Cryptography is the science of how to keep a message private

Cryptology is a branch of mathematics that studies the mathematical foundations of cryptographic methods.

Cryptography periods:

1. The first period (from about the 3rd millennium BC) is characterized by the dominance of mono-alphabetic ciphers (the basic principle is the replacement of the alphabet of the source text with another alphabet through the replacement of letters with other letters or symbols)

CEPHAR CAESAR
(shift code, Caesar's shift)

An example of a Caesar cipher (encryption using the key K = 3):

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

We encrypt the word “FAMILI”
We get: IDPLOL (shift by 3)

An example of encryption using the key K = 3 in the Russian alphabet.

Source Alphabet:

А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Encrypted:

Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Original text:

To succeed, students need to catch up with those in front and not wait for those who is behind.

Ciphertext is obtained by replacing each letter
the original text with the corresponding letter of the encrypted alphabet:

Tskzrlngp yhsdyu tuzstsfzha rgzhs zhsyosrhja hzsh nkhs etzuzzhl l rz yzhghya hzsh nhs tskggl

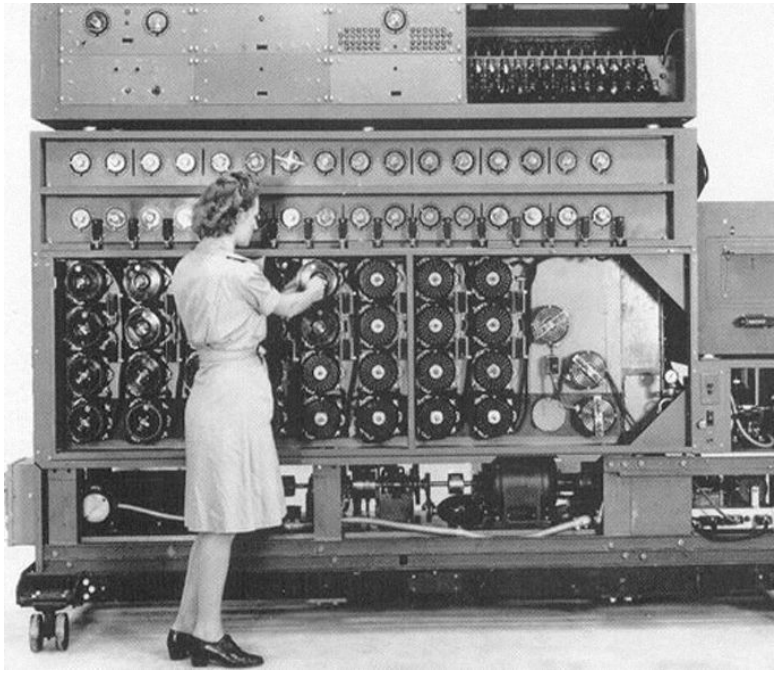
2. The second period (chronological framework - from the 9th century in the Middle East (Al-Kindi) and from the 15th century in Europe (Leon Battista Alberti) - until the beginning of the 20th century) was marked by the introduction of polyalphabetic ciphers

For example, in the process of encryption, the Vigenère table is used, which is structured as follows: the entire alphabet is written in the first line, in each next one a cyclic shift is made by one letter. This results in a square table, the number of rows of which is equal to the number of letters of the alphabet.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

3. The third period (from the beginning to the middle of the 20th century) is characterized by the introduction of electromechanical devices into the work of cryptographers. At the same time, the use of polyalphabetic ciphers continued.

For example, the German Enigma machine was used to encrypt classified information during World War II. The Second World War served as a kind of catalyst for the development of computer systems - through cryptography.



Wehrmacht Enigma

Cryptographic machine of the Third Reich. The code created using Enigma is considered one of the strongest used in the Second World War.

Turing Bombe

Developed under the guidance of Alan Turing decoder. Its use allowed the Allies to split the Enigma code, which seemed monolithic.

4. The fourth period - from the middle to the 70s of the XX century - the period of transition to mathematical cryptography. In the work of Shannon, rigorous mathematical definitions of the amount of information, data transfer, entropy, and encryption functions appear. A mandatory step in the creation of a cipher is the study of its vulnerability to various known attacks - linear and differential cryptanalysis. However, until 1975, cryptography remained "classical" or, more correctly, cryptography with a secret key.

5. The modern period of cryptography development (from the end of the 1970s to the present) is distinguished by the emergence and development of a new direction - public-key cryptography.

Cryptanalysis is the science of how to open an encrypted message, that is, how to extract plain text without knowing the key.

Interrelation of Algebra and Critology

Def. 1. Encryption is the reversible conversion of plaintext to ciphertext. It is defined by two mutually inverse mappings,

Ek: T →C и *Dk*: C→T,

where T is the set of plaintexts, C is the set of all ciphertexts, k is the key selected from the key space K. If we denote by E the set {Ek: k∈K} of all encryption mappings, and by D the set {Dk: k∈K } of all decryption mappings, then for any t ∈T, k∈K the equality
Dk(Ek(t)) =t.

Then the collection (T, C, K, E, D) is called a cipher, or cipher system. The simplest and oldest classes of ciphers are permutation ciphers and replacement ciphers. In these ciphers, C = T =, where A is the alphabet of the text, n is the length of the message.

Def. 2. The role of the key k in the permutation cipher is played by an arbitrary permutation k∈Sn from the permutation group of the set {1, ..., n}; Thus, the key space K = Sn, the encryption mapping is determined by the equality:

$$E_k(a_1, a_2, \ldots a_n) = a_{k(1)} a_{k(2)} \ldots a_{k(n)},$$

and the decryption mapping is determined by the equality:

$$D_k(a_1, a_2 \ldots a_n) = a_{k-1(1)} a_{k-1(2)} \ldots a_{k-1(n)}.$$

Def. 3. The role of the key k in the replacement cipher is played by an arbitrary permutation k∈ Sn from the permutation group of the alphabet A; Thus, the key space K = Sn, the encryption mapping is determined by the equality

$$E_k(a_1, a_2, \dots a_n) = k(a_1), k(a_2), \dots k(a_n),$$

and the decryption mapping is determined by the equality:

$$D_k(a_1, a_2, \dots a_n) = k^{-1}(a_1)k^{-1}(a_2) \dots k^{-1}(a_n).$$

Example. 1. If you believe the story, then the first permutation cipher was used in Sparta. A narrow parchment ribbon was wound tightly around the cylinder, which was called a scital. Then, along the cylinder axis, text was written. When the code was removed from the cylinder, a string of letters remained on it, at first glance, completely random. The tape was rewound and transmitted to the addressee who read the message, reeling up the tape on the same page. After that, the text became clear again. The key to the cipher is the diameter of the crystals. Therefore, she did not protect the confidential secrets very well, because soon enough, Aristotle came up with an anti-scital device that suggested winding the tape onto the cone, moving it from the top to the base of the cone. Where the diameter of the conical section coincided with the diameter of the text, meaningful syllables and words appeared on the tape, after which a text of the corresponding diameter was made and the letters were folded into a coherent text.

Example 2. The first replacement code was invented by Julius Caesar. As a permutation of the letters of the alphabet, he used just a cyclic shift by three letters. The reverse permutation, of course, is also a cyclic shift. In general, a shift of the form used in this cipher

$$i \to (i + k) \mathrm{mod} 26,$$

and the key was the number k. Since the key space is small, Caesar's encryption algorithm apparently didn't advertise much.

Example 3. The class of permutation ciphers includes route permutation ciphers. They have such an idea. The message is written to the table along one route, for example horizontally, and is read in a different way, such as vertically. To increase the key space, another rearrangement of the table columns was used.

CHANGE WITH REPLACEMENT OF LETTERS TO NUMBERS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

for example :«LIFE» - «12 9 6 5»

Digital table

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	Y
6	Z	1	2	3	4
7	5	6	7	8	9
8	0	.	,	?	!

The first digit in the cipher is a column, the second is a string, or vice versa. So the word “MIND” can be encrypted as “33 24 34 14”.

SQUARE OF POLYBIA

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

1 METHOD. Instead of each letter in the word, the corresponding letter is used below (A = F, B = G, etc.). Example: CIPHER - HOUNIW.

2 METHOD. The numbers from the table corresponding to each letter are indicated. The first is written horizontally, the second - vertically. (A = 11, B = 21 ...). Example: CIPHER = 31 42 53 32 51 24

Color chart

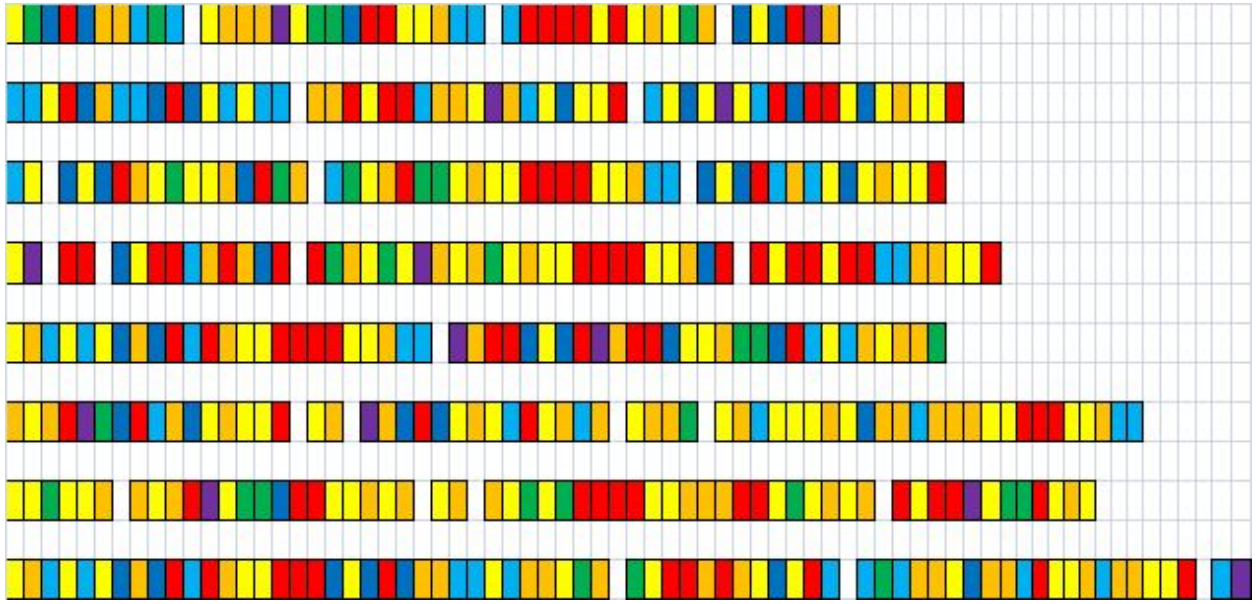
	А	Б	В	Г	Д	Е	Ё
	Ж	З	И	Й	К	Л	М
	Н	О	П	Р	С	Т	У
	Ф	Х	Ц	Ч	Ш	Щ	Ъ
	Ы	Ь	Э	Ю	Я	0	1
	2	3	4	5	6	7	8
	9	.	,	:	;	!	?

The first color in the cipher is a row, the second is a column

Source text:

The purpose of studying this topic is to familiarize students with the theory of encryption of texts, as well as the formation of skills in the study of mathematical objects and methods of their use in teaching and organizing research work of schoolchildren; involving students in research activities.

Ciphertext:



Julian Assange

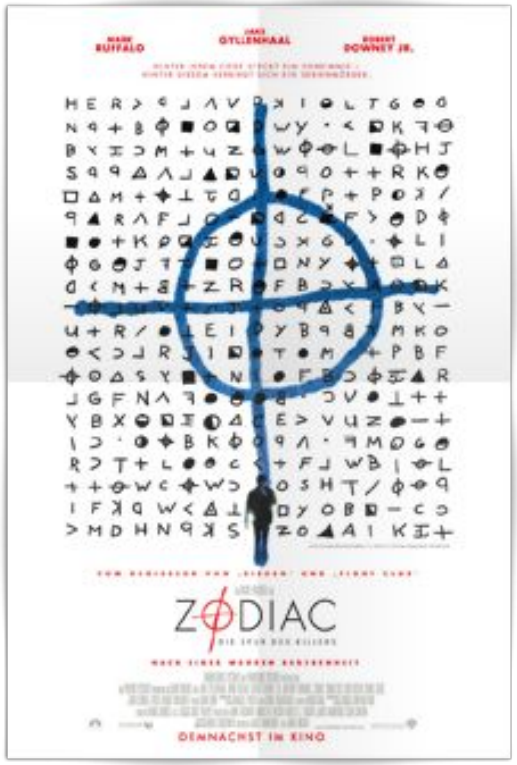
Y. 1971

On its portal, WikiLeaks has publicly demonstrated to all comers the wrong side of many government structures. Corruption, war crimes, top-secret secrets - in general, everything that an active libertarian has reached has become public. In addition, Assange is the creator of a hellish cryptosystem called Deniable encryption. This is a way to compose encrypted information, which provides the possibility of a plausible denial of its presence.

Bram Cohen

Y. 1975

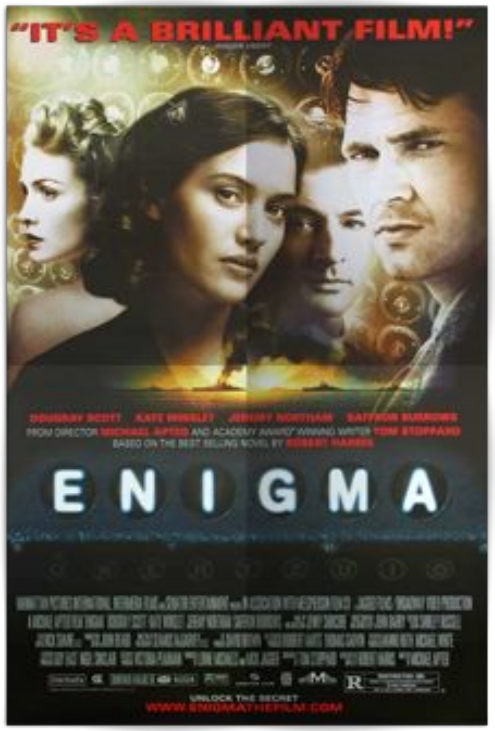
American programmer, originally from sunny California. To the delight of the whole world, I came up with the BitTorrent protocol, which has been used unsuccessfully to this day.



Zodiac

2007 Y.

The intense thriller of David Fincher, built on real events. For most of the movie, the smartest San Francisco police officers try in vain to crack the cipher of a presumptuous maniac.



Enigma

2001 Y.

Fiction film in the scenery of World War II: brilliant mathematicians gather in Bletchley Park to unravel the new cipher of the insidious Nazis. The picture is full of inexplicable puzzles and secrets - however, this can be guessed by name.

Familiarity with cryptography will be required for each user of electronic means of exchanging information, so cryptography in the future will become a "third literacy" along with a "second literacy" - computer skills and information technology.