CECS 378: Intro to Computer Security Principles

Lecture 2

Louis Uuh

Week 2

What is Cryptography?

- Is the science of keeping information secure
  - In the sense of confidentiality and integrity (hashing)
- Commonly referred to as encryption
  - It is a subset of cryptography
  - Transformation of unencrypted data, called plaintext or clear text to its encrypted form
- Decryption is the process of recovering the plaintext message
- The science of breaking through encryption is referred to as cryptanalysis

Symmetric Encryption

- Two of the most important symmetric encryption algorithms
  - ➢Data Encryption Standard (DES)
  - ➢ Advance Encryption Standard (AES)
- Often refer to as conventional encryption or single-key encryption
- Was the only type of encryption prior to public key encryption in the late 1970s
- It is still the more widely used between the two types of encryption

5 Ingredients of Symmetric Encryption

- Plaintext
  - Original message or data to be fed
- Encryption algorithm
  - Algorithm use to perform various substitutions and transformations to the plaintext
- Secret key
  - Input to the encryption algorithm, exact substitutions and transformations dependent on the key
- Ciphertext
  - Scrambled message produced as the output.
- Decryption algorithm
  - Essentially the encryption algorithm run in reverse. It takes the ciphertext and secret key and produces the original plaintext.

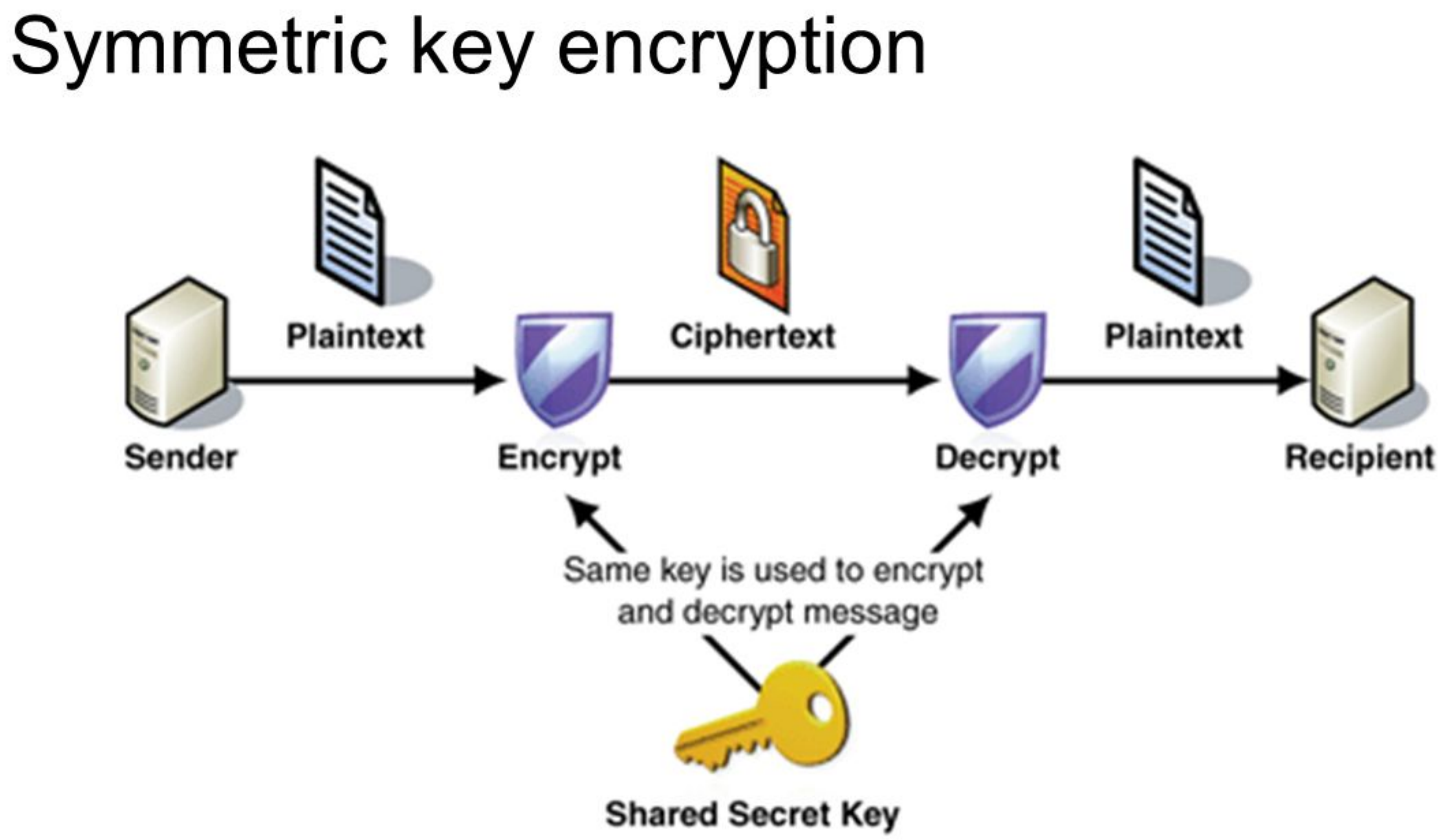
Symmetric Block Encryption Algorithm

- Most commonly used algorithm
- Processed the plaintext input in fixed-size blocks and produces a block of ciphertext of equal size for each plaintext block
- Most important algorithms DES, Triple DES, and AES

Symmetric Cryptography

- Known as Private Key Cryptography
- Single key for both encryption and decryption
- Symmetric key cryptography by itself can only provide confidentiality, and not integrity
- Currently using AES block cipher, supporting:
  - 128 – bit key
  - 192 – bit key
  - 256 – bit key

Symmetric Cryptography



DES Algorithm

- Adopted by National Institute of Standards and Technology (NIST) in 1977
- Refer to as the Data Encryption Algorithm (DEA)
- It takes a plaintext block of 64 bits and a key of 56 bits, to produce a ciphertext block of 64 bits

Triple DES Algorithm

BEACH

- Successor to DES
- Same algorithm, but it involves repeating the algorithm 3 times. Using either two or three unique keys
- Key size of 112 or 168 bits
- Two main attractions for 3DES
  - Its 168-bit key length ,which overcomes the brute-force vulnerability of DES
  - The algorithm has been subjected to more scrutiny than any other algorithm and no effective cryptanalytic attack has been found

AES Algorithm

- Successor to DES
- Same algorithm, but it involves repeating the algorithm 3 times. Using either two or three unique keys
- Key size of 112 or 168 bits
- Two main attractions for 3DES
  - Its 168-bit key length ,which overcomes the brute-force vulnerability of DES
  - The algorithm has been subjected to more scrutiny than any other algorithm and no effective cryptanalytic attack has been found

Symmetric Encryption Algorithms

BEACH

	DES	Triple DES	AES
Plaintext block size (bits)	**64**	**64**	**128**
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

2 General Attacks for Symmetric

- Cryptanalysis
  - Rely on the nature of the algorithm plus having some knowledge of the general characteristics of the plain text
  - Main purpose is to try to deduce a specific plaintext or to deduce the key being used
- Brute-force attack
  - Tries every single possible key on a piece of ciphertext
  - Compression can make this a bit difficult

Feistel Cipher Structure

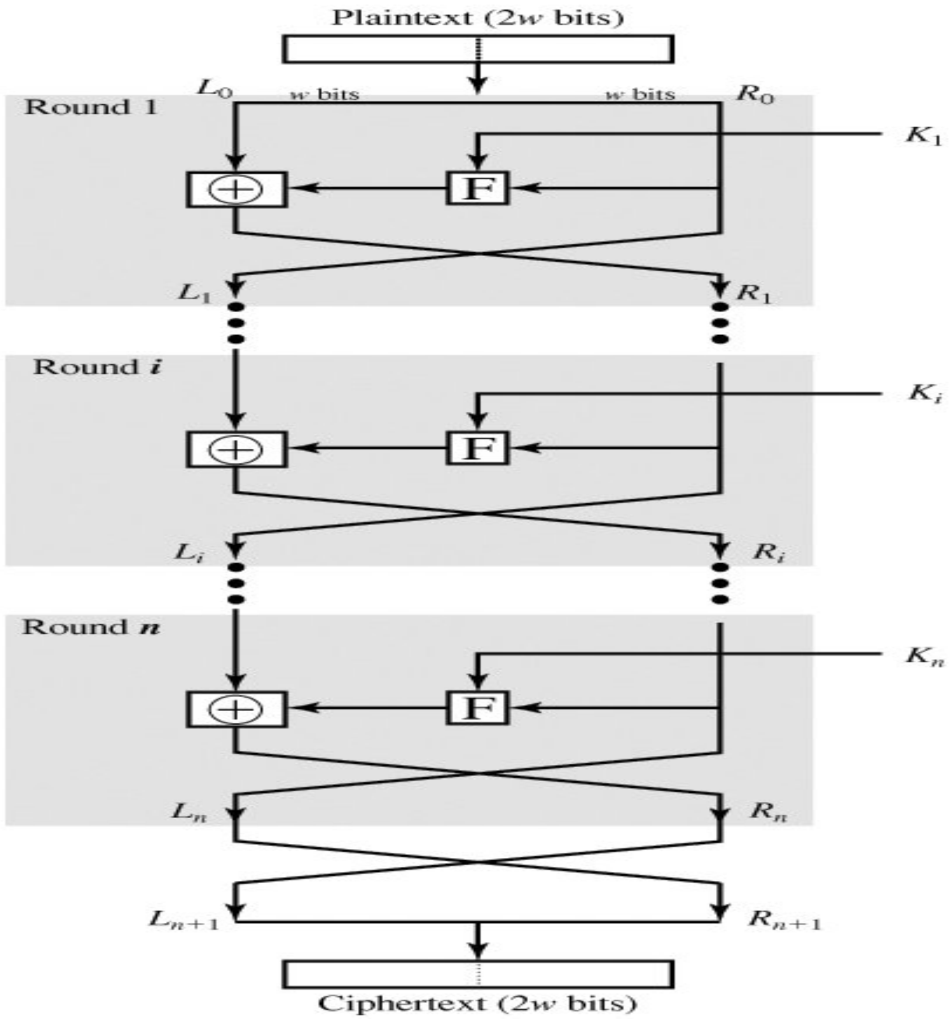
- Horst Feistel devised the Feistel cipher
  - based on concept of invertible product cipher
- Most Block cipher techniques will follow the Feistel structure
- The first step in the Feistel structure states that the plain text should be broken down into two halves
  - process through multiple rounds which:
  - perform a substitution on left data half
  - based on round function of right half & sub key
  - then have permutation swapping halves

Feistel Cipher Structure

BEACH

- Virtually all conventional block encryption algorithms including data encryption standard (DES) are based on Feistel Cipher Structure.
- The plaintext is divided into two halves
  - Then the two halves pass through *n* rounds of processing then combine to produce the cipher block.
- Each round i has as input L_{i-1} and R_{i-1} derived from the previous round as well as a sub-key K_i derived from the overall K

Feistel Cipher Structure



Feistel Cipher Design Principles

BEΛCH

- **Block Size:** (larger block means greater security) 64 bits
- **Key Size**:56 bits
- **Number of Rounds**: a single round offers inadequate security, a typical size is 16 rounds
- **Sub-key Generation Algorithms**: greater complexity should lead to a greater difficulty of cryptanalysis
- **Round function:** Again, greater complexity generally means greater resistance to cryptanalysis

Feistel Cipher Design Principles

- **Block Size:** (larger block means greater security) 64 bits
- **Key Size**:56 bits
- **Number of Rounds**: a single round offers inadequate security, a typical size is 16 rounds
- **Sub-key Generation Algorithms**: greater complexity should lead to a greater difficulty of cryptanalysis
- **Round function:** Again, greater complexity generally means greater resistance to cryptanalysis

Feistel Cipher Design Principles