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
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 depso otedt nttte ointt caite cattl stree breet ptbhr hrrml lestr
50: oabaa ottsn tafep coiat ionor iaalt snpti ntbea cwtth srar
100: wnhst hnhfh nttth ntooc hoang mttav fnttb tonat fgphi otatt
150: ttheo attoe swott tttdt sbeea tiiti ntndb ththr tfttb ewnth
200: thtnn ttttde posit eotta stede otiinh itdrt tanda oigte ffoos
250: eesth btdls tttt ttta ghtta obbed indtw efief ornds oosaa
300: ieroi posit tdnhn iihtb eeftt nttse nthes econd watmn dnttu
350: ttfft eentw enntth ntwfs aonst ototot bhte eefsh astre dcnos
400: eiemp oands hssoa owtto welii cafof edato eigtte teiah ttffti
450: alerm fseoti wffso btaia idtns tehaa tinep chang etotw intgo
500: ntftt tattto nttdl alaia tattt gfttt rhtss andtt aaga theab
550: oieit secrb tatpc eohdi nihfh ohthw ittdg ttchi ittth elitt
600: tnith alftit fined watrs tonts ndthli itate atres tonth ltdst
650: onett oittee tnttt twar ttggb hptoe rtamd eront ditcc ttttt
700: heopi atloc alitt ttsttt imtdd tttha tftti ostea lttwi lafit
750: adtt indtt 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.

<table>
<thead>
<tr>
<th>Location</th>
<th>Word</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>miles</td>
</tr>
<tr>
<td>334</td>
<td>second</td>
</tr>
<tr>
<td>485</td>
<td>change</td>
</tr>
<tr>
<td>208</td>
<td>deposit</td>
</tr>
<tr>
<td>464</td>
<td>obtain</td>
</tr>
</tbody>
</table>

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 Ntte ointt OaitD stresa boapt hrrMI LBSr
50: oaba otSt tafeo coict IONwOr iaalt snpiti ntseoa owtht Servm
100: whst hhfhEh ndTthn ngOof hcanG mtaw tontf tonat fcPhI otamt
150: TTHeo atttE Swctt ttttt saebar tititI Nntnd ththFr tftht EwtNh
200: kthotn tttDE POSIT eofta SteDO otInh itDrt tANDa ogtte tfoos
250: esthr htiida snttt httla Ghta oDeBD inDtw eftef ornsS cosaa
300: ieroi Posit tDnhi ilah Eeftt Ntteee NthES BCOND wAtmW Dnttu
350: tIFHt EENtw Entth Ntwfs ansSt ottot htINE ttfhn setre Dcnos
400: EiENP oancD hmaoa owtlo wEili oacbc eDaso HIGtt tEIAh tttf
450: aiErn ISoti wfsSO BTAIn iDTNS tehaa tInEp CHANG Ettow intgo
500: Nkftt tatt NtdI aiall tattt gttit rHtsS anDtt aaiGS THEab
550: oaeit sBcrb tatPc eohDl nhbfh ohthw ltttgd tchi ittth EiItf
600: lnhth afllt fINEd wettS tOnTs Nthdi istEe arsEe tonhth lttdSt
650: ONttt oitEe tintw htttt hPice rCamD EroNT Dtcq ttttT
700: heopi atLOC ALItt tftttg imtdt ttTHa tfthl ostea lttwi lafit
750: aDttt InDntn 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 the correct plaintext. The author made the following adjustments to the output:

<table>
<thead>
<tr>
<th></th>
<th>DeposotEd</th>
<th>deposited</th>
</tr>
</thead>
<tbody>
<tr>
<td>354</td>
<td>tEENtwEntt</td>
<td>teentwenty</td>
</tr>
<tr>
<td>707</td>
<td>LOCALity</td>
<td></td>
</tr>
<tr>
<td>399</td>
<td>SEIENPoandS</td>
<td>sevenpounds</td>
</tr>
<tr>
<td></td>
<td>ahaVe</td>
<td>ihave</td>
</tr>
<tr>
<td>548</td>
<td>aoboVe</td>
<td></td>
</tr>
</tbody>
</table>

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 ITTEDt Ntteee oINTY OaitD stresa boapt hrrMI LBSr
50: OaBaA otStt táfep coçt IONwOr iaalt snpiti ntseoa owtht Servm
100: whst hhfhEh ndTthn ngOof hcanG mtaw tontf tonat fcPhI otaMt
150: TTHeo atttE Swctt ttttt saebar tititI Nntnd ththFr tftht EwtNh
200: kthotn tttDE POSIT eofta SteDO otInh itDrt tANDa ogtte tfoos
250: esthr htiida snttt httla Ghta oDeBD inDtw eftef ornsS cosaa
300: ieroi Posit tDnhi ilah Eeftt Ntteee NthES BCOND wAtmW Dnttu
350: tIFHt EENtw Entth Ntwfs ansSt ottot htINE ttfhn setre Dcnos
400: EiENP oancD hmaoa owtlo wEili oacbc eDaso HIGtt tEIAh tttf
450: aiErn ISoti wfsSO BTAIn iDTNS tehaa tInEp CHANG Ettow intgo
500: Nkftt tatt NtdI aiall tattt gttit rHtsS anDtt aaiGS THEab
550: oaeit sBcrb tatPc eohDl nhbfh ohthw ltttgd tchi ittth EiItf
600: lnhth afllt fINEd wettS tOnTs Nthdi istEe arsEe tonhth lttdSt
650: ONttt oitEe tintw htttt hPice rCamD EroNT Dtcq ttttT
700: heopi atLOC ALItt tftttg imtdt ttTHa tfthl ostea lttwi lafit
750: aDttt InDntn 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:

<table>
<thead>
<tr>
<th>283</th>
<th>TWElVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>435</td>
<td>EIGHTY-EIGHT</td>
</tr>
<tr>
<td>419</td>
<td>twelve</td>
</tr>
<tr>
<td>315</td>
<td>EIGHT</td>
</tr>
</tbody>
</table>

and the new output was given by:

0: I HAVE DEPOS ITEDT NTHTe oINTy OaitD strsa boapt hrrMI LESTr
50: OaBUa oTSt tafEp coVAT IONOr VaALt snptE nTBea owtHt Ssaram
100: wnhst hfhfbh nTDTh toooHf hcaNH mttlW lntBt tonGT fcphI otaYT
150: tTHEo atToE sWott ttttD SaBEg tVEti NtndB tthIr tfhtb EwNth
200: Thotn ttttD POSIT eotI STeDO oTENH iDrt tanaD OigTE tfcoS
250: estth btLDs ttttD htYEI GHTta oDBED INDtW ElVEf OrNDS GoSia
300: VERO POSIT tDNYV EIGHTE BFTt nTfEe NTHEs ECONd WAtmW Dntu
350: tfht BENTW EwNth Ntwfs aONSt oTtot htINE TtfNh UetreDoNOS
400: EVENP OUNDS hsGOa owtoT WELVE oafob EDato EIGHT YEIGH Tffti
450: aBHRM LSOE wtfSO BTAIN EoBNS TchUsa tINEp CHANG Btow Vntgo
500: Nfttt taTto NttDV aLElI taThT qtttB rhtSS aNDtt aaigS THERAB
550: OVEIt SECRb tayPEC eOHDi N1HfH othtw ITTgEY ttCHV BTTTH EVItf
600: Thith afTLY FINED WsStS ToNtA NDTHE VsttE atres TOnNH LdDSt
650: ONEIt oTBe ttttD httHb hPioE rT/umd ERONT DITcG tlllT
700: Heopi aTLOC ALITY ttSSt Vmdt ttTHa tfttI oStea LTYWi LAFbT
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
250 VaALt vault
297 SlaVEr silver
331 thE THE
448 tiaVEr silver
446 tf OF
295 Oo OF

and the output was then modified as follows:

0: I HAVE DEPOS ITEDT NTHTe oINTy OaitD strsa boUpt hrrMI LESTr
50: OaBUa oTSt tafEp coVAT IONOr VAULT snptE nTBEl owtHt Ssaram
100: wnhst hfhfbh nTDTH toooHf hcaNH mttlW lntBt tonGT fcphI otaYT
150: tTHEo atToE SwoOS ttttD SaBEg tVEti NtndB tthIr tfhtb EwNth
Cryptanalysis of Beale Cipher Number Two

200: THotn tStDE POSIT oCtTI SThDO PTENH itDRt taNDA OigTE tfcoes
250: estOth btLDs tItTt hINEh GTHU oDbed iNDTWF ELVEF OrNDS OPsiL
300: VERDE POSIT tDNFHV EIGHT EfTiT tNTEE NTHES ECOND wATmW Dnttu
350: tIFHT ENNTW ENTYh Ntwfs aONSt ottot hINEH tTfNH UetRE DcNoS
400: EVENP OUNDs hSGOL owTOt WELVE oFchE oDatO EIGHT YEIGH TOFSI
450: LVERm LSotE wtFSO BTAIN EdTns TeHuA tINEp CHANG EtoSw Vntgo
500: NSFot TtTTo NtDV AlJUEF tATtHt gTTtIt RHosS aNdTT LaIGs THEAB
550: OVEIS hCSbrb tLyPC eOdDI NtBhf othtw ITtdg OtchV ElSTH EvITf
600: TnItTH UtFLY FINEd WsTts ToNTA NDTHE VtSsE atREs TOnSh lTdST
650: ONStt DitEE OwNTt tWuAR hTHTb hPIoE RtuMrd ERONt DsScg tIttT
700: Heopi aTLOC ALITY OsTTt VntDd tTThA tFTtI PsteA lTVWI lLrEf
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 OFSiLer.” 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: THAve DePOS ITEDt NTHTe oNTY OaitD stRaS boUpT hURMr lBStR
50: oABuA ottSt tanEp COVAT iNgor VAULT snpTe nTBEl OWTHT SeRam
100: wNSt hChBh ntDTH nOoF hCaNG mtTlw LnsBT toNGt NSPhI oTaYT
150: OTHel aTtCO SwoOs tttDE SAbEG tVETI NtNdb thTHg RfHHb wQsTh
200: tHotn tStDE POSIT oCttI sThDO PTENH itDRt taNDA OigTE tNOcs
250: estOth btLDs tItTt hINEh GTHU oDbed iNDTWF ELVEF OUNDs OpsiL
300: VERDE POSIT tDNFHV EIGHT EfTiT tNTEE NTHES ECOND wATmW Dnttu
350: EIGHT ENNTW ENTYh NtwFs aONSt ottot hINEH tTfNH UetRE DcNoS
400: EVENP OUNDs hSGOL owTOt WELVE oFChE oDatO EIGHT YEIGH TOFSI
450: LVERm LsoTE wtFSO BTAIN EdTns TeHuA tINEp CHANG EtoSw Vntgo
500: NSFot TtTTo NtDV AlJUEF tATtHt gTTtIt RHosS aNdTT LaIGs THEAB
550: OVEIS hCSbrb tLyPC eOdDI NtBhf othtw ITtdg OtchV ElSTH EvITf
600: TnItTH UtFLY FINEd WsTts ToNTA NDTHE VtSsE atREs TOnSh lTdST
650: ONStt DitEE OwNTt tWuAR hTHTb hPIoE RtuMrd ERONt DsScg tIttT
700: Heopi aTLOC ALITY OsTTt VntDd tTThA tFTtI PsteA lTVWI lLrEf
750: aDStt INDTn Gtn

At this point, another educated guess was required. At position 263, the author saw the phrase “EIGHTIU oDBed iNDTWF ELVEF OUNDs OFSiLer.” 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:
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 likely that the 1907 pounds is of gold considering that the author saw the characters GOL shortly after the number.

Exhausting all characters for position 19, the author saw that “county” is the most likely word. Similarly, examining 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
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 "CONSISTING" 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 BEiONGING belonging

to continue the recovery of the message.
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.

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.
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 NTHS COUNTRY OFBED FORDA BOUTF OURMI LBSFR
50: OMBUF ORDISI NANCE CAVAT IONOR VAULT SIXFE BTFEL OWTHE SURFA
100: CEHOPT NEGRO UNDTH BOLL OWING ARTIC LESBE LONGI NGOI NTLYT
150: OTHEP ARTIE SNAME SAREC IVENI NNUNB BRTHR EWH
200: THEFI BSTD DE POSIT CONSI STCD PTHENI UNDRE DANDF OURTE ENPOU
250: NDOSF GOLDA NTHS FTYHI GTHHI NDRED ANDTW ELVEP OUNDS OPSIL
300: VERDE POSIT EDNOV RIGHT EENNII NTHS ECOND WASMA DEDEC
350: EIGHT EENTW ENTO NEAND CONSI STEDO FNINE THENH UNDRE DANDS
400: EVENP OUNDS OPGOL DANDT WELEN HDGRE EDAND EIGHT EYIGH TOFSI
450: LVERA LSOJE WELSO EATIN EDINS TLOUI SINEX CHANG ETOSA VETRA
500: NSFOR TATIO NANDV ALUED ATTHI STBEE RHOUS ANDDO LLLARS THEAB
550: OVEIS SECUR ELYPA CKEDI NIORD POTSW ITHIR ONCOV ERTSH EVAUL
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 reprints of this document through other sources. Many of these reprints 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 reprints 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
Cryptanalysis of Beale Cipher Number Two

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, then the cipher is decoded into

```
0: ihaae deop sttedi nthc ocntc ofged forda boarf ourmi lesfr
50: omutf oredl lsaaew caaat ionor aaloat sifwe etbeie owthe sirfa
100: ceott tanro hidth efolo onrng artic lesbe loqni aqjoi attct
150: othep attie avtos aiavl sareq iaepl niwhm ehtbr lthor ewth
200: thtfi tstde posit copsi stcd oftenn updre dandf curte epoi
250: odohe golde pathi hctei ghtha adred andtw elaep onuds ofsil
300: aerd spin ednna eight aaili netae nenem aconw watma deasac
350: linht evntw entco naad consi ftoih piine itltn toare danis
400: aaneo onds ofgoi lapit welae taarid edapi eight ceigh tofai
450: aarai ishe wecso btain edins tilotr sinew chang etosa astra
500: nspor tatio napda altes apthi rteep rheaos anddo ltrsc theab
550: oaeis secur llicpa cpadi niroa potsw ithir opcso ersth eapo
600: tiano anhlc oined withs tonea ndthe aesse thres tonso lidst
650: onal darel cserl dwppr othor spae ritmb erone deser ifahlt
700: hctwa ctloc alitic oftho aarot totha tahai ffcu ltcwli l1beh
750: adlfr 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

---

¹Ward 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, 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 "ABFDEFGHIJKLMNOP." 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

---

2Scanned 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 reprints (e.g., Gold in the Blue Ridge) have attempted to correct mistakes found in the Beale ciphers.

3One 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 KEYPFILE   "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(i);
}

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

printf ("\n\n");  

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;
    login[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[login[logindex]] = lognew[logindex];
    newkey[login[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");
    }
}
close (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)
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