BCA SEM-6

Assistant Professor

KBPCCS

CRYPTOGRAPHY

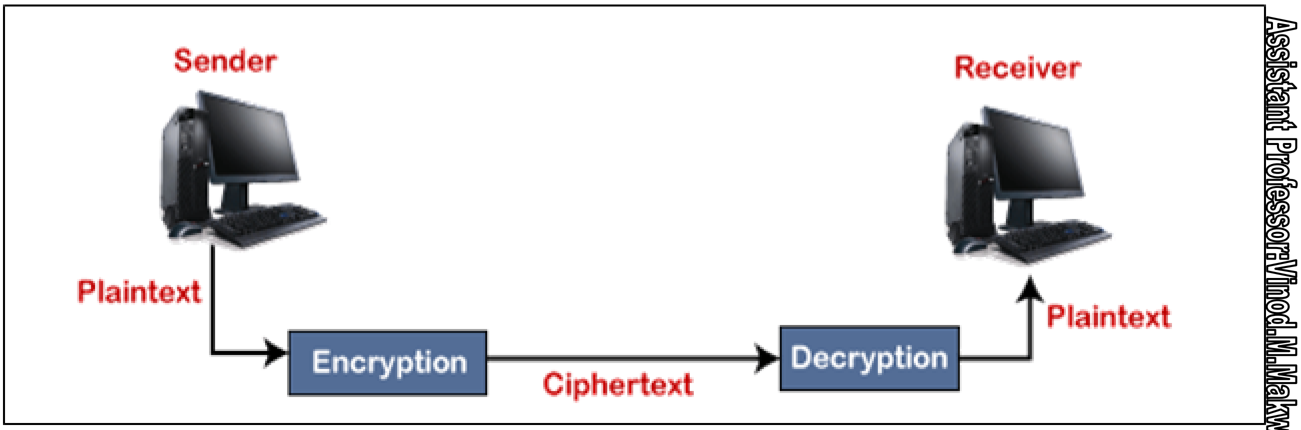
Unit-2

Unit-2	Cryptography	11	18
	- Concept of Cryptography. - Basic terms: Cryptography, Plaintext, Cipher text, Cipher, Key, Encryption and Decryption. - Cryptography Keys: Public Key and Private Key - Types of Cryptography: Symmetric key, Asymmetric key Cryptography. - Symmetric Cryptography: Substitutuonal and Transposition Cipher.		

BCA SEM-6

Que : 1 what is cryptography?

- Cryptography is derived from the Greek word, which means "Hidden Secrets."
- In other words, it is an art in which we can protect our data and information.
- Through cryptography, we convert our data into Unreadable Secret Codes, called Cipher Text and can read this data only, which will have the secret key to decrypt it.
- Decrypt data is called plain text. It maintains the security and integrity of the data.
- In cryptography, encryption and decryption are two processes.
- It is used to protect the Messages, Credit/Debit Card details, and other relevant information.
- In encryption, plain text is converted to cipher text, and in decryption, the cipher text is converted to plain text.



Cryptography has many advantages because encryption makes your data completely secure and safe. After encrypting the data, even if it is hacked or stolen, no one can access or read your data.

Que: 2 Explain different terms used in cryptography

Plaintext and Ciphertext

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

We refer to encryption and decryption algorithms as ciphers. The term cipher is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

Encryption

In cryptography, encryption is a process in which the information is converted into a secret code called ciphertext. Ciphertext cannot be easily understood, only experts can understand it. The main purpose of encryption is to secure digital data or information, which transmit via the internet.

Decryption

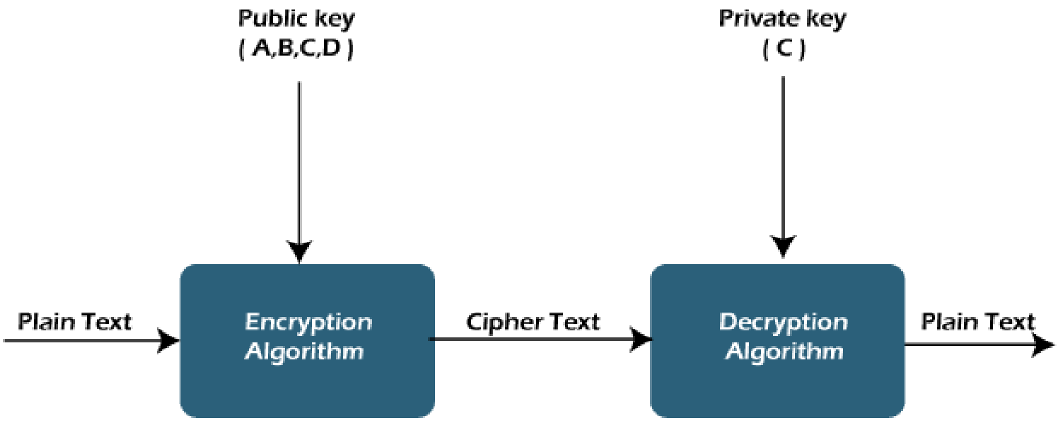
Decryption is a process in which encrypted data is converted back to original data. The encrypted data is called ciphertext, and the original data is called plain text, and the conversion of ciphertext to plain text is called decryption.

Que: 3 Explain cryptography keys in detail.

Public key

It is an encryption technique that uses a pair of keys (public and private key) for secure data communication. In the pair of keys, the public key is for encrypting the plain text to convert it into ciphertext, and the private key is used for decrypting the ciphertext to read the message.

The private key is given to the receiver while the public key is provided to the public. Public Key Cryptography is also known as asymmetric cryptography.



The public key can be shared without compromising the security of the private one. All asymmetric key pairs are unique, so a message encrypted with a public key can only be read by the person who has the corresponding private key. The keys in the pair have much longer than those used in symmetric cryptography. So, it is hard to decipher the private key from its public counterpart. Many of us, heard about RSA, which is the most common algorithm for asymmetric encryption in use today.

Public-key encryption is slower than secret-key encryption. In secret key encryption, a single shared key is used to encrypt and decrypt the message, while in public-key encryption, different two keys are used, both related to each other by a complex mathematical process. Therefore, we can say that encryption and decryption take more time in public-key encryption.

Applications of public key

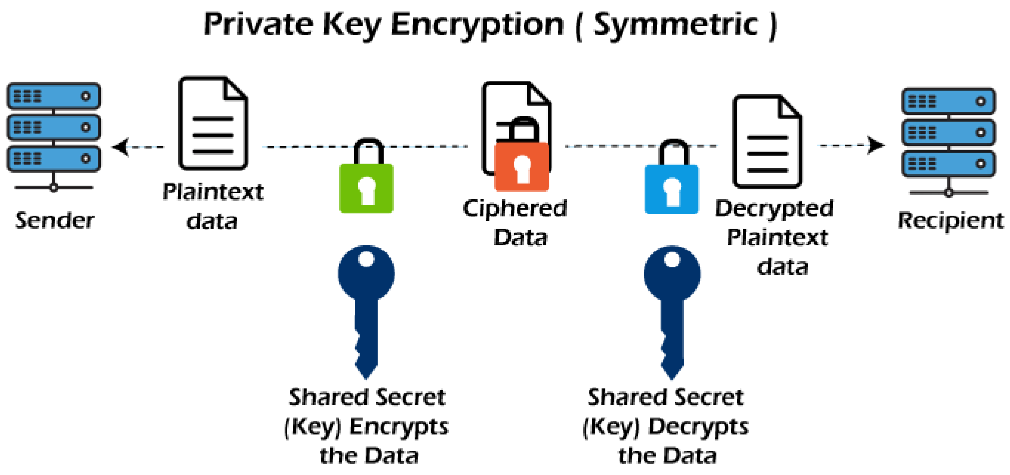
The applications of public key are -

- Public key cryptography can be used to encrypt Emails to keep their content confidential.
- Asymmetric cryptography or public-key cryptography is also used in Secure socket layer (SSL) protocol to make secure connections to websites.
- Public key is also used in Blockchain and cryptography technology. For example, a pair of keys is generated, while setting up a new cryptocurrency wallet.
- It can be used to create a digital signature in the Operating System software such as Ubuntu, Red Hat Linux packages distribution, etc.

Private Key

In private key, the same key (or secret key) is used by both the parties, i.e., the sender and receiver, for Encryption/Decryption technique.

The sender uses the secret key and encryption algorithm for encryption, whereas for decryption, the receiver uses this key and decryption algorithm. In Secret Key Encryption/Decryption technique, the algorithm used for encryption is the inverse of the algorithm used for decryption. It means that if the combination of addition and multiplication is used in the encryption algorithm, then the decryption algorithm will use the combination of subtraction and division.


Private Key Encryption (Symmetric)
Sender
Plaintext data
Ciphered Data
Decrypted Plaintext data
Recipient
Shared Secret (Key) Encrypts the Data
Shared Secret (Key) Decrypts the Data

The secret key encryption algorithm is also known as **symmetric encryption algorithm** because the same secret key is used in bidirectional communication. The mechanism of private key is faster than the mechanism of public-key cryptography. The reason for this is that the size of the key is small.

Public key v/s Private key

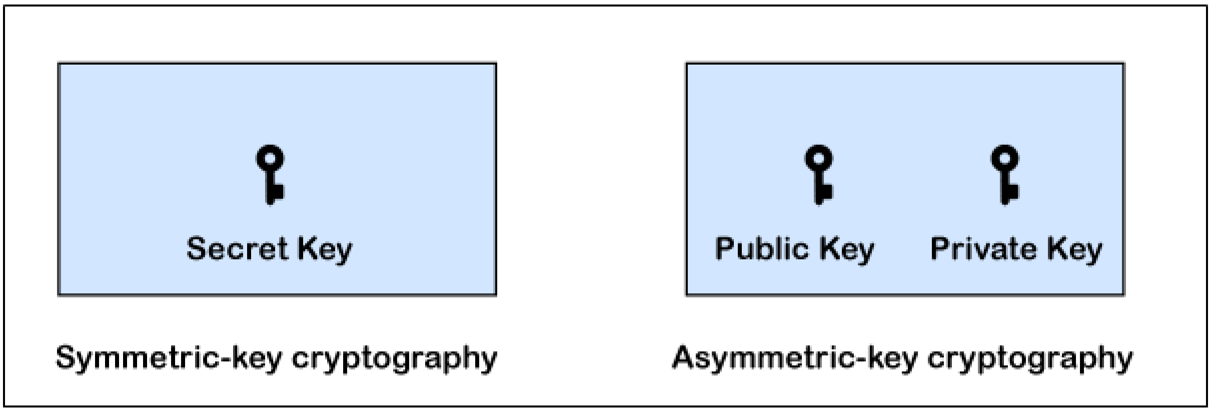
That's about the description of both public and private keys. Now, let's see the comparison chart between both keys. We are comparing both keys based on some characteristics.

On the basis of	Public key	Private key
Definition	It is defined as the technique that uses two different keys for encryption and decryption.	It is defined as the technique that uses a single shared key (secret key) to encrypt and decrypt the message.
Known as	It is also called as Asymmetric key encryption.	It is also called as symmetric key encryption. It is because the same secret key is used in bidirectional communication.
Efficiency	It is inefficient as this technique is used only for short messages.	It is efficient as this technique is recommended for large amounts of text.
Speed	It is slower as it uses two different keys; both keys are related to each	It is faster as it uses a single key for encryption and decryption.

	other through the complicated mathematical process.	
Secret	It is free to use.	Apart from the sender and receiver, the private key is kept secret and not public to anyone.
Purpose	The main purpose of the public key algorithm is to share the keys securely.	The main purpose of the secret key algorithm is to transmit the bulk data.
Loss of key	There is a less possibility of key loss, as the key held publicly.	There is a possibility of losing the key that renders the system void.

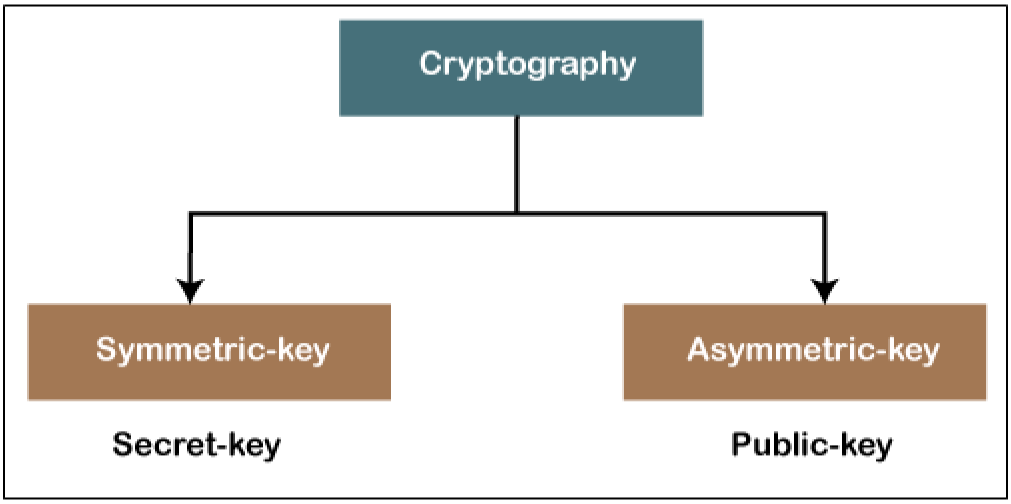
Que: 4 Explain different types of cryptography.

There are used three different types of the key in cryptography: a secret key, public key, and private key. The secret key is used in the symmetric-key cryptography, and the other two keys is used in the asymmetric key cryptography, as shown in the figure.



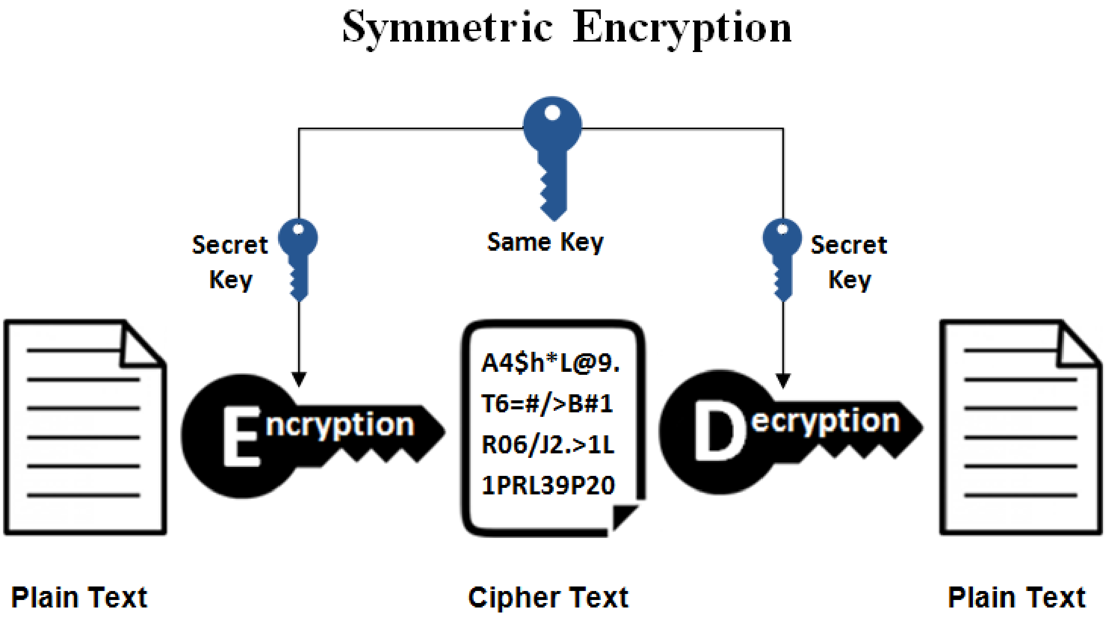
There are two types of cryptography

1. Symmetric key cryptography
2. Asymmetric key cryptography



Symmetric key cryptography

Symmetric key cryptography is that cryptography in which the same key (only one key) is used for encryption of plain text and decryption of ciphertext. Symmetric key cryptography is also known as secret-key cryptography.

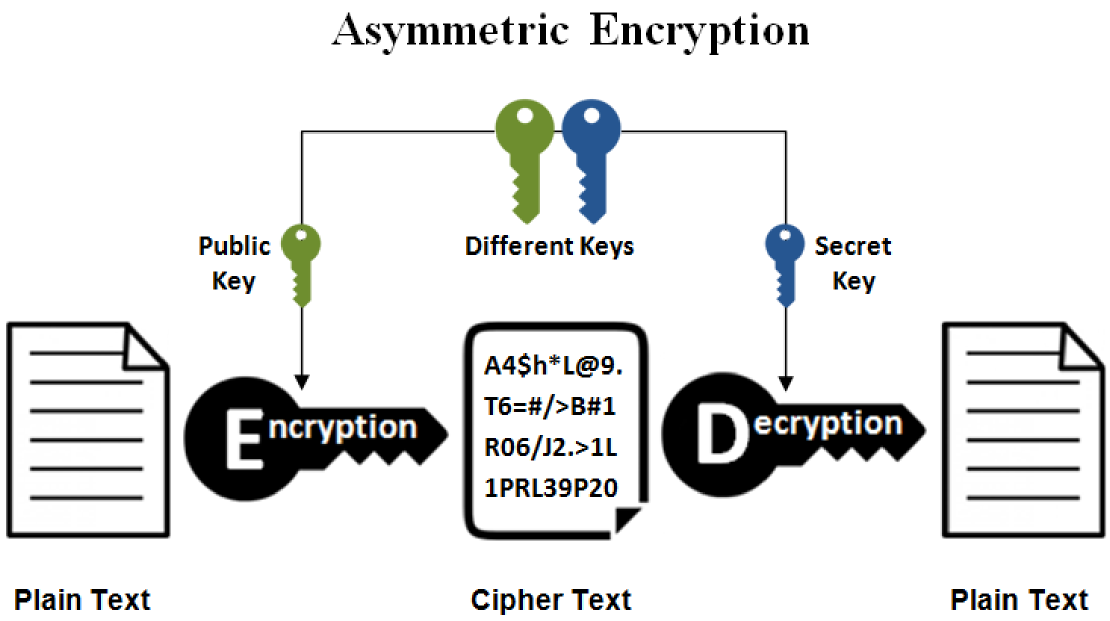


This is the simplest kind of encryption that involves only one secret key to cipher and decipher information. Symmetric encryption is an old and best-known technique. It uses a secret key that can either be a number, a word or a string of random letters. It is a blended with the plain text of a message to change the content in a particular way. The sender and the recipient should know the secret key that is used to encrypt and decrypt all the messages. Blowfish, AES, RC4, DES, RC5, and RC6 are examples of symmetric encryption. The most widely used symmetric algorithm is AES-128, AES-192, and AES-256.

The main disadvantage of the symmetric key encryption is that all parties involved have to exchange the key used to encrypt the data before they can decrypt it.

Asymmetric key cryptography

Asymmetric key cryptography is that cryptography in which both encryption and decryption have different keys. In this, the public key is used to do encryption, and the private key is used to do the decryption. It is also called public-key cryptography.



Asymmetric encryption is also known as public key cryptography, which is a relatively new method, compared to symmetric encryption. Asymmetric encryption uses two keys to encrypt a plain text. Secret keys are exchanged over the Internet or a large network. It ensures that malicious persons do not misuse the keys. It is important to note that anyone with a secret key can decrypt the message and this is why asymmetric encryption uses two related keys to boosting security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept a secret so that you can only know.

A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes ElGamal, RSA, DSA, Elliptic curve techniques, PKCS.

Que: 5 what is symmetric cryptography? Explain substitution and transposition cipher with example

Symmetric key cryptography is that cryptography in which the same key (only one key) is used for encryption of plain text and decryption of cipher text. Symmetric key cryptography is also known as secret-key cryptography.

Substitution Cipher

Hiding some data is known as encryption. When plain text is encrypted it becomes unreadable and is known as cipher text. In a Substitution cipher, any character of plain text from the given fixed set of characters is substituted by some other character from the same set depending on a key. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

Mathematical representation

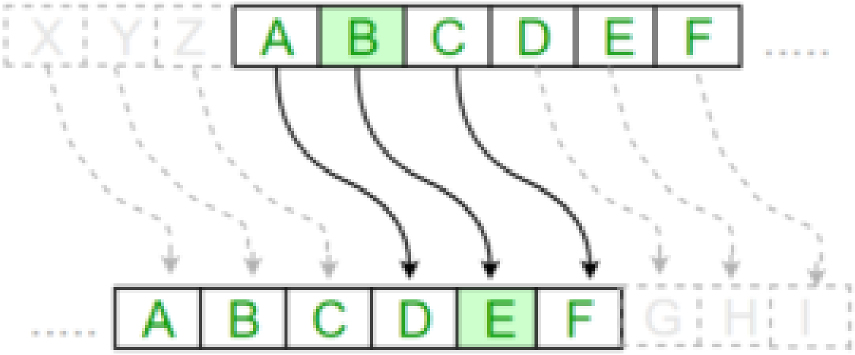
The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,..., Z = 25. Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)



Assistant Professor:Vinod.M.Makwana

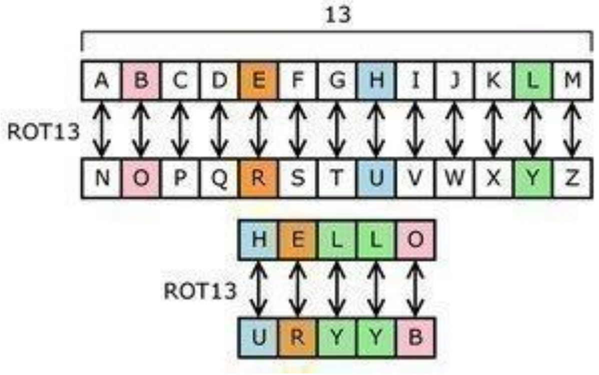
Examples [1]:key-4

Plain Text: I am studying Data Encryption
Key: 4
Output: M eq wxyhCmrk Hexe IrgvCtxmsr

Plain Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Key: 4
Output: EFGHIJKLMNOPQRSTUVWXYZabcd

EXAMPLE [2]: key-13

"VOYAGER" being encrypted with the Caesar substitution cipher:



Example: 3 key-3

Plaintext	V	O	Y	A	G	E	R
Key	+3	+3	+3	+3	+3	+3	+3
Ciphertext	Y	R	B	D	J	H	U

Example 4: key 123

A more complex substitution cipher would be created if, instead of incrementing each character by three, we used a more complex key. This table shows a simple substitution cipher with a key of “123”.

Plaintext	V	O	Y	A	G	E	R
Key	+1	+2	+3	+1	+2	+3	+1
Ciphertext	W	Q	B	B	I	H	S

Transposition cipher

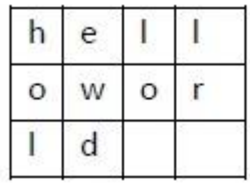
- Transposition cipher changes the position of symbols instead of substituting one character for another.
- It rearranges the location of plain text characters.
- In this technique the location of the character is changed other than the identity of the character is not changed.
- Transposition ciphers are of two kinds, Keyless and Keyed transportation cipher.
- The long sections of readable plaintext will be disclosed by keys that were neared to the right key.
- Rail fence Cipher is the best example of Transposition Cipher

Example of Transposition cipher

[1]This table shows “VOYAGER” being encrypted with a primitive transposition cipher where every two letters are switched with each other:

V	O	Y	A	G	E	R
O	V	A	Y	E	G	R

[2]Consider the plain text **hello world**, and let us apply the simple columnar transposition technique as shown below



h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as **: holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.