CRYPTOGRAPHY

BY......
• Shaista Khan...07-184
• Nirali Supe......06-1
CRYPTOGRAPHY

- Has Greek origin

- Combination of two words
  
  *Krupto* (Secret) + *Graft* (Writing)

- First documented use of cryptography in writing dates back to circa 1900 B.C.
**DEFINITION**

- *Cryptography* is science of converting a stream of text into coded form in such a way that only the originator and receiver of the coded text can decode the text.

- *Cryptology* = *Cryptography* + *Cryptanalysis.*
MODEL OF CRYPTOGRAPHY

The Term Used In Cryptography

**Intruder**: Intruder is a person who is not authorized to access the information.

**Plain text**: It is human language.

**Cipher text**: Encoded message.

**Encryption**: Encoding plain text to cipher text.

**Decryption**: Decoding cipher text to plain text.
Two types of cipher text

- **Stream cipher**: It operates on a single bit (byte or computer word) at a time and implements some form of feedback mechanism so that the key is constantly changing.

- **Block cipher**: It encrypts one block of data at a time using the same key on each block.
Important 4 modes for block cipher

- **Electronic Codebook (ECB) mode**:
  In this, the secret key is used to encrypt the plaintext block.

- **Cipher Block Chaining (CBC) mode**:
  In this, the plaintext is XORed with the previous cipher block.
• **Cipher Feedback (CFB) mode:**
  CFB mode allows data to be encrypted in units smaller than the block size.

• **Output Feedback (OFB) mode:**
  Prevents the same plaintext block from generating the same cipher text block by using an internal feedback mechanism.
PROCESS OF CRYPTOGRAPHY

Encryption method → Network → Decryption method

Plaintext → Cipher text → Plain text

Encryption key
Decryption key

Passive intruder
Active intruder
TYPES OF CRYPTOGRAPHY

1. SYMMETRIC KEY ENCRYPTION
2. NON-SYMMETRIC KEY ENCRYPTION
   ➔ KEY MANAGEMENT
Symmetric Key Encryption

- Single key is used for encryption and decryption.
Data Encryption Standards-(DES)

- DES
- DES-2
- DES-3
- RC5
- RC2
- IDEA...

56 Bit KEY

64 bit Plaintext

Step 1: Initial Transposition
Step 2: Iteration 1
Step 2: Iteration 2
Step 16: Iteration 16
32 Bit Swap
Inverse Transposition

64 bit Cipher text
Disadvantages

- Only one key used hence intruder if gets to know the key can easily encrypt as well as decrypt message.

- One key per set of communication parties required
Asymmetric Key Encryption

- Two keys are used
- *Public Key* is used for encryption
- *Private Key* is used for decryption

**SENDER**
- “A”
  - Plain Text

**Encrypt using B’s Public Key**

**Cipher Text**

**Decrypt using B’s Private Key**

**RECEIVER**
- “B”
  - Plain Text
RSA Algorithm

- Choose two large prime nos. \( P \) and \( Q \)
- Compute \( N = P \times Q \)
  and \( Z = (P-1) \times (Q-1) \)
- Choose a no. \textit{relatively prime} to \( Z \)...call this decryption key \( D \)
- Find encryption key \( E \) such that \( E \times D = 1 \ mod \ Z \)
- Cipher Text \( \rightarrow \ C = M^E \ mod \ N \)
- Plain Text \( \rightarrow \ M = C^D \ mod \ N \)
Example

- Let $P=7$ & $Q=17$
- Hence $N = (7 \times 17) = 119$
  
  $Z = (6 \times 16) = 96$

Since $D$ is relatively prime to $Z$ $\Rightarrow$ $D = 5$

- Calc. $E$ such that $\Rightarrow E \times D = 1 \mod Z$
  
  Hence $E = 77$

- Now
  
  $C = M^E \mod N = 6^{77} \mod 119 = 27$

  $M = C^D \mod N = 27^5 \mod 119 = 6$
KEY MANAGEMENT

Distribution of keys in symmetric key encryption

- KDC (Key Distribution Centre)
  - Secret key is established between KDC and each member
Diffie-Hellman Key Exchange

A picks $x$

B picks $y$

A computes

$(g^y \mod n)^x \mod n$

$= g^{xy} \mod n$

B computes

$(g^x \mod n)^y \mod n$

$= g^{xy} \mod n$
Distribution of keys in asymmetric key encryption

*The private key should be known only to the user.*

*The public should be available to everyone.*

- Public Announcement
- Trusted Center
- Certification Authority
Thank You !!!