Block Ciphers

Murat Kantarcioglu

Intuitions Related to Block Ciphers

- Block ciphers are considered to be pseudo-random permutations (more on this theory later)
- Consider a block cipher as a permutation defined on n bit strings to n bit strings based on the secret key.
- It is assumed that if the key is secret the output of the block cipher will look like random

Block Cipher

- $\mathcal{P} : \{0,1\}^n$
- $\mathcal{C} : \{0,1\}^n$
- $\mathcal{K} : \{0,1\}^k$
- $F : \mathcal{K} \times \mathcal{P} \mapsto \mathcal{C}$ where F is a permutation on $\{0,1\}^n$
- $F^{-1} : \mathcal{K} \times \mathcal{C} \mapsto \mathcal{P}$ is the inverse of F

Ideal Block Cipher

- An ideal block cipher is a totally random permutation from n bit strings to n bit strings (more on this later)
  - It is not efficient to represent all possible permutations
  - Key length is too big for large n

$$\log(2^n!) \geq \log((2^{n-1})^{2^{n-1}}) = (n-1).2^{n-1}$$

  - Our goal is to approximate ideal block ciphers in practice.

Common Block Cipher Designs

- Most modern block cipher use an iterated cipher based on some substitution-permutation network (Though exceptions exist)
- There are years of research on how to design good block ciphers
- Good block cipher should be as close as possible to an “ideal block cipher”

Iterated Cipher

- Requires the specification of an invertible round function g and key schedule function Ks and Number of rounds Nr.

$$
\begin{aligned}
&F(K, x)\\
&\{\\
&\quad (K^1, \ldots K^{Nr}) \leftarrow Ks(K)\\
&\quad w^0 \leftarrow x\\
&\quad w^i \leftarrow g(w^{i-1}, K^{i-1}) \text{for } Nr \geq i \geq 1\\
&\quad \text{Return } w^{Nr}\\
&\}
\end{aligned}
$$

Inverting an Iterated Cipher

- Since function g is invertible. We can easily decipher the output of an iterated cipher

$$
\begin{aligned}
&F^{-1}(K, y)\\
&\{\\
&\quad (K^1, \ldots K^{Nr}) \leftarrow Ks(K)\\
&\quad w^{Nr} \leftarrow y\\
&\quad w^{i-1} \leftarrow g^{-1}(w^i, K^i) \text{ for } Nr > i \geq 1\\
&\quad \text{Return } w^0\\
&\}
\end{aligned}
$$

History of DES

- Based on Lucifer cipher developed at IBM in late 60s (Lucifer has 128 bit keys!)
- DES is based on a special iterated Cipher called Feistel
- Became standard in 1977
- Turned out to be fairly durable due to its good design

Feistel Ciphers

- Feistel Type Cipher has a specific type of round functions g

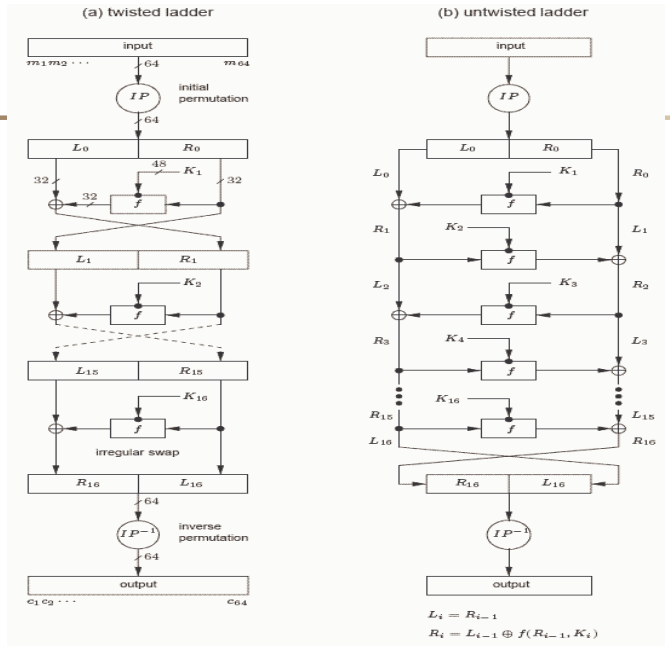
$g(L^{i-1}, R^{i-1}, K^i)$
{
  $L^i \leftarrow R^{i-1}$
  $R^i \leftarrow L^{i-1} \oplus f(R^{i-1}, K^i)$
  Return (L^i, R^i)
}

$g^{-1}(L^i, R^i, K^i)$
{
  $L^{i-1} \leftarrow R^i \oplus f(L^i, K^i)$
  $R^{i-1} \leftarrow L^i$
  Return (L^{i-1}, R^{i-1})
}

DES

$DES(K, M)$ $//|K| = 56, |M| = 64$
{
  $(K^1, \ldots, K^{16}) \leftarrow Keys(K)$
  $M \leftarrow IP(M)$
  $(L^0, R^0) \leftarrow M$
  for $r = 1$ to 16{
    $L^i \leftarrow R^{i-1}$
    $R^i \leftarrow L^{i-1} \oplus f(R^{i-1}, K^i)\}$
  Return $IP^{-1}(L^{16}, R^{16})$
}

- DES is 16-round Feistel Network with an initial permutation at the beginning and a reverse permutation at the end.



Initial Permutation and Final Permutation

IP(x)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

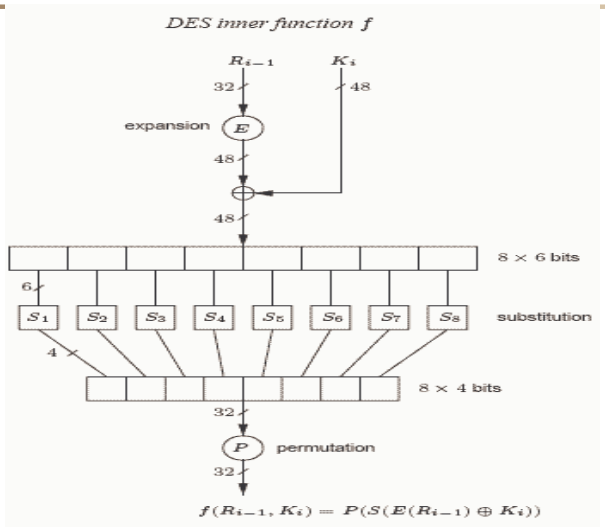
$IP^{-1}(x)$

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES f function Details

function $f(J,R)$ // $|J| = 48$ and $|R| = 32$
  $R \leftarrow E(R)$; $R \leftarrow R \oplus J$
  Parse R as $R_1 \| R_2 \| R_3 \| R_4 \| R_5 \| R_6 \| R_7 \| R_8$ // $|R_i| = 6$ for $1 \le i \le 8$
  for $i = 1,\ldots,8$ do
    $R_i \leftarrow \mathbf{S}_i(R_i)$ // Each S-box returns 4 bits
  $R \leftarrow R_1 \| R_2 \| R_3 \| R_4 \| R_5 \| R_6 \| R_7 \| R_8$ // $|R| = 32$ bits
  $R \leftarrow P(R)$
  return R

DES f function



DES S-boxes

- The S-boxes are the only non-linear elements in DES design
- Needed to protect against differential cryptanalysis

S_5 :

		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
0	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
1	0	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1	1	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

DES Key Scheduling

$Keys(K)$ $//|K| = 56$
{
  $K \leftarrow PC1(K)$
  $(C^0, D^0) \leftarrow K$
  for $r = 1$ to 16
  {
    if $r \in \{1, 2, 9, 16\}$ then $j \leftarrow 1$ else $j \leftarrow 2$
    $C^r \leftarrow lshift_j(C^{r-1})$
    $D^r \leftarrow lshift_j(D^{r-1})$
    $K_r \leftarrow PC2(C^r||D^r)$
  }
  return $(K^1, \ldots, K^{16})$
}

Cryptanalysis of DES

- Linear/Differential Cryptanalysis
- Exhaustive Key Search

Differential Cryptanalysis

- Attacker knows pairs of plaintext and ciphertext (P,C) pairs such that

$$\delta_p = P_1 \oplus P_2, \delta_C = C_1 \oplus C_2$$

- Distribution of differences could be used to guess some certain key bits.
- DES is relatively resistant to Differential Cryptanalysis. It turns out S-boxes were designed to prevent such attacks.
  - Differential Cryptanalysis requires 2^{47} ciphertexts

Linear Cryptanalysis

- The goal is to approximate the block cipher using simple linear models
- It requires 2^{43} plaintext/ ciphertext pairs for 16 rounds of DES
- Not practical for DES.

Brute Force Attacks

- Try all possible key pairs to find a key that matches known plaintext/ciphertext pair.
- Need to try 2^{56} keys.
- Time consuming
- A 250K machines + distributed computing were able to find the DES key in 10 hours in 1999.
- The main attack against DES.

Increasing DES Key Size

- The following are the popular choices for increasing DES key sizes.

$$3DES(K^1, K^2, K^3, M) \ //|K^1| = |K^2| = K^3| = 56$$
$$\{$$
$$\quad \text{return } DES(K^3, DES^{-1}(K^2, DES(K^1, M))))$$
$$\}$$

$$DESX(K^1, K^2, K^3, M) \ //|K^1| = 56, |K^2| = K^3| = 64$$
$$\{$$
$$\quad \text{return } DES(K^1, M \oplus K2) \oplus K_3$$
$$\}$$

Summary

- DES was a surprisingly effective cipher
- The main weakness was the key size.
- It is know replaced with AES.