

# 1 Introductory Synopsis

*En cryptographie, aucune règle n'est absolue.*

[In cryptography, no rule is absolute.]

Étienne Bazeris (1901)

## 1.1 Cryptography and Steganography

We must distinguish between cryptography (Greek *kryptos*, hidden) and steganography (Greek *steganos*, covered). The term *cryptographia*, to mean *secrecy in writing*, was used in 1641 by John Wilkins, a founder with John Wallis of the Royal Society in London; the word ‘cryptography’ was coined in 1658 by Thomas Browne, a famous English physician and writer. It is the aim of cryptography to render a message incomprehensible to an unauthorized reader: *ars occulte scribendi*. One speaks of *overt secret writing*: overt in the sense of being obviously recognizable as secret writing.

The term *steganographia* was also used in this sense by Caspar Schott, a pupil of Athanasius Kircher, in the title of his book *Schola steganographia*, published in Nuremberg in 1665; however, it had already been used by Trithemius in his first (and amply obscure) work *Steganographia*, which he began writing in 1499, to mean ‘hidden writing’. Its methods have the goal of concealing the very *existence* of a message (however that may be composed)—communicating without incurring suspicion (Francis Bacon, 1623: *ars sine secreti latentis suspicione scribendi*). By analogy, we can call this *covert secret writing* or indeed ‘steganography’.

Cryptographic methods are suitable for keeping a private diary or notebook—from Samuel Pepys (1633–1703) to Alfred C. Kinsey (1894–1956)—or preventing a messenger understanding the dispatch he bears; steganographic methods are more suitable for smuggling a message out of a prison—from Sir John Trevanion (Fig. 13), imprisoned in the English Civil War, to the French bank robber Pastoure, whose conviction was described by André Langie, and Klaus Croissant, the lawyer and Stasi collaborator who defended the Baader-Meinhof terrorist gang. The imprisoned Christian Klar used a book cipher.

Steganography falls into two branches, linguistic steganography and technical steganography. Only the first is closely related to cryptography. The technical aspect can be covered very quickly: invisible inks have been in use since Pliny’s time. Onion juice and milk have proved popular and effective through the ages (turning brown under heat or ultraviolet light). Other classical props are hollow heels and boxes with false bottoms.

Among the modern methods it is worth mentioning high-speed telegraphy, the spurt transmission of stored Morse code sequences at 20 characters per second, and frequency subband permutation ('scrambling') in the case of telephony, today widely used commercially. In the Second World War, the *Forschungsstelle* (research post) of the *Deutsche Reichspost* (headed by *Postrat Dipl.-Ing.* Kurt E. Vetterlein) listened in from March 1942 to supposedly secure radio telephone conversations between Franklin D. Roosevelt and Winston Churchill, including one on July 29, 1943, immediately before the cease-fire with Italy, and reported them via Schellenberg's *Reichssicherheitshauptamt, Amt VI* to Himmler.

Written secret messages were revolutionized by microphotography; a *microdot* the size of a speck of dirt can hold an entire quarto page—an extraordinary development from the macrodot of Histiaëus<sup>1</sup>, who shaved his slave's head, wrote a message on his scalp; then waited for the hair to grow again. Microdots were invented in the 1920s by Emanuel Goldberg. The Russian spy Rudolf Abel produced his microdots from spectroscopic film which he was able to buy without attracting attention. Another Soviet spy, Gordon Arnold Lonsdale, hid his microdots in the gutters of bound copies of magazines. The microdots used by the Germans in the Second World War were of just the right size to be used as a full stop (period) in a typewritten document.

## 1.2 Semagrams

Linguistic steganography recognizes two methods: a secret message is either made to appear innocent in an *open code*, or it is expressed in the form of visible (though often minute) graphical details in a script or drawing, in a *semagram*. This latter category is especially popular with amateurs, but leaves much to be desired, since the details are too obvious to a trained and wary eye. The young Francis Bacon (1561–1626) invented the use of two type-faces to convey a secret message (Fig. 1), described in the Latin translation *De dignitate et augmentis scientiarum* (1623) of his 1605 book *Proficience and Advancement*. It has never acquired any great practical importance (but see Sect. 3.3.3 for the binary code he introduced on this occasion).

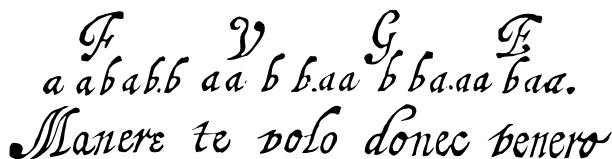


Fig. 1. Francis Bacon: Visible concealment of a binary code ('biliteral cipher') by means of different types of script. Note the different forms of /e/ in the word *Manere*

The same steganographic principle appears to have been known in Paris at the same time, and was mentioned by Vigenère in 1586. Despite its clumsiness it

<sup>1</sup> Kahn spells the name Histiaëus on p. 81, Histaeius on p. 780, and Histaieus in the index of his book *The Codebreakers*. Verily an example of *ars occulta scribendi* in an otherwise very reliable book!

In Königsberg i. Pr. gabelt sich der Pregel und umfließt eine Insel, die *Kneiphof* heißt. In den dreißiger Jahren des achtzehnten Jahrhunderts wurde das Problem gestellt, ob es wohl möglich wäre, in einem Spaziergang jede der sieben Königsberger Brücken genau einmal zu überschreiten.

Daß ein solcher Spaziergang unmöglich ist, war für L. EULER der Anlaß, mit seiner anno 1735 der Akademie der Wissenschaften in St. Petersburg vorgelegten Abhandlung *Solutio problematis ad geometriam situs pertinentis* (Commentarii Academiae Petropolitanae 8 (1741) 128-140) einen der ersten Beiträge zur Topologie zu liefern.

Das Problem besteht darin, im nachfolgend gezeichneten Graphen einen einfachen Kantenzug zu finden, der alle Kanten enthält. Dabei repräsentiert die Ecke vom Grad 5 den Kneiphof und die beiden Ecken vom Grad 2 die Krämerbrücke sowie die Grüne Brücke.

Fig. 2. Semagram in a 1976 textbook on combinatory logic (the passage deals with the famous Königsberg bridges problem). The lowered letters give the message “*nieder mit dem sowjetimperialismus*” [down with Soviet imperialism]

has lasted well: the most recent uses known to me are A. van Wijngaarden’s alleged usage of roman (.) and italic (.) full stops in the ALGOL 68 report. A second steganographic principle consists of marking selected characters in a book or newspaper; for example, by dots or by dashes. It is much more conspicuous than the above-mentioned method—unless an invisible ink is used—but simpler to implement. A variant (in a book on combinatory logic) uses an almost imperceptible lowering of the letters concerned (Fig. 2).

*Arnold dear, it was good news to hear that  
you have found a job in Paris. Anna hopes  
you will soon be able to send for her. She's  
very eager to join you now the children are  
both well. Sonia*

Fig. 3. Visible concealment of a numeric code by spacing the letters (Smith)

A third principle uses spaces between letters within a word (Fig. 3). In this example, it is not the letter before or after the space that is important, but the number of letters between successive letters ending with an upward stroke, 3 3 5 1 5 1 4 1 2 3 4 3 3 3 5 1 4 5 ... . In 1895, A. Boetzel and Charles O’Keenan demonstrated this steganographic principle, also using a numeric code, to the French authorities (who remained unconvinced of its usefulness, not without reason). It appears to have been known before then in Russian anarchist circles, combined with the “Nihilist cipher” (Sect. 3.3.1). It was also used by German U-boat officers in captivity to report home on the Allies’ antisubmarine tactics.



Fig. 4. Secret message solved by Sherlock Holmes (AM HERE ABE SLANEY), from *The Adventure of the Dancing Men* by Arthur Conan Doyle

All these are examples of semagrams (visibly concealed secret writing). And there are many more. In antiquity Æneas used the *astragal*, in which a cord threaded through holes symbolized letters. A box of dominoes can conceal a message (by the positions of the spots), as can a consignment of pocket watches (by the positions of the hands). Sherlock Holmes' dancing men (Fig. 4) bear a message just as much as hidden Morse code (Fig. 5): “compliments of CP&SA MA to our chief Col. Harold R. Shaw on his visit to San Antonio May 11th 1945” (Shaw had been head of the Technical Operations Division of the US government’s censorship division since 1943).



Fig. 5. Semagram. The message is in Morse code, formed by the short and long stalks of grass to the left of the bridge, along the river bank and on the garden wall

A maze is a good example of a clear picture hidden in a wealth of incidental detail: the tortuous paths of Fig. 6 reduce to a graph which can be taken in at a glance. Autostereograms which require the viewer to stare or to squint in order to see a three-dimensional picture (Fig. 7) are also eminently suitable for concealing images, at least for a while.

Of greater interest are those methods of linguistic steganography that turn a secret message into one that is apparently harmless and easily understood, although wrongly (open code). The principle is closer to that of cryptography. Again, there are two subcategories: masking and veiling.

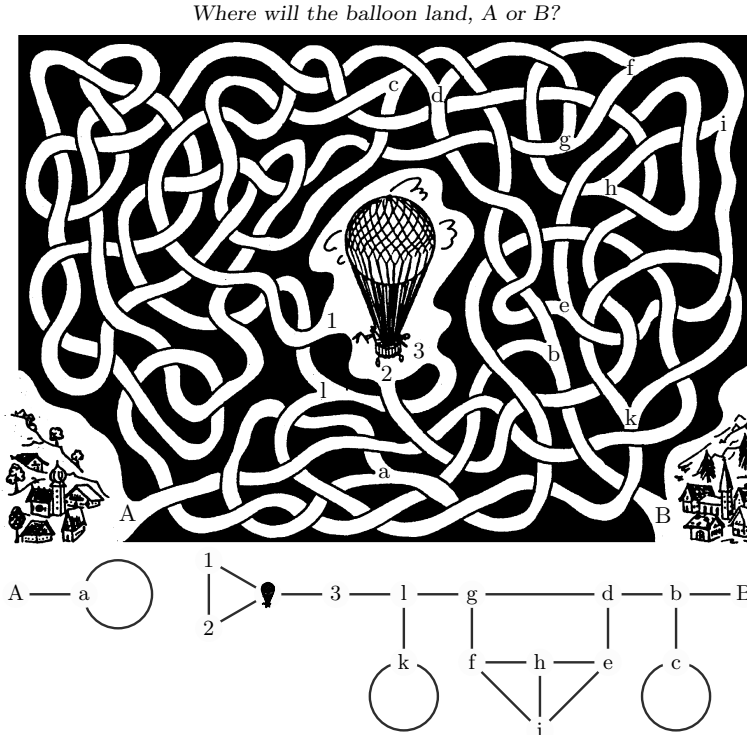


Fig. 6. Maze and its associated graph

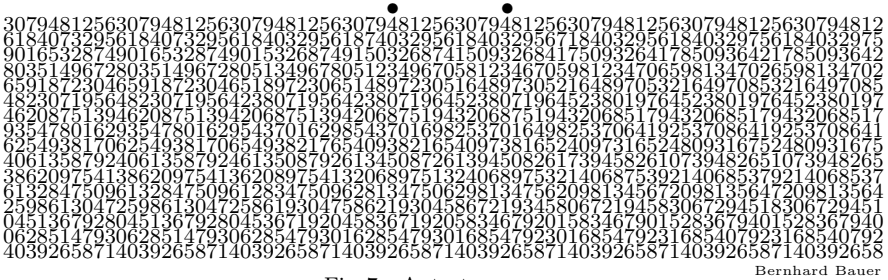


Fig. 7. Autostereogram

### 1.3 Open Code: Masking

A secret writing or message masked as an open communication requires a prior agreement as to the true meaning of seemingly harmless phrases. This is probably the oldest form of secrecy technique—it is to be found in all cultures. Oriental and Far Eastern dealers and gamblers (and some Western ones) are reputed to be masters in the use of gestures and expressions. The following system is said to be common among American card cheats. The manner of

holding a cigarette or scratching one's head indicates the suit or value of the cards held. A hand on the chest with the thumb extended means "I'm going to take this game. Anybody want to partner me?" The right hand, palm down, on the table means "Yes", a clenched fist, "No, I'm working single, and I discovered this guy first, so scram!" The French conjurer Robert Houdin (1805–1871) is said to have used a similar system around 1845, with I, M, S, V standing for *cœur*, *carreau*, *trèfle*, *pique*: *il fait chaud* or *il y a du monde* means "I have hearts", as it starts with /I/. Things were no more subtle in English whist clubs in Victorian days; "Have you seen old Jones in the past fortnight?" would mean hearts, as it starts with /H/. The British team was suspected of exchanging signals at the world bridge championships in Buenos Aires in 1965—nothing could be proved, of course.

Sometimes, a covert message can be transmitted masked in an innocent way by using circumstances known only to the sender and the recipient. This may happen in daily life. A famous example was reported by Katia Mann: In March 1933, she phoned from Arosa in Switzerland her daughter Erika in Munich and said: "*Ich weiß nicht, es muß doch jetzt bei uns gestöbert werden, es ist doch jetzt die Zeit*" [I don't know, it is the time for spring-cleaning]. But Erika replied "*Nein, nein, außerdem ist das Wetter so abscheulich. Bleibt ruhig noch ein bisschen dort, ihr versäumt ja nichts*" [No, no, anyway, the weather is so atrocious. Stay a little while, you are not missing anything here]. After this conversation, it became clear to Katia and Thomas Mann that they could not return to Germany without risk.



Fig. 8. Tramps' secret marks (German *Zinken*), warning of a policeman's house and an aggressive householder (Central Europe, around 1930)

Secret marks have been in use for centuries, from the itinerant scholars of the Middle Ages to the present-day vagrants, tramps, hoboes and loafers. Figure 8 shows a couple of secret marks, such as could still be seen in a provincial town of Central Europe in the 1930s; Fig. 9 shows a few used in the midwestern United States in the first half of the 20th century. Tiny secret marks are also used in engravings for stamps or currency notes as a distinguishing mark for a particular engraver or printer.

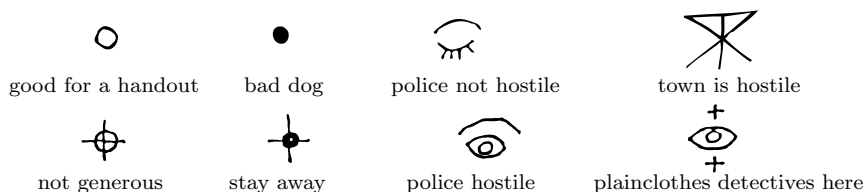


Fig. 9. Hoboes' secret marks for 'police not hostile' and other messages (midwestern United States, first half of 20th century)

Languages specific to an occupation or social class, collectively known as jargon, above all the kinds used by beggars, vagabonds, and other rascals, variously called *argot* (France, USA), *cant* (UK), *thieves' Latin* (UK), *rotwelsch* (Germany), *fourbesque* (Italy), *alemania* (Spain), or *calão* (Portugal), and which serve to shield (and keep intact) a social group, often make use of masking. Masked secret writing is therefore called *jargon code*.

The oldest papal code in the 14th century used *Egyptians* for the Ghibellines, and *Sons of Israel* for the Guelphs. One French code in the 17th century used jargon exclusively: *Jardin* for Rome, *La Roze* for the Pope, *Le Prunier* for Cardinal de Retz, *La Fenestre* for the King's brother, *L'Écurie* (meaning either stable or gentry) for Germany, *Le Roussin* for the Duke of Bavaria, and so on. A simple masking of names was used in a Bonapartist plot in 1831.

The languages of the criminal underworld are of particular steganographic interest. French argot offers many examples, some of which have become normal colloquial usage: *rossignol* (nightingale) for skeleton key, known since 1406; *mouche* (fly) for informer ('nark' in British slang), since 1389. Alliterative repetition is common: *rebecca* for rebellion, *limace* (slug) for *lime* (file), which in turn is *fourbesque* for shirt; *marquise* for *marque* (mole or scar), which in turn is *alemania* for a girl; *frisé* (curly) for Fritz (a popular name for a German). Not quite so harmless are metaphors: *château* for hospital, *mitraille* (bullet) for small change, or the picturesque but pejorative *marmite* (cooking pot) for a pimp's girlfriend, and *sac à charbon* (coal sack) for a priest. Sarcastic metaphors such as *mouthpiece* for a lawyer are not confined to the underworld.

Some jargon is truly international: 'hole'—*trou*—*Loch* for prison; 'snow'—*neige*—*Schnee* or 'sugar'—*sucre* for cocaine; 'hot'—*heiß* for recently stolen goods; 'clean out'—*nettoyer*—*abstauben* for rob; 'rock'—*galette*—*Kohle* for money. All kinds of puns and plays on words find their place here. The British 'Twenty Committee' in the Second World War, which specialized in double agents, took its name from the Roman number XX for 'double cross'.

Well-masked secret codes for more or less *universal* use are hard to devise and even harder to use properly—the practised censor quickly spots the stilted language. The abbot Johannes Trithemius (1462–1516), in his *Polygraphiae Libri*, six books printed in 1508–1518 (Fig. 10), presented a collection of Latin words as codes for individual letters (Fig. 11), the *Ave Maria* cipher. "Head", for example, could be masked as "ARBITER MAGNUS DEUS PIISSIMUS". In fact, there were 384 such alphabets in the first book, to be used successively—a remarkable case of an early polyalphabetic encryption (Sect.2.3.3).

It could be that present-day censors are not sufficiently well versed in Latin to cope with that. A favorite trick in censorship is to reformulate a message, preserving the semantics. In the First World War a censor altered a despatch from "Father is dead" to "Father is deceased". Back came the message "Is father dead or deceased?"

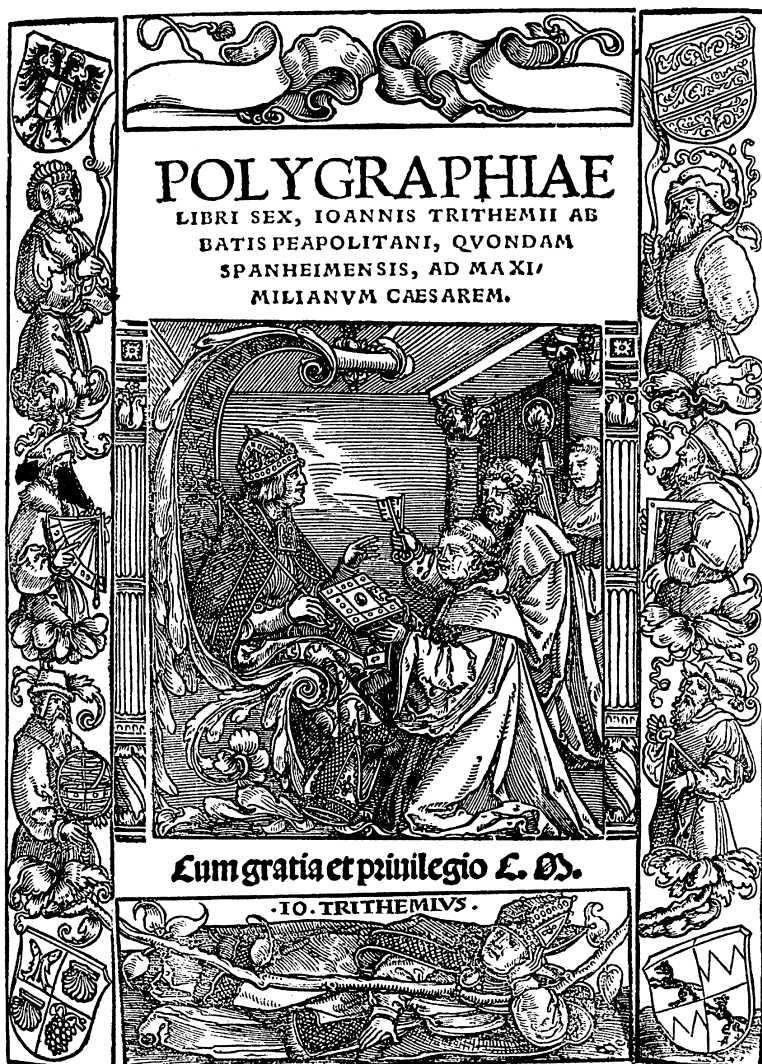


Fig. 10. Title page (woodcut) of the first printed book on cryptography (1508)

Allegorical language is of little help here. In Louis XV's diplomatic service, Chevalier Douglas was sent on a secret mission to Russia in 1755 with an allegorical arsenal from the fur trade, with *le renard noir était cher* for "the influence of the English party is increasing", *le loup-cervier avait son prix* for "the Austrian party (under Bestuchev) retains its dominant influence". Bestuchev himself, who was friendly to Prussia, was *le loup-cervier*, while *une peau de petit-gris* meant 3000 mercenaries in the pay of the British.

It is to be hoped that the chevalier was more subtle in the use of his allegorical code than the German spies, in the guise of Dutch merchants, who—as told by



A Deus	A clemens
B Creator	B clementissimus
C Conditor	C pius
D Opifex	D pijssimus
E Dominus	E magnus
F Dominator	F excelsus
G Confolator	G maximus
H Arbiter	H optimus

Fig. 11.  
The first entries of  
Trithemius' *Ave Maria* cipher

Major-General Kirke—ordered cigars in batches of thousands from Plymouth one day, Portsmouth the next; then Gravesend and so on—1000 coronas stood for one battleship. Their inadequate system brought their lives to a premature end on July 30, 1915. Luck was on the side of Velvalee Dickinson, a Japanophile woman in New York City, who kept up a lively correspondence on broken dolls in 1944. Things came to light when a letter to an address in Portland, Oregon was returned, and the sender's name turned out to be false. The lady really did sell exquisite dolls from a shop in Madison Avenue. Technical Operations Division, the agency for detecting especially hard to find hidden messages, and the FBI managed to produce evidence for the prosecution, but she got away with ten years in prison and a \$10 000 fine. In the Audrey Hepburn movie of 1961 *Breakfast at Tiffany's*, Miss Holly Golightly spent a night behind bars because she helped a gangster conduct his cocaine dealership from his prison cell by means of "weather reports"—it did occur to her, she admitted, that "snow in New Orleans" sounded somewhat improbable.

## 1.4 Cues

The most important special case of masking, i.e., of a jargon-code message, concerns the use of a *cue* (French *mot convenu*), a prearranged phrase or verse to mean a particular message. The importance of the message is linked to the time of transmission; the message serves as an alarm or acknowledgement. Large numbers of messages were broadcast by the BBC to the French *Résistance* during the Second World War. It therefore attracted little attention when some masked messages with an importance several orders of magnitude greater than the others were broadcast—for example, on June 1, 1944 when the 9 o'clock news was followed by a string of "personal messages", including the first half of the first verse of the poem *Chanson d'Automne* by Paul Verlaine (translated: "The long sobs of the violins of autumn"); the second half (translated: "Wound my heart with a monotonous languor") followed on June 5th. The German command structure had already in January 1944 been informed by Admiral Canaris' *Abwehr* of the jargon code and its significance. When the 15th Army picked up the expected cue (Fig. 12), German command posts were warned, but for reasons that have not been fully

Tag	Darstellung der Ereignisse
Uhrzeit	(Dabei wichtig: Beurteilung der Lage (Feind- und eigene), Eingangs- und Abgangszeiten von Meldungen und Befehlen)
Ort und Art der Unterkunft	
5.6.44	Am 1., 2. und 3.6.44 ist durch die Nast innerhalb der "Messages personnels" der französischen Sendungen des britischen Rundfunks folgende Meldung abgehört worden : "Les sanglots longs des violons de l'automne". Nach vorhandenen Unterlagen soll dieser Spruch am 1. oder 15. eines Monats durchgegeben werden, nur die erste Hälfte eines ganzen Spruches darstellen und ankündigen, dass binnen 48 Stunden nach Durchgabe der zweiten Hälfte des Spruches, gerechnet von 00.00 Uhr des auf die Durchgabe folgenden Tages ab, die anglo-amerikanische Invasion beginnt.
21.15 Uhr	Zweite Hälfte des Spruches "Blessent mon coeur d'une longueur monotone" wird durch Nast abgehört.
21.20 Uhr	Spruch an Ic-AO durchgegeben. Danach mit Invasionsbeginn ab 6.6. 00.00 Uhr innerhalb 48 Stunden zu rechnen. Überprüfung der Meldung durch Rückfrage beim Militärbefehlshaber Belgien/Nordfrankreich in Brüssel. (Major von Wangenheim).
22.00 Uhr	Meldung an O.B. und Chef des Generalstabes.
22.15 Uhr	Weitergabe gemäß Fernschreiben (Anlage 1) an Generalkommandos. Mündliche Weitergabe an 16. Flak-Division.

Fig. 12. Extract from a log kept by the 15th Army's radio reconnaissance section (Lt. Col. Helmuth Meyer, Sgt. Walter Reichling). Here, *automne* is to be read *automne*, *longeur* is to be read *longueur*

explained to this day the alarm did not reach the 7th Army, on whose part of the coast the invasion took place within 48 hours, on June 6, 1944.

The Japanese used a similar system in 1941. For example, HIGASHI NO KAZE AME (east wind, rain), inserted into the weather report in the overseas news and repeated twice, was used to announce "war with the USA". The US Navy intercepted a diplomatic radio message to that effect on November 19, 1941 and succeeded in solving it by the 28th. As tension mounted, numerous reconnaissance stations in the USA were monitoring Japanese radio traffic for the cue. It came on December 7th—hours after the attack on Pearl Harbor—in the form NISHI NO KAZE HARE (west wind, clear), indicating the commencement of hostilities with Britain, which came as very little surprise by then. Perhaps the whole thing was a Japanese double cross.

Technically, masked secret writing shows a certain kinship with enciphered secret writing (Sect. 2.2), particularly with the use of substitutions (Chap. 3) and codes (Sect. 4.4).

In a different category are secret writings or messages veiled as open ones (invisibly concealed secret writing). Here, the message to be transmitted is

somehow embedded in the open, harmless-looking message by adding nulls. In order to be able to reconstruct the real message, the place where it is concealed must be arranged beforehand (*concealment cipher*). There are two obvious possibilities for using *garbage-in-between* (Salomaa): by specifying rules (*null cipher*, *open-letter cipher*) or by using a *grille* (French for ‘grating’).

## 1.5 Open Code: Veiling by Nulls

Rules for veiled messages are very often of the type “the  $n$ th character after a particular character”, e.g., the next letter after a space (“family code”, popular among soldiers in the Second World War, to the great displeasure of the censors); better would be the third letter after a space, or the third letter after a punctuation mark. Such secret messages are called *acrostics*. A practised censor usually recognizes immediately from the stilted language that something is amiss, and his sharp eye will certainly detect what

PRESIDENT’S EMBARGO RULING SHOULD HAVE IMMEDIATE  
NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW.  
STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW  
JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY

means—a message intercepted in the First World War.

If necessary, it can help to write out the words one below the other:

↓  
I N S P E C T  
D E T A I L S  
F O R  
T R I G L E T H  
A C K N O W L E D G E  
T H E  
B O N D S  
F R O M  
F E W E L L

The disguise falls away; the plain text “jumps out of the page”.

Sir John Trevanion, who fought on the Royalist side against Oliver Cromwell (1599–1658) in the English Civil War, saved himself from execution by using his imagination. In a letter from his friend R. T. he discovered the message “panel at east end of chapel slides”—and found his way out of captivity (Fig. 13).

There is a story of a soldier in the US Army who arranged with his parents that he would tell them the name of the place he had been posted to by means of the initial letter of the first word (after the greeting) in consecutive letters home—from a cryptographic and steganographic point of view not such a bad idea. However, his cover was blown when his parents wrote back “Where is Nutsi? We can’t find it in our atlas.” The poor fellow had forgotten to date his letters.

Worthie Sir John: — Hoſe, thăt is ye beſte comfort of ye afflicted, cañnot much, I fear me, help you now. Thăt I would ſaye to you, is thīs only: if ęver I may be able to requite that I do owe you, ſtānd not upon asking me. 'Tiſ not much that I can do: buť what I can do, beę ye verie ſure I wille. I kñowe that, if đethe comes, if őrdinary men fear it, it frights not you, acćounting it for a high honour, to ĥave ſuch a rewarde of your loyalty. Prāy yet that you may be ſpared this ſoe bitter, cuř. I fear not that you will grudge any ſufferings; only if bie ſubmiſſion you can turn them away, 'tiſ the part of a wiſe man. Tell me, an if you can, to đo for you anythinge that you wolde have done. Thě general goes back on Wednesday. Reſtinge your ſervant to command. — R. T.

Fig. 13. Message to Sir John Trevanion: *panel at east end of chapel slides* (third letter after punctuation mark)

Acrostics have also been used to conceal slogans. The nationalistic Austrian mathematician Roland Weitzenböck, in the preface to his book *Invariantentheorie* (Groningen 1928), wrote “*nieder mit den Franzosen*” as an acrostic. The technique of acrostics even found its way into belletristic literature. In the classical acrostic, it was the initial letters, syllables, or words of successive lines, verses, sections, or chapters which counted. Words or sentences (Fig. 14) were enciphered in this way, also author’s names, and even the addressee of invectives: ‘The worst airline’, ‘Such a bloody experience never again’. Acrostics also served as an insurance against omissions and insertions: an early example of the present-day parity checks or error-detecting codes.

In a similar way, the chronogram conceals a (Roman) numeral in an inscription; usually it is a date; for example, the year when the plaque was erected: In the baroque church of the former Cistercian monastery Fürstenfeld near Munich, in 1766 a statue of the Wittelsbachian founder *Ludwig der Strenge* (1229–1294) was placed, below which there is a tablet with the chronogram

LVDoVICVs seVerVs DVX baVarVs aC paLatInVs,  
hIC In ſanCta paCe qViesCIť.

(*Ludwig the Severe, Duke of Bavaria and Count Palatine, rests here in holy peace.*)

If the chronogram consists of a verse, then the technical term is a *chronostichon*—or *chronodistichon* for a couplet.

Composers have concealed messages in their compositions, either in the notes of a musical theme (a famous example<sup>2</sup> is B A C H), or indirectly by means of a numerical alphabet: if the *i*-th note of the scale occurs *k* times, then the *k*-th letter of the alphabet is to be entered in the *i*-th position. Johann Sebastian Bach was fond of this cipher; in the theme of the organ chorale ‘*Vor deinen Thron*’, written in 1750 in the key of G major, g occurs twice (B), a once (A), b three times (C), and c eight times (H).

Nulls are also used in many jargons: simply appending a syllable (parasitic suffixing) is the simplest and oldest system. In French, for example,

<sup>2</sup> In German, b is used for b flat, h for b. In G major, g is first, a second, h third, etc.

*floutiere* for *flou*, *argot* for ‘go away!’, *giorolle* for *gis*, *argot* for ‘yes’; *mezis* for *me*; *icicaille* for *ici*

and there are hundreds of similar forms. Cartouche (18th century) has  
 vousierge trouvaille bonorgue ce gigotmouche  
 where the nulls are underlined.

### Fast writing method

He must have had a special trick, said Robert K. Merton, for he wrote such an amazing quantity of material that his friends were simply astonished at his prodigious output of long manuscripts, the contents of which were remarkable and fascinating, from the first simple lines, over fluently written pages where word after word flowed relentlessly onward, where ideas tumbled in a riot of colorful and creative imagery, to ends that stopped abruptly, each script more curiously charming than its predecessors, each line more whimsically apposite, yet unexpected, than the lines on which it built, ever onward, striving toward a resolution in a wonderland of playful verbosity. Fuller could write page after page so fluently as to excite the envy of any writers less gifted and creative than he. At last, one day, he revealed his secret, then died a few days later. He collected a group of acolytes and filled their glasses, then wrote some words on a sheet of paper, in flowing script. He invited his friends to puzzle a while over the words and departed. One companion took a pen and told the rest to watch. Fuller returned to find the page filled with words of no less charm than those that graced his own writings. Thus the secret was revealed, and Fuller got drunk. He died, yet still a space remains in the library for his collected works.

Ludger Fischer / J. Andrew Ross

Fig. 14. Self-describing acrostic

Tut Latin, a language of schoolchildren, inserts TUT between all the syllables. Such school jargons seem to be very old; as early as 1670 there are reports from Metz (Lorraine) of a ‘stuttering’ system, where, for example, *undrequ* *foudrequ* stood for *un fou*.

The Javanais language is also in this class:

*jave* for *je*; *laveblavanc* for *le blanc*; *navon* for *non*;  
*chavaussavurave* for *chaussure*.

Other systems use dummy syllables with duplicated vowels, such as B talk in German:

GABARTEBENLAUBAUBEBE for *gartenlaube* (bower)

or Cadogan in French:

CADGADODGOGADGAN for *cadogan*.

Joachim Ringelnatz (1883–1934) wrote a poem in *Bi* language (Fig. 15).

**Gedicht in Bi-Sprache**

**Ibich habibebi dibich,  
 Lobittebi, sobi liebib.  
 Habist aubich dubi mibich  
 Liebib: Neibin, vebirgibib.**

**Nabih obidebir febirn,  
 Gobitt seibi dibir gubit.  
 Meibin Hebirz habit gebirn  
 Abin dibir gebirubiht.**

Fig. 15.  
 Poem in the *Bi* language  
 by Joachim Ringelnatz

Simple reversing of the letters, called back slang, occurs in cant: OCCABOT for ‘tobacco’, KOOL for ‘look’, YOB for ‘boy’, SLOP for ‘police’. Permutation of the syllables is found in the French *Verlan* (from *l’envers*): NIBERQUE for *berniq*ue (“nothing doing”, said to be related to *bernic*les, tiny shells); LONTOU for *Toulon*, LIBRECA for *calibre* (in the sense of a firearm); DREAUPER for *perdreau* (partridge, to mean a policeman); RIPOU for *pourri* (rotten); BEUR for *rebeu* (Arab). More recent are FÉCA for *café*, TÉCI for *cit*é.

More complicated systems involve shuffling the letters, i.e., a transposition (Sect. 6.1). Criminal circles were the origin of the Largonji language:

*leudé* for *deux* [francs]; *linvé* for *vingt* [sous]; *laranqué* for *quarante* [sous]; with the phonetic variants

*linspré* for *prince* (Vidocq, 1837); *lorcefée* for *La Force*, a Paris prison;

and of the Largonjem language:

*lonbem* for *bon* (1821); *loucherbem* for *boucher*; *olrapem* for *opéra* (1883).

The name Largonji is itself formed in this way from ‘jargon’.

A variant with suppression of the initial consonant is the Largondu language: *lavedu* for *cave*; *loquedu* for *toque*; *ligodu* for *gigo(t)*.

Similar formation rules lie behind the following:

*locromuche* for *maquerau* (pimp); *leaubiche* for *beau*;

*nebdutac* for *tabac* (1866); *licelargu* for *cigare* (1915).

These systems also have parallels in East Asia (Hanoi, Haiphong). Pig Latin, another school language, puts AY at the end of a cyclically permuted word: third becomes IRDTHAY. Cockneys have a rhyming slang with nulls: TWIST AND TWIRL for *girl*, JAR OF JAM for *tram*, BOWL OF CHALK for *talk*, FLEAS AND ANTS for *pants*, APPLES AND PEARS for *stairs*, BULL AND COW for *row*, CAIN AND ABEL for *table*, FRANCE AND SPAIN for *rain*, TROUBLE AND STRIFE for *wife*, PLATES OF MEAT for *feet*, LOAF OF BREAD for *head*. The actual rhyming word is usually omitted—the initiated can supply it from memory. Some of these expressions have entered the language (lexicalization): few people are aware of the origin of “use your loaf” or “mind your plates”.

Jonathan Swift (1667–1745) was not overcautious in his *Journal to Stella*, who in fact was Esther Johnson (1681–1728): in a letter on Feb. 24, 1711 he merely inserted a null as every second character.

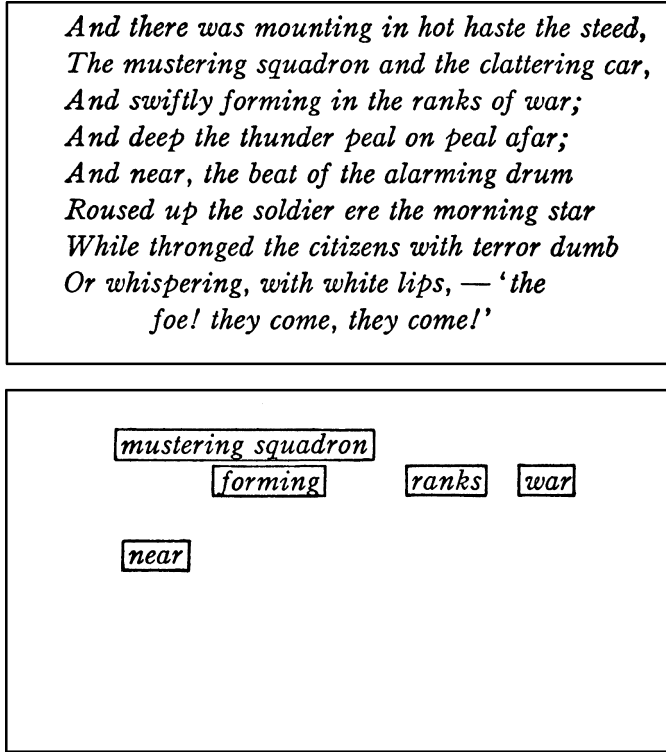


Fig. 16. Lord Byron's hypothetical message

## 1.6 Open Code: Veiling by Grilles

The method of the grille, which goes back to Geronimo Cardano (in *De Subtilitate*, 1550, is simple to understand, but suffers from the disadvantage that both sides must possess and retain the grille—in the case of a soldier in the field or a prisoner, not something that can be taken for granted. It is also awfully hard to compose a letter using it. If Lord Byron (1788–1824)—admittedly no ordinary soldier—had used the method, his talents would have come in extremely handy for composing a poem such as that in Fig. 16. He would presumably also have been able to lay it out so attractively that the plain text fitted the windows of the grille without calling attention.

Cardano, incidentally, insisted on copying out the message three times, to remove any irregularities in the size or spacing of the letters. The method was occasionally used in diplomatic correspondence in the 16th and 17th centuries. Cardinal Richelieu is said to have made use of it. The modern literature also mentions some more cunning rules; for example, to convey binary numbers (in turn presumably used to encipher a message), in which a word with an even number of vowels represents the digit 0, or an odd number the digit 1.

Veiled secret writing is a concealment cipher. In professional use, it is usually considered as enciphered secret writing (Sect. 2.2), it shows a certain kinship particularly in the use of nulls (Sect. 2.3.1) and of transposition (Sect. 6.1.4).

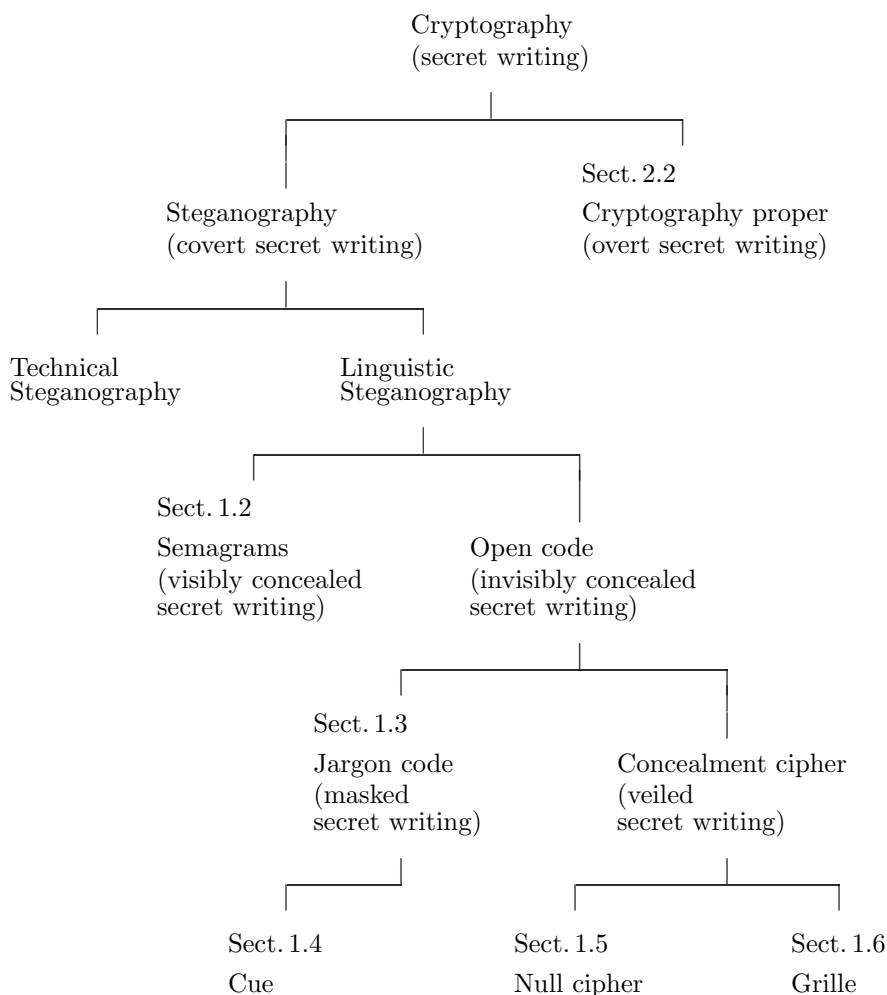


Fig. 17. Classification of steganographic and cryptographic methods

## 1.7 Classification of Cryptographic Methods

Figure 17 shows a diagrammatic summary of the classification of methods of steganography and cryptography proper as given in this and the next chapter. Masking and veiling have been treated in detail here because they provide a methodical guide: masking leads to substitution, veiling leads to transpo-



sition. These are the two basic elements of cryptography proper. We shall introduce them in the next chapter.

Steganography also reveals an important maxim: natural language—spoken, written, or in gestures—has its own particular rules, and it is even harder to imitate them (as in steganography) than to suppress them (as in cryptography).

Linguistic steganography is therefore treated with caution by pure cryptographers; it is a censor's job to combat it. By its very nature, an amateur steganogram can be rendered harmless by suppressing or revealing it. For the censorship, the actual solution is often of little importance (except, perhaps, to provide evidence for a subsequent court case).

The professional use of linguistic steganography can be justified only in special cases—unless it represents a concealment of a cryptographic method.

Steganography and cryptography proper fall under the concept of cryptology. The term *cryptologia* was used, like *cryptographia*, by John Wilkins in 1641, to mean *secrecy in speech*. In 1645, 'cryptology' was coined by James Howell, who wrote "cryptology, or epistolizing in a clandestine way, is very ancient". The use of the words *cryptography*, *cryptographie*, *crittografia*, and *Kryptographie* has until recently dominated the field, even when cryptanalysis was included.



Claude Shannon (1916–2001)

Claude Shannon, in 1945, still called his confidential report on safety against unauthorized decryption *A Mathematical Theory of Cryptography*. Within book titles, the French *cryptologue* was used by Yves Gylden (1895–1963) in 1932 and in more modern times *cryptologist* by William F. Friedman (1891–1969) in 1961. The term *cryptology* showed up in the title of an article by David Kahn in 1963; it was used internally by Friedman and Lambros D. Callimahos (1911–1977) in the 1950s. With Kahn's *The Codebreakers* of 1967, the word 'cryptology' was firmly established to involve both cryptography and cryptanalysis, and this is widely accepted now.

With the widespread availability of sufficiently fast computer-aided image manipulation, steganography nowadays sees a revival. By subtle algorithms, messages can be hidden within pictures.

**Decrypted Secrets**

**Methods and Maxims of Cryptology**

Bauer, F.L.

2007, XIV, 525 p. 183 illus., 16 illus. in color., Hardcover

ISBN: 978-3-540-24502-5