Vigenère cipher

The **Vigenère cipher** (French pronunciation: [viʒnɛːʁ]) is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution.[1][2]

First described by Giovan Battista Bellaso in 1553, the cipher is easy to understand and implement, but it resisted all attempts to break it until 1863, three centuries later. This earned it the description **le chiffre indéchiffrable** (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenère ciphers.[3] In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenère ciphers.

In the 19th century the scheme was misattributed to Blaise de Vigenère (1523–1596), and so acquired its present name.[4]

The Vigenère cipher is named after Blaise de Vigenère (pictured), although Giovan Battista Bellaso had invented it before Vigenère described his autokey cipher.

A reproduction of the Confederacy's cipher disk used in the American Civil War on display in the National Cryptologic Museum

Contents

History

The first well-documented description of a polyalphabetic cipher was by Leon Battista Alberti around 1467 and used a metal cipher disk to switch between cipher alphabets. Alberti's system only switched alphabets after several words, and switches were indicated by writing the letter of the corresponding alphabet in the ciphertext. Later, Johannes Trithemius, in his work *Polygraphiae* (which was completed in manuscript form in

1508 but first published in 1518),[5] invented the tabula recta, a critical component of the Vigenère cipher.[6] The Trithemius cipher, however, provided a progressive, rather rigid and predictable system for switching between cipher alphabets.[note 1]

In 1586 Blaise de Vigenère published a type of polyalphabetic cipher called an autokey cipher – because its key is based on the original plaintext – before the court of Henry III of France.[7]. The cipher now known as the Vigenère cipher, however, is that originally described by Giovan Battista Bellaso in his 1553 book *La cifra del Sig. Giovan Battista Bellaso*.[8] He built upon the tabula recta of Trithemius but added a repeating "countersign" (a key) to switch cipher alphabets every letter. Whereas Alberti and Trithemius used a fixed pattern of substitutions, Bellaso's scheme meant the pattern of substitutions could be easily changed, simply by selecting a new key. Keys were typically single words or short phrases, known to both parties in advance, or transmitted "out of band" along with the message. Bellaso's method thus required strong security for only the key. As it is relatively easy to secure a short key phrase, such as by a previous private conversation, Bellaso's system was considerably more secure.

In the 19th century, the invention of Bellaso's cipher was misattributed to Vigenère. David Kahn, in his book, *The Codebreakers* lamented this misattribution, saying that history had "ignored this important contribution and instead named a regressive and elementary cipher for him [Vigenère] though he had nothing to do with it".[9]

The Vigenère cipher gained a reputation for being exceptionally strong. Noted author and mathematician Charles Lutwidge Dodgson (Lewis Carroll) called the Vigenère cipher unbreakable in his 1868 piece "The Alphabet Cipher" in a children's magazine. In 1917, *Scientific American* described the Vigenère cipher as "impossible of translation".[10][11] That reputation was not deserved. Charles Babbage is known to have broken a variant of the cipher as early as 1854 but did not publish his work.[12] Kasiski entirely broke the cipher and published the technique in the 19th century, but even in the 16th century, some skilled cryptanalysts could occasionally break the cipher.[9]

The Vigenère cipher is simple enough to be a field cipher if it is used in conjunction with cipher disks.[13] The Confederate States of America, for example, used a brass cipher disk to implement the Vigenère cipher during the American Civil War. The Confederacy's messages were far from secret, and the Union regularly cracked its messages. Throughout the war, the Confederate leadership primarily relied upon three key phrases: "Manchester Bluff", "Complete Victory" and, as the war came to a close, "Come Retribution".[14]

Cryptographic slide rule used as a calculation aid by the Swiss Army between 1914 and 1940.

A Vernam cipher whose key is as long as the message becomes a one-time pad, a theoretically unbreakable cipher.[15] Gilbert Vernam tried to repair the broken cipher (creating the Vernam–Vigenère cipher in 1918), but the technology he used was so cumbersome as to be impracticable.[16]

Description

In a Caesar cipher, each letter of the alphabet is shifted along some number of places. For example, in a Caesar cipher of shift 3, A would become D, B would become E, Y would become B and so on. The Vigenère cipher has several Caesar ciphers in sequence with different shift values.

To encrypt, a table of alphabets can be used, termed a *tabula recta*, *Vigenère square* or *Vigenère table*. It has the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption

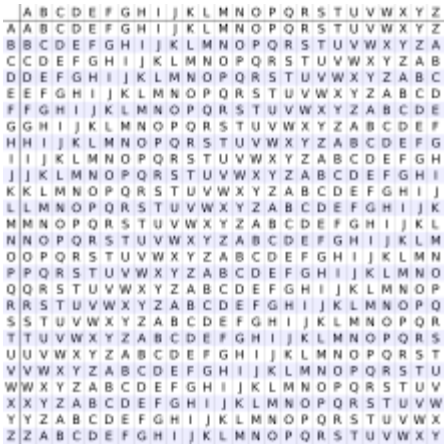
process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

For example, suppose that the plaintext to be encrypted is

```
ATTACKATDAWN.
```

The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword "LEMON":

```
LEMONLEMONLE
```



The Vigenère square or Vigenère table, also known as the *tabula recta*, can be used for encryption and decryption.

Each row starts with a key letter. The rest of the row holds the letters A to Z (in shifted order). Although there are 26 key rows shown, a code will use only as many keys (different alphabets) as there are unique letters in the key string, here just 5 keys: {L, E, M, O, N}. For successive letters of the message, successive letters of the key string will be taken and each message letter enciphered by using its corresponding key row. The next letter of the key is chosen, and that row is gone along to find the column heading that matches the message character. The letter at the intersection of [key-row, msg-col] is the enciphered letter.

For example, the first letter of the plaintext, A, is paired with L, the first letter of the key. Therefore, row L and column A of the Vigenère square are used, namely L. Similarly, for the second letter of the plaintext, the second letter of the key is used. The letter at row E and column T is X. The rest of the plaintext is enciphered in a similar fashion:

Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in that row and then using the column's label as the plaintext. For example, in row L (from *L*EMON), the ciphertext L appears in column A, which is the first plaintext letter. Next, in row E (from L*E*MON), the ciphertext X is located in column T. Thus T is the second plaintext letter.

Algebraic description

Vigenère can also be described algebraically. If the letters A–Z are taken to be the numbers 0–25 ($A \mathrel{\widehat{=}} 0$, $B \mathrel{\widehat{=}} 1$, etc.), and addition is performed modulo 26, Vigenère encryption E using the key K can be written as

$$C_i = E_K(M_i) = (M_i + K_i) \bmod 26$$

and decryption D using the key K as

$$M_i = D_K(C_i) = (C_i - K_i + 26) \bmod 26,$$

in which $M = M_1 \dots M_n$ is the message, $C = C_1 \dots C_n$ is the ciphertext and $K = K_1 \dots K_n$ is the key obtained by repeating the keyword $\lceil n/m \rceil$ times in which m is the keyword length.

Thus, by using the previous example, to encrypt $A \mathrel{\widehat{=}} 0$ with key letter $L \mathrel{\widehat{=}} 11$ the calculation would result in $11 \mathrel{\widehat{=}} L$.

$$11 = (0 + 11) \bmod 26$$

Therefore, to decrypt $R \mathrel{\widehat{=}} 17$ with key letter $E \mathrel{\widehat{=}} 4$, the calculation would result in $13 \mathrel{\widehat{=}} N$.

$$13 = (17 - 4) \bmod 26$$

In general, if Σ is the alphabet of length ℓ, and m is the length of key, Vigenère encryption and decryption can be written:

$$C_i = E_K(M_i) = (M_i + K_{(i \bmod m)}) \bmod \ell,$$

$$M_i = D_K(C_i) = (C_i - K_{(i \bmod m)}) \bmod \ell.$$

M_i denotes the offset of the *i*-th character of the plaintext M in the alphabet Σ. For example, by taking the 26 English characters as the alphabet $\Sigma = (A, B, C, \ldots, X, Y, Z)$, the offset of A is 0, the offset of B is 1 etc. C_i and K_i are similar.

Cryptanalysis

The idea behind the Vigenère cipher, like all other polyalphabetic ciphers, is to disguise the plaintext letter frequency to interfere with a straightforward application of frequency analysis. For instance, if P is the most frequent letter in a ciphertext whose plaintext is in English, one might suspect that P corresponds to E since E is the most frequently used letter in English. However, by using the Vigenère cipher, E can be enciphered as different ciphertext letters at different points in the message, which defeats simple frequency analysis.

The primary weakness of the Vigenère cipher is the repeating nature of its key. If a cryptanalyst correctly guesses the key's length, the cipher text can be treated as interwoven Caesar ciphers, which can easily be broken individually. The Kasiski examination and Friedman test can help to determine the key length (see below: § Kasiski examination and § Friedman test).

Kasiski examination

In 1863, Friedrich Kasiski was the first to publish a successful general attack on the Vigenère cipher.[17] Earlier attacks relied on knowledge of the plaintext or the use of a recognizable word as a key. Kasiski's method had no such dependencies. Although Kasiski was the first to publish an account of the attack, it is clear that others had been aware of it. In 1854, Charles Babbage was goaded into breaking the Vigenère cipher when John Hall Brock Thwaites submitted a "new" cipher to the Journal of the Society of the Arts.[18][19] When Babbage showed that Thwaites' cipher was essentially just another recreation of the Vigenère cipher, Thwaites presented a challenge to Babbage: given an original text (from Shakespeare's *The Tempest* : Act 1, Scene 2) and its enciphered version, he was to find the key words that Thwaites had used to encipher the original text. Babbage soon found the key words: "two" and "combined". Babbage then enciphered the same passage from Shakespeare using different key words and challenged Thwaites to find Babbage's key words.[20] Babbage never explained the method that he used. Studies of Babbage's notes reveal that he had used the method later published by Kasiski and suggest that he had been using the method as early as 1846.[21]

The Kasiski examination, also called the Kasiski test, takes advantage of the fact that repeated words are, by chance, sometimes encrypted using the same key letters, leading to repeated groups in the ciphertext. For example, consider the following encryption using the keyword ABCD:

```
Key:        ABCDABCDABCDABCDABCDABCDABCD
Plaintext:  CRYPTOISSHORTFORCRYPTOGRAPHY
Ciphertext: CSASTPKVSIQUTGQUCSASTPIUAQJB
```

There is an easily noticed repetition in the ciphertext, and so the Kasiski test will be effective.

The distance between the repetitions of CSASTP is 16. If it is assumed that the repeated segments represent the same plaintext segments, that implies that the key is 16, 8, 4, 2, or 1 characters long. (All factors of the distance are possible key lengths; a key of length one is just a simple Caesar cipher, and its cryptanalysis is much easier.) Since key lengths 2 and 1 are unrealistically short, one needs to try only lengths 16, 8 or 4. Longer messages make the test more accurate because they usually contain more repeated ciphertext segments. The following ciphertext has two segments that are repeated:

```
Ciphertext: VHVSSPQUCEMRVBVBBBVHVSURQGIBDUGRNICJQUCERVUAXSSR
```

The distance between the repetitions of VHVS is 18. If it is assumed that the repeated segments represent the same plaintext segments, that implies that the key is 18, 9, 6, 3, 2 or 1 character long. The distance between the repetitions of QUCE is 30 characters. That means that the key length could be 30, 15, 10, 6, 5, 3, 2 or 1 character long. By taking the intersection of those sets, one could safely conclude that the most likely key length is 6 since 3, 2, and 1 are unrealistically short.

Friedman test

The Friedman test (sometimes known as the kappa test) was invented during the 1920s by William F. Friedman, who used the index of coincidence, which measures the unevenness of the cipher letter frequencies to break the cipher. By knowing the probability κ_p that any two randomly chosen source language letters are the same (around 0.067 for monocase English) and the probability of a coincidence for a uniform random selection from the alphabet κ_r (1/26 = 0.0385 for English), the key length can be estimated as the following:

$$\frac{\kappa_p - \kappa_r}{\kappa_o - \kappa_r}$$

from the observed coincidence rate

$$\kappa_o = \frac{\sum_{i=1}^{c} n_i(n_i - 1)}{N(N-1)}$$

in which c is the size of the alphabet (26 for English), N is the length of the text and n_1 to n_c are the observed ciphertext letter frequencies, as integers.

That is, however, only an approximation; its accuracy increases with the size of the text. It would, in practice, be necessary to try various key lengths that are close to the estimate.[22] A better approach for repeating-key ciphers is to copy the ciphertext into rows of a matrix with as many columns as an assumed key length and then to compute the average index of coincidence with each column considered separately. When that is done for each possible key length, the highest average I.C. then corresponds to the most-likely key length.[23] Such tests may be supplemented by information from the Kasiski examination.

Frequency analysis

Once the length of the key is known, the ciphertext can be rewritten into that many columns, with each column corresponding to a single letter of the key. Each column consists of plaintext that has been encrypted by a single Caesar cipher. The Caesar key (shift) is just the letter of the Vigenère key that was used for that column. Using methods similar to those used to break the Caesar cipher, the letters in the ciphertext can be discovered.

An improvement to the Kasiski examination, known as Kerckhoffs' method, matches each column's letter frequencies to shifted plaintext frequencies to discover the key letter (Caesar shift) for that column. Once every letter in the key is known, all the cryptanalyst has to do is to decrypt the ciphertext and reveal the plaintext.[24] Kerckhoffs' method is not applicable if the Vigenère table has been scrambled, rather than using normal alphabetic sequences, but Kasiski examination and coincidence tests can still be used to determine key length.

Key elimination

The Vigenère cipher, with normal alphabets, essentially uses modulo arithmetic, which is commutative. Therefore, if the key length is known (or guessed), subtracting the cipher text from itself, offset by the key length, will produce the plain text encrypted with itself. If any "probable word" in the plain text is known or can be guessed, its self-encryption can be recognized, which allows recovery of the key by subtracting the known plaintext from the cipher text. Key elimination is especially useful against short messages.

Variants

The running key variant of the Vigenère cipher was also considered unbreakable at one time. This version uses as the key a block of text as long as the plaintext. Since the key is as long as the message, the Friedman and Kasiski tests no longer work, as the key is not repeated.

If multiple keys are used, the effective key length is the least common multiple of the lengths of the individual keys. For example, using the two keys `GO` and `CAT`, whose lengths are 2 and 3, one obtains an effective key length of 6 (the least common multiple of 2 and 3). This can be understood as the point where both keys line up.

Plaintext:	`ATTACKATDAWN`
Key 1:	`GOGOGO`**`GOGOGO`**
Key 2:	`CATCAT`**`CATCAT`**
Ciphertext:	`IHSQIRIHCQCU`

Encrypting twice, first with the key `GO` and then with the key `CAT` is the same as encrypting once with a key produced by encrypting one key with the other.

Plaintext:	`GOGOGO`
Key:	`CATCAT`
Ciphertext:	`IOZQGH`

This is proven by encrypting `ATTACKATDAWN` with `IOZQGH`, to produce the same ciphertext as in the original example.

Plaintext:	`ATTACKATDAWN`
Key:	`IOZQGHIOZQGH`
Ciphertext:	`IHSQIRIHCQCU`

If key lengths are relatively prime, the effective key length grows exponentially as the individual key lengths are increased. This is especially true if each key length is individually prime. For example, the effective length of keys 2, 3, and 5 characters is 30, but that of keys of 7, 11, and 13 characters is 1,001. If this effective key length is longer than the ciphertext, it achieves the same immunity to the Friedman and Kasiski tests as the running key variant.

If one uses a key that is truly random, is at least as long as the encrypted message, and is used only once, the Vigenère cipher is theoretically unbreakable. However, in that case, the key, not the cipher, provides cryptographic strength, and such systems are properly referred to collectively as one-time pad systems, irrespective of the ciphers employed.

Confederate cipher wheel, captured at the surrender of Mobile, Alabama, in May 1865 – National Cryptologic Museum

Vigenère actually invented a stronger cipher, an autokey cipher. The name "Vigenère cipher" became associated with a simpler polyalphabetic cipher instead. In fact, the two ciphers were often confused, and both were sometimes called *le chiffre indéchiffrable*. Babbage actually broke the much-stronger autokey cipher, but Kasiski is generally credited with the first published solution to the fixed-key polyalphabetic ciphers.

A simple variant is to encrypt by using the Vigenère decryption method and to decrypt by using Vigenère encryption. That method is sometimes referred to as "Variant Beaufort". It is different from the Beaufort cipher, created by Francis Beaufort, which is similar to Vigenère but uses a slightly modified enciphering mechanism and tableau. The Beaufort cipher is a reciprocal cipher.

Despite the Vigenère cipher's apparent strength, it never became widely used throughout Europe. The Gronsfeld cipher is a variant created by Count Gronsfeld (Josse Maximilaan van Gronsveld né van Bronckhorst); it is identical to the Vigenère cipher except that it uses just 10 different cipher alphabets, corresponding to the digits 0 to 9). A Gronsfeld key of 0123 is the same as a Vigenere key of ABCD. The Gronsfeld cipher is strengthened because its key is not a word, but it is weakened because it has just 10 cipher alphabets. It is Gronsfeld's cipher that became widely used throughout Germany and Europe, despite its weaknesses.

See also

- Roger Frontenac (Nostradamus quatrain decryptor, 1950)

References

Citations

1. Bruen, Aiden A. & Forcinito, Mario A. (2011). *Cryptography, Information Theory, and Error-Correction: A Handbook for the 21st Century* (https://books.google.com/books?id=fd2LtVgFzoMC&pg=PA21). John Wiley & Sons. p. 21. ISBN 978-1-118-03138-4.
2. Martin, Keith M. (2012). *Everyday Cryptography* (https://books.google.com/books?id=1NHli2uzt_EC&pg=PT142). Oxford University Press. p. 142. ISBN 978-0-19-162588-6.
3. Laurence Dwight Smith (1955). *Cryptography: The Science of Secret Writing* (https://books.google.com/books?id=8EERL-T-ziwC&pg=PA80). Courier Corporation. p. 81. ISBN 978-0-486-20247-1.

4. Rodriguez-Clark, Dan (2017), *Vigenère Cipher* (https://crypto.interactive-maths.com/vigenegravere-cipher.html), Crypto Corner
5. Gamer, Maximilian (2015). "Die Polygraphia des Johannes Trithemius. Zwei Fassungen eines frühneuzeitlichen Handbuchs zur Geheimschrift [The Polygraphia of Johannes Trithemius. Two editions of an early modern handbook on cryptography]". In Baier, Thomas; Schultheiß, Jochen (eds.). *Würzburger Humanismus* [*The Humanism of Würzburg*] (in German). Tübingen, Germany: Narr Verlag. pp. 121–141. See pp. 121–122.
6. Trithemius, Joannis (1518). "Liber quintus exordium capit (Book 5, Ch. 1)". *Polygraphiae, libri sex …* [*Cryptography, in six books …*] (in Latin). Reichenau, (Germany): Johann Haselberg. p. 471. Available at: George Fabyan Collection (Library of Congress; Washington, D.C., U.S.A.) (http://lcweb2.loc.gov/cgi-bin/ampage?collId=rbc3&fileName=rbc0001_2009fabyan12345page.db&recNum=470) (Note: The pages of this book are not numbered.)
7. Vigenère, Blaise de (1586). *Traicté des Chiffres, ou Secretes Manieres d'Escrire* (http://gallica.bnf.fr/ark:/12148/bpt6k94009991.image) [*Treatise on ciphers, or secret ways of writing*] (in French). Paris, France: Abel l'Angelier.
8. Bellaso, Giovan Battista (1553). *La Cifra del Sig. Giovan Battista Belaso …* (in Italian). Venice, (Italy). Available at: Museo Galileo (Florence (Firenze), Italy) (https://bibdig.museogalileo.it/Teca/Viewer;jsessionid=E02FA6976F859981BC4EC1DF5CC3B240?an=976325&vis=D#page/1/mode/2up)
9. David, Kahn (1999). "On the Origin of a Species". *The Codebreakers: The Story of Secret Writing*. Simon & Schuster. ISBN 0-684-83130-9.
10. (Anon.) (27 January 1917). "A new cipher code" (https://babel.hathitrust.org/cgi/pt?id=uc1.31210000211050;view=1up;seq=69). *Scientific American Supplement*. **83** (2143): 61. However, see also:
    - Borden, Howard A. (3 March 1917). "Letter to the Editor: Cipher codes" (https://babel.hathitrust.org/cgi/pt?id=uc1.31210000211050;view=1up;seq=147). *Scientific American Supplement*. **83** (2148): 139.
    - Holstein, Otto (14 April 1917). "Letter to the Editor: A new cipher" (https://babel.hathitrust.org/cgi/pt?id=uc1.31210000211050;view=1up;seq=243). *Scientific American Supplement*. **83** (2154): 235.
    - Holstein, Otto (October 1921). "The ciphers of Porta and Vigenère: The original undecipherable code, and how to decipher it" (https://babel.hathitrust.org/cgi/pt?id=pst.000018628043;view=1up;seq=338). *Scientific American Monthly*. **4**: 332–334.
11. Knudsen, Lars R. (1998). "Block Ciphers—a survey". In Bart Preneel and Vincent Rijmen (ed.). *State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptograph Leuven Belgium, June 1997 Revised Lectures* (https://archive.org/details/stateartappliedc00pren). Berlin ; London: Springer. pp. 29 (https://archive.org/details/stateartappliedc00pren/page/n35). ISBN 3-540-65474-7.
12. Singh, Simon (1999). "Chapter 2: Le Chiffre Indéchiffrable". *The Code Book* (https://archive.org/details/codebook00simo/page/63). Anchor Books, Random House. pp. 63–78 (https://archive.org/details/codebook00simo/page/63). ISBN 0-385-49532-3.
13. Codes, Ciphers, & Codebreaking (http://www.vectorsite.net/ttcode_03.html#m2) (The Rise Of Field Ciphers)
14. David, Kahn (1999). "Crises of the Union". *The Codebreakers: The Story of Secret Writing*. Simon & Schuster. pp. 217–221. ISBN 0-684-83130-9.
15. Stanislaw Jarecki, "Crypto Overview, Perfect Secrecy, One-time Pad" (http://www.ics.uci.edu/~stasio/fall04/lect1.pdf), *University of California*, September 28, 2004, Retrieved November 20, 2016
16. Simmons, Gustavus J., *Vernam-Vigenère cipher* (https://www.britannica.com/topic/Vernam-Vigenere-cipher), Encyclopedia Britannica

17. Kasiski, F. W. (1863). *Die Geheimschriften und die Dechiffrir-Kunst* (https://books.google.com/books?id=fB5dAAAAcAAJ&pg=PP7#v=onepage&q&f=false) [*Cryptograms and the art of deciphering*] (in German). Berlin, (Germany): E.S. Mittler und Sohn.
18. See:
    - Thwaites, J.H.B. (11 August 1854). "Secret, or cypher writing" (https://books.google.com/books?id=nxw9AQAAIAAJ&pg=PA663#v=onepage&q&f=false). *Journal of the Society of Arts*. **2** (90): 663–664.
    - "C." (Charles Babbage) (1 September 1854). "Mr. Thwaites's cypher" (https://books.google.com/books?id=nxw9AQAAIAAJ&pg=PA707#v=onepage&q&f=false). *Journal of the Society of Arts*. **2** (93): 707–708.
    - Babbage, Charles (1864). *Passages from the Life of a Philosopher* (https://archive.org/details/bub_gb_2T0AAAAAQAAJ). London, England: Longman. p. 496 (https://archive.org/details/bub_gb_2T0AAAAAQAAJ/page/n509).
19. Thwaites filed for a patent for his "new" cipher system:
    - "Weekly list of patents sealed. … 1727. John Hall Brock Thwaites, Bristol – Improvements in apparatus to facilitate communication by cypher." (https://babel.hathitrust.org/cgi/pt?id=gri.ark:/13960/t4gn2h303;view=1up;seq=798) in: *Journal of the Society of Arts*, **2** (99): 792 (13 October 1854).
    - "Thwaites, John Hall Brock, of Bristol, dentist. *Improvements in apparatus to facilitate the communication by cypher*. Application dated August 7, 1854. (No. 1727.)" (https://books.google.com/books?id=7xEFAAAAQAAJ&pg=PA211#v=onepage&q&f=false) in: *The Mechanics' Magazine*, **62** (1647): 211 (3 March 1855).
20. See:
    - Thwaites, John H.B. (15 September 1854). "Secret or cypher writing" (https://babel.hathitrust.org/cgi/pt?id=gri.ark:/13960/t4gn2h303;view=1up;seq=738). *Journal of the Society of Arts*. **2** (95): 732–733.
    - "C" (Charles Babbage) (6 October 1854). "Mr. Thwaites's cypher" (https://babel.hathitrust.org/cgi/pt?id=gri.ark:/13960/t4gn2h303;view=1up;seq=782). *Journal of the Society of Arts*. **2** (98): 776–777.
21. Ole Immanuel Franksen (1985). *Mr. Babbage's Secret: The Tale of a Cypher and APL* (https://books.google.com/books?id=53dQAAAAMAAJ). Prentice Hall. ISBN 978-0-13-604729-2.
22. Henk C.A. van Tilborg, ed. (2005). *Encyclopedia of Cryptography and Security* (https://archive.org/details/encyclopediacryp00tilb) (First ed.). Springer. pp. 115 (https://archive.org/details/encyclopediacryp00tilb/page/n127). ISBN 0-387-23473-X.
23. Mountjoy, Marjorie (1963). "The Bar Statistics". *NSA Technical Journal*. **VII** (2, 4). Published in two parts.
24. "Lab exercise: Vigenere, RSA, DES, and Authentication Protocols" (https://web.archive.org/web/20110723140549/http://courses.umass.edu/cs415/labs/lab1/415-lab1-crypto.pdf) (PDF). *CS 415: Computer and Network Security*. Archived from the original (http://courses.umass.edu/cs415/labs/lab1/415-lab1-crypto.pdf) (PDF) on 2011-07-23. Retrieved 2006-11-10.

Sources

- Beutelspacher, Albrecht (1994). "Chapter 2". *Cryptology*. translation from German by J. Chris Fisher. Washington, DC: Mathematical Association of America. pp. 27–41. ISBN 0-883-85504-6.
- Singh, Simon (1999). "Chapter 2: Le Chiffre Indéchiffrable". *The Code Book*. Anchor Book, Random House. ISBN 0-385-49532-3.
- Helen F. Gaines (18 November 2014). *Cryptanalysis: A Study of Ciphers and Their Solution* (https://books.google.com/books?id=Zb2RBQAAQBAJ&pg=PA117&lpg=PA117&focus=viewport&vq=%22Chapter+XIII+The+Gronsfeld,+Porta+and+Beaufort+Ciphers%22&dq=Gaines,+Helen+

Fouche+%22Cryptanalysis+a+Study+of+Ciphers+and+Their+Solutions%22+1939+%22The+Gronsfeld,+Porta+and+Beaufort+Ciphers%22). Courier Corporation. p. 117. ISBN 978-0-486-80059-2.
- Mendelsohn, Charles J (1940). "Blaise De Vigenere and The 'Chiffre Carre' ". *Proceedings of the American Philosophical Society*. **82** (2).

Notes

1. In a separate manuscript that Trithemius called the *Clavis Polygraphiae* (The Key to the Polygraphia), he explained (among other things) how to encipher messages by using a polyalphabetic cipher and how to decipher such messages. The *Clavis Polygraphiae* was not always included in the original 1518 printed copies, and even when it was included, it wasn't always inserted in the same location in the *Polygraphiae*. From (Gamer, 2015), p. 129: *"Eine eigene Stellung innerhalb … in den Ausführungen zu Buch VI."* (The *Clavis* occupies a peculiar place within the text that's been passed down only in print. Trithemius alludes several times in other places to the existence of a *Clavis Polygraphiae* as a separate work, contemporaneous with the manuscript of 1508. However, we know only the edition that is bound with the printed version, which was sporadically adapted to changes during printing, as often as not – as, for example, in the case of the shifted chapter on alphanumeric number notation. The *Clavis* didn't accompany this relocation: the explanations of the representations of numbers remained in the remarks on Book VI.)
   The *Clavis* explains how to encipher and decipher messages by using polyalphabetic ciphers. In Trithemius' examples, he decoded a message by using two Vignere tables – one in which the letters are in normal alphabetical order and the other in which the letters are in reversed order (see (Gamer, 2015), p. 128). From (Trithemius, 1518), pp. 19–20 (http://reader.digitale-sammlungen.de/de/fs1/object/display/bsb11200432_00019.html):
   Original Latin text: *"In primis tabulam descripsimus rectam, alphabeta quatuor & viginti continentem, per cuius intelligentiam tot poterunt alphabeta componi, quot stellae numerantur in firmamento caeli. Quot enim in ipsa tabula sunt grammata, totiens consurgunt ex arte decies centena milia per ordinem alphabeta. Post haec tabulam distribuimus aversam, quae totiens consurget in aliam, quotiens literam mutaveris a capite primam. Est autem litera prima in tabula recta b, & in aversa z. In quarum locum quotiens reposueris quamlibet aliam variatam totiens invenies tabulam per omnia novam, & ita usque ad infinitum. Deinde primam tabulam rectam expandimus, unicuique literae transpositae nigrae illam quam repraesentat ad caput eius cum minio collocantes, ut modum scribendi faciliorem lectori praeberemus. Est autem modus iste scribendi, ut in primo alphabeto nigro, capias occultae sententiae literam unam, de secundo aliam, de tertio tertiam, & sic consequenter usque ad finem. Quo cum perveneris, totiens ad ordinem primum redeundum memineris, quousque mentis tuae secretum mysterium occultando compleveris. Verum ut ordinem videas, ponamus exemplum. Hxpf gfbmcz fueib gmbt gxhsr ege rbd qopmauwu. wfxegk ak tnrqxyx. Huius mystici sermonis sententia est. Hunc caveto virum, quia malus est, fur, deceptor, mendax & iniquus. Cernis iam nunc lector quam mirabilem transpositionem literarum alphabeti haec tabula reddat, cum sit nemo qui sine noticia eius hoc valeat penetrare secretum. Exedit enim modus iste scribendi omnem transpositionem literarum communem, cum unaquaeque litera semper de una serie alphabeti mutetur in aliam. Ex tabula quoque aversa quam simili distributione per ordinem expandimus, pro introductione tale ponamus exemplum. Rdkt, stznyb, tevqz, fnzf, fdrgh, vfd. Cuius arcani sensus est talis, Hunc caveto virum, quia malus [est]. Et nota quod sub exemplo tabulae recte iam posito seriem occultam a principio per totum eius deduximus, & deinceps continuando similiter per aversam, rursusque circulum facimus, ut cernis ad principium tabulae rectae."*
   English translation: In the first [illustration], we have transcribed a regular table [i.e., *tabula recta*, a table in which the letters of alphabet are listed in their normal order; see (Trithemius, 1518), p. 471. (http://lcweb2.loc.gov/cgi-bin/ampage?collId=rbc3&fileName=rbc0001_2009fabyan12345page.db&recNum=470)] containing 24 alphabets [Note: Trithemius used alphabets containing only 24 letters by setting j=i and v=u.], by which knowledge they will be able to

compose as many alphabets as stars are numbered in the firmament of heaven. For in the table itself there are as many letters as arise by [applying] skill – a million per alphabetical row. [That is, the letters in the table need not be listed in alphabetical order, so many enciphering tables can be created.] After this, we arrange [the alphabets in] the reverse table [i.e., *tabula aversa*, a table in which the letters of the alphabet are listed in reverse order; see (Trithemius, 1518), p. 472. (http://lcweb2.loc.gov/cgi-bin/ampage?collId=rbc3&fileName=rbc0001_2009fabyan12345page.db&recNum=471)], which will arise in the other [reversed table] as many times as you will have changed [i.e., permuted] the first letter of the top [of the regular table]. And so the first letter in the regular table is b, and z in the reverse [table]. As often as you will have put in its place another changed [table], you will find a new table for everything, and so on indefinitely. [That is, again, many enciphering tables can be created.] Next we explain the first regular table: it shows how it is assigning, to each transposed black letter, [a letter] in red [ink along] its [i.e., the table's] top [border], in order to show to the reader an easier way of writing [i.e., of deciphering messages]. And that is a way of writing so that in the first black alphabet [i.e., an alphabet printed in the table using black, not red, ink], you will get one letter of the hidden sentence [i.e., the deciphered message]; from the second [black alphabet], another [deciphered letter]; from the third [black alphabet], a third [deciphered letter]; and thus accordingly until the end. You will have arrived there [i.e., at the end] when you will have recalled returning many times to the first row, until you will have completed concealing the secret mystery of your thought. [That is, the message is deciphered by deciphering its first 24 letters by using the *tabula recta*, then repeating the procedure by using the same *tabula recta* to decipher the next 24 letters of the message, and so on.] However, so that you [can] see the sequence [i.e., procedure], we present an example: *Hxpf gfbmcz fueib gmbt gxhsr ege rbd qopmauwu wfxegk ak tnrqxyx.* The meaning of this mystical sentence is: *Hunc caveto virum, quia malus est, fur, deceptor, mendax et iniquus.* (Beware of this man, who is bad, a thief, a deceiver, a liar, and unjust.) You already discern now, reader, how this table renders an astonishing transposition of the letters of the alphabet, because there is no one who, without acquaintance of this, can penetrate the secret. For that method of writing corrodes every transposition of common letters, because each and every letter of one sequence of the alphabet is always changed into another [letter]. Likewise, we explain how [to decipher a message], by means of the sequence [i.e., the deciphering procedure], from the reverse table with a similar arrangement [of letters]; as an introduction, we present such an example: *Rdkt, stznyb, tevqz, fnzf, fdrgh, vfd.* The secret meaning of which is such: *Hunc caveto virum, quia malus [est].* (Beware of this man, who is bad.) And note about the example of the regular table [that was] already presented [i.e., the example that began with *Hxpf*], that we derived the secret series [i.e., the deciphered message] from the beginning through all of it [i.e., of the regular table], and thereafter by continuing similarly by means of the reverse [table], and again we make a circle, so that you are looking at the beginning of the regular table. [That is, the message is deciphered by using the regular table, but if the message is longer than 24 characters, then the decipherment continues by using the reverse table, and if necessary, one continues to decipher by returning to the regular table – and so forth.]

External links

Articles

- History of the cipher from Cryptologia (https://web.archive.org/web/20110624100854/http://www.aolnews.com/2010/12/25/civil-war-message-in-a-bottle-opened-decoded/)
- Basic Cryptanalysis (https://www.bbc.co.uk/dna/h2g2/alabaster/A613135) at H2G2
- "Lecture Notes on Classical Cryptology" (http://www.math.ucdenver.edu/~wcherowi/courses/m5410/m5410cc.html) including an explanation and derivation of the Friedman Test

---