INT307 Multimedia Security System

Encryption of Digital Media

Shengchen Li

Xi'an Jiaotong-Liverpool University

25th Aug 2022

Aims

- Understand the purpose of encryption
- Master basic principles of encryption
- Understand basic standards of encryption
- Understand the application of encryption

Encryption

- Some media is suppose to be transmitted privately
- Suppose that the information space $\hat{M}$ and encrypted space $\hat{C}$, the encryption process could be considered as a mapping E such that

$$E(M) = C \tag{1}$$

where $M \in \hat{M}, C \in \hat{C}$.

- M is message, C is cipher.

Decryption

- Encrypted file could be a “random” file making little sense
- Decryption process could be represented as

$$D(C) = E^{-1}(E(M)) \tag{2}$$

Type of Encryption

- Usually, a key K will be used to encrypt / decrypt information *i.e.*

$$E_k(M) = C \tag{3}$$

$$D_{k'}(C) = M \tag{4}$$

- If $k = k'$, the encryption system is a single key system (symmetric encryption)
- If $k \neq k'$, the encryption system is a dual key system (asymmetric encryption)

- k is said to belong to a space of key *i.e.* $k \in \hat{K}$

Recall

- The definition of entropy

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x) \quad (5)$$

- Entropy measures the uncertainty (quantity of information)

Basics

- Message (M) and key (K) determines and cipher (C) *i.e.*

$$H(C|M,K) = 0 \tag{6}$$

$$H(M|C,K) = 0 \tag{7}$$

- Knowing cipher, obtaining the key is as hard as obtaining the message

$$H(M|C) = H(K|C) \tag{8}$$

- Obtaining the key, knowing message is equivalent to knowing cipher

$$H(M|K) = H(C|K) \tag{9}$$

Basics (Continued)

- Knowing the message, the encrypted message is as uncertain as the key

$$H(K|M) = H(C|M) \tag{10}$$

- With the message, it is easy to find the key from cipher

$$H(K|C, M) = 0 \tag{11}$$

Complete Confidentiality

- The best encryption system is completely confidential *i.e.*

$$H(M|C) = H(M) \tag{12}$$

- For a message M, the probability of receiving cipher C is equal to the probability that cipher C represents other messages *i.e.*

$$p(C|M) = p(C) \tag{13}$$

Decipher

- Knowing only cipher, what makes the work of decipher harder? $H(C)$
- Will the knowledge about encryption process E help decipher? Why?

$$H(M|E,K) \leq H(M|K) \tag{14}$$

- There are three possible results for a decipher
  - Correctly decipher the message
  - Impossible to decipher
  - A wrong but sensible decipher text
- Sometimes it may take too much time to decipher a cipher such that the process becomes senseless (Computational confidentiality)

Classical Cipher

There are two types of classical cipher

- Substitution cipher
  - Caesar cipher
  - Vigenere cipher
  - Hill cipher
- Transposition cipher

Substitution Cipher

- Caesar Cipher

$$c = E(m) = (m + k) \mod (N) \tag{15}$$

- Vigenere cipher

$$c_i = (m_i + k_i) \mod N \tag{16}$$

where N is usually 26, $\mathbf{k} = (k_1, k_2, \ldots, k_l)$ is considered as the key

- Hill cipher

$$\mathbf{C} = \mathbf{K} \cdot \mathbf{M} \mod N \tag{17}$$

$$\mathbf{M} = \mathbf{K}^{-1} \cdot \mathbf{C} \mod N \tag{18}$$

Block Cipher vs Stream Cipher

- Block Cipher: divide message into several blocks where each block contains several bits

- Stream Cipher: each bit of message is processed individually

Transposition Cipher

Classical transposition cipher is usually rule-based

- Change the first letter of each word
  - Wasted the Term → Tasted the Werm
  - Smoke a pipe → Poke a Smipe
- Path Copy

$$
\begin{array}{cccccc}
I & c & h & b & I & n \\
D & e & r & d & o & k \\
T & o & r & e & l & s \\
E & n & b & a & r & t
\end{array}
$$

If read by column, we have *IDTECEONHRRBBDEAIOIRNKST*

From Classical to Modern

- Classical: Break the context of letters (alphabet)
- Key: confusion and diffusion
  - Confusion: make cipher and key independent to each other
  - Diffusion: eliminate the characteristics of message via expanding (any bit in cipher is affected by many as many bits in message as possible)
- Randomness: the ideal case for cipher is always completely random (uniformly distributed) regardless of message (but how?)

Modern Cipher

- Feistel Network
- DES
  - S-DES
  - Triple DES
  - IDEA
  - AES
- RSA
- PGP

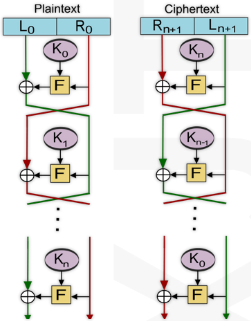
Feistel Network

- Basic unit of structure for many modern block cipher
- The cipher and message have the same length

$$L_i = R_{i-1} \tag{19}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \tag{20}$$

- Key issues
  - The round function F
  - The generation process K
- Larger block and longer key means better security but slower processing speed
- A single round is not secure enough usually more rounds introduce better security (usually 16 rounds)

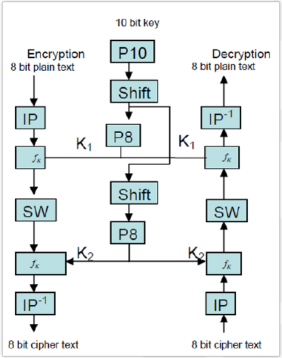


S-DES

- S-DES represents simplified DES
- It has a two-round Feistel Network structure with a pair of initial transposition blocks at the beginning and the end

$$C = IP^{-1}(f_{k_2}(SW(f_{k_1}(IP(M))))) \qquad (21)$$

- The block size is 8 bits
- Next we discuss about how keys k_i are generated and how the round function f_{k_i} is designed

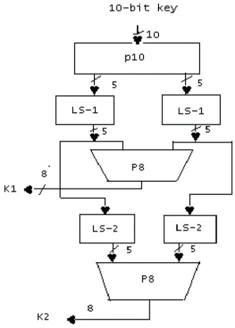


S-DES: Key Generation Process

- Two transposition functions are prepared
  - P_{10} that transpositions all 10 bits
  - P_8 that truncates and transpositions 8 bits in 10 bits
- The key for the *i*th round can be written as

$$k_i = P_8(shift_i(P_{10}(\text{key}))) \tag{22}$$

- The key for each round is generated by a general key that is to be transmitted privately



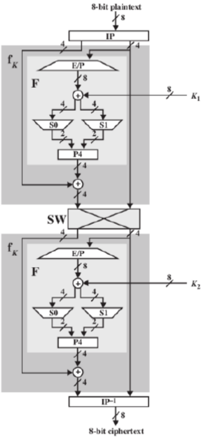
Key generation for simplified DES

S-DES: Round Function

- The round function has also a section of substitution and a section of transposition.
- It only processes the left 4 bits i.e.

$$f_{k_i}(L, R) = (L \oplus F(R, k_i), R) \qquad (23)$$

- For function F
  - E/P function: expend and transposition (4 bits $\rightarrow$ 8 bits)
  - XOR operation (other functions may work) with the key
  - Read the output from two matrices (S boxes): S_0 and S_1 where resulting bits are used as the index of elements
  - Transposition of the output (P_4)



Triple DES

- Why triple (not double)?
- There might be a K_3 existed such that $E_{K_2}[E_{K_1}(M)] = E_{K_3}(M)$

- Encryption process: $C = E_{K_3}[D_{K_2}[E_{K_1}(M)]]$ is known as a three-key system
- When $K_3 = K_1$, this is a two-key system
- When $K_3 = K_2$ or $K_2 = K_1$, this is a standard DES system

IDEA

- 64 bits input (block size) with 128 bits key
- Inputs are divided into 4 groups
- Usually has 8 rounds
- For each round, each group operates XOR, addition and multiplications with 6 16-bit keys

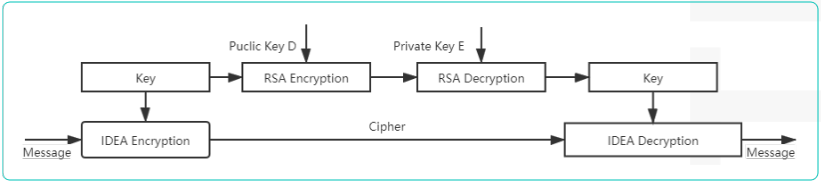
AES

- Replace DES but AES is not a Feistel network
- Block size: 128 bits, Key size: 128/192/256 bits
- Procedures of AES
  - Byte substitution (S boxes)
  - Transposition of rows
  - Confusion of columns
  - Encryption with the round key
  - (Round key expansion)

RSA

- Encryption: $C = M^e \% n$
- Decryption: $M = C^d \% n = (M^e)^d \% n = M^{de} \% n$
- Public key: e, n
- Private key: d, n
- The procedure of finding key pairs:
  1. $N = p * q$
  2. $L = lcm(p - 1, q - 1)$
  3. Find e such that $1 < e < L$ AND $gcd(e, L) = 1$
  4. Find d such that $1 < d < L$ AND $ed \% L = 1$

PGP encryption



- An example of asymmetric encryption system
- Key point for privacy: how the private key is transmitted

Summary

- Basics of Encryption
- Classical Cipher: Substitution and Transposition
- Modern Cipher
  - Confusion and Diffusion
  - Symmetric and Asymmetric
  - Randomness Requirement