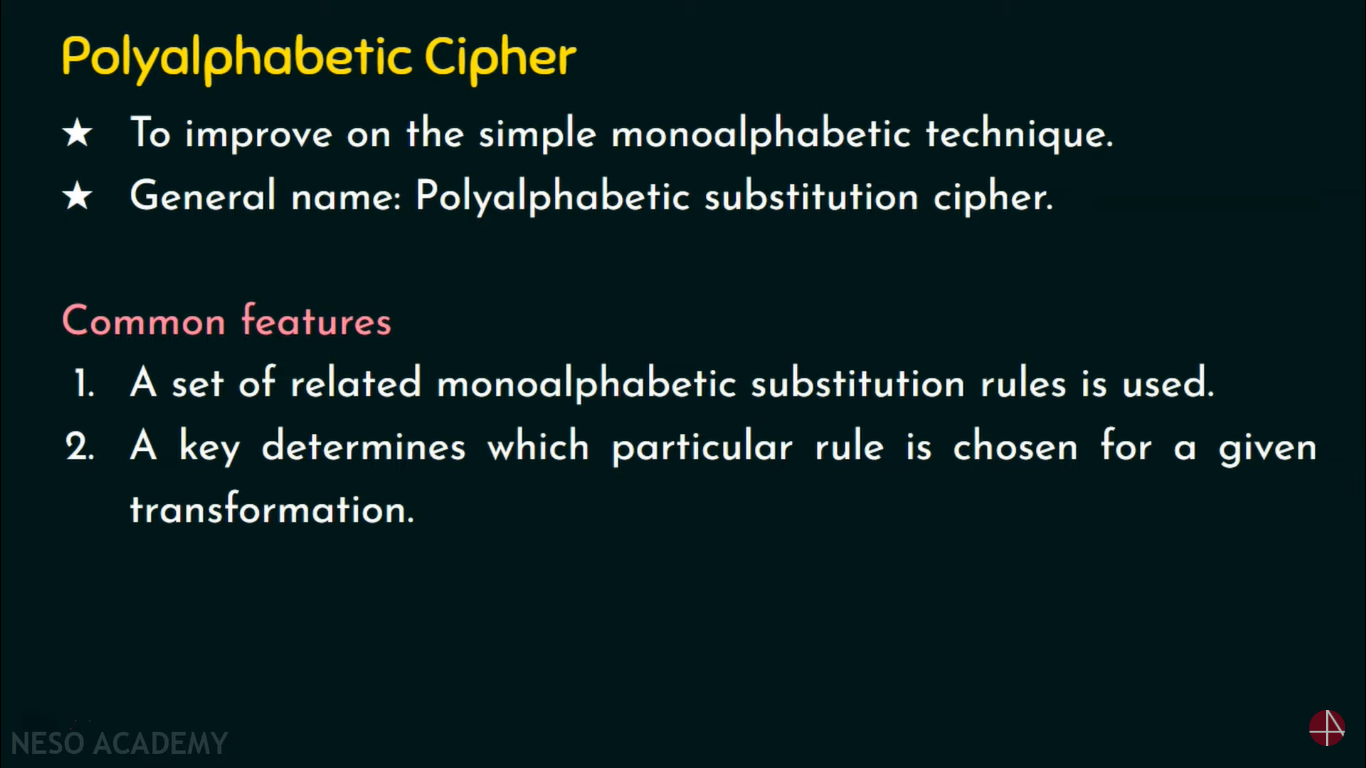


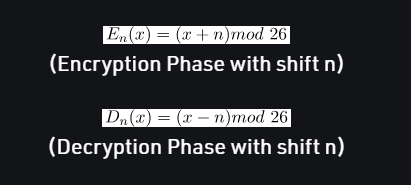
Substitution is also called confusion and Transposition is also called diffusion

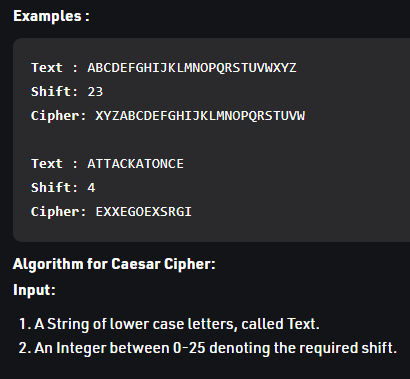


1. CAESAR/SHIFT CIPHER

. to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.

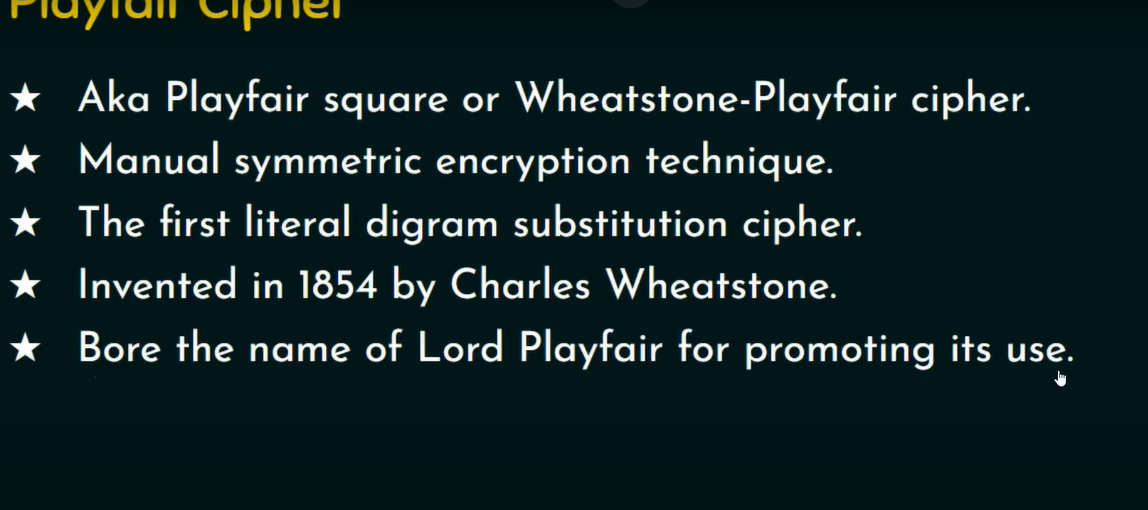
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.



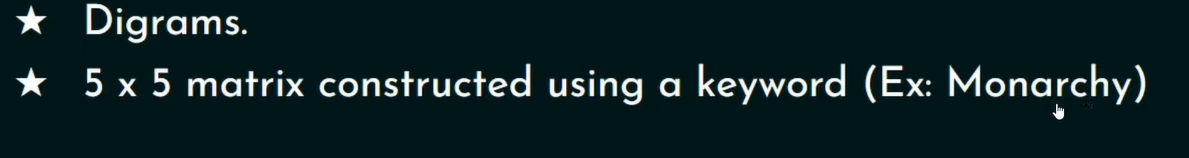


.

1. Playfair CIPHER

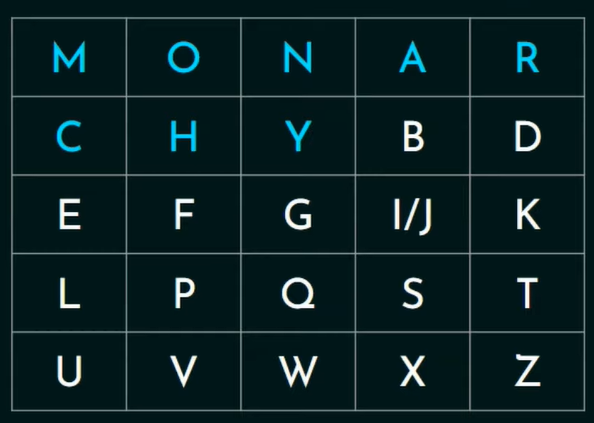


It is a multiple level encryption cipher, that means if in a plaintext containing two occurrences of a letter “d” , first d is replaced by m, it is not necessary that the second d will also be replaced by m only.



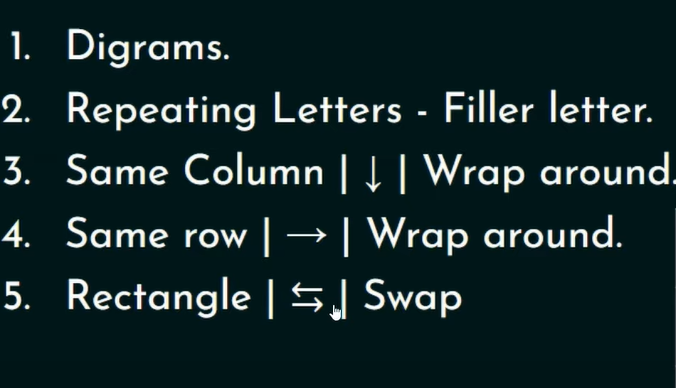


In case the keyword has a repeating alphabet, while filling the matrix, skip that repeating occurance.



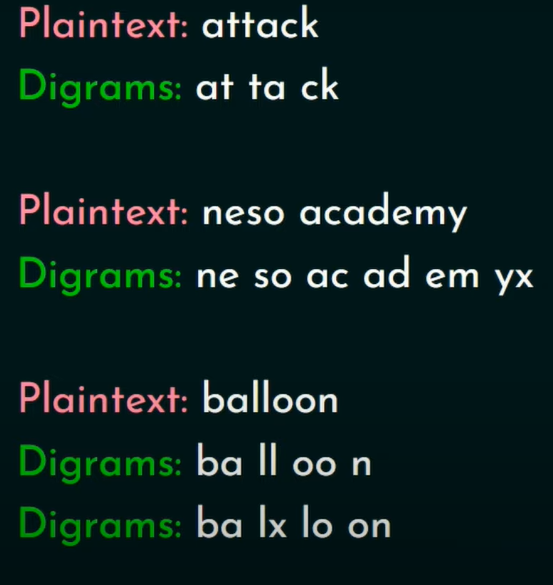
After filling the keyword, start filling up the matrix with the alphabets from a-z, keeping note that no same alphabet should be there. Because English has only 25 alphabets and our matrix has 5x5 i.e 25 spaces, we have combined I/J. If the keyword comprises of either I or J , just write that alphabet instead.

Rules for encryption of Playfair cipher

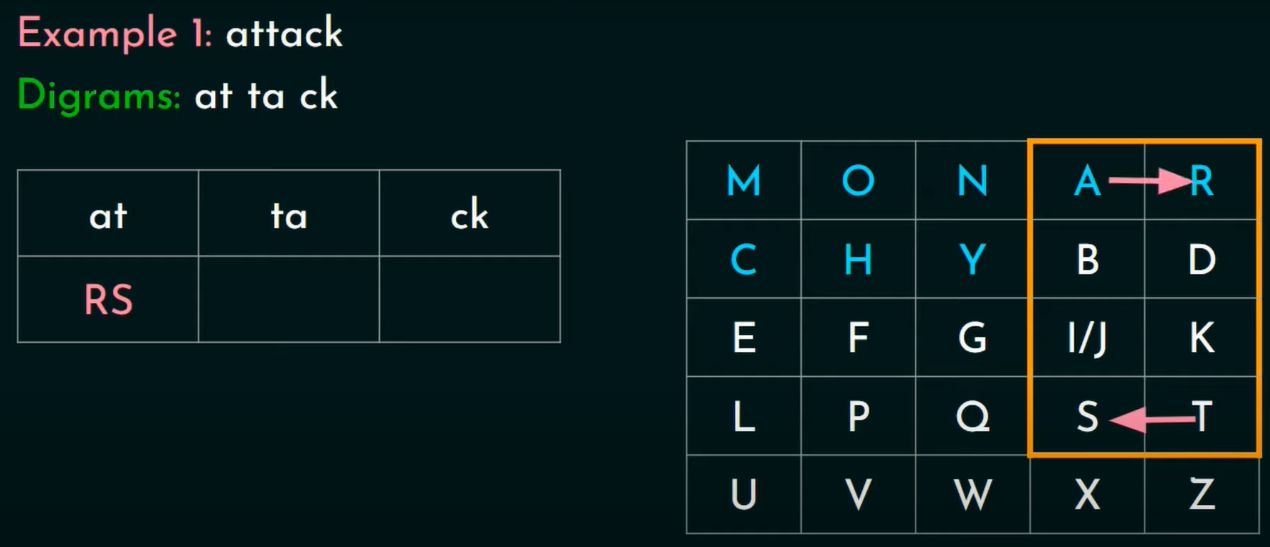


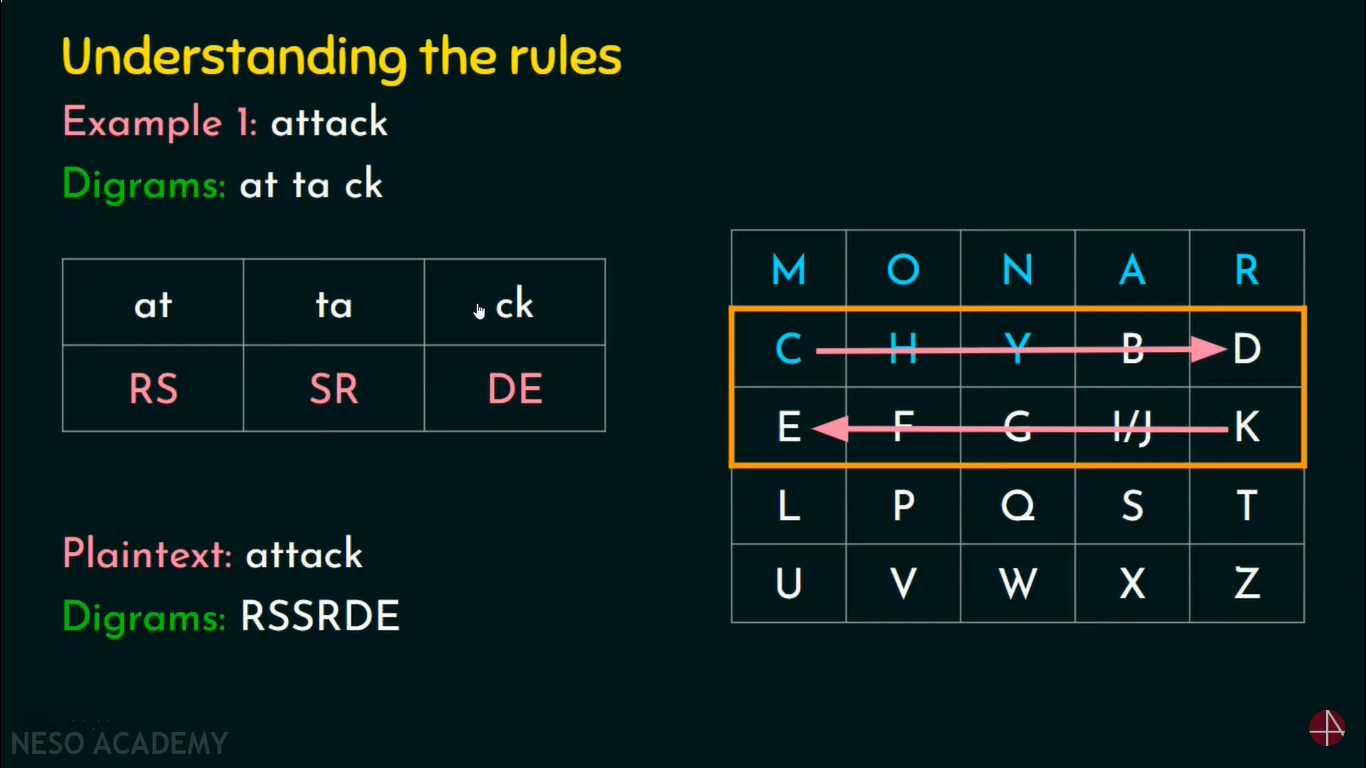
a)Digrams

i) Creating Digrams

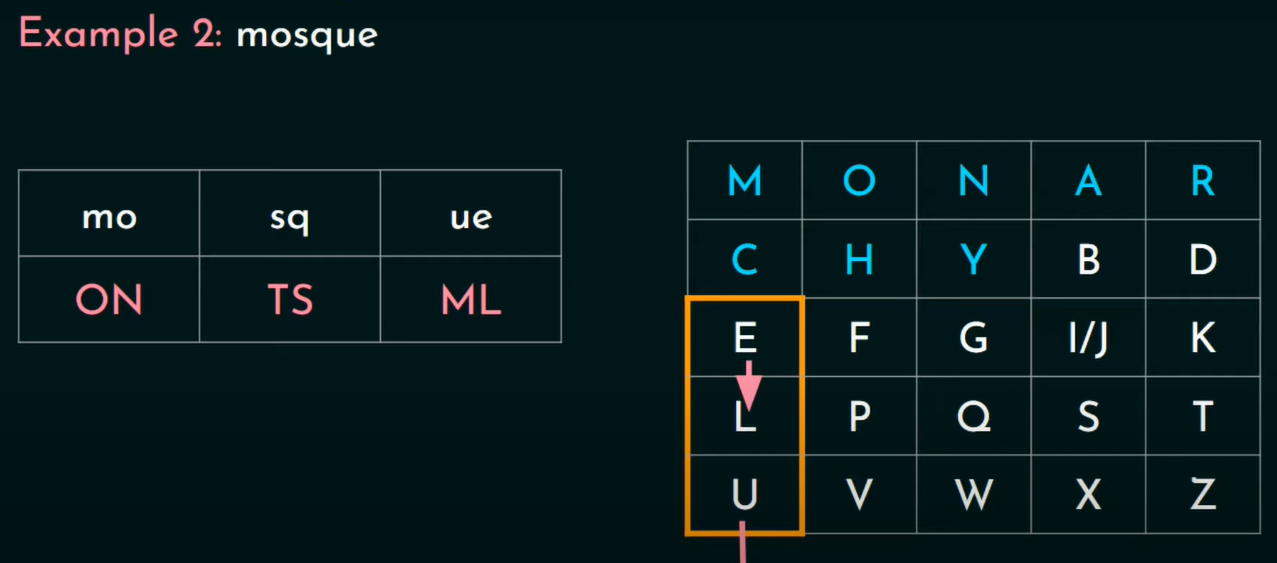


1. Encrypting them.





Example 2



1. vernam cipher

Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text. 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 whose length should be equal to the length of the plain text.

Vernam cipher is also known as one time-pad.

Encryption Algorithm:

Assign a number to each character of the plain-text and the key according to alphabetical order.

Bitwise XOR both the number (Corresponding plain-text character number and Key character number).

Subtract the number from 26 if the resulting number is greater than or equal to 26, if it isn’t then leave it.

Example 1

Plain-Text: O A K

Key: S O N

O ==> 14 = 0 1 1 1 0

S ==> 18 = 1 0 0 1 0

Bitwise XOR Result: 1 1 1 0 0 = 28

Since the resulting number is greater than 26, subtract 26 from it. Then convert the Cipher-Text character number to the Cipher-Text character.

28 - 26 = 2 ==> C

CIPHER-TEXT: C

Similarly, do the same for the other corresponding characters,

PT: O A K

NO: 14 00 10

KEY: S O N

NO: 18 14 13

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

CT-NO: 02 14 07

CT: C O F

One Time Pad algorithm is the improvement of the Vernam Cipher, proposed by An Army Signal Corp officer, Joseph Mauborgne.

It is the only available algorithm that is unbreakable(completely secure).

The two requirements for the One-Time pad are

The key should be randomly generated as long as the size of the message.

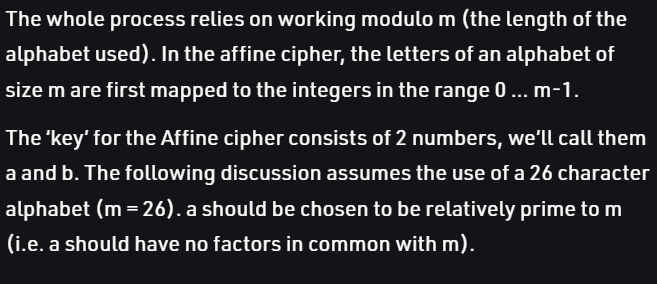
The key is to be used to encrypt and decrypt a single message, and then it is discarded.

So to encrypt every new message requires a new key of the same length as the new message in one-time pad.

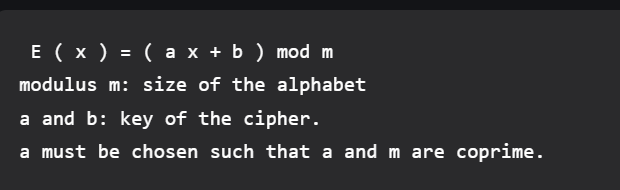
The ciphertext generated by the One-Time pad is random, so it does not have any statistical relation with the plain text.

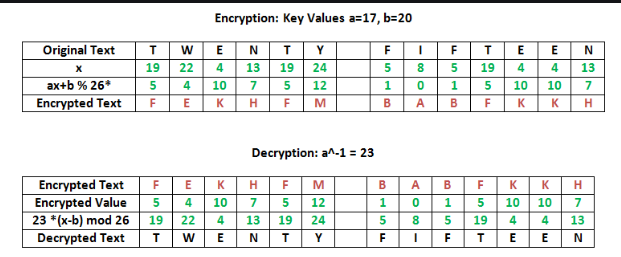
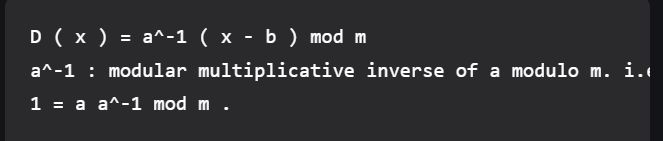
1. Affine CIPHER

It is a monoalphabetic Substitution Cipher used for encryption and decryption of the plain text.

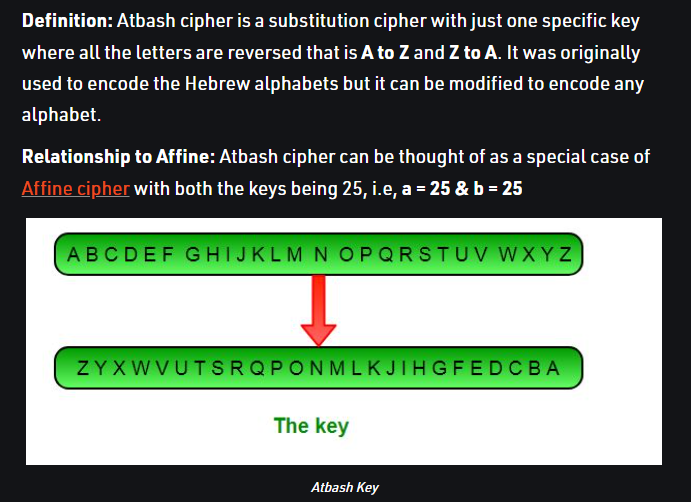


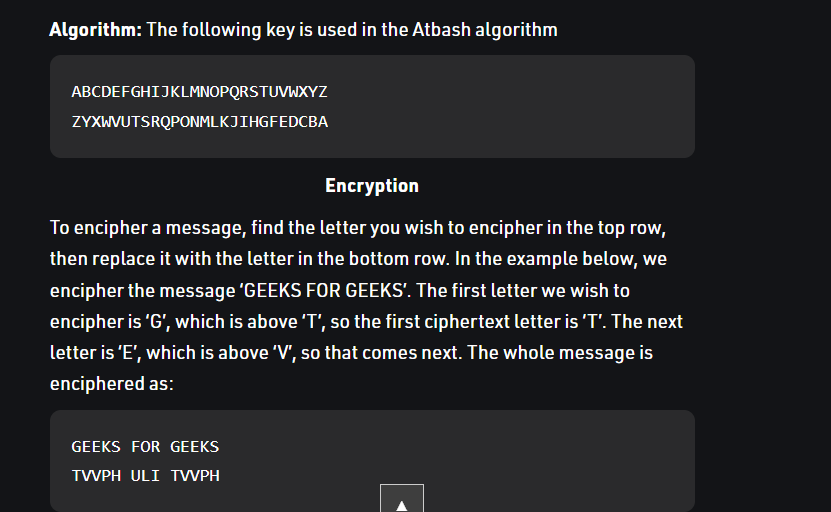
Where A=0,B=,C=3,2D=3,……….Z=25.





1. Atbash CIPHER



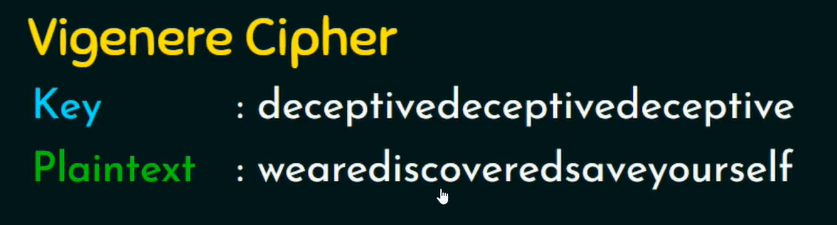


1. VIGENERE CIPHER

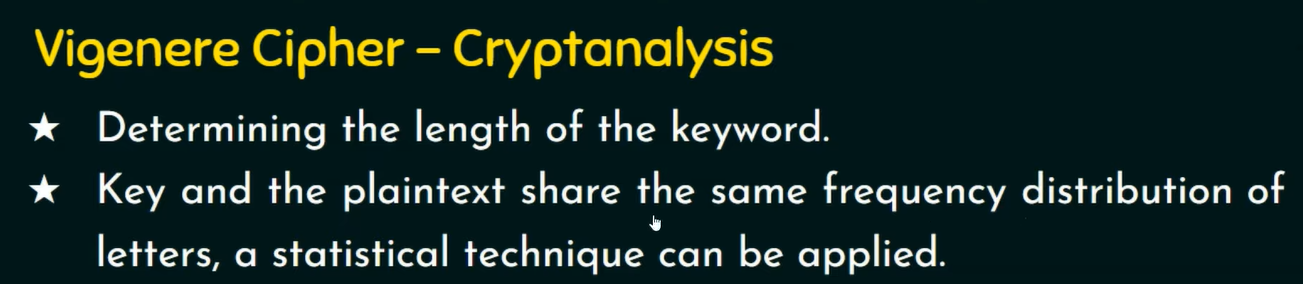


It is a polyalphabetic substitution Cipher

Here we have to repeat the key until it reaches the length of the plain text.







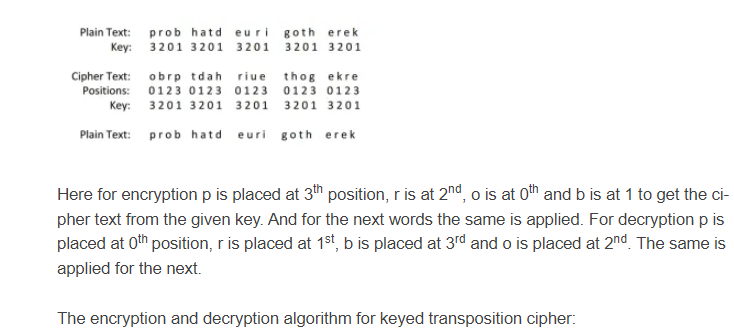
1. KEYED TRANSPOSITION

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 cipher text constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bi-jective function is used on the characters’ positions to encrypt and an inverse function to decrypt.

**Keyed Transposition Cipher:**

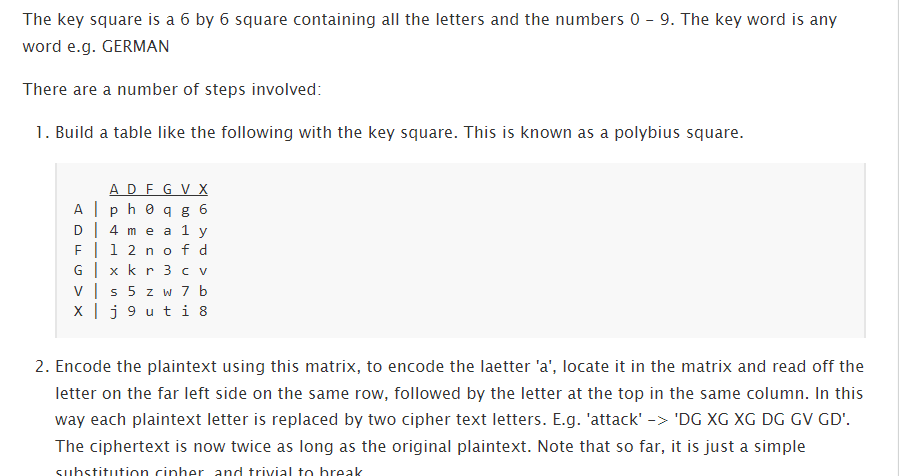
Keyed transposition cipher uses keys to encrypt and decrypt the messages. It shares the same secret key among the senders and the receivers. Key is used as position finder for the cipher text. We can illustrate this by giving a nice example as-

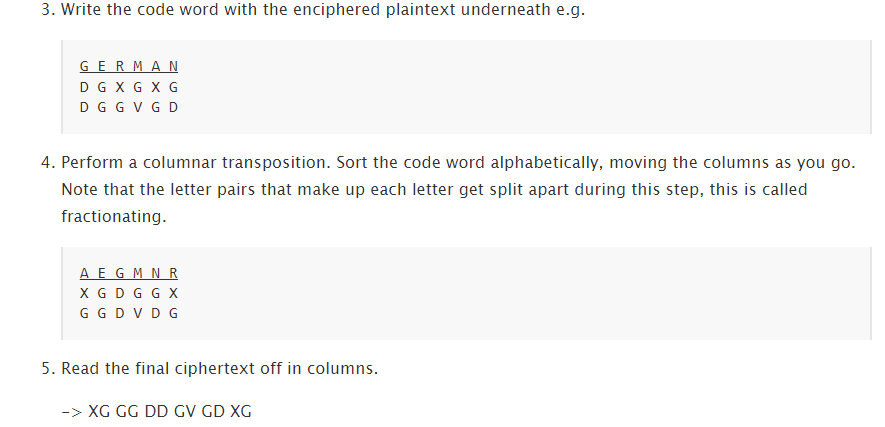
Suppose given plaintext is- “prob hatd euri goth erek”. And lets the key is=3201. Then the cipher text will be-(Here I assumed starting from 0)



1. ADFGVX CIPHER

 the cipher is a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition. The cipher is named after the six possible letters used in the ciphertext: A, D, F, G, V and X. These letters were chosen deliberately because they sound very different from each other when transmitted via morse code. The intention was to reduce the possibility of operator error.

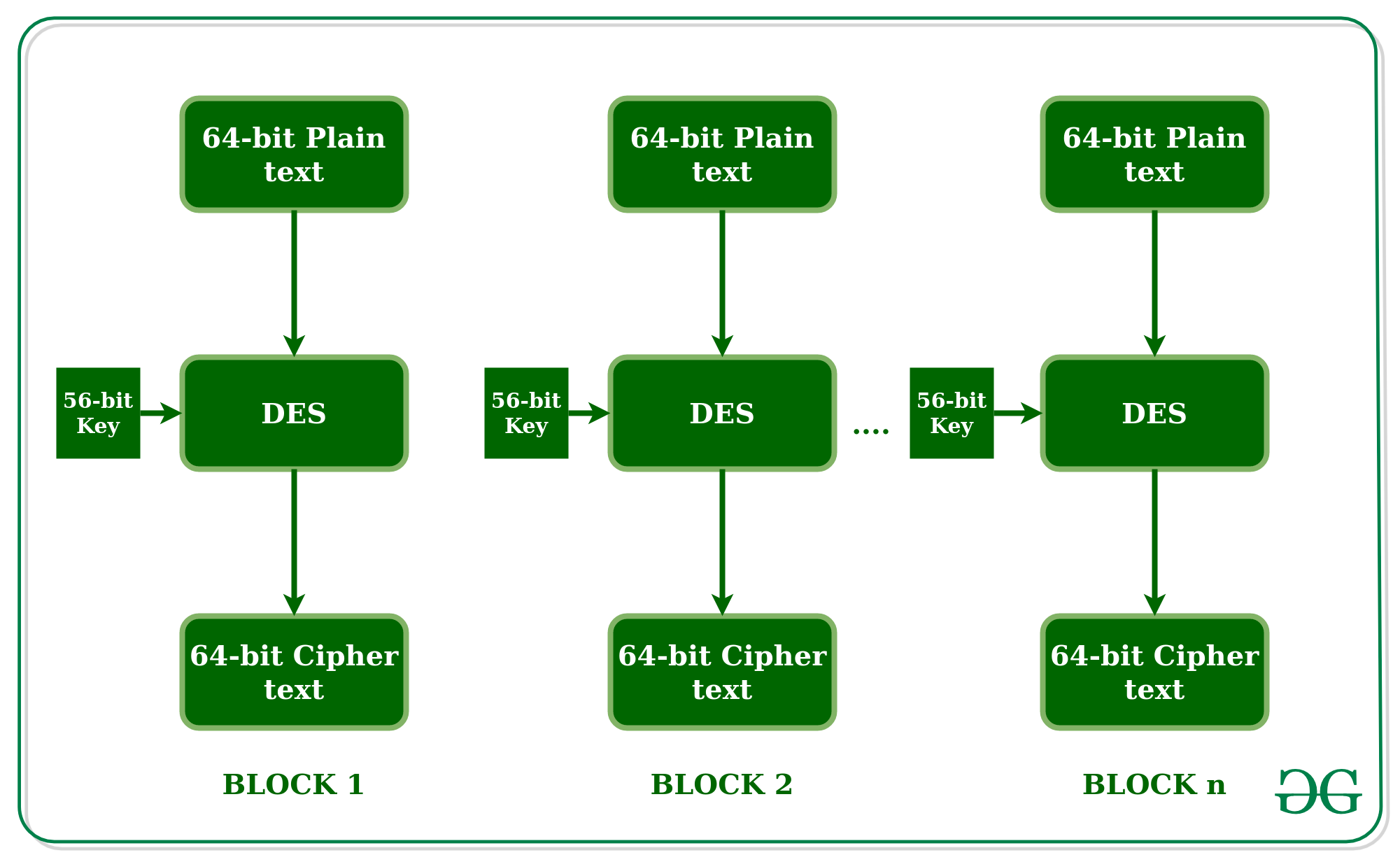




1. DES

Data encryption standard

It is a block cipher and encrypts data in blocks of 64 bits each which means 64 bits of input to DES ,which produces 64 bits of cipher text. Same keys are used for the encryption and decryption with a slight differences. The length of the key is 56 bits.



The initial key is of 64 bits, but after discarding every 8th bit of the key, it becomes a 56-bit key.

DES is based on these 2 fundamental aspects;

* Substitution (Known as confusion)
* Transposition (Known as diffusion)

DES contains 16 steps which are also known as Rounds , each of which contains the steps of substitution and transposition.

Steps:-

1. In the first step, the 64-bit plain text is handed over to the Initial Permutation(IP) function.
2. The IP is performed on the plain text.
3. The IP produces two halves of the permuted blocks;-
4. Left plain text (LPT)
5. Right plain text(RPT)
6. In the end LPT and RPT are combined and a Final permutation is performed on the combined block.
7. The final block is the 64-bit cipher text.

Initial Transposition

IP happens only once, before the first round. For example, it says that that IP of the first bit of the plain text should be replaced with the IP of the 58th bit of plain text, IP of 2nd bit with 44th bit and so on. It is a random transposition of the bits in the plain text.

After the IP is done, the block is divided into two halves each of 32-bits each, which further will undergo 16 rounds , containing broader steps each;-

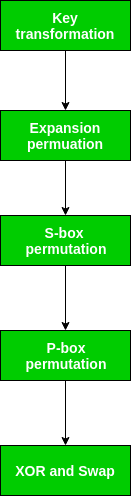
1. Key transformation/Compression permutation.

The 56-bit generated key is converted into a 48-bit key in each of the 16 rounds. The process is that the 56-bit key is divided into 2 parts ,28 bits each. A circular shift towards the left is applied, one or two times depending on the round. After an appropriate shift, the 48 bits are selected.

1. Expansion permutation

The 32-bit plain text (RPT) obtained after the IP, it is expanded into 48 bits. First 32-bit Plain text is broken down into 8 blocks of 4 bits each, and then permutation is applied and 2 bits more are added to those blocks. Then The 48-bit key is XOR with 48 bit Plain text and given as an input in the S-box permutation.

1. S-box Permutation



1. FIESTEL CIPHER MODEL

Fiestel Cipher is a model or structure used to develop block Ciphers such as DES.

**Feistel cipher algorithm**

* Create a list of all the Plain Text characters.
* Convert the Plain Text to Ascii and then 8-bit binary format.
* Divide the binary Plain Text string into two halves: left half (L1)and right half (R1)
* Generate a random binary keys (K1 and K2) of length equal to the half the length of the Plain Text for the two rounds.

First Round of Encryption

* **a.**Generate function f1 using R1 and K1 as follows:

f1= xor(R1, K1)

* **b.**Now the new left half(L2) and right half(R2) after round 1 are as follows:

R2= xor(f1, L1)

L2=R1

Second Round of Encryption

* **a.**Generate function f2 using R2 and K2 as follows:

f2= xor(R2, K2)

* **b.**Now the new left half(L3) and right half(R3) after round 2 are as follows:

R3= xor(f2, L2)

L3=R2

* Concatenation of R3 to L3 is the Cipher Text
* Same algorithm is used for decryption to retrieve the Plain Text from the Cipher Text.

1. TRIPLE DES

Double DES is a encryption technique which uses two instance of DES on same plain text. In both instances it uses different keys to encrypt the plain text. Both keys are required at the time of decryption. The 64 bit plain text goes into first DES instance which then converted into a 64 bit middle text using the first key and then it goes to second DES instance which gives 64 bit cipher text by using second key.

However double DES uses 112 bit key but gives security level of 2^56 not 2^112 and this is because of meet-in-the middle attack which can be used to break through double DES.

**Triple DES:**

Triple DES is a encryption technique which uses three instance of DES on same plain text. It uses there different types of key choosing technique in first all used keys are different and in second two keys are same and one is different and in third all keys are same.

1. Kerckhoffs's principle

Kerckhoffs’ Principle states that the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.

 The principle holds that a [cryptosystem](https://en.wikipedia.org/wiki/Cryptosystem) should be secure, even if everything about the system, except the [key](https://en.wikipedia.org/wiki/Cryptographic_key), is public knowledge.

1. AES

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember

AES is a block cipher.

The key size can be 128/192/256 bits.

Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data.

**Working of the cipher :**  
AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

* 128 bit key – 10 rounds
* 192 bit key – 12 rounds
* 256 bit key – 14 rounds

1. Steganography

The word **Steganography** is derived from two Greek words- ‘stegos’ meaning ‘to cover’ and ‘grayfia’, meaning ‘writing’, thus translating to ‘covered writing’, or ‘hidden writing’. **Steganography** is a method of hiding secret data, by embedding it into an audio, video, image, or text file. It is one of the methods employed to protect secret or sensitive data from malicious attacks.