Определение. Block cipher processes the input one block of elements at a time, producing an output block for each input block

Определение. Plaintext - an original message.

Определение. Ciphertext - the coded message.

Определение. Attack - an assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Определение. Brute-force attack - The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. On average, half of all possible keys must be tried to achieve success

Определение. Caesar cipher - substitution cipher, that involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Определение. Computationally secure - cipher, if these two criteria are met:

- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Определение. Conventional encryption - single-key encryption, symmetric encryption

Определение. cryptographic system (cipher) - scheme of encryption

- Plaintext: This is the original intelligible message or data that is fed into the algorithm as input.
- Encryption algorithm: The encryption algorithm performs various substitutions and transformations on the plaintext.
- Secret key: The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key. (In symmetric cipher there is only one key that is used for both encryption and decryption, but in different systems like asymmetric ciphers there are two different keys for encryption and decryption)
- Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message, two different keys will produce two different ciphertexts. The ciphertext is an apparently random stream of data and, as it stands, is unintelligible.
- Decryption algorithm: This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext

Определение. Cryptography - study, which area are constituted by the many schemes used for encryption

Определение. Cryptanalysis - study of techniques used for deciphering a message without any knowledge of the enciphering details
(AS AN ATTACK):
Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs. This type of attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

Определение. Cryptology - study, which area is the areas of cryptography and cryptanalysis

Определение. Deciphering (decryption) - restoring the plaintext from the ciphertext

Определение. Digram - two-letter combinations

Определение. Enciphering (encryption) - the process of converting from plaintext to ciphertext

Определение (Hill cipher)**.** This encryption algorithm takes successive plaintext letters and substitutes for them ciphertext letters. The substitution is determined by linear equations in which each character is assigned a numerical value ($a = 0, b = 1, \ldots, z = 25$)

$$C = E(K, P) = PK \mod 26$$
$$P = D(K, C) = CK^{-1} \mod 26 = PKK^{-1} = P$$

C and P are row vectors of length 3 representing the plaintext and ciphertext, and K is a matrix representing the encryption key.

Определение. monoalphabetic (substitution) cipher - type of cipher, where ciphertext and plaintext have the same alphabet.

Определение (one-time pad)**.** An Army Signal Corp officer, Joseph Mauborgne, proposed an improvement to the Vernam cipher that yields the ultimate in security. Mauborgne suggested using a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, known as a one-time pad, is unbreakable. It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.

Vernam cipher:

$$c_i = p_i \oplus k_i$$

$$p_i = c_i \oplus k_i$$

Определение. Playfair cipher.

The Playfair algorithm is based on the use of a 5×5 matrix of letters constructed using a keyword. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:

1. Repeating plaintext letters that are in the same pair are separated with a filler letter, such as x, so that balloon would be treated as ba lx lo on.
2. Two plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, ar is encrypted as RM.
3. Two plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, mu is encrypted as CM.
4. Otherwise, each plaintext letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Определение (polyalphabetic cipher)**.** Another way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is **polyalphabetic substitution cipher**. All these techniques have the following features in common:

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation

Определение (rail fence cipher)**.** The simplest such cipher is the rail fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows. For example, to encipher the message "meet me after the toga party" with a rail fence of depth 2, we write the following: m e m a t r h t g p r y
e t e f e t e o a a t The encrypted message is
MEMATRHTGPRYETEFETEOAAT

Определение (steganography)**.** is the practice of representing information within another message or physical object, in such a manner that the presence of the information is not evident to human inspection.

A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text

1. Character marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.
2. Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

Определение. Stream cipher processes the input elements continuously, producing output one element at a time, as it goes along

Определение. Symmetric encryption - is a form of cryptosystem in which encryption and decryption are performed using the same key.

Определение (transposition cipher)**.** All the techniques examined so far involve the substitution of a ciphertext symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Определение. Unconditionally secure - an encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available.

Определение (Vigenère cipher)**.** We can express the Vigenère cipher in the following manner. Assume a sequence of plaintext letters and a key consisting of the sequence of letters , where typically $<$ .The sequence of ciphertext letters is calculated as follows:

$$C_i = (p_i + k_{i \mod m}) \mod 26$$

$$p_i = (C_i - k_{i \mod m}) \mod 26$$