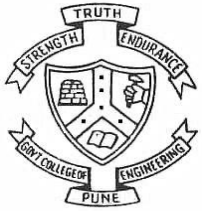
Cryptography and Network Security

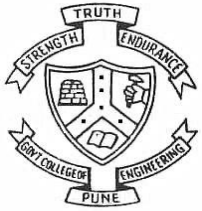
Session 13

Dr. V. K. Pachghare



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

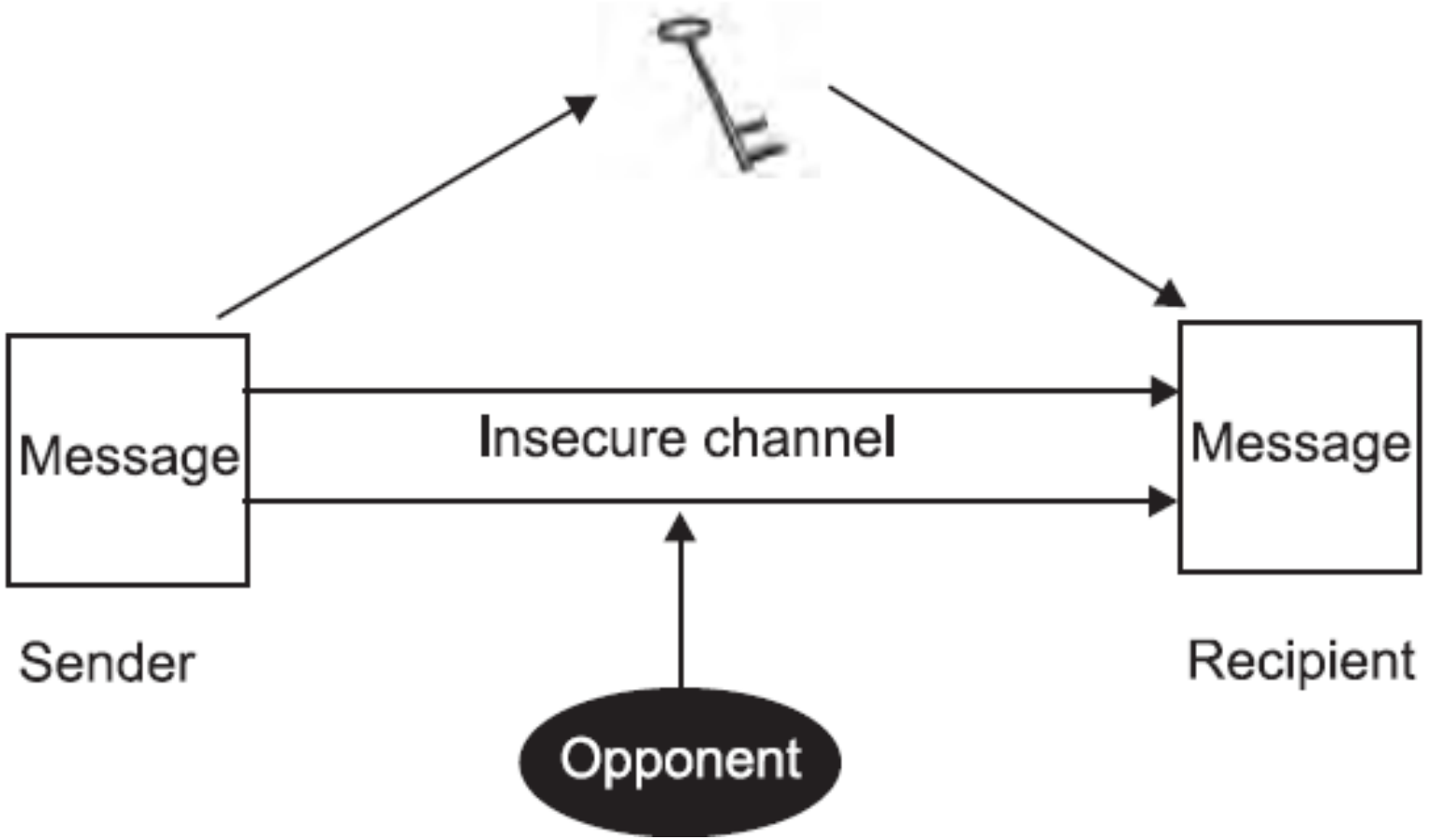
ENCRYPTION TECHNIQUES



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

- Encryption techniques are useful to provide the confidentiality to the data.
- Encryption techniques are :
- block encryption techniques and
- stream encryption techniques.
- This classification is based on the number of bits processed at a time.

- Block cipher: a block of fixed number of bits is processed at a time
- Stream cipher: one bit is processed at a time.
- Block ciphers are faster than stream cipher.


Message
Insecure channel
Message
Sender
Recipient
Opponent

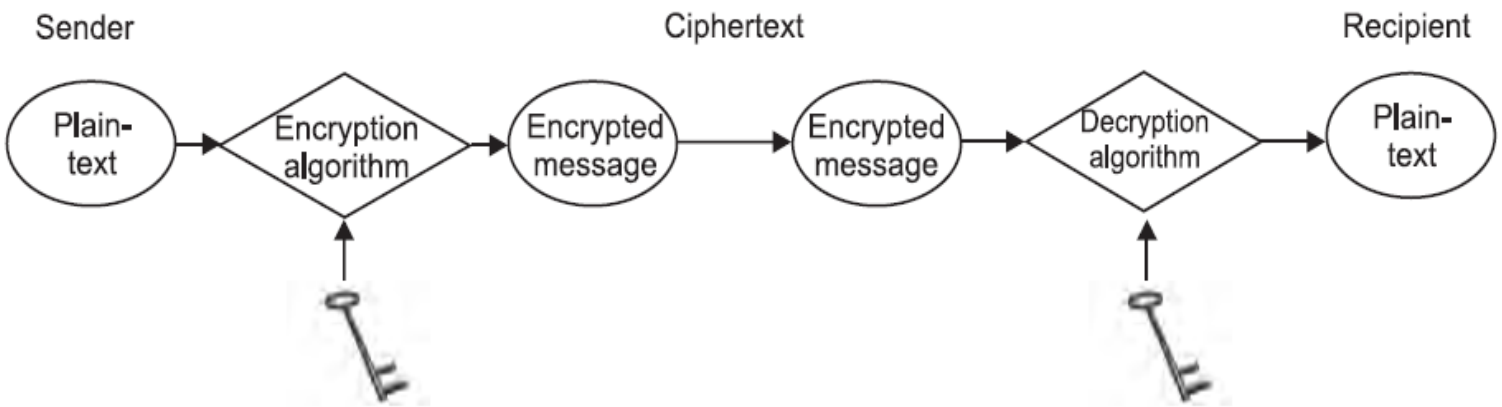
Types of Encryption

- Symmetric Encryption
- Asymmetric Encryption (Public key cryptography)

Symmetric Encryption

- Only one key is required
- The same key is used for encryption as well as decryption of the data.
- DES, AES, IDEA, and 3DES

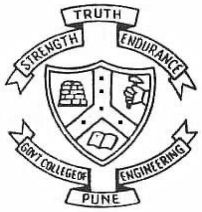
Components of Symmetric Encryption



Asymmetric Encryption

- Two different keys are required
- keys are mathematically related to each other.
- called public key and private key
- The key which is publically available for all are called public key
- The key which is known only to the owner of the key is called private key.
- Diffie-Hellman, RSA, and Elliptic Curve Cryptography (ECC)

Symmetric Encryption



Department of Computer Engineering and Information Technology
College of Engineering Pune (COEP)
Forerunners in Technical Education

Feistel Structure

- Building block for many block ciphers
- The design of data encryption standard (DES) algorithm is based on Feistel structures

- The plaintext is split into the blocks of equal size
- Each block is split into two equal parts: left part and right part
- The Feistel structure has many rounds and each round has different subkeys

- Subkeys are generated from the key entered by the user
- The security of Feistel cipher depends on the key size and hash function

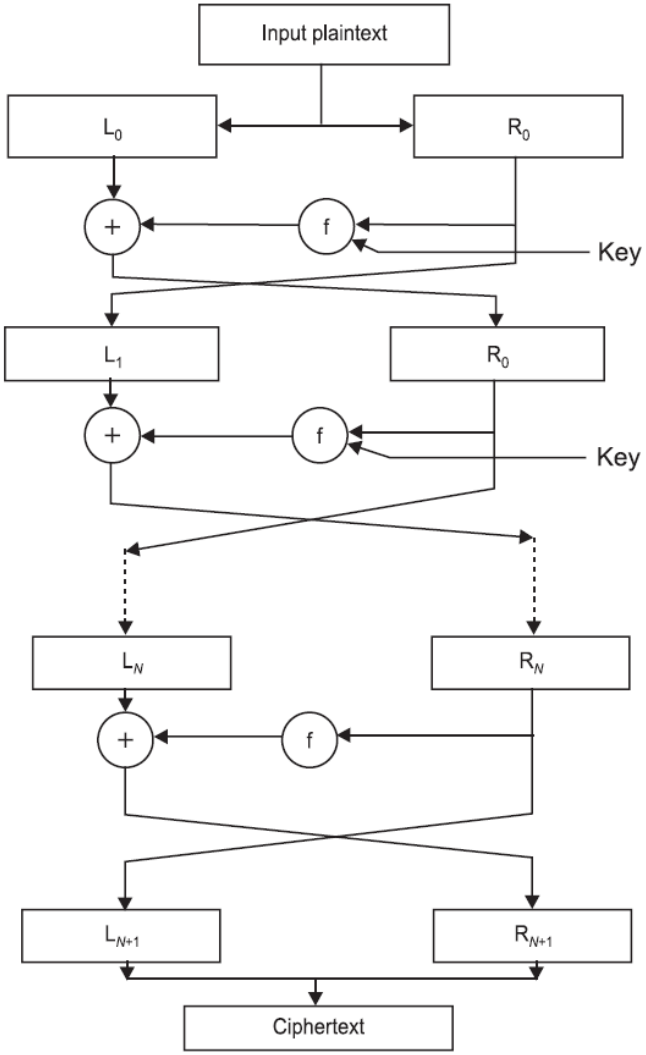
The Design Parameters

1. Block size
2. Key length
3. Number of rounds
4. Subkeys
5. Round function

1. **Block size:** Block size indicates the total number of bits in a block. Larger block sizes mean greater security
2. **Key length:** It is the length of key. Larger key sizes mean greater security but may reduced the speed
3. **Number of rounds:** The security of any block ciphers depend on the number of rounds in the cipher. Multiple rounds offer increasing security.

4. **Subkeys:** Each round uses different keys called subkeys. These subkeys are derived from an original key. Greater complexity in this algorithm should lead to greater difficulty in cryptanalysis

5. **Round function:** The mathematical operation performs on each plaintext block in each round called round function. Greater complexity means greater resistance to cryptanalysis


Input plaintext
L_0
R_0
+
f
Key
L_1
R_0
+
f
Key
L_N
R_N
+
f
L_{N+1}
R_{N+1}
Ciphertext

Questions?

vkp.comp@coep.ac.in