Ρ	0
А	Т	F	Е	0	в	٧	М	Е	Е	Ν	Е	0	Е	L	н	Н
L	Е	R	Н	R	А	Т	Е	Ν	Y	R	Ν	0	s	R	۷	s
Е	Е	Ν	Y	А	Е	Α	Т	А	С	0	Ν	В	0	U	Т	М
0	Е	R	Н	G	R	L	Y	Т	Н	F	А	W	Е	Е	W	G
н	Н	w	w	Y	А	w	Е	L	А	D	T	R	U	Т	w	С

・ 同 ト ・ ヨ ト ・ ヨ ト …

- 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	Α	А	s	0	Н	0	s	н	Α	С	L	T	F	Е	T	S
s	Н	0	U	٧	L	R	Е	Ν	Ν	Е	С	Е	R	0	А	А
М	Т	Е	А	0	s	Е	А	٧	R	Е	0	Ν	н	s	Е	F
А	L	Ν	D	T	т	н	Е	Е	٧	F	Е	Е	т	т	Ρ	0
А	Т	F	Е	0	в	۷	М	Е	Е	Ν	Е	0	Е	L	Н	Н
L	Е	R	Н	R	А	Т	Е	Ν	Y	R	Ν	0	s	R	۷	s
Е	Е	Ν	Y	А	Е	А	Т	Α	С	0	Ν	в	0	U	Т	М
0	Е	R	Н	G	R	L	Y	T	Н	F	А	W	Е	Е	W	G
Н	Н	w	w	Y	Α	w	Е	T	А	D	T	R	U	Т	w	С

A B > A B >

- 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

* 注入 * 注入 -

= nar

The Z340 Substitution Key and Transposition

The final key and transposition for the Z340.

ANKOJO BDJ C9 DOAS EOBNUJ FF GL H+ I<HPXY LAQI MO NOADDY OMRVA PAT ROETXZ SP-JU TEMPOTIG U/MO VO WOW YOC



Sam Blake The Quest to Solve the Zodiac 340 Cipher

э.

Submitting our Solution to the FBI

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

	Z340 has been solved > Inbox ×								
Ø	David Oranchak «doranchak@gmail.com» Image: 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								
	Vex • Sea was was was was was was was was was wa								

◆□▶ ◆□▶ ◆ ミ ▶ ◆ ミ ▶ ● ○ ○ ○ ○

- 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.



#Breaking - Our statement regarding the **#Zodiac** cipher:

The FBI is aware that a cipher attributed to the Zodiac Killer was recently solved by private citizens. The Zodiac Killer case remains an ongoing investigation for the FBI San Francisco division and our local law enforcement partners. The Zodiac Killer terrorized multiple communities across Northern California and even though decades have gone by, we continue to seek justice for the victims of these brutal crimes. Due to the ongoing nature of the investigation, and out of respect for the victims and their families, we will not be providing further comment at this time.

FBI FEDERAL BUREAU OF INVESTIGATION

SAN FRANCISCO DIVISION

- 4 同 ト 4 ヨ ト 4 ヨ ト

6:21 AM · Dec 12, 2020

- 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.



#Breaking - Our statement regarding the #Zodiac cipher:

The FBI is aware that a cipher attributed to the Zodiac Killer was recently solved by private citizens. The Zodiac Killer case remains an ongoing investigation for the FBI San Francisco division and our local law enforcement partners. The Zodiac Killer terrorized multiple communities across Northern California and even though decades have gone by, we continue to seek justice for the victims of these brutal crimes. Due to the ongoing nature of the investigation, and out of respect for the victims and their families, we will not be providing further comment at this time.

FBI FEDERAL BUREAU OF INVESTIGATION

SAN FRANCISCO DIVISION

・ 同 ト ・ ヨ ト ・ ヨ ト

6:21 AM · Dec 12, 2020

- 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.



#Breaking - Our statement regarding the **#Zodiac** cipher:

The FBI is aware that a cipher attributed to the Zodiac Killer was recently solved by private citizens. The Zodiac Killer case remains an ongoing investigation for the FBI San Francisco division and our local law enforcement partners. The Zodiac Killer terrorized multiple communities across Northern California and even though decades have gone by, we continue to seek justice for the victims of these brutal crimes. Due to the ongoing nature of the investigation, and out of respect for the victims and their families, we will not be providing further comment at this time.

FBI FEDERAL BUREAU OF INVESTIGATION

SAN FRANCISCO DIVISION

・ 同 ト ・ ヨ ト ・ ヨ ト

6:21 AM · Dec 12, 2020

- 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.



#Breaking - Our statement regarding the **#Zodiac** cipher:

The FBI is aware that a cipher attributed to the Zodiac Killer was recently solved by private citizens. The Zodiac Killer case remains an ongoing investigation for the FBI San Francisco division and our local law enforcement partners. The Zodiac Killer terrorized multiple communities across Northern California and even though decades have gone by, we continue to seek justice for the victims of these brutal crimes. Due to the ongoing nature of the investigation, and out of respect for the victims and their families, we will not be providing further comment at this time.

FBI FEDERAL BUREAU OF INVESTIGATION

SAN FRANCISCO DIVISION

くぼ ト く ヨ ト く ヨ ト

6:21 AM · Dec 12, 2020

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.



< ロ > < 同 > < 三 > < 三 >

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

Subscribe Now \$1/8 weeks

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

the Zodiac murderer of CORONAVIRUS AND PANDEMIC > U.S. angling to secure more of Pfizer's coronavirus vaccine last 15 his D, black power, melvin eats SoCal cities consider renewed 'hero pay' for STIRE 18, 1948 grocery store workers amid COVID-19 surge This is the Zodiac speaking By the way have you created Joe Biden and Mike Pence will receive COVID-19 the last cipher I vaccine soon 13 nome AENOSKOMOJNAM I am mildly cerous as to how ICU capacity explained you have on my moner hope you do not Party, Anotherization over, Samo Solid, Dout Some Rail, somethip at more Classes, front will 7 M Automatic nend now. shirk that I was the one to sequences Slage, factory, Latante, Hardworkley who wiped out that blue Straining & Tauto meannie with a bomb at the Hundreds of state prison inmates in San Diego County sickened with COVID-19 cop station . Amateur sleuths from the U.S., Australia and Belgium teamed up to decipher a coded letter the Zodiac Killer sent to the San

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

Cases statewide » 1,699,181 confirmed

< ロ > < 同 > < 三 > < 三 >

21,887

By ASSOCIATED PRESS

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

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

Edit

・ 同 ト ・ ヨ ト ・ ヨ ト …

3

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



A long-unsolved puzzle sent by the Zodiac Killer to

く 同 と く ヨ と く ヨ と

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



Photo illustration.

• = • • = •



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 1966 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 naradise all the sonore because I now



This is a file copy of a cryptogram sent to the San Francisco Chronicia in 1980 by the Zodia: Killer. A coded letter mailed to a San Francisco newspaper by the Zodia: serial killer in 1969 has been deciphered by a team of amateur eleuths from the United States, Australia and Bedjium, the San Francisco Chronicle reported Friday, Dec. 11, 2020. San Francisco Chronicle Wa AP, File

・ 同 ト ・ ヨ ト ・ ヨ ト





イロト イポト イヨト イヨト



- n c c

THE ASSAULAGE

World North America Crime

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

By Sharon Bernstein

December 12, 2020 - 11.19pm



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.



< ∃ →

• 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?

• = • • = •

• 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?

• = • • = •

- 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?

• = • • = •

- 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?

A B > A B >

- 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 guickly.

- 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?

A B > A B >

- 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?

A B M A B M

- 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?

A B M A B M
- 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?

A B M A B M

э.

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



This is the Zodiac speaking By the way have you cracked the last cipher I sent you ? AENGOKOMOJNAM

- 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.

・ロト ・ 一下・ ・ ヨト・

э

This is the Zodiac speaking By the way have you cracked the last cipher I sent you ? AENGOKOMOJNAM

- 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.

・ロト ・ 同 ト ・ ヨ ト ・ ヨ ト

This is the Zodiac speaking By the way have you cracked the last cipher I sent you ?. My name is -AENGOKOMOJNAM

- 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.

This is the Zodiac speaking By the way have you cracked the last cipher I sent you ?. My name is -AENOOKOMOJNAM

- 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.

- 小田 ト イヨト 一日

This is the Zodiac speaking By the way have you cracked the last cipher I sent you ?. My name is — AENOOKOMOJNAM

- 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.

- 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.

э

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト …

э

- 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.

・ 同 ト ・ ヨ ト ・ ヨ ト

- 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.

- 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.

* E * * E *

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.

<回>< E> < E> < E> <

∃ 990