

7 November 2021

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/f2607e5e-6ba8-4aa1-b534-29b5ed6229a5/D3_241243.docx

Key Encryption Concepts and Definitions

Substitution

the act, process, or result of substituting one thing for another.

b: **replacement** of one mathematical entity by another of equal value.

2: one that is substituted for another.

In cryptography, a substitution cipher is **a method of encrypting in which units of plaintext are replaced with the ciphertext**, in a defined manner, with the help of a key; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth.



Substitution: The process of exchanging one letter or byte for another. An example is the Caesar cipher, where each letter was shifted by 3 characters. An "A" was represented by a "D," a "B" was represented by an "E," a "C" was represented by an "F," and so on.

Transposition



Transposition or permutation: The process of reordering the plaintext to hide the message, but keeping the same letters.

Vernam

Vernam Cipher is a method of encrypting alphabetic text. It is one of the Transposition techniques for converting plain text into ciphertext. In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, ... z = 25).

Method to take key: In the Vernam cipher algorithm, we take a key to encrypt the plain text which length should be equal to the length of the plain text.

In cryptography, a transposition cipher is **a method of encryption by which the positions held by units of plaintext** (which are commonly characters or groups of characters) are shifted according to a regular system so that the ciphertext constitutes a permutation of the plaintext.

Encryption Algorithm:

- Assign a number to each character of the plain text and the key according to alphabetical order.
- Add both the number (Corresponding plain-text character number and Key character number).
- Subtract the number from 26 if the added number is greater than 26, if it isn't then leave it.

Example:

Plain-Text: RAMSWARUPK
Key: RANCHOBABA

Now according to our encryption algorithm, we assign a number to each character of our plain-text and key.

```
PT:  R A M S W A R U P K
NO:  17 0 12 18 22 0 17 20 15 10

KEY: R A N C H O B A B A
NO:  17 0 13 2 7 14 1 0 1 0
```

Now add the number of Plain-Text and Key and after doing the addition and subtraction operation (if required), we will get the corresponding Cipher-Text character number.

```
CT-NO: 34 0 25 20 29 14 18 20 16 10
```

In this case, two numbers are greater than the 26 so we have to subtract 26 from them and after applying the subtraction operation the new Cipher text character numbers are as follow:

```
CT-NO: 8 0 25 20 3 14 18 20 16 10
```

New Cipher-Text is after getting the corresponding character from the number.

```
CIPHER-TEXT: I A Z U D O S U Q K
```

Note: For the *Decryption* apply the just reverse process of encryption.

Information theory

<https://www.scientificamerican.com/article/claude-e-shannon-founder/>

Caesar Cipher

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher

Caesar Cipher in Cryptography - GeeksforGeeks

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some

↻ <https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/?ref=rp>



Null cipher

A null cipher, also known as concealment cipher, is an **ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material**. Today it is regarded as a simple form of steganography, which can be used to hide ciphertext.

Keyspace

Keyspace: This represents the total number of possible values of keys in a cryptographic algorithm or another security measure, such as a password. For example, a 20-bit key would have a keyspace of 1,048,576. A 2-bit key would have a keyspace of 4.

The key range is a range of values that are valid for use as a key for a specific algorithm.

Bit size is nothing more than the number of binary digits.

Key length

The key **length determines the maximum number of combinations required to break an encryption algorithm**. If a key is n bits long, then there are two to the n th power (2^n) possible keys. For example, if the key is one bit long, and that one bit can either be a zero or a one, there are only two possible keys, 0 or 1.

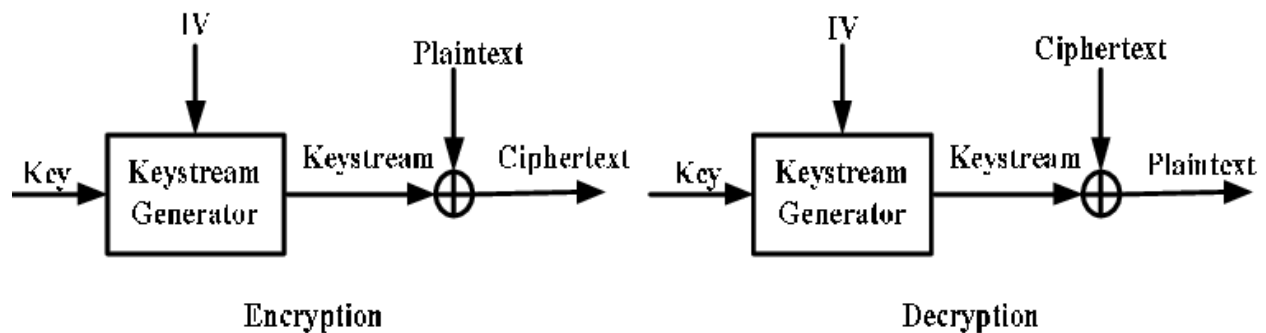
The key length is **an important parameter of symmetrical or asymmetric encryption processes**. It provides information on how many different key values a key can accept in a specific protocol. The key length is typically specified as a logarithm in form of bits.



A typical value is **256 bits**. The public key is a group element, which is much larger than the private key. A typical value is 2048 bits.

Synchronous

Symmetric: This is a term used in cryptography to indicate that the same key is required to encrypt and decrypt. The word “symmetric” means “the same,” and we are referring to the key that is required at both ends to encrypt and decrypt. Symmetric key cryptography has the fundamental problem of secure key distribution.



Asynchronous

Asymmetric: This word means “not the same.” This is a term used in cryptography in which two different but mathematically related keys are used where one key is used to encrypt and another is used to decrypt.



Hash function

Hash function: A hash function is a one-way mathematical operation that reduces a message or data file into a smaller fixed-length output, or hash value. By comparing the hash value computed by the sender with the hash value computed by the receiver over the original file, unauthorized changes to the file can be detected, assuming they both used the same hash function. Ideally, there should never be more than one unique hash for a given input and one hash exclusively for a given input.

Registration authority

A registration authority (RA) is **an authority in a network that verifies user requests for a digital certificate** and tells the certificate authority (CA) to issue it. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signatures.

SP network

cryptography, an **SP-network**, or **substitution-permutation network (SPN)**, is a series of linked mathematical operations used in block cipher algorithms such as AES (Rijndael), 3-Way, Kalyna, Kuznyechik, PRESENT, SAFER, SHARK, and Square.

Such a network takes a block of the plaintext and the key as inputs and applies several alternating "rounds" or "layers" of substitution boxes (S-boxes) and permutation boxes (P-boxes) to produce the ciphertext block. The S-boxes and P-boxes transform (sub-)blocks of input bits into output bits. It is common for these transformations to be operations that are efficient to perform in hardware, such as exclusive or (XOR) and bitwise rotation. The key is introduced in each round, usually in the form of "round keys" derived from it. (In some designs, the S-boxes themselves depend on the key.)

Decryption is done by simply reversing the process (using the inverses of the S-boxes and P-boxes and applying the round keys in reversed order).

Confusion

▼ Definition

Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

The property of confusion hides the relationship between the ciphertext and the key.

This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of most or all of the bits in the ciphertext will be affected.

Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

Diffusion

Diffusion means that if we change a single bit of the plaintext, then about half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then about half of the plaintext bits should change.[3] This is equivalent to the expectation that encryption schemes exhibit an avalanche effect.

The purpose of diffusion is to hide the statistical relationship between the ciphertext and the plain text. For example, diffusion ensures that any patterns in the plaintext, such as redundant bits, are not apparent in the ciphertext.[2] Block ciphers achieve this by "diffusing" the information about the plaintext's structure across the rows and columns of the cipher.

Brute force

A block cipher breaks down plaintext messages into fixed-size blocks before converting them into ciphertext using a key.

A stream cipher, on the other hand, breaks a plaintext message down into single bits, which then are converted individually into ciphertext using key bits.



Brute force is a hacking technique used to find out the user Credentials by typing various possible credentials.

- Guessing the credentialls
- Trial and error

- Username list and password list

Cryptogram

A **cryptogram** is a type of puzzle that consists of a short piece of encrypted text.

[1] Generally the cipher used to encrypt the text is simple enough that the cryptogram can be solved by hand. Substitution ciphers where each letter is replaced by a different letter or number are frequently used. To solve the puzzle, one must recover the original lettering. Though once used in more serious applications, they are now mainly printed for entertainment in newspapers and magazines.

Cipher

Ciphers, also called encryption algorithms, are **systems for encrypting and decrypting data**. A cipher converts the original message, called plaintext, into ciphertext using a key to determine how it is done. Ciphers, also called encryption algorithms, are **systems for encrypting and decrypting data**. A cipher converts the original message, called plaintext, into ciphertext using a key to determine how it is done.

Steganography

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

Kry Clustering

A **weakness** in cryptography where a plain-text message generates identical cipher-text messages using the same algorithm but different keys.

▼ What is Cryptanalysis ?

Cryptanalysis is the science of deciphering (or breaking) ciphertext without the cryptographic key. Practitioners of cryptanalysis are known as cryptanalysts.

▼ End to end encryption


With end-to-end encryption, packets are encrypted once at the original encryption source and then decrypted only at the final decryption destination.

▼ Link encryption

Link encryption Link encryption requires that each node (for example, a router) has separate key pairs for its upstream and downstream neighbors. Packets are encrypted and decrypted, then re-encrypted at every node along the network path. The advantage of using link encryption is that the entire packet (including routing information) is encrypted. However, link encryption has the following two disadvantages: Latency: Packets must be encrypted/ decrypted at every node, which creates latency (delay) in the transmission of those packets. Inherent vulnerability: If a node is compromised or a packet's decrypted contents are cached in a node, the message can be compromised.

Cyptography Flashcards by Daniel Handley | Brainscape

Cryptography can also be used to ensure the integrity (or accuracy) of information through the use of hashing algorithms and message digests. With end-to-end encryption, packets are encrypted once at

 <https://www.brainscape.com/flashcards/cyptography-2511830/packs/4413088>



Brainscape