SNS COLLEGE OF TECHNOLOGY
Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

19ECT301-COMMUNICATION NETWORKS III YEAR/ V SEMESTER

UNIT 4- NETWORK & DATA SECURITY

TOPIC –Introduction to Cryptography

Introduction

Cryptography:

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit.

German **Lorenz cipher** machine, used in **World War II** to encrypt very-high-level **general staff** messages.

History

BCE: Spartan use of scytale, the Egyptians develop *hieroglyphic* writing and Notable Roman ciphers such as the Caesar cipher.

1-1799: Leon Battista Alberti invents **polyalphabetic cipher**, also known first mechanical cipher machine.

1800-1899: Joseph Henry builds an electric. In Crimean War, Charles Babbage broke Vigenère's autokey cipher (the 'unbreakable cipher' of the time).

1900-1949: First break of German Army Enigma by Marian Rejewski in Poland.

1950-1999: Charles Bennett and Gilles Brassard design the first quantum cryptography protocol, BB84.

2000 to present: Microsoft and its allies vow to end "full disclosure" of security vulnerabilities by replacing it with "responsible" disclosure guidelines.

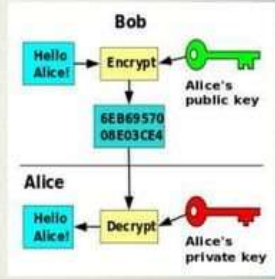
Classic cryptography

The Greek's idea on cryptography was to wrap a tape around a stick, and then write the message on the wound tape. When the tape was unwound, the writing would be meaningless. The receiver of the message would of course have a stick of the same diameter and use it to decipher the message.

Reconstructed **ancient Greek** ***scytale***, an early cipher device.

Computer era

Cryptanalysis of the new mechanical devices proved to be both difficult and laborious. Just as the development of digital computers and electronics helped in cryptanalysis, it made possible much more complex ciphers. Furthermore, computers allowed for the encryption of any kind of data representable in any binary format, unlike classical ciphers which only encrypted written language texts.



An example of simple cryptography

Terminology

Plaintext:

Message that is going to be transmitted or stored is plain text. Anyone can read plaintext.

Encryption:

The method by which we can hide the actual meaning of plaintext is called Encryption.

Cipher text:

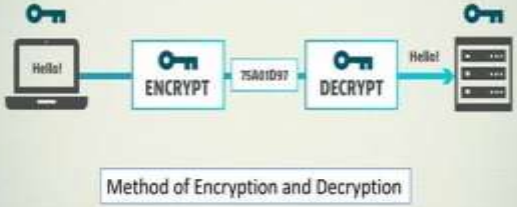
The result of encryption which results in unreadable gibberish is called Cipher text.

Decryption:

The method by which the original meaning of cipher text can be recovered is called Decryption. Simply the process of converting Cipher text to plaintext is called Decryption.

Key:

Key is the secret piece of information which is used for encryption and decryption in Cryptography.



Method of Encryption and Decryption

❖ Some more terms:

Cryptanalysis:

The science of retrieving the plain text from cipher without knowing the key.

Cryptanalysts:

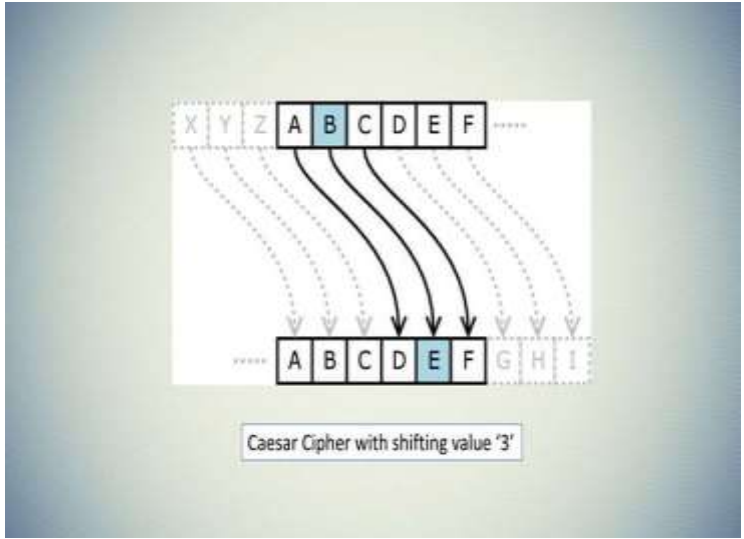
The people who practice cryptanalysis are called Cryptanalyst.

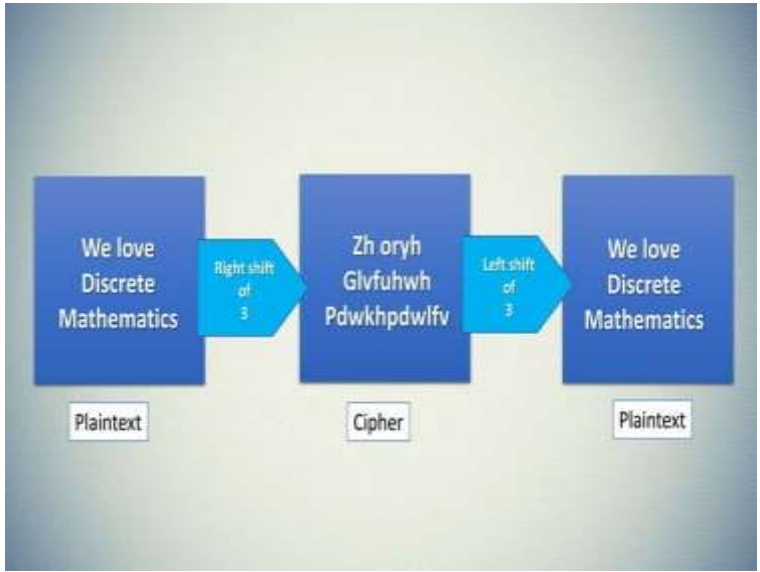
Cryptosystem:

The combination of algorithm, key, and key management functions used to perform cryptographic operations.

❖ Caesar Cipher

The Caesar cipher, also known as a shift cipher, is one of the simplest forms of encryption. It is a substitution cipher where each letter in the original message (called the plaintext) is replaced with a letter corresponding to a certain number of letters up or down in the alphabet.

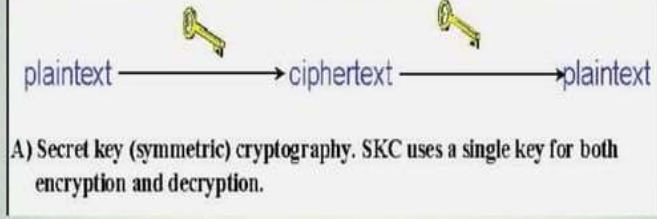

X Y Z A B C D E F
A B C D E F G H I
Caesar Cipher with shifting value '3'


We love Discrete Mathematics
Right shift of 3
Zh oryh Glvfuhwh Pdwkhpdwlfv
Left shift of 3
We love Discrete Mathematics
Plaintext
Cipher
Plaintext

Cryptography Methods

Symmetric Key:

With Symmetric key Cryptography, a single key is used for both encryption and decryption. In this figure we can see that the sender uses the key to encrypt the plain text and send the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plain text because a single key is used for both function. Symmetric key Cryptography is also called secret key Cryptography. With this from of Cryptography, it is obvious that the key must be known to both the sender and the receiver.

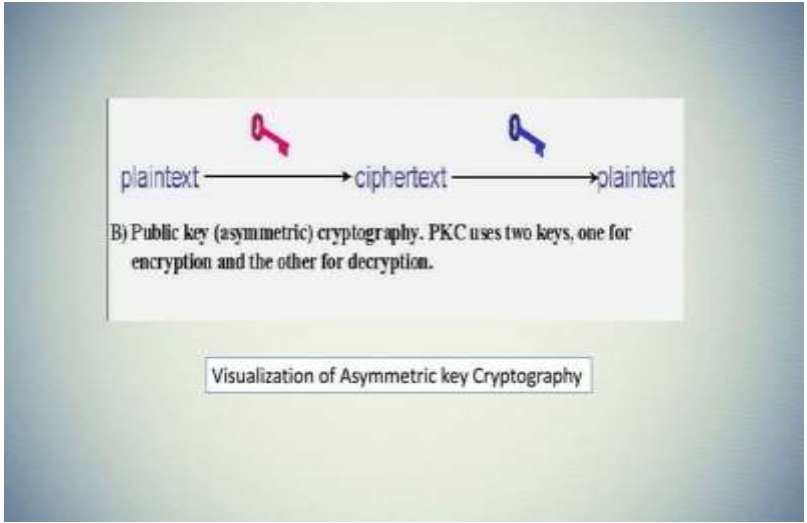


A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

Visualization of Symmetric key Cryptography

Asymmetric Key:

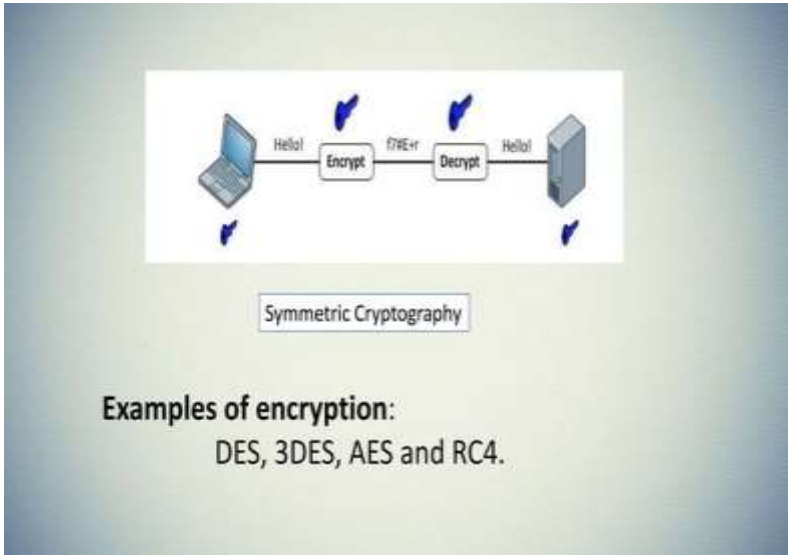
Asymmetric cryptography was first publicly described by martin Hellman and his student Whitfield Diffie in 1976. There are two different keys are used for encryption and decryption. One key is used to encrypt the plaintext and the other key is used to decrypt the cipher text the important point is that it doesn't matter which key is applied first but the both key is required for the work. Every user has both a public key and a private key. The private key is kept secret at all times, but the public key may be freely distributed.

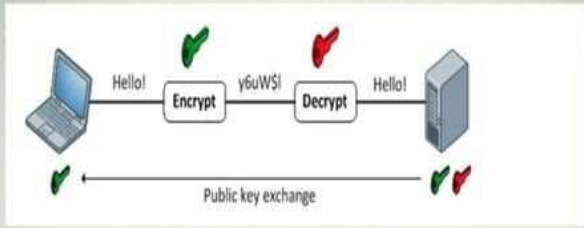


Visualization of Asymmetric key Cryptography

Difference between Methods

SYMMETRIC KEY CRYPTOGRAPHY	ASYMMETRIC KEY CRYPTOGRAPHY
1) The same algorithm with the same key is used for encryption and decryption.	1) One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2) The key must be kept secret.	2) One of the two keys must be kept secret.
3) It may be impossible or at least impractical to decipher a message if no other information is available.	3) It may be impossible or at least impractical to decipher a message if no other information is available.


Hello!
Encrypt
f78E+r
Decrypt
Hello!
Symmetric Cryptography
Examples of encryption:
DES, 3DES, AES and RC4.



Asymmetric Cryptography

Examples of encryption:

The most common asymmetric encryption algorithm is RSA

Applications

1. ATM
2. Email-Passwords
3. E-Payment
4. E-Commerce
5. Electronic Voting
6. Defence Services
7. Securing Data
8. Access Control


Thank You!