Lecture Notes

Advanced Discrete Structures

COT 4115.001 S15

2015-02-05

Recap

- Attacks on Hill Ciphers
- Base Systems
  - Binary
- ASCII
- One Time Pads
- Random Number Generation
  - Blum Blum Shub

The Data Encryption Standard - Section 4.1

INTRODUCTION

DES History

- <u>1973</u> – the NBS (now NIST) issued a public request for a cryptographic standard
- <u>1974</u> – IBM submitted an algorithm called LUCIFER based on an algorithm designed by *Horst Feistel*
  - The NBS sent it to the NSA, who modified it
- <u>1975</u> – the NBS released it for free use
- <u>1977</u> – the NBS made it the official data encryption standard (DES)
- <u>1990</u> – Eli Biham and Adi Shamir showed how differential cryptanalysis could attack DES
  - <u>1994</u> – a member of the LUCIFER team publishes a paper stating that IBM was well aware of the differential cryptanalysis method in 1974
  - NSA also knew about differential cryptanalysis too and helped to strengthen DES against it, but weakened it against brute force (128 bit to 56 bit)

The Data Encryption Standard - Section 4.6

BREAKING DES

DES History

- 1975 – Diffie and Hellman publish "Exhaustive Cryptanalysis of the NBS Data Encryption Standard"
  - Propose that a machine could be built for $20 million that could crack DES in a day
- 1987 – NSA opposes recertification of DES as the NBS standard
  - Despite oppositions NBS recertifies DES and again in 1992
- 1993 – Michael Wiener proposes a new design for a brute force DES attack machine
- 1998 – The Electronic Frontier Foundation (EFF) built the DES Cracker for $250,000 that could crack a 56-bit DES key in around 4.5 days
- 2000 – The NIST accepted the Rijndael algorithm as the Advanced Encryption Standard to supersede DES

The Data Encryption Standard - Section 4.2

A SIMPLIFIED DES-TYPE ALGORITHM

Simplified DES-Type Algorithm Setup

1. **Message**: a single 12-bit binary block
   - $M = L_0 R_0$, (both L_0 and R_0 are 6-bits)

2. **Key**: K is 9-bit ($K \in \mathbb{Z}_2{}^9$)

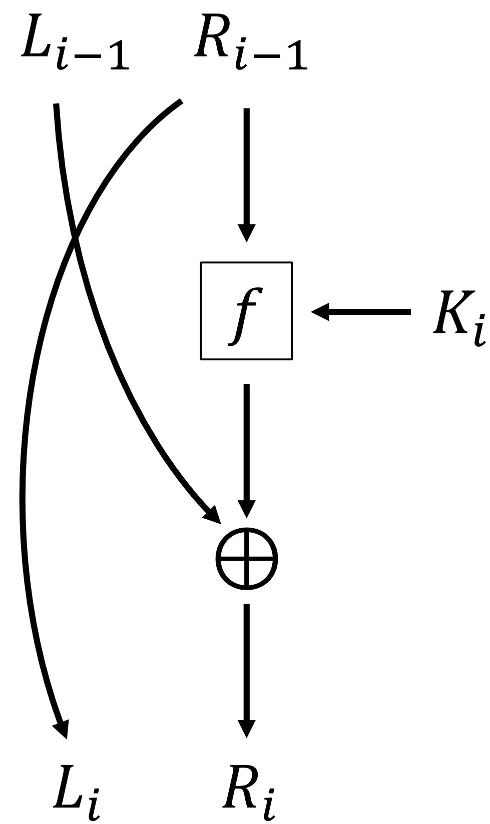
3. **Function**:

$$f: \mathbb{Z}_2{}^6 \times \mathbb{Z}_2{}^8 \rightarrow \mathbb{Z}_2{}^6,$$

   i.e., input for f is a 6-bit and 8-bit string and output of f is a 6-bit string

Simplified DES-Type – Encryption

$$
\begin{array}{c}
M = L_0 \, R_0 \\
\downarrow \\
L_1 \, R_1 \leftarrow K_1 \\
\downarrow \\
L_2 \, R_2 \leftarrow K_2 \\
\downarrow \\
\vdots \quad \leftarrow \quad \vdots \\
\downarrow \\
L_n \, R_n \leftarrow K_n
\end{array}
$$



$$\boxed{L_i = R_{i-1} \quad \text{and} \quad R_i = L_{i-1} \bigoplus f(R_{i-1}, K_i)}$$

Simplified DES-Type – Decryption

1. Switch L_n and R_n, i.e., $L_nR_n \to R_nL_n$

2. Use the encryption procedure with the keys in reverse order:

$$K_n, K_{n-1}, \ldots, K_2, K_1$$

3. Reverse final R_0L_0 to recover the message $M = L_0R_0$.

Simplified DES-Type – Decryption

Encryption:

$$[L_{i-1}]\ [R_{i-1}] \ \rightarrow\ [R_{i-1}]\ [L_{i-1} \oplus f(R_{i-1}, K_i)] = [L_i]\ [R_i]$$

Decryption: $[R_i]\ [L_i] \ \rightarrow\ [L_i]\ [R_i \oplus f(L_i, K_i)]$

From encryption,

$$[R_i \oplus f(L_i, K_i)] = [(L_{i-1} \oplus f(R_{i-1}, K_i)) \oplus f(R_{i-1}, K_i)] = [L_{i-1}]$$

because $f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i) = 2f(R_{i-1}, K_i) \equiv 0 \pmod 2.$ Thus,

$[L_i]\ [R_i \oplus f(L_i, K_i)] = [R_{i-1}]\ [L_{i-1}]$ so $[R_i]\ [L_i] \ \rightarrow\ [R_i]\ [L_i].$

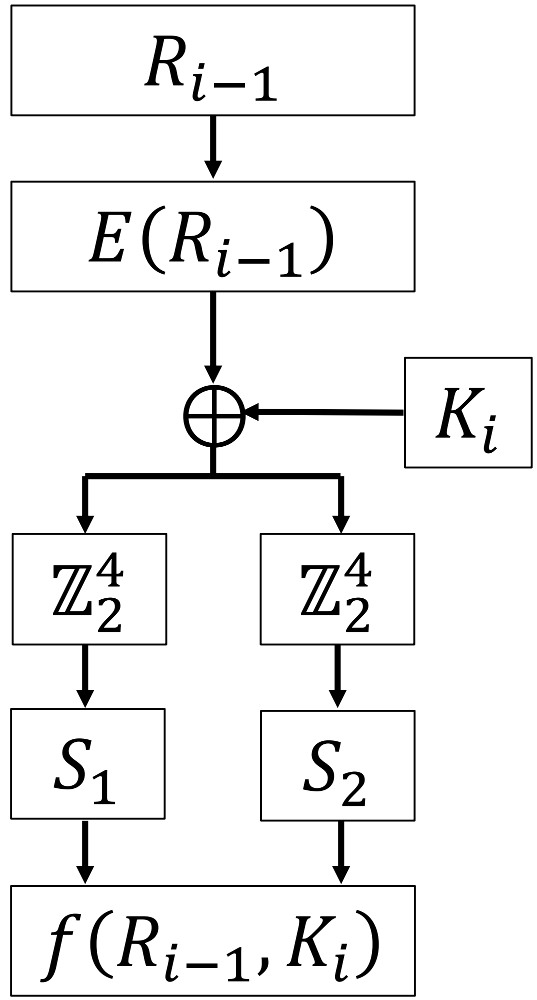
Simplified DES-Type – f

- Since f gets cancelled in the decryption, any f works in this simplified DES-type algorithm
  - However, since we wish to learn the DES algorithm, pick an f that is similar to DES
- DES uses a Feistel f function with four stages:
  1. Expansion
  2. Key Mixing
  3. Substitution
  4. Permutation

We will use these 3 steps in the simplified DES-type algorithm

f function – Outline

1. Expansion
2. Key Mixing
3. Substitution

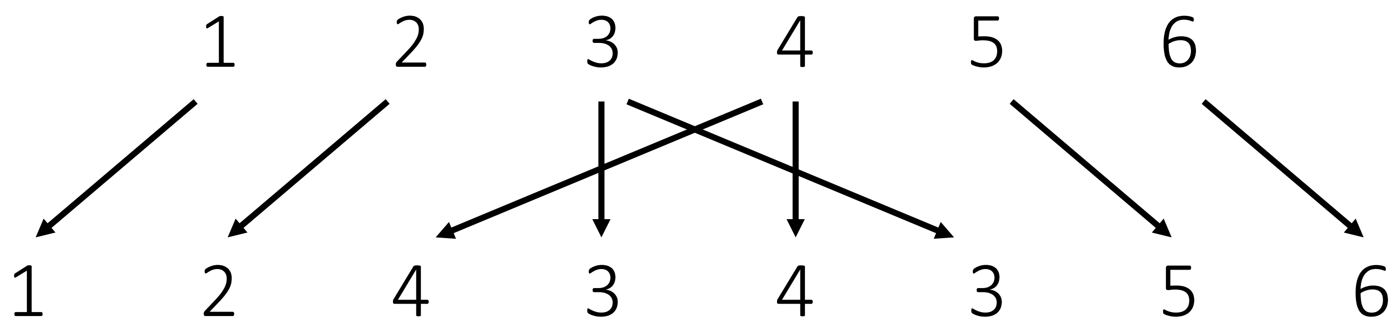


1: 6-bit
1: 8-bit
2: 8-bit
2: 4-bit
2: 3-bit
1: 6-bit

f function – 1. Expansion

Expansion function

$$E : \mathbb{Z}_2^6 \to \mathbb{Z}_2^8$$



$$R_2 = 001011$$

$$E(R_2) = E\left(00\underline{10}11\right) = 00\underline{0101}11$$

f function – 2. Key Mixing

1. Start with a 9-bit key K
2. Generate K_i by taking the first 8-bits of K starting at bit i and wrapping around

$$K = 100111010$$

$$K_1 = 10011101, \qquad K_4 = 11101010,$$

$$K_2 = 00111010, \qquad K_5 = 11010100,$$

$$K_3 = 01110101, \qquad K_6 = 10101001, \ldots$$

3. Compute $E(R_{i-1}) \oplus K_i$

$$E(R_2) \oplus K_3 = 00010111 \oplus 01110101 = 01100010$$

f function – 3. Substitution

1. Split the mixed key 8-bit block into two 4-bit blocks
2. Each block has an associated **S-box**:

S_1

101	010	001	110	011	100	111	000
001	100	110	010	000	111	101	011

S_2

100	000	110	101	111	001	011	010
101	011	000	111	110	010	001	100

3. The first block uses S_1; the second block uses S_2:
   - The first bit of each block determines the row and the remaining three bits determine the column of the S-box

Example: Block 1 = $\underline{1}010 \Longrightarrow 110$, Block 2 = $\underline{0}110 \Longrightarrow 011$

f function – Outline