Cryptography – Encryption/Decryption

Cryptography (Encryption / Decryption)

- What is Cryptography?
- What is Encryption / Decryption?
- What are the types of Cryptography?
- What is a Key?
- What is Block Cipher?
- Encryption / Decryption Techniques
  - DES
  - AES

What is Cryptography?

Cryptography derived its name from a Greek word called “Kryptos” which means “Hidden Secrets”.

Cryptography is the practice and study of hiding information. It is the Art or Science of converting a plain intelligible data into an unintelligible data and again retransforming that message into its original form.

It provides
Confidentiality, Integrity, Accuracy.

What is Encryption / Decryption

- Encryption –
  - The process of converting plain text into an unintelligible format (cipher text) is called Encryption.
- Decryption –
  - The process of converting cipher text into a plain text is called Decryption.

What are the Types of Cryptography

- **Symmetric Key Cryptography (Secret Key Cryptography)**
  - **Same Key is used by both parties**

Advantages

1. **Simpler and Faster**

Disadvantages

1. **Less Secured**

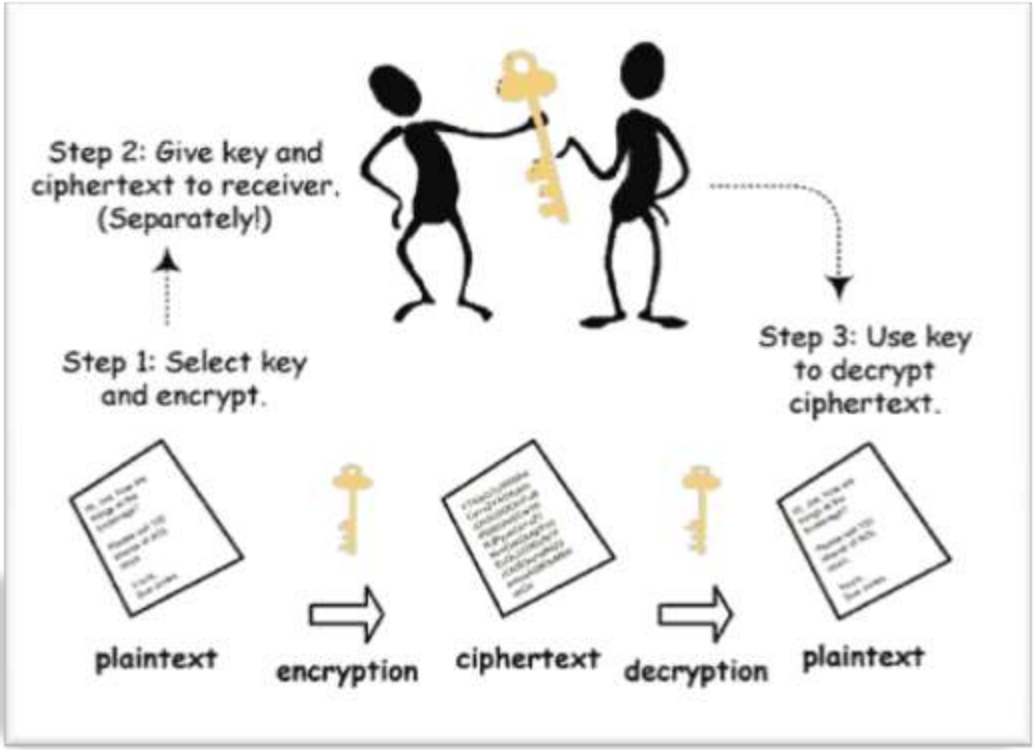

Image taken from :-

www.google.com

- **Asymmetric Key Cryptography (Public Key Cryptography)**
  - **2 different keys are used**
  - **Users get the Key from an Certificate Authority**

Advantages

1. **More Secured**
2. **Authentication**

Disadvantages

1. **Relatively Complex**

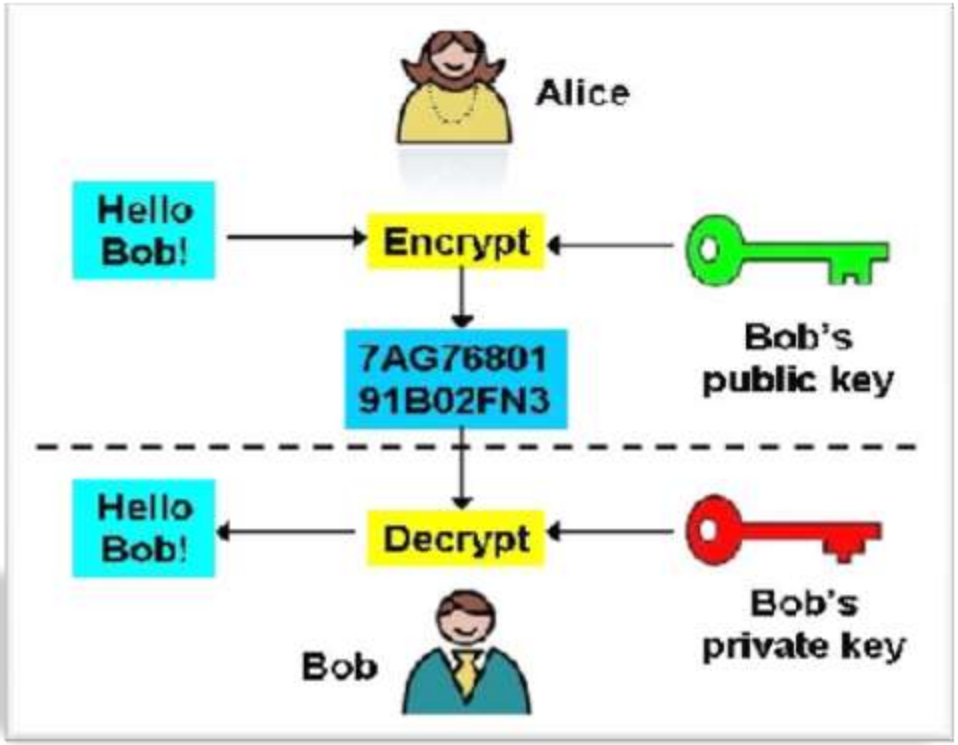

Image taken from :-

www.google.com

- **What is a Key**
  - **In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.**

- **What is a Block Cipher?**
  - **A method of encrypting / decrypting data**
  - **Key is used for encryption / decryption.**
  - **Same size of I/P and O/P**

- **What is Initialization Vector?**
  - **An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption.**
  - **It is a group of hex values.**

- **What is DES?**
  - **The Data Encryption Standard (DES) is a previously predominant algorithm used for encryption/decryption of electronic data. DES was developed in the early 70's by IBM which was then submitted to the National Bureau of Standards (NBS).**
  - **Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.**
  - **DES uses a 56 bit encryption key which can give around 2^56 (ie) 256 combinations to encrypt the plain text. DES is restricted with a Block Size of just 64bits.**
  - **Sometimes DES is said to use 64 bit key, but 8bits out of it is used for some other purpose.**
  - **The maximum amount that can be transferred with a single encryption is 32GB. DES uses the Feistel Network which divides block into 2 halves before going through the encryption steps.**

- **What is AES?**
  - **The Advanced Encryption Standard (AES) is a specification for the Encryption of electronic data. Originally called "Rijndael" the cipher was developed by 2 Belgian Cryptographers "Joan Daemen" and "Vincent Rijmen" who submitted to the AES Selection process held by the NIST (National Institute of Standards and Technology) in the year 1997 which continued for 3 years and the end result was given on 2nd October 2002 where Rijndael was chosen as the proposed standard.**
  - **The algorithm described by AES is a Symmetric-Key Algorithm, meaning the same key is used for encrypting and decrypting the data. AES standard is a variant of Rijndael where the block size is restricted to 128bits and the key size of 128, 192, 256 bits can be used.**
  - **AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware.**

DES Encryption	AES Encryption
DES uses only 56 bits key which provides a combination of 2^56 = 256 combinations for encryption.	AES can use 128, 192, 256 bits keys which provides 2^128, 2^192, 2^256 combinations for encryption.
DES is restricted to use a Block Size of only 64 bits	AES is restricted to use a Block Size of 128 bits (double of what is used in DES)
With 64 bits block size, the amount of data that can be transferred with a single encryption key is just 32GB.	With AES, it is possible to transfer around 256 billion GB of data. It is probably safe to say that you can use a single AES encryption key for any application.
DES uses a Feistel network, which divides the block into 2 halves before going through the Encryption steps.	AES uses Permutation-Substitution method, which involves a series of substitution and permutation steps to create the encrypted block.
DES encryption is breakable through Brute Force attack.	AES encryption on the other hand is still not breakable, though there are some theoretical discussions about breaking the AES.
DES is an old technique used for encryption/decryption	AES is relatively new.
Time required to check all the possible keys at 50 billion keys per second – For a 128-bit key: $5x10^{21}$ years (which makes it difficult for the hackers to decrypt the data)	Time required to check all the possible keys at 50 billion keys per second – For a 56-bit key: 400 days.

THANK YOU