Unit – 03: Symmetric-Key Cryptography

- Glosis field theory,
- AES, overview of Rijndael comparison with others.
- Symmetric ciphers,
- Blowfish in practice,
- RC4, RC5, RC6, IDEA, RSA

Questions to be discussed:

1. What do you mean by Glosis field theory explain with example?
2. Write the difference between AES and DES.
3. Differentiate between block cipher and stream cipher.
4. Explain RC4, RC5 and RC6 in brief.
5. Write short notes on:
    a. Rijndael algorithm
    b. Blowfish
    c. IDEA
    d. RSA

Symmetric-Key Cryptography:

- In cryptography Symmetric-key algorithms are algorithms that use the same cryptographic keys for both the encryption of plaintext and the decryption of cipher text.
- The keys may be identical, or there may be a simple transformation to go between the two keys.

Galois fields theory:

- Galois field named after Evariste Galois also known as Finite Field.
- It is a set of numbers that consists of a finite number of elements.
- It has two operations, addition and multiplication, that follow specific rules.
- The rules for these operations ensure that the Galois Field remains closed.
- That means the result of any operation performed within the set will also be an element of the set.
- Galois Fields are useful in various fields, such as cryptography, coding theory, and error correction, due to their unique mathematical properties.
- The size of a Galois Field is represented by a prime number 'p', and it is denoted by GF(p), where p is a prime number.

  Example:

  - One example of a Galois Field is a field with 2 elements, denoted by GF(2).
  - This field has two elements, 0 and 1, and the rules for addition and multiplication operations are defined as follows:

  1. **Addition:** The addition operation in GF(2) is equivalent to the XOR operation.
     For example, $0 + 0 = 0$, $0 + 1 = 1$, and $1 + 1 = 0$.
  2. **Multiplication:** The multiplication operation in GF(2) is equivalent to the AND operation.
     For example, $0 * 0 = 0$, $0 * 1 = 0$, and $1 * 1 = 1$.

Advanced Encryption Standard (AES):

- AES stands for Advanced Encryption Standard.
- It 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.

Difference between AES and DES:

AES	DES
AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
The date of creation is 2001.	The date of creation is 1977.
Byte-Oriented.	Bit-Oriented.
Key length can be 128-bits, 192-bits, and 256-bits	The key length is 56 bits in DES.
Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
It can generate Ciphertext of 128, 192, 256 bits.	It generates Ciphertext of 64 bits.
AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.
It is faster than DES.	It is slower than AES.
It is flexible.	It is not flexible.
It is efficient with both hardware and software.	It is efficient only with hardware.

Rijndael Algorithm:

- It is a symmetric key algorithm.
- Rijndael Algorithm also called Advance Encryption Standard(AES).
- Rijndael is a family of Ciphers having distinctive keys and block sizes.
- The algorithm changed into created by way of the cryptologists, Joan Daemen and Vincent Rijmen.
- The word Rijndael was derived from their surnames.
- It's a block cipher that works iteratively.
- Block size available in three different bit key versions that are 128-bit size, 192-bit size or 256-bit size.

Symmetric ciphers:

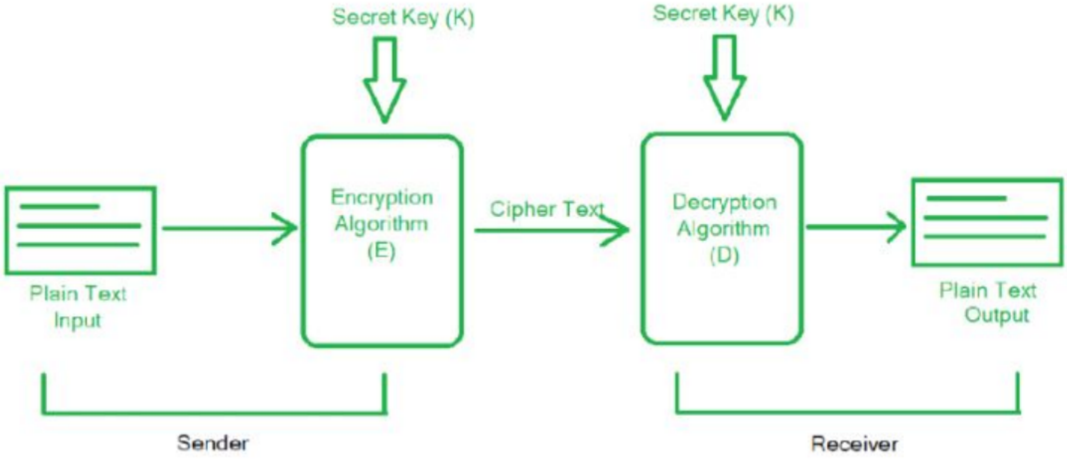
- Symmetric Encryption is the most basic and old method of encryption.
- It uses only one key for the process of both the encryption and decryption of data.
- Thus, it is also known as Single-Key Encryption.
- A few basic terms in Cryptography are as follows:

Plain Text: original message to be communicated between sender and receiver

Cipher Text: encoded format of the original message that cannot be understood by humans

The Symmetric Cipher Model:

A symmetric cipher model is composed of five essential parts:



What is Blowfish?

- Blowfish is a variable-length, symmetric, 64-bit block cipher.
- Designed by Bruce Schneier in 1993 as a "general-purpose algorithm.
- It was intended to provide a fast, free, drop-in alternative to the aging DES & IDEA.
- Blowfish is significantly faster than DES and IDEA and is unpatented and available free for all uses.
- However, it couldn't completely replace DES due to its small block size, which is considered insecure.
- Blowfish features a 64-bit block size and takes a variable-length key, from 32 bits to 448 bits.
- Blowfish uses a single encryption key to both encrypt and decrypt data.

What is cipher?

- Ciphertext is encrypted text.
- It is transformed from plaintext using an encryption algorithm.
- Ciphertext can't be read until it has been converted into plaintext (decrypted) with a key.
- The decryption cipher is an algorithm that transforms the ciphertext back into plaintext.
- The term cipher is sometimes used as a synonym for ciphertext.

Difference between block cipher and stream cipher:

Block Cipher	Stream Cipher
Block Cipher is the kind of encryption that converts plaintext by taking each block individually.	Stream cipher is the kind of encryption that converts plaintext by taking one byte of the plaintext at a time.
It uses both diffusion and confusion principles for the conversion (used later in encryption).	Only the confusion principle is used by Stream Cipher for the conversion.
In Block cipher, decryption is more difficult than stream cipher.	In a stream cipher, XOR is used for encryption that can quickly converted back to plain text.
Block Cipher uses both confusion and diffusion.	Stream cipher relies on confusion only.
Simple design	Complex comparatively
64 Bits or more	8 Bits

RC4:

- RC4 stands for Rivest Cipher 4 or Ron's Code 4.
- RC4 is a form of stream cipher.
- It encrypts messages one byte at a time.
- RC4 is a variable key-size stream cipher with byte-oriented operations.
- The RC4 cipher became the most widely used stream cypher due to its speed and simplicity.
- It is used in common protocols such as Wired Equivalent Privacy(WEP), Secure Sockets Layer(SSL) and Transport Layer Security (TLS).

RC5:

- RC5 stands for "Rivest Cipher 5", or alternatively, "Ron's Code 5".
- RC5 is a form of block cipher.
- In cryptography, RC5 is a symmetric-key block cipher notable for its simplicity.
- RC5 is a 32/64/128-bit block cipher developed in 1994.
- It is notable for being simple, fast and consumes less memory.
- RC5 is known for its fast encryption and decryption speeds.
- It uses simple mathematical operations such as modular arithmetic and bit shifting, which can be efficiently implemented on modern CPUs and hardware.

RC6:

- RC6 stands for "Rivest Cipher 6", or alternatively, "Ron's Code 6".
- RC6 is a form of block cipher.
- RC6 is a 128-bit block cipher based on RC5, was developed in 1997.
- Its variable block size and key size make it highly adaptable to different applications or system.
- RC6 encryption is widely used in various industries, including data protection, network security, and digital rights management.

IDEA:

- IDEA stands for International Data Encryption Algorithm
- It is a symmetric-key block cipher that was first introduced in 1991.
- IDEA is considered to be a good and secure algorithm.
- IDEA uses a block cipher with a block size of 64 bits and a key size of 128 bits.
- The cipher is designed to be highly secure and resistant to various types of attacks.
- It was designed to provide secure encryption for digital data and is used in a variety of applications, such as secure communications, financial transactions, and electronic voting systems.

RSA:

- RSA is the most common public-key algorithm.
- It was invented in 1978 by scientists Rivest, Shamir and Adleman.
- RSA is a public-key encryption method used in data security.
- This algorithm is safe and reliable for the transfer of data across the internet.
- It takes care of the privacy of the data.
- The process of implementing the RSA algorithm is quite simple.
- RSA is safe and reliable for mechanisms, hence, there is no risk in sending private data.