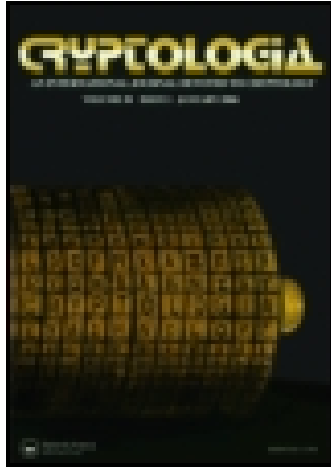




Cryptologia

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/ucry20>

BREAKING AN EIGHTEENTH CENTURY SHORTHAND SYSTEM

James J. Gillogly^a

^a 2520 Chard Ave., Topanga CA 90290 USA.

Published online: 04 Jun 2010.

To cite this article: James J. Gillogly (1987) BREAKING AN EIGHTEENTH CENTURY SHORTHAND SYSTEM, *Cryptologia*, 11:2, 93-98, DOI: [10.1080/0161-118791861857](https://doi.org/10.1080/0161-118791861857)

To link to this article: <http://dx.doi.org/10.1080/0161-118791861857>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms & Conditions of access and use can be found at <http://www.tandfonline.com/page/terms-and-conditions>

BREAKING AN EIGHTEENTH CENTURY SHORTHAND SYSTEM

James J. Gillogly

ADDRESS: 2520 Chard Ave., Topanga CA 90290 USA.

ABSTRACT: William Coleman wrote a letter in longhand and shorthand dated 14 Jun 1796. This paper describes the cryptanalysis of the shorthand portions of the letter and the subsequent identification of the system as Byrom's Shorthand.

KEYWORDS: Shorthand; Coleman, William; Byrom's Shorthand Writing.

Cracking an unknown shorthand system is much like dealing with a simple substitution cipher, but presents three unique problems. The first is determining the units of meaning: where does each letter or sound begin? The second problem is the spelling: shorthand systems are typically phonetic, rendering standard pattern-word lists useless and making word recognition more difficult. The third and potentially most serious problem is abbreviation: each shorthand system defines short strokes or sequences for common words and affixes. Worse, the shorthand writer may create his own idiosyncratic abbreviations.

In January 1986 *Cryptologia* Louis Kruh asked for help reading a letter written partly in shorthand by William Coleman (1766-1829) [1]. The longhand portions of the letter instruct "Tim" to liquidate some of Coleman's assets. The shorthand portions are reproduced in Figure 1, with some of the cleartext context around them. The lines of shorthand are lettered A through I for reference. For clarity I will call the longhand portions "cleartext", the shorthand portions "ciphertext", and the decrypted shorthand "plaintext." Following the Gregg shorthand definition, the shorthand "words" (which may include more than one word) will be called "outlines."

Despite the fairly small amount of material, the presence of several "cribs" and the mixing of cleartext with ciphertext give a plausible entry into the system. Near the beginning of line A an outline has a word above it that appears to say "numbered." I took this to be the work of the letter's recipient, deciphering a difficult outline. The cleartext "Virginia" and "150000" on line C appear to tie in with the second section of cleartext discussing his large land holdings. The crossed-out outline at the end of line D might well be an attempt at "September", which appears as cleartext at the beginning of line D. Line D has a fairly clear "repay" near the beginning. Two rather obscure decipherments appear over words in line E. The first might be "hazy" or "crazy", and the second might be "résumé" or something else. On line F we have cleartext "Tim" and probably "groped", and on line G the cleartext "Military" suggests the "military warrants" of the first cleartext section, while "Virginia" may refer again to the land

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

Downloaded by [The University of Manchester Library] at 08:09 20 October 2014

We can now look at "resumé" on line F and decide that it really isn't. We have R-Z-R-Z, with a dot at the bottom between the first R-Z. Adding in vowels, this could be RESOURCE, and the crib above it can be made to look like "resource" also. The dot near the bottom could be the E or the O vowel in RESOURCE, since it follows the first R and precedes the second. The horizontal line can now be used for either S or Z. Moving to line G, the guess that the outline after "Military" is "warrants" seems to be confirmed: it includes an R near the beginning and an S on the end. This gives us W as a counter-clockwise loop followed by a vertical downward stroke (assuming that doesn't include the A of warrants), N as a concave-upward stroke, and T as a vertical stroke, which we will assume can go either up or down like the R.

D GD CHNS WR I ? NTS NMBRED M THM FR MY DTRS FALTO MK MY PAMOT CH V BKM DU D I M deTASed I SR UTO A VR GRT
 A. (4 w 1. e y) 6, V 8 1. 2 9 9 9 C. (2 7. 7. 1.) 2
 B. DGR DIV NT NJON MY S A M M FR THS WBS BSDS TO AD TO MY EMBESMENT I PL MY S. PRSED WITH TO GRT
 C. GNTT F VIRGINIA LND CH I NO V IN HNT N SLD AMNTING TO 150000 AKRS FR CH I Y TO ADYNS NKST
 D. SEPTEMBER 18000 \$ D ALS TO 5000 \$ MR CH I V B Red FR THE PRPS F MKS THE PRCHS ALI CHN DU WITH L THS
 E. MYN NL CHNS I DGLR TO U TEM (D TH MST GO NO FRTR) D I AM LMST LUGY D V NO HUPUL B TO TRN AWA FRM THE SITH? F
 F. MY STATION S WE TURN AWA FRM THE PRSPOT F D TH NW TEM N THS S STNS I DU NT FL M S J-Fed N PRSDI... FRTIRL I V GROPED
 G. A LT. T F THS H RD DRKNESS I W SL MY MILITARY WENTS I W SL MY FI K AT A VR SML PRFT D THE PRTOLE PRS F THS
 H. LTR
 I. THS TRKT F LND OTHANS IT W SNK WE DN NTO A BTMLS GLULPH FR HVNS S K RT ME ALTR AS SNS S THS RUNS U D

Figure 2. Solution before adding vowels and "brief forms."

Comparing the outline after the first dot on line G and the single outline on line H, we have xTx and xTR as two words, where x represents some unknown letter. Assigning x = L gives the words LITTLE and LETTER; LETTER fits in well with the cleartext sentence that follows, so we accept this as well.

We have now identified several letters and the general system, so the next step is to fill in the known strokes throughout the ciphertext and use them to deduce more letters. The result of this effort is shown in Figure 2. At this point much of the letter can now be read and the sense is clear: in the cleartext Coleman is giving business-like instructions for his property disposal, and in the shorthand portions he is expressing urgency and his fears that he will be financially ruined.

A Table containing the Alphabet, the common words which the letters stand for, the Prepositions and Terminations.

	Names	Prepositions	Terminations
1 \	b be but	be	ble or able
(	d and	ve or dis	&
\	f of	for	ify
2	g against		
9 d	h have had		
9 d	j Judge Just		
2	k {can could	con or com	ical
1 2	l all		
(	m amongst	mis	ment
	{an	ante or an	
(	n in	inter or in	ness
	{under	under	
)	p upon	pro per pro	
7	q question		
1	r or	re	ary
	{as	super	a } e } i } u } tion or sion
-	{is	circum	
z	{us	sub	
1	t the	trans	ity
1 6	w will would	with	ward
1 9	x accept exercise	ac or extra	
2	y yet		
2	ch which		
1 6	sh shall should		ship
1 \	th that		

Figure 3. John Byrom's Short-hand. Plate CL.

However, some words are still obscure — not because the strokes making them up are unknown, but because single letters represent complete words. Some “brief forms” are clear from context, but at the beginning of the letter, for example, is a series of words that could be read in several ways. Without more ciphertext or less well-supported guesses, it appeared that this was as far as it could be taken. However, while looking for clues in various reference books I found the facsimile edition of the first printing of *Encyclopaedia Britannica*, published in 1771 [2]. The first volume credits “Byrom’s short-hand writing” as one of its source references, and the third volume gives an extensive course in this particular system. The alphabetical page (Figure 3) closely duplicated my own worksheet, except for the vowel system which I had reconstructed correctly only for the vertical strokes.

The *Britannica* article gave several pages of examples, including all of the brief forms used by Coleman. The completed solution can now be read:

[Cleartext ... TILL IT ENDS IN THE BANKRUPTCY OF MANY PERSONS OF APPARENT PROPERTY.] And God knows whether I should not be numbered amongst them, for my debtors fail to make my payments which have become due, and I am depressed I assure you, to a very great degree, and I have not enjoyed myself a moment for these 5 weeks. Besides, to add to my embarrassment I feel myself oppressed with too great quantity of [cleartext VIRGINIA] land which I now have in hand unsold, amounting to 150000 acres, for which I have to advance next [cleartext SEPTEMBER] 8000\$ and also to repay 5000\$ more which I have borrowed for the purpose of making the purchase. All [?] I can do with all this heaven only knows, I declare to you Tim (and this must go no further) and I am almost crazy, and have no resource[s] by to turn from the [situ? sight?] of my situation. So we turn away from the prospect of death. Now [cleartext TIM], in this circumstance, I do not feel myself justified in proceeding further, till I have [cleartext GROPED] a little out of this horrid darkness. I will sell my [cleartext MILITARY] warrants, I will sell my [cleartext VIRGINIA], if I can, at a very small profit, and the particular purpose of this letter [cleartext IS TO REQUEST YOU ASSISTANCE ...]

[Cleartext NOW TIM IT IS ABSOLUTELY NECESSARY I SHOULD GET RID OF] this tract of land. Otherwise it will sink me down into a bottomless [cleartext GULPH]. For heaven’s sake, write me a letter as soon as this reaches you and [cleartext DIRECT TO ME AT GREENFIELD].

In many places in this letter Coleman wrote a stroke upside down, with the loop on the wrong side. This was confusing, and suggested that he was making occasional mistakes in his writing. However, the *Britannica* article considered this a “feature” rather than a “bug”: if a letter connection is clumsy, either letter may be replaced by its mirror image. The shorthand system is not strictly phonetic, either: in the first line the word “knows” is written with the K stroke (upside-down) first.

The experiences described in this letter did not improve Coleman’s grasp of business. After his bankruptcy he went to New York and started a newspaper with the help of Alexander Hamilton and other Federalist friends. William Cullen Bryant wrote, “He had no skill as a manager of property; he took little thought for the morrow; when he happened to have any money, it was spent freely, or given away, or somebody who would never return it contrived

to borrow it. In a short time the finances of the Evening Post became greatly confused and embarrassed." Coleman's friends gave financial control of the paper to another man, and the Evening Post and Coleman soon got out of trouble and became prosperous. Coleman was quite successful as a journalist, and remained the editor until his death in 1829 [3].

A later edition of the *Britannica* [4] provides more perspective on Byrom's Short-hand System and its inventor, John Byrom (1692-1763):

To secure lineality in the writing and facility in consonantal joinings he [Byrom] provided two forms for b, h, j, w, x, sh, th, and three for l. A, e, i, o, u he represented by a dot in five positions with respect to a consonant. Practically it is impossible to observe more than three (beginning, middle and end). With all its merits, the system lacks rapidity, the continual recurrence of the loop seriously retarding the pen.

Despite these perceived problems, Byrom used his shorthand to take down speeches in the House of Commons over the objections of some of the members, and Coleman later used it to transcribe articles Hamilton dictated for the Evening Post.

SUMMARY

Despite the difficulties of vowel elimination, vowel placement and letter reflection, it was possible to arrive at an almost complete and unambiguous decryption of the letter. The process was greatly sped up by the existence of cribs written in above the outlines, and the final result was refined when the system was identified as Byrom's Short-hand Writing.

REFERENCES

1. Kruh, L. 1986. 18th Century Shorthand Expert Needed. *Cryptologia*. 10: 60-62.
2. A Society of Gentlemen. 1771. Short-hand Writing. *Encyclopaedia Britannica* (First Edition). 3: 586-599.
3. Bryant, W. C. 1902. *New York Evening Post*. One Hundredth Anniversary.
4. Chisholm, H. (ed.) 1910. Byrom, John. *Encyclopaedia Britannica* (Eleventh Edition). 4: 897.

BIOGRAPHICAL SKETCH

James J. Gillogly designs and writes software, mainly for UNIX machines and personal computers, and enjoys most the jobs where he gets paid to do cryptography. He received his PhD from Carnegie-Mellon University in Computer Science, specializing in Artificial Intelligence. He has written programs to solve or help solve dozens of the cryptosystems used by the American Cryptogram Association, but still has not figured out the Voynich Manuscript.