

Ciphertext number one

THYFX BLLUV MZJVA ZDHZV UAYPH SMVYA YLHZV
UZOLO HKILL UHJJB ZLKVM WSVAA PUNAV HZZHZ
ZPUHA LXBLL ULSPG HILAO PUVYK LYAVA HRLAO
LLUNS PZOJY VDUMV YOLYZ LSMZP YMYHU JPZDH
SZPUN OHTLS PGHIL AOZWY PUJPW HSZLJ YLAHY
FOHKH SYLHK FHYYL ZALKA OLVAO LYJVU ZWPYH
AVYZL EAYHJ ALKJV UMLZZ PVUZH UKLEL JBALK
AOLTU VDOLW SHUUL KAVWY VCLAO HATHY FDHZH
AAOLO LHYAV MAOLW SVAHU KDHZA OLYLM VYLLX
BHSSF JBSWH ISLHU KLXBH SSFKL ZLYCP UNVMK
LHAO

Suetonius, the gossip columnist of ancient Rome, says that [Julius] Caesar [100? – 44 B.C.] wrote to Cicero and other friends in a cipher in which the plaintext letters were replaced by letters standing three place further down the alphabet ...

David Kahn, *The Codebreakers*

Kerckhoffs' principles

Classical cryptology was “ruled” by Auguste Kerckhoffs’ (1835 – 1903) principles, which were stated in 1883. Kerckhoffs enumerated six principles for field ciphers.

Desiderata for military cryptography

It is necessary to distinguish between a system of enciphered writing designed for a temporary exchange of letters among several isolated persons, and a method of cryptography intended to control for an unlimited time the communications of different military leaders. The latter, indeed, may not change their conventions at will or at any given moment. Further, they should never keep on their persons any object or note that would be such as to shed light for the enemy on the meaning of any secret messages that might fall into his hands.

A large number of ingenious arrangements achieve the result desired in the first case. For the second a system must satisfy certain exceptional conditions which I will summarize under the following six headings:

1. The system must be practically, if not mathematically, indecipherable.

2. It must not rely upon secrecy, and it must be able to fall into the enemy's hands without disadvantage.
3. The key should be able to be communicated and stored without the help of written notes, and to be changed or modified at the will of the correspondents.
4. It must be usable for telegraphic communications.
5. It must be portable, and its handling and operation must not require the assistance of many people.
6. Finally, it is necessary, in light of the circumstances in which it must be used, that the system be easy to use, not requiring extreme mental effort nor the knowledge of a large number of rules that must be followed.

These principles appear in Kerckhoffs' 64-page *La Cryptographie militaire* (1883).

Only a few books in the history of science may be called great. Some of these report a technical innovation that radically alters the content of the science. Through the 19th century, Alberti's and Kasiski's were the two books of this kind in cryptology. Such books look inward.

Other great books look outward. They bring the science up to date – make it consonant with its time – and so renew its utility to men. They do this by assimilating developments in relevant fields ... , by summing up the lessons of recent experience and deducing their meaning for the current age, and by reorganizing the concepts of the science according to this new knowledge. This does not mean simple popularization, though such a work usually does have an

organic persuasiveness. Rather, it amounts to a reorientation, a new perspective.

For 300 years, the only great book of this kind in cryptology was Porta's. He was the first to delineate a coherent image of cryptology. His ideas remained viable so long because cryptology underwent no essential change; communication was by messenger, and consequently the nomenclator reigned. But his views no longer sufficed after the invention of the telegraph. New conditions demanded new theses, new insights. And in 1883 cryptology got them in the form of its second great book of the outward-looking kind, *La Cryptographie militaire*.

[Kerckhoffs' principles] still compromise the ideal which military ciphers aim at. ...

There appears to be a certain incompatibility among [the principles] that makes it impossible to institute all of them at once. The requirement that is usually sacrificed is the first. Kerckhoffs argues strongly against the notion of a field cipher that would simply resist solution long enough for the orders to be carried out. This is not enough, he said, declaring that "the secret matter in communications sent over a distance very often retains its importance beyond the day on which it was transmitted."

Perhaps the most startling requirement, at first glance, was the second. Kerckhoffs explained that by "system" he meant "the material part of the system; tableaux, code books, or whatever mechanical apparatus may be necessary," and not "the key proper." Kerckhoffs here makes for the first time the distinction, now basic to cryptology, between the general system and the specific key.

... Kerckhoffs second requirement has become widely accepted under a form that is sometimes called the fundamental assumption of military cryptography: that the enemy knows the general system. But he must still be unable to solve messages in it without knowing the secret key. *The Codebreakers* by David Kahn

The second requirement is often called Kerckhoff's law. This requirement means that a cryptosystem should be secure even if an enemy knows everything about the system except the key; it argues against "security through obscurity" – that the security of a cryptosystem would depend on keeping the method of encryption secret. The same idea was stated (in the 1940s) by Claude Shannon (1916 – 2001), the founder of information theory, as "the enemy knows the system." The latter is called Shannon's maxim.

Frequency analysis

*Cryptanalysis rests upon the fact that the letters of language have "personalities" of their own. ... Though in a cryptogram they wear disguises, the cryptanalyst observes their actions and idiosyncrasies, and infers their identity from these traits. In ordinary monoalphabetic substitutions, [the cryptanalyst's] task is fairly simple because each letter's camouflage differs from every other letter's and the camouflage remains the same throughout the cryptogram. David Kahn, *The Codebreakers*.*

Frequency analysis is the basic tool of the cryptanalyst. It can be used to identify the type of cipher, and it can be used to identify plaintext/ciphertext correspondences.

Here are the plaintext frequencies:

| | |
|---|----------------|
| a | 1111111 |
| b | 1 |
| c | 111 |
| d | 1111 |
| e | 11111111111111 |
| f | 111 |
| g | 11 |
| h | 1111 |
| I | 1111111 |
| j | |
| k | |
| l | 1111 |
| m | 111 |
| n | 11111111 |
| o | 1111111 |
| p | 111 |
| q | |
| r | 11111111 |
| s | 111111 |
| t | 1111111111 |
| u | 111 |
| v | 1 |
| w | 11 |
| x | |
| y | 11 |
| z | |

Abraham Sinkov (who was one of William Friedman's cryptanalysts during World War II) in his text *Elementary Cryptanalysis: A Mathematical Approach* points out the following patterns which are useful for elementary cryptanalysis:

1. a, e, and I are all high frequency letters (at the beginning of the plaintext alphabet), and they are equally spaced (four letters apart) with e the most frequent.
2. n and o form a high frequency pair (near the middle of the plaintext alphabet).
3. r, s, and t form a high frequency triple (about 2/3 of the way through the plaintext alphabet).
4. j and k form a low frequency pair (just before the middle of the plaintext alphabet).
5. u, v, w, x, y, and z form a low frequency six-letter string (at the end of the plaintext alphabet).

Because a Caesar cipher just translates the letters of the plaintext alphabet to the right, it translates to the right the frequency patterns we expect with plaintext.

Ibn ad-Durhim [1312 – 1361] has said: When you want to solve a message which you received in code, begin first of all by counting the letters, and then count how many times each symbol is repeated and set down the totals individually. ... Quote is from *The Codebreakers* by David Kahn.

Cryptographic Devices

Over the years, cryptographers have created disk or slide devices to show the plaintext/ciphertext correspondence for use when encrypting and decrypting.

The Italian cryptologist Leon Battista Alberti (1404 – 1472), who is called the Father of Western Cryptology, developed a cipher disk.

*“I make two circles out of copper plates. One, the larger, is called stationary, the smaller is called movable. ... I divide the circumference of each circle into ... equal parts. These parts are called cells. In the various cells of the larger circle I write the capital letters, one at a time ..., in the usual order of the letters.” ... In each of the ... cells of the movable circle [Alberti] inscribed “a small letter ... [Alberti used a random ordering of the letters in the cells of the smaller circle] After completing these arrangements we place the smaller circle upon the larger so that a needle driven through the centers of both may serve as the axis of both and the movable plate may be revolved about it.” Leon Battista Alberti quoted in David Kahn’s *The Codebreakers*.*

CIPHER DISK

The disk that is shown has the letters in the cells of the smaller circle in the usual order. Sender and receiver must agree which circle corresponds to plaintext and which circle corresponds to ciphertext. The disk that is pictured has plaintext on the smaller circle and ciphertext on the larger circle. The disk has been set to Caesar’s original cipher – a shift of 3.

The Dutch cryptologist Auguste Kerckhoffs (1835 – 1903) named the cryptographic slide. In 1883, Kerckhoffs published *La Cryptographie militaire*, which became a major cryptological work.

[Kerckhoffs] called the slide the St.-Cyr system, after the French national military academy where it was taught. A St.-Cyr slide consists of a long piece of paper or cardboard,

called the stator, with an evenly spaced alphabet printed on it and with two slits cut below and to the sides of the alphabet. Through these slits runs a long strip of paper – the slide paper – on which the alphabet is printed twice. David Kahn, The Codebreakers.

MODERN ST.-CYR SLIDE

A modern St.-Cyr slide is shown. Plaintext is on the slide, and ciphertext is on the stator. The slide has been set to Caesar's original cipher – a shift of 3.

[Kerckhoffs] pointed out that a cipher disk was merely a St.-Cyr slide turned round to bite its tail. David Kahn, The Codebreakers.

The name of the slide refers to the French national military academy. The academy was founded in 1802 by Napoleon and moved to Saint-Cyr-L'École in 1806. The school remained there until the defeat of the French in 1940 when it moved to the free zone. After Germany occupied the free zone, the school disbanded. It reformed after the war.

Attacks on Caesar Cipher

Ciphertext attack

Frequency

Brute force: try all possible keys

Known plaintext attack

Search for an encrypted version of the

The name is a bit deceiving because sometimes we only “suspect” rather than “know” a piece of the plaintext message. Consider that in a message of reasonable length we should expect to find the word `the`. If it occurs in a message encrypted with a Caesar cipher, it was encrypted one of the following ways:

| Trigraph | Shift |
|----------|-------|
| THE | 0 |
| UIF | 1 |
| VJG | 2 |
| WKH | 3 |
| XLI | 4 |
| YMJ | 5 |
| ZNK | 6 |
| AOL | 7 |
| BPM | 8 |
| CQN | 9 |
| DRO | 10 |
| ESP | 11 |
| FTQ | 12 |
| GUR | 13 |
| HVS | 14 |
| IWT | 15 |
| JXU | 16 |
| KYV | 17 |
| LZW | 18 |
| MAX | 19 |
| NBY | 20 |
| OCZ | 21 |
| PDA | 22 |
| QEB | 23 |
| RFC | 24 |
| SGD | 25 |

Ciphertext number two

IDPEE GTRXP ITIWT UPRII WP IIW TRGNE IDVGP
EWTGH SXSCD IZCDL IWTE D HXIXD CDUIW TRDGT
HDUIW TLWTT TAHYJ HIQTR PJHTI WTNZC TLIWT
XCXIX PAEDH XIXDC DCTDC ANWPH IDXBP VTIWT
HXIJP IXDCX UIWTG XCVHD CIWTL WTTAH LTGTI
DQTWT ASHIX AA

Ciphertext number three

FTQFM EWOAZ RDAZF UZSPU XXIKZ WZAJM ZPMXM
ZFGDU ZSFTQ BDUYM DKNDU FUETO DKBFM ZMXKE
FEIME FAPQF QDYUZ QFTQB MDFUO GXMDE QFFUZ
SEARF TQQZS UYMYM OTUZQ GEQPF AQZOU BTQDM
BMDFU OGXMD YQEEM SQ

Chapters VIII and IX of Gaines
Chapter 1 of Singh

Exercises

1.

| | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|---|
| KVKXD | EBSXQ | CCYMS | KVYBS | QSXCV | KITEC | DYXDR | |
| OLYBN | OBVSX | OLODG | OOXDR | OVKXN | ONQOX | DBIKX | |
| NDROM | YWWOB | MSKVM | VKCCO | CKCWO | BMRKX | DCCYV | |
| NSOBC | KXNMV | OBQIW | OXRSC | KXMOC | DYBCR | KNLOO | |
| XQOXD | VOWOX | LEDXY | DYPDR | OCODD | VONUS | XNWKX | |
| IRKNW | KNODR | OSBGK | IDRBY | EQRDR | OOHZK | XCSYX | |
| YPLBS | DSCRS | XDOBO | CDCDR | BYEQR | YEDDR | OGYBV | N |

2.

| | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|--|
| MHILY | LZAZB | HLXBZ | XBLMV | YABUH | LHWWP | BZJSH | |
| BKPBZ | JHLJB | ZKPJA | BTHYJ | HUBTL | ZAULB | AYVU | |

3.

| | | | | | | | |
|-------|-------|-------|-------|-------|-------|-------|--|
| VINAI | WOMOR | IAXLE | XMJLI | AEWXS | FVIEO | XLIGS | |
| HILIA | SYPHJ | MVWXL | EZIXS | GSRWX | VYGXE | VITPM | |
| GEIRM | KQEQE | GLMRI | XSHSX | LMWLI | ASVOI | HSYXE | |
| JSVQY | PEALM | GLLIL | TSIHA | SYPHI | REFPI | LMQXS | |
| HMWGS | ZIVXL | IAMVM | RKMRW | MHIXL | IALII | PXLEX | |
| AEWTP | EGIHS | RXLIV | MKLX | | | | |