Taylor & Francis
Taylor & Francis Group

Cryptanalysis of Beale Cipher Number Two

TODD D. MATEER

Abstract This article documents the author's attempt to solve Beale Cipher Number Two using a transcript of the original Declaration of Independence. This was a much more difficult task than suggested in *The Beale Papers*. Based on discoveries learned in this process, the author concludes that the Beale ciphers are likely a hoax.

Keywords Beale cipher, cryptanalysis, Declaration of Independence

1. Introduction

In 1885, J. B. Ward published a booklet called *The Beale Papers* [1] which describes a fabulous treasure that he claimed is buried somewhere in the Blue Ridge Mountains of Virginia. The location of the treasure is described in three ciphers written by a Thomas Jefferson Beale and given to Robert Morriss, the owner of a tavern near the present city of Roanoke. The document also claims to provide the solution of one of the ciphers.

The two remaining ciphers have never been solved, meaning that the buried treasure possibly remains unclaimed today. However, there are those that believe that *The Beale Papers* are a fraud and no such treasure exists.

To explore the question of the validity of the Beale ciphers, the present author first undertook a careful study of the solved cipher. He attempted to follow the instructions given in *The Beale Papers* to transform the seemingly random sequence of numbers into the message provided in *The Beale Papers*. This article documents the author's progress in this task. The reader is encouraged to attempt to reproduce the results on his or her own to determine the likelihood of whether a person without computer technology could have actually solved one of the Beale ciphers.

2. Cryptanalysis of Beale Cipher Number Two

The solved cipher is assigned the number two in the series of three ciphers. According to *The Beale Papers*, the numbering of the ciphers was determined by Beale as communicated in one of his letters to Morriss.

In *The Beale Papers*, the author describes that Cipher Number Two can be solved by numbering each word in the Declaration of Independence. Each number in the cipher is then translated into the first letter of the corresponding numbered word in the Declaration of Independence. For example, since the first word of the

Address correspondence to Todd D. Mateer, Howard Community College, 10901 Little Patuxent Pkwy, Columbia, MB 21044, USA. E-mail: tmateer@howardcc.edu

Declaration of Independence is "when," then a 1 in the cipher would be translated into the letter W. By following this process for each letter in the second cipher, the author of *The Beale Papers* claims that one should obtain the message given in the pamphlet describing the treasure.

The author attempted to follow these instructions without any additional aide from the pamphlet. As a first step, the author obtained a transcript of the Declaration of Independence from the National Archives through their website [4]. The author then wrote a computer program which would create the key using the first letter from each word in the Declaration of Independence. The program then replaced each number in the cipher with its corresponding letter in the array. The results were as follows:

```
  0: ahaie depos otedt nttte ointt oaitd strsa boapt hrrmi lestr
 50: oabaa ottst tafep coiat ionor iaalt snpti ntbea owtht ssram
100: wnhst hhfbh ntdth ntoof hcang mttaw fntbt tonat fgphi otatt
150: ttheo attoe swott tttdt sabea tiiti ntndb ththr tfttb ewnth
200: thotn tttde posit eotta stedo otinh itdrt tanda oigte tfoos
250: estth btlds tittt http ghtta odbed indtw efief ornds oosaa
300: ieroi posit tdnhi iiaht eeftt nttee nthes econd watmw dnttu
350: tifht eentw entth ntwfs aonst ottot htine ttfnh aetre dcnos
400: eienp oands hsaoa owtot welii oafob edato eigtt teiah ttfti
450: aierm fsoti wtfso btain idtns tehaa tinep chang etotw intgo
500: ntftt tatto nttdi alail tattt gttit rhtss andtt aaigs theab
550: oieit secrb tatpc eohdi nibhf ohthw ittdg ttchi ittth eiitf
600: tnith aftlt fined wstts tonta ndthi itste atres tonth ltdst
650: onett oitee tintt twuar htttb hpioe rtamd eront ditcg tlttt
700: heopi atloc alitt tsttt imtdt tttha tftti ostea lttwi lafit
750: adstt indtn gtn
```

This is very different from the plaintext advertised in *The Beale Papers*. After checking the program several times for errors, this is the correct output of the deciphering process if the instructions are followed and the original Declaration of Independence is used to decrypt the message.

Although the above message is unintelligible, several words from the English language appear in the output. The following table gives five words observed in the output along with their location in the putative plaintext above.

43	miles
334	second
485	change
208	deposit
464	obtain

Since it is highly unlikely that these words would appear in the output using an incorrect key, this is a clue that the author was on the right track. The program was modified to replace these characters with capital letters in the output since the author was somewhat confident that these parts of the message were deciphered correctly. Additionally, whenever a character was changed, the program would also change all other characters encrypted with the same key value. The new output of the deciphering process was as follows:

```
  0: ahaie Depos otEdt Nttte ointt OaitD strsa boapt hrrMI LEStr
 50: oaBaa ottSt tafep coiat IoNOr iaalt snpti ntBea owtht Ssram
100: wnhst hhfbh ntDth ntOof hcaNG mttaw fntBt tonat fGphI otatt
150: tTHeo attoE Swott tttdt sabea tiitI Ntndb thtHr tfttb EwntH
200: thotn tttDE POSIT eotta SteDO otiNh itDrt taNDa oigte tfoos
250: estth btlds tiTtt httia Ghtta oDbED iNDtw efief orndS oosaa
300: ieroi Posit tDnhi iIaHt Eeftt Nttee NthES ECOND wAtmw dnttu
350: tIfHt EENtw Entth Ntwfs aonSt ottot htINE ttfnh aetre DcNoS
400: EiENP oandS hsaoa owtot wElii oafob eDato EIGtt tEIah ttfti
450: aiErm fSOti wtfSO BTAIN iDtNS tehaa tInEp CHANG Etotw intgo
500: Ntftt tatto NttDi aLail tattt gttit rHtsS anDtt aaigS THEab
550: oieit sEcrb tatPc eohdI nIbhf ohthw Ittdg ttchi ittth Eiitf
600: tnith aftlt fINeD wsttS toNta Ndthi itstE atreS tonth ltdSt
650: ONEtt oitEe tintt twuar htttb hPice rtamd EroNt Ditcg tlttT
700: heopi atLOC ALItt tsttt imtdt ttTHa tfttI ostea Lttwi lafit
750: aDstt InDtN Gtn
```

By reviewing the above output, the reader should be able to observe some additional words which are "almost correct." It was hypothesized that there are some minor error(s) in the cipher or key that prevents the remainder of the message from being deciphered correctly.

The program was modified so that a user could interactively change these sections of the output to what is believed to be the correct plaintext. The author made the following adjustments to the output:

5	DeposotEd	deposited
354	tEENtwEntt	teentwenty
707	LOCALItY	
399	SEiENPoandS	sevenpounds
0	ahaVe	ihave
548	aboVe	

The middle column gives the original characters in the plaintext and the rightmost column documents the author's change to the output. Changes made to words at the top of the table above also changed some characters in the words at the bottom of the table since all characters using the same key value are changed simultaneously by the program. The results of these changes were as follows:

```
  0: IHAVE DEPOS ITEDt Nttte oiNtY OaitD strsa boapt hrrMI LEStr
 50: OaBUa ottSt tafEp coVAT IONOr Vaalt snpti nTBEa owtHt Ssram
100: wnhst hhfbh ntDTh ntOof hcaNG mttIw fntBt toNat fGphI otaYt
150: tTHEo atToE Swott tttdt SabEa tVitI NtndB thtHr tfttb EwntH
200: thotn tttDE POSIT eottI SteDO otiNH itDrt taNDa OigTE tfoos
250: estth btlDs tiTtt htYiI GHtta oDbED iNDTW EfVEf OrNDS OoSIa
300: VEroi POSit tDNhV iIaHt EEftt NttEE NthES ECOND wAtmw Dnttu
350: tIfHT EENTW ENTYh Ntwfs aONSt ottot htINE ttfNh UetrE DcNoS
400: EVENP OUNDS hsaOa owtot wElVi oafob EDato EIGtt YEIaH Ttfti
450: aVErm fSOti wtfSO BTAIN iDtNS TehUa tINEp CHANG Etotw Vntgo
500: Ntftt tatto NttDV aLUil tattt gttit rHtsS aNDtt aaigS THEAB
```

```
550: OVEit SEcrb taYPc eohDI NIbhf ohthw Ittdg ttchV ittTH EVitf
600: tnith aftlY fINED WsttS ToNtA NDtHi VtstE atrES TONth ltDST
650: ONEtt oitEe tVntt tWuar htttb hPioE rtUmd ErONt Ditcg tlttT
700: Heopi aTLOC ALITY tsttt Vmtdt ttTHa tfttI ostea LTYWi lafit
750: aDstt INDtN Gtn
```

At this point, the author observed two numbers in the above changes. He next concentrated on finding other portions of the output that looked like they could also be numbers. The next set of changes were as follows:

283	TWEfVE	twelve
435	EIGttYEIaHT	eightyeight
419	twElVi	twelve
315	EIGHT	

and the new output was given by

```
  0: IHAVE DEPOS ITEDt NTHte oiNtY OaitD strsa boapt hrrMI LEStr
 50: OaBUa ottSt tafEp coVAT IONOr VaaLt snptE nTBEa owtHt Ssram
100: wnhst hhfbh ntDTh ntOof hcaNG mttIw LntBt toNGt fGphI otaYT
150: tTHEo atToE Swott tttdt SabEG tVEtI NtndB thtHr tfHtb EWntH
200: Thotn tttDE POSIT eottI STeDO oTENH itDrt taNDa OigTE tfoos
250: estth btLDs tiTtt htYEI GHtta oDbED iNDTW ELVEf OrNDS OoSIa
300: VEroE POSit tDNhV EIGHT EEftt NtTEE NthES ECOND wAtmw Dnttu
350: tIfHT EENTW ENTYh Ntwfs aONSt ottot htINE TtfNh UetrE DcNoS
400: EVENP OUNDS hsGOa owtoT WELVE oafob EDato EIGHT YEIGH Ttfti
450: aVErm LSOtE wtfSO BTAIN EDtNS TehUa tINEp CHANG Etotw Vntgo
500: Ntftt taTto NttDV aLUEl taTHt gttEt rHtsS aNDtt aaigS THEAB
550: OVEit SEcrb taYPc eohDI NIbhf ohthw ITtdg ttchV EttTH EVitf
600: Tnith aftLY fINED WsttS ToNtA NDtHE VtstE atrES TONth LtDST
650: ONEtt oitEe tVntt tWuar htHtb hPioE rtUmd ErONt DEtcg tltTT
700: Heopi aTLOC ALITY tsTtt Vmtdt ttTHa tfttI ostea LTYWi LafEt
750: aDstt INDtN Gtn
```

Since the author knew that the message output had to do with a treasure, he next looked for words that related to this subject. The next set of changes were

303 oEPOSit	deposit
75 VaaLT	vault
297 SIaVEr	silver
331 thE	THE
448 tiaVEr	silver
446 tf	OF
295 Oo	OF

and the output was then modified as follows:

```
  0: IHAVE DEPOS ITEDt NTHte oiNtY OaitD stRsa boUpt hrRMI LEStR
 50: OaBUa ottSt tafEp coVAT IONOR VAULT snptE nTBEL owtHt SsRam
100: wnhst hhfbh ntDTH ntOof hcaNG mttIw LnSBt toNGt fGphI otaYT
150: OTHEo atToE SwoOS tttdt SabEG tVEtI NtndB thtHR tfHtb EWnTH
```

```
200: THotn tStDE POSIT eottI STeDO FTENH itDRt taNDa OigTE tfoos
250: estOh btLDs tiTtt htYEI GHttU oDbED iNDTW ELVEf OrNDS OFSIL
300: VERDE POSIT tDNhV EIGHT EEftt NtTEE NTHES ECOND wAtmw Dnttu
350: tIfHT EENTW ENTYh Ntwfs aONSt ottot htINE TtfNH UetRE DcNoS
400: EVENP OUNDS hsGOL owtoT WELVE oUfob EDato EIGHT YEIGH TOFSI
450: LVERm LSOtE wtfSO BTAIN EDtNS TehUa tINEp CHANG EtoSw Vntgo
500: NSfOt TaTto NttDV aLUEl taTHt gttEt RHOsS aNDtt LaigS THEAB
550: OVEIS SEcrb tLYPc eohDI NIbhf ohthw ITtdg OtchV EtSTH EVitf
600: Tnith UftLY fINED WsttS ToNtA NDTHE VtsSE atRES TONSh LtDST
650: ONEtt DitEe OVntt tWuar hTHtb hPioE RtUmd ERONt DEScg tlttT
700: Heopi aTLOC ALITY OsTtt VmtdT ttTHa tfttI Fstea LTYWI LLfEt
750: aDstt INDtN Gtn
```

At this point, most easier recoveries had been made, and it was time to start making some educated guesses. The author concentrated on the portion of the text beginning at position 289 which read, "TW ELVEf OrNDS OFSILVER." By exhausting all possible choices for the "f" and "r" in this segment of output, the most logical choice for these characters forms the word "pounds." After another round of looking for numbers in the output, the author made the following changes:

289	fOrNDS	pounds
319	TEEf	teen
350	tifHTEEN	eighteen
268	EIGHT	
87	BELOW	

with output

```
  0: IHAVE DEPOS ITEDt NTHte oiNtY OaitD stRsa boUpt hURMI LEStR
 50: OaBUa ottSt taNEp coVAT IONOR VAULT snptE nTBEL OWTHt SsRam
100: wnhst hhGbh ntDTH ntOof hcaNG mttIw LnSBt toNGt NGphI otaYT
150: OTHEo atToE SwoOS tttdE SabEG tVEtI NtndB thTHR EfHtb EWnTH
200: THotn tStDE POSIT eOttI STeDO FTENH itDRt taNDa OigTE tNoos
250: estOh btLDs tiTtt htYEI GHTtU oDbED iNDTW ELVEP OUNDS OFSIL
300: VERDE POSIT tDNhV EIGHT EENtt NtTEE NTHES ECOND wAtmw Dnttu
350: EIGHT EENTW ENTYh NtwNs aONSt ottot htINE TEfNH UetRE DcNoS
400: EVENP OUNDS hsGOL owtoT WELVE oUNob EDato EIGHT YEIGH TOFSI
450: LVERm LSOtE wtfSO BTAIN EDtNS TehUa tINEp CHANG EtoSw VnTgo
500: NSPOt TaTto NttDV aLUEl taTHt gttEt RHOsS aNDtt LaigS THEAB
550: OVEIS SEcUb ELYPc eohDI NIbhN ohthW ITtdg OtchV EtSTH EVitf
600: Tnith UGtLY fINED WsTtS ToNtA NDTHE VtsSE atRES TONSh LtDST
650: ONEtt DitEe OVntE tWuar hTHtb hPioE RtUmd ERONt DEScg tlttT
700: Heopi aTLOC ALITY OsTtt VmtdT ttTHa tNttI Fstea LTYWI LLfEt
750: aDstt INDtN Gtn
```

At this point, another educated guess was required. At position 263, the author saw the phrase "EI GHTtU oDbED iNDTW ELVEP OUNDS OFSILVER." Certainly a treasure of twelve pounds of silver would not be very exciting. Thus, the most logical solution for the unknown characters is "HUNDRED AND." The author then looked for other places where the word "hundred" looked like a good fit. The resulting changes were as follows:

273	tUoDbEDiND	hundredand
425	oUNoREDato	hundredand
310	tD	ED
389	HUetREDcND	hundredand
381	tINETEfN	nineteen
323	NtNE	nine
555	SEcURELY	securely
262	THIhtY	thirty
229	HiNDRttaND	hundredand

with revised output

```
  0: IHAVE DEPOS ITEDI NTHEe oUNTY OaiED stRsa boUpt hURMI LEStR
 50: OaBUa otDSI NANEp coVAT IONOR VAULT snptE nTBEL OWTHE SsRam
100: wnhst hhGRh nNDTH ntOof hcaNG mtTIw LnSBE toNGI NGphI NtaYT
150: OTHEo AtToE SwHOS tNtdE SAREG IVENI NNndB ERTHR EEHtR EWnTH
200: THotn tStDE POSIT eONtI STeDO FTENH UNDRE DANDa OUgTE ENoos
250: NstOh btLDs NiTHI RTYEI GHTHU NDRED ANDTW ELVEP OUNDS OFSIL
300: VERDE POSIT EDNhV EIGHT EENNI NETEE NTHES ECOND wAtmw DnDEu
350: EIGHT EENTW ENTYh NtwNs aONSI ottDt hNINE TEENH UNDRE DANDS
400: EVENP OUNDS hsGOL owNDT WELVE HUNDR EDAND EIGHT YEIGH TOFSI
450: LVERm LSOtE wEfSO BTAIN EDINS TehUa tINEp CHANG EToSw VnTgo
500: NSPOt TATIo NtNDV ALUEl taTHI gTEEN RHOsS aNDDt LaAgS THEAB
550: OVEIS SECUR ELYPA eohDI NIRhN ohthW ITHdg ONchV EtSTH EVAtf
600: Tnith UGHLY fINED WsTHS ToNEA NDTHE VEsSE atRES TONSh LIDST
650: ONEtN DAtEe OVntE DWuar hTHtR hPAoE RNUmd ERONE DESCg IlttT
700: HeopA aTLOC ALITY OsTHt VmtdT ttTHA TNtDI FsIea LTYWI LLfEH
750: ADsNt INDIN Gin
```

Again, additional educated guesses were required. First, the author concentrated on the portion of the message beginning at position 233: "TENH UNDRE DANDa OUgTE EN." If one considers all of the numbers in the range from thirteen to nineteen, only fourteen has "OU" in the second and third characters.

Next, at position 43 the author saw the word, "miles." An adjective likely precedes this word, and most likely it would describe the number of miles. The only number that ends with "UR" is the number four.

Once these changes are made, the word after miles becomes "FROa." This is highly likely to be the word "from."

Next, starting at position 380, the author saw that the message describes 1907 pounds of something. Since a component of silver is described shortly later in the message, it is logical that the 1907 pounds is of gold considering that the author saw the characters GOL shortly after the 1907.

Exhausting all characters for position 19, the author saw that "county" is the most likely word. Similarly, exhausting the characters at position 218, the author saw that "consist" is the most likely word here.

239	aOUgTEEN	fourteen
39	thUR	four
48	FROa	from

410	OsGOLowND	ofgoldand
19	eOUNTY	county
215	CONtIST	consist

```
  0: IHAVE DEPOS ITEDI NTHEC OUNTY OFiED FtRsa boUpF OURMI LESFR
 50: OMBUF OtDSI NANEp coVAT IONOR VAULT snpFE nTBEL OWTHE SsRFm
100: wnOst hhGRO nNDTH nFOof OcaNG mtTIw LnSBE toNGI NGpOI NtaYT
150: OTHEo AtToE SwHOS tNtdE SAREG IVENI NNndB ERTHR EEHtR EWnTH
200: THoFn tStDE POSIT CONSI STCDO FTENH UNDRE DANDF OURTE ENoOs
250: NstOh btLDs NiTHI RTYEI GHTHU NDRED ANDTW ELVEP OUNDS OFSIL
300: VERDE POSIT EDNOV EIGHT EENNI NETEE NTHES ECOND wAtmA DnDEu
350: EIGHT EENTW ENTYO NtANs aONSI ottDt hNINE TEENH UNDRE DANDS
400: EVENP OUNDS OFGOL DANDT WELVE HUNDR EDAND EIGHT YEIGH TOFSI
450: LVERm LSOtE wEfSO BTAIN EDINS TeOUa SINEp CHANG EToSA VnTRo
500: NSPOt TATIO NtNDV ALUE1 taTHI RTEEN RHOsS aNDDt LaARS THEAB
550: OVEIS SECUR ELYPA CohDI NIRON oOthW ITHdR ONcOV EtSTH EVAtf
600: TnitO UGHLY fINED WsTHS ToNEA NDTHE VEsSE atRES TONSO LIDST
650: ONEtN DAtEC OVntE DWuar OTHtR hPAoE RNUmd ERONE DESCR I1ttT
700: HCopA aTLOC ALITY OFTHt VmtdT ttTHA TNtDI FFICa LTYWI LLfEH
750: ADsNF INDIN Gin
```

At this point, the author encountered a complication. Clearly, the word which begins at position 215 is "consisted." Yet, when the author attempted to make this change in the computer program, other correct characters changed to incorrect values. The reason for this is that all of these characters share the same key value. Since it is impossible to reconcile this value consistently throughout the message, the logical conclusion is that there is at least one error in the original cipher message. The author decided to leave the word in position 215 to be "CONSISTCD" in order to minimize the number of errors in the plaintext.

With this in place, the author then deduced the following educated guesses:

619	stone	
563	PACohD	packed
733	DIFFICaLTY	difficulty
761	In	it
133	BEtONGING	belonging

to continue the recovery of the message.

```
  0: IHAVE DEPOS ITEDI NTHEC OUNTY OFiED FtRsa bOUpF OURMI LESFR
 50: OMBUF OtDSI NANEp coVAT IONOR VAULT snpFE nTBEL OWTHE SsRFm
100: wnOst hEGRO nNDTH nFOof OcaNG mtTIw LnSBE tONGI NGpOI NtaYT
150: OTHEo AtToE SwHOS tNtdE SAREG IVENI NNndB ERTHR EEHtR EWnTH
200: THoFn tStDE POSIT CONSI STCDO FTENH UNDRE DANDF OURTE ENoOs
250: NstOh btLDs NiTHI RTYEI GHTHU NDRED ANDTW ELVEP OUNDS OFSIL
300: VERDE POSIT EDNOV EIGHT EENNI NETEE NTHES ECOND wAtmA DnDEu
350: EIGHT EENTW ENTYO NtANs aONSI ottDt hNINE TEENH UNDRE DANDS
400: EVENP OUNDS OFGOL DANDT WELVE HUNDR EDAND EIGHT YEIGH TOFSI
450: LVERm LSOtE wEfSO BTAIN EDINS TeOUa SINEp CHANG ETOSA VnTRo
500: NSPOt TATIO NtNDV ALUE1 taTHI RTEEN RHOsS aNDDt LaARS THEAB
```

```
550: OVEIS SECUR ELYPA CKEDI NIRON oOthW ITHdR ONcOV EtSTH EVAtf
600: TnitO UGHLY fINED WsTHS TONEA NDTHE VEsSE atRES TONSO LIDST
650: ONEtN DAtEC OVntE DWuar OTHtR hPAoE RNUmd ERONE DESCR IlttT
700: HCopA aTLOC ALITY OFTHt VmtdT ttTHA TNtDI FFICU LTYWI LLfEH
750: ADsNF INDIN GIT
```

At position 513, the author saw the word THIRTEEN. He must determine the answer to the question "Thirteen of what?" Starting at position 538, the author saw the characters "DtLaARS." This is almost certainly the word "dollars." The characters right before "dollars" are "sand." Since this is a message describing a treasure, the logical conclusion is that the message somehow involves "thirteen thousand dollars." Keep in mind that $13,000 in 1822 would be equivalent to millions of dollars in today's currency.

In the following list of changes,

538 DtLaARS	dollars
539 RHOsSAND	thousand
49 T	R
181 NndBER	number
731 Nt	no
681 NUmdER	number
676 PAoER	paper
34 AbOUp	about
247 POUNst	pounds

observe that there is a second probable error in the original cipher. It is not possible to change character 530 to a T without also changing some other characters which are almost certainly correct. The author decided to leave character 530 as an R.

```
  0: IHAVE DEPOS ITEDI NTHEC OUNTY OFiED FORDA BOUTF OURMI LESFR
 50: OMBUF OtDSI NANEp coVAT IONOR VAULT snpFE nTBEL OWTHE SURFm
100: wnOst hEGRO UNDTH nFOof OcaNG mtTIw LnSBE tONGI NGpOI NtLYT
150: OTHEP AtToE SwHOS tNtME SAREG IVENI NNUMB ERTHR EEHtR EWnTH
200: THoFn tStDE POSIT CONSI STCDO FTENH UNDRE DANDF OURTE ENPOU
250: NDSOh btLDs NiTHI RTYEI GHTHU NDRED ANDTW ELVEP OUNDS OFSIL
300: VERDE POSIT EDNOV EIGHT EENNI NETEE NTHES ECOND wAtMA DnDEu
350: EIGHT EENTW ENTYO NtAND aONSI ottDO hNINE TEENH UNDRE DANDS
400: EVENP OUNDS OFGOL DANDT WELVE HUNDR EDAND EIGHT YEIGH TOFSI
450: LVERm LSOtE wEfSO BTAIN EDINS TeOUa SINEp CHANG ETOSA VnTRo
500: NSPOt TATIO NtNDV ALUEl taTHI RTEEN RHOUS ANDDO LLARS THEAB
550: OVEIS SECUR ELYPA CKEDI NIRON POthW ITHdR ONcOV EtSTH EVAtf
600: TnitO UGHLY fINED WsTHS TONEA NDTHE VEsSE LSRES TONSO LIDST
650: ONEtN DAtEC OVntE DWuar OTHtR hPAPE RNUMB ERONE DESCR IltST
700: HCopA aTLOC ALITY OFTHt VmtdT tOTHA TNODI FFICU LTYWI LLfEH
750: ADsNF INDIN GIT
```

At this point, enough of the output message was recovered that the remaining characters could be deduced by the context of the known words. The reader is encouraged to try to recover the remainder of the message using the computer program given in the Appendix of this document and his or her own reasoning skills. The author's recovery process is documented in the table below.

27	iEDFORD	bedford
142	pOINTLY	jointly
615	WsTH	with
364	ONt	one
370	aONSIoTtDOh	consistedof
196	WnTH	with
200	THoFItST	thefirst
154	PARToRSwHOSE	partieswhose
166	NtMES	names
80	sIpFEnT	sixfeet
63	EXcoVATION	excavation
104	thE	the
347	DEu	dec
497	TRANSPOtTIONAND	transportationand
575	POTh	POTS
583	dRON	iron
690	DESCRIlES	describes
747	fE	BE
95	SURFmwEOs	surfaceof
340	wAt	was
253	OhbtLDsNi	ofgoldand
514	VALUElAa	valuedat
666	WuTr	with
720	VARdT	vault
722	u	r
596	VAtfTIi	vaultis
116	FOoLOcaNG	following
135	t	L (belonging)
458	tEWELS	jewels
474	STeOUIS	stlouis

The author had some difficulty with the final recovery. In particular, he became fixated on the belief that position 472 represented one word which started with the characters "inst." In reality, it was two words: "in" and "st" (an abbreviation for Saint).

The end result of the cryptanalysis was

```
  0: IHAVE DEPOS ITEDI NTHEC OUNTY OFBED FORDA BOUTF OURMI LESFR
 50: OMBUF ORDSI NANEX CAVAT IONOR VAULT SIXFE ETBEL OWTHE SURFA
100: CEOFT HEGRO UNDTH EFOLL OWING ARTIC LESBE LONGI NGJOI NTLYT
150: OTHEP ARTIE SWHOS ENAME SAREG IVENI NNUMB ERTHR EEHER EWITH
200: THEFI RSTDE POSIT CONSI STCDO FTENH UNDRE DANDF OURTE ENPOU
250: NDSOF GOLDA NDTHI RTYEI GHTHU NDRED ANDTW ELVEP OUNDS OFSIL
300: VERDE POSIT EDNOV EIGHT EENNI NETEE NTHES ECOND WASMA DEDEC
350: EIGHT EENTW ENTYO NEAND CONSI STEDO FNINE TEENH UNDRE DANDS
400: EVENP OUNDS OFGOL DANDT WELVE HUNDR EDAND EIGHT YEIGH TOFSI
450: LVERA LSOJE WELSO BTAIN EDINS TLOUI SINEX CHANG ETOSA VETRA
500: NSPOR TATIO NANDV ALUED ATTHI RTEEN RHOUS ANDDO LLARS THEAB
550: OVEIS SECUR ELYPA CKEDI NIRON POTSW ITHIR ONCOV ERSTH EVAUL
```

```
600: TISRO UGHLY LINED WITHS TONEA NDTHE VESSE LSRES TONSO LIDST
650: ONEAN DAREC OVERE DWITH OTHER SPAPE RNUMB ERONE DESCR IBEST
700: HCEXA CTLOC ALITY OFTHE VARLT SOTHA TNODI FFICU LTYWI LLBEH
750: ADINF INDIN GIT
```

Note that it is impossible to change additional characters in this output without introducing other errors in the message.

Comparing the final message to the output given in Ward's publication, the author saw that it is possible to eventually recover the intended message using the original Declaration of Independence as the key for a book cipher. However, considerably more effort was required than *The Beale Papers* suggest.

3. Analysis of the Key Document

At this point, the author must compare the key used to generate the final output to the original Declaration of Independence. The program was modified to output the key values for both the original document as well as the array used for the final message. Comparing the two sets of keys, some interesting differences can be observed.

The first difference in the two keys occurs at position 79. Here, the original Declaration of Independence uses the word "self-evident" while the solution to the above cipher suggests that at this position, the text should read "self evident" instead. This omission of the hyphen significantly corrupts the plaintext since all cipher components with value greater than 79 are decrypted incorrectly.

Once the hyphen has been removed from the Declaration of Independence, the second major difference occurs somewhere between words 154 and 158 of the Declaration of Independence. Comparing Ward's pamphlet with a history book owned by the author, the author saw that the word "a" was added prior to the phrase "new government" in Ward's pamphlet. The version of the Declaration of Independence found in the history book reads: "it is the Right of the People to alter or to abolish it, and to institute new Government." Suspecting that perhaps this was a typographical error in the history book, the author then carefully examined the original Declaration of Independence. A scanned copy of the actual Declaration of Independence is also available through the National Archives website for inspection [4]. The wording without the extra word "a" is the correct language used in the actual Declaration of Independence.

By studying *The Beale Papers* at this point, the author saw that *The Beale Papers* used a different version of the Declaration of Independence than the original version. The author decided to investigate why Beale would not have used the actual version of the Declaration of Independence.

In the days before computers, people did not have easy access to documents like people do today. In the case of the Declaration of Independence, people had to rely upon reprintings of this document through other sources. Many of these reprintings introduced minor changes to the document as the editors attempted to "improve" the work of our Founding Fathers. Stephen Matyas, Jr. compiled a "checklist" [6] of all of the known reprintings of the Declaration of Independence prior to 1825. This would likely include all of the versions of the document available to the author of the Beale ciphers.

Matyas described a number of common themes in the altered versions of the Declaration of Independence. Many differed from the version found in the National

Archives by adding or deleting hyphens or adding or subtracting words, such as the addition of the word "a" prior to "new Government." One particular item of discussion is whether the rights given to men by their Creator are "inalienable" or "unalienable." In Thomas Jefferson's draft of the Declaration of Independence, he used the word "inalienable." However, when John Adams wrote the final version of the Declaration of Independence, the wording was changed to "unalienable". Although both words mean essentially the same thing, the actual Declaration of Independence uses the word "unalienable" whereas the version of the Declaration of Independence used by Ward and the author of the Beale ciphers uses the word "inalienable."

If one assumes that both the author of the Beale ciphers and Ward happened to select a version of the Declaration of Independence that omitted the hyphen in "self-evident," added "a" prior to "new Government," and did not include any of the other deviations described in Matyas's paper,[1] then the cipher is decoded into

```
  0: ihaae depos ttedi nthec ountc ofged forda boarf ourmi lesfr
 50: ombtf ordsi iaaew caaat ionor aaalt siwfe etbel owthe sirfa
100: ceott tanro hidth efolo onrng artic lesbe longi agjoi attct
150: othep attie swtos aiaml sareg iaepi nihmb ehthr lthor ewith
200: thtfi tstde posit copsi stcdo ftenh updre dandf ourte eapoi
250: odhoh goldc pathi htcei ghtha adred andtw elaep ounds ofsil
300: aerde posit ednoa eight eeaii netee nthes econd watma deaec
350: linht eentw entco naaad consi ftoih piine tltnh toare danis
400: eaenp otnds ofgol lapit welae taair edapi eight ceigh tofsi
450: laera lsohe weoso btain edins tlotr sinew chang etosa aetra
500: nspor tatio napda altea apthi rteep rhois anddo ltars theab
550: oaeis secur llcpa cpadi niroa potsw ithir opcoa ersth eaapo
600: tiaro anhlc oined withs tonea ndthe aesse thres tonso lidst
650: oneai darec oaerl dwppr othor spape ritmb erone descr ifaht
700: hctwa ctloc alitc oftho aarot totha tahai fficu ltcwi llbeh
750: adipf indin gin
```

It is much easier to resolve the errors in this message than to go through the process with the original Declaration of Independence. But what are the chances that given so many versions of the Declaration of Independence that both the author of the ciphers and the author of *The Beale Papers* happened to select the same version?

Inspection of *The Beale Papers* shows that a version of the Declaration of Independence with "self-evident" was used, yet the author counted this as two words to generate the key. Perhaps the author of the Beale ciphers used a version with "self evident," but how did the author of *The Beale Papers* know to interpret the "self-evident" in his version of the Declaration of Independence as two words?

More troubling, however, is what happens around position 480. In order to produce the correct plaintext for Beale Cipher Number Two, one must delete 10 words from the Declaration of Independence. Upon examination of page 18 of the Beale

[1]Ward used inalienable vs. unalienable, but it is unclear which version was used by the original author since the character involved is not included in the Beale cipher.

ciphers,[2] one sees that the author of *The Beale Papers* makes the mistake of using the number 480 two times when counting the words in the Declaration of Independence. In order for Ward's version to correctly decode Beale Cipher Number Two, then the author of the Beale ciphers would have also had to make the same mistake in the same location. Furthermore, there are two additional miscountings of words of the Declaration of Independence: once around position 630 and again around 670. By studying the original version of *The Beale Papers*, one can see that there are 11 words between numbers 630 and 640 and again 11 words between 670 and 680. How could both Ward and Beale have made the same mistake?

4. A Possible Hoax

It seems reasonable that if there were such problems in using the Declaration of Independence to decipher Beale Cipher Number Two, then Ward should have made some mention of these problems in his presentation of the solution to the cipher. Yet no mention is made of any problems deciphering in the Beale ciphers. Given this evidence and the unlikeliness of the authors of the ciphers and *The Beale Papers* both choosing the same version of the Declaration of Independence, the author of this article concludes that the logical explanation is that the author of *The Beale Papers* is also the author of the ciphers and that the publication is a hoax.

There is further evidence to support the argument that the Beale ciphers are a hoax. James Gillogly [5] applied the Declaration of Independence to Beale Cipher Number One. This was not the correct key as one observes a random sequence of letters when this key is applied to the cipher. However, around position 187, one sees the sequence of characters "ABFDEFGHIIJKLMMNOHPP."[3] The probability of seeing a pattern of letters like this in a supposedly random set of letters of the alphabet is extremely small. A popular argument against Beale Cipher Number Three is that the number of characters in the cipher is too small to contain the names and addresses of 30 people. These arguments are described in numerous references, including [3].

5. Further Exploration

The interested reader can attempt to verify the results presented in Section 2 using the computer program mentioned throughout this article. The online version of the article also contains the appendix with the source code for the program written in the C programming language.

Although the author of this article has concluded that the Beale ciphers are very likely a hoax, there are others who still argue that the Beale ciphers are real. The counterargument to the above criticism of Beale Cipher Number One is that it was encrypted using the Declaration of Independence using some sort of double encryption scheme. Another person claimed to have discovered a completely different solution to Beale Cipher Number one, and his solution can be found on the

[2]Scanned copies of the original version of *The Beale Papers* can be found by searching the Internet. It is important to locate the original version of *The Beale Papers* as other reprintings (e.g., Gold in the Blue Ridge) have attempted to correct mistakes found in the Beale ciphers.

[3]One does not see the letter Q in the pattern. Also, there is no word in the Declaration of Independence which begins with the letter Q.

Internet [2]. The author of the current article has thus far been unsuccessful at replicating this solution.

There are numerous additional theories about the Beale cipher proposed over the years. One is that the ciphers were an elaborate hoax proposed by Edgar Allan Poe as a joke. Another is that the treasure is really a stash of Confederate gold, hidden after the Civil War. These and many additional claims can be discovered by reading books on the Beale cipher, such as [3].

If one does decide to believe in the existence of the Beale Treasure, he or she would be wise to heed the advice given in *The Beale Papers*: "Devote only such time as can be spared from your legitimate business to the task [of solving the Beale ciphers], and if you can spare no time, then let the matter alone . . . By following this policy, your interests will not suffer, your family will be cared for, and your thoughts will not be absorbed to the exclusion of other important affairs."

6. Appendix

```
// Program to interactively solve
// Beale Cipher Number Two (or any other book cipher)
// Author: Todd Mateer

// Include files
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <ctype.h>

// Input / output files
#define LOGFILE            "log4a.txt"
#define CIPHERFILE         "beale2.txt"
#define KEYFILE            "DOI_2.txt"
#define KEY_OUTPUT         "key29a.txt"
#define PLAINTEXT_OUTPUT   "sol15.txt"

int main(int argc, char **argv)
{
   char word[100];
   int  number;
   int  i = 1;
   int  j = 1;
   char origkey[1500];
   char newkey[1500];
   int  cipher[1000];
   int  cipherlength = 0;
   int  keylength = 0;
   char command;
   char letters[1000];
   int  logind[5000];
   int  logkin[5000];
   char logold[5000];
   char lognew[5000];
   char dum[12][80];
   int  logindex;
   int  change[1500] = {0};
   int  validcommand;
   int  changes;
```

```
// Open input files
FILE *cfile   = fopen (CIPHERFILE, "r");
FILE *doi     = fopen (KEYFILE, "r");
if ( !doi || !cfile )
{
   printf ("Could not open input files \n");
   return(1);
}

// Read in Declaration of Independence
i = 1;
while (!feof (doi) )
{
   fscanf (doi, "%s ", word);
   newkey[i]    = (char) tolower(word[0]);
   origkey[i++] = (char) tolower(word[0]);
}
keylength = i;

// Read in the cipher
i = 0;
while ( !feof (cfile) )
{
   fscanf (cfile, "%s ", word);
   number = atoi(word);
   cipher[i++] = number;
}
cipherlength = i;

// If the log file is nonempty, then
// use its contents to restore the user's
// previous progress in the cipher solution
logindex = 0;
FILE *logfile = fopen (LOGFILE, "r");
if (logfile)
{
   while (!feof(logfile))
   {
      fscanf (logfile, "%s %s %s %s %s %s %s %s %s %s %s %s \n",
              dum[0], dum[1], dum[2], dum[3], dum[4], dum[5],
              dum[6], dum[7], dum[8], dum[9], dum[10], dum[11]);

      // Index of change
      logind[logindex] = atoi(dum[4]);

      // Cipher value at that position
      logkin[logindex] = atoi(dum[8]);
```

```
      // Old key value at that position
      logold[logindex] = dum[9][0];

      // New key value at that position
      lognew[logindex] = dum[11][0];

      newkey[logkin[logindex]] = lognew[logindex];
      logindex++;
   }
}

// Start the interactive mode
validcommand = 1;
do
{
   if (validcommand)
   {
      changes = 0;

      // Display current cipher to screen
      printf ("%3d: ", 0);
      for (i = 0; i < cipherlength; i++)
      {
         printf ("%c", newkey[cipher[i]]);
         if (i % 5 == 4)
            printf (" ");
         if (i % 50 == 49)
         {
            printf ("\n");
            printf ("     ");
            for (j = 0; j < 50; j++)
            {
               if (change[cipher[i-49+j]] != 0)
               {
                  printf ("%c", change[cipher[i-49+j]]);
                  changes++;
               }
               else
                  printf (" ");
               if (j % 5 == 4)
                  printf (" ");
               if (j % 10 == 9)
                  printf ("   ");
            }
         }

         if (i % 50 == 49)
           printf ("%3d: ", i+1);
```

```
        else if (i % 10 == 9)
          printf ("%2d ", (i % 100) + 1);
     }

     printf ("\n");
     printf ("     ");

     for (j = cipherlength - (cipherlength % 50); j < cipherlength; j++)
     {
        if (change[cipher[j]] != 0)
        {
           printf ("%c", change[cipher[j]]);
           changes++;
        }
        else
           printf (" ");
        if (j % 5 == 4)
           printf (" ");
        if (j % 10 == 9)
           printf ("   ");
     }

     for (i = 0; i < 1500; i++)
     {
        change[i] = 0;
     }

     printf ("\nChanges: %d \n", changes);
     printf ("\n\n");
     printf ("Enter command (C Change, U Undo, Q quit) : ");
  }

  // Get next command from user
  fflush (stdout);
  scanf ("%c", &command);
  command = (char) toupper(command);
  validcommand = 0;

  // Process the command
  if (command == 'C')
  {
     // Change the output
     validcommand = 1;
     printf ("Enter starting position: ");
     scanf ("%d", &i);
     printf ("Enter letter string: ");
     scanf ("%s", letters);
     for (j = 0; j < (int) strlen(letters); j++)
```

```
        {
           logind[logindex] = i + j;
           logkin[logindex] = cipher[i+j];
           logold[logindex] = newkey[cipher[i+j]];
           change[cipher[i+j]] = newkey[cipher[i+j]];
           newkey[cipher[i+j]] = (char) toupper(letters[j]);
           lognew[logindex] = newkey[cipher[i+j]];
           logindex++;
        }
     }
     if (command == 'U' && logindex > 0)
     {
        // Undo the previous change
        validcommand = 1;
        logindex--;
        change[logkin[logindex]] = lognew[logindex];
        newkey[logkin[logindex]] = logold[logindex];
     }
     printf ("\n");
  }
  while (command != 'Q');

  // Create a file showing differences between
  // the original key and the key at the end of
  // the current session
  FILE *ofile1  = fopen (KEY_OUTPUT, "w");
  for (i = 1; i < keylength; i++)
  {
     if (toupper(newkey[i]) == newkey[i])
     {
        fprintf (ofile1, "%d  : %2c  %2c  ", i, origkey[i], newkey[i]);
        if (toupper(origkey[i]) != toupper(newkey[i]))
           fprintf (ofile1, "********* ");
        fprintf (ofile1, "\n");
     }
  }
  fclose (ofile1);

  // Create an output file containing the
  // plaintext at the end of the current session
  FILE *ofile2  = fopen (PLAINTEXT_OUTPUT, "w");
  fprintf (ofile2, "%3d: ", 0);
  for (i = 0; i < cipherlength; i++)
  {
     fprintf (ofile2, "%c", newkey[cipher[i]]);
     if (i % 5 == 4)
        fprintf (ofile2, " ");
     if (i % 50 == 49)
```

```
            fprintf (ofile2, "\n");
         if (i % 50 == 49)
            fprintf (ofile2, "%3d: ", i+1);
      }
      fprintf (ofile2, "\n\n");
      fclose (ofile2);

      // Create a log file with the results of
      // the current session.
      FILE *logfile2 = fopen (LOGFILE, "w");
      for (i = 0; i < logindex; i++)
      {
         fprintf (logfile2, "%3d : ", i);
         fprintf (logfile2, "   Position = %3d ", logind[i]);
         fprintf (logfile2, "   Key index = %3d ", logkin[i]);
         fprintf (logfile2, "   %c -> %c \n", logold[i], lognew[i]);
      }
      fclose (logfile2);

      return 0;
   }
```

About the Author

Dr. Todd Mateer received his PhD in Mathematical Sciences from Clemson University in 2008 under the direction of Dr. Shuhong Gao. His dissertation discusses Fast Fourier Transform Algorithms and their applications in signal analysis, computer algebra, and coding theory. He was the first student to earn two undergraduate degrees from Grove City College a BSEE degree and a BS degree in Mathematics/Computer Science. In 1999, he earned a Masters Degree from Clemson University under the direction of Dr. Joel Brawley, where he conducted a mathematical analysis of video poker in South Carolina and mathematically proved that one can profit from certain casino games such as video poker over a long period of time with the appropriate strategy. In 2001, he joined Howard Community College where he currently serves as Master Adjunct Instructor. During the summers, Dr. Mateer teaches elementary classical cryptography, the mathematics of casino games, and the drawbacks of gambling at the Math and Related Sciences camps held at the University of Maryland Eastern Shore. He also does work for the Department of Defense, has four children, and is an amateur magician. His magic tricks teach basic concepts of coding theory and computer science.

References

1. *The Beale Papers*. 1885. Original document can be observed at http://www.archive.org/details/TheBealePapers.
2. "The Beale Treasure Website". http://bealesolved.tripod.com.
3. Belfield, R. 2006. *"Can You Crack the Enigma Code?"* London: Orion Publishing.
4. "The Declaration of Independence". http://www/archives.gov/exhibits/charters/declaration.html.
5. Gillogly, J. 1980. "The Beale Ciphers: A Dissenting Opinion," *Cryptologia*, 4(2): 116–119
6. Matyas, S. Jr. "Declaration of Independence: A Checklist of Books, Pamphlets, and Periodicals Printing the U.S. Declaration of Independence, pp. 1776–1825" in date. USDeclarationofIndependence.com