Block Ciphers — Introduction

Orr Dunkelman

Computer Science Department
University of Haifa, Israel

March 10th, 2013

Outline

What?

- This is a seminar about cryptanalytic techniques for block ciphers.
- Seminar:
  - I shall give a few introductory lectures,
  - Each one will present one paper in a 45-minute time slot.
- The papers are real-life research papers.
- You shall present them to the class.
- Which means: you need to know the material, and you need to pass it on to your peers.

Why?

- For most computer systems, block ciphers are the default encryption mechanism.
- Hard-disk encryption, most of SSL options or IPsec options are actually the encryption using block ciphers.
- Intel to introduce AES support to its chips (the AES-NI instruction set).

Where, When, and Who?

- Location: TBD
- Sun., 16:15–17:45.
- Lecturer:
  - Orr Dunkelman
  - Email: orrd (at-sign) cs (dot) haifa (dot) ac (dot) il
  - Office: Jacobs 408.
  - Office hour: Sun., 10:30–11:30.
  - Phone: 8447

Grades

- 60% — Lecturer's evaluation,
- 20% — Participation in classes (it is mandatory to attend at least 10 meetings),
- 20% — Peers' evaluation.

Perquisites

- Introduction to Cryptography (203.4444)

It is highly recommended to take a look at the slides of the introduction to cryptography course.

Modeling the Adversary

- This is an academic cryptanalysis course.
- We will discuss only the “standard” model:
  1. The description of the cipher is known to the adversary,
  2. The adversary tries to analyze the cipher’s strength, and not the implementation (i.e., no side-channel attacks),
  3. The adversary gets (different levels of) access to the input and output of the cipher,
- This is also known as the “Kerckhoffs’s principle”.

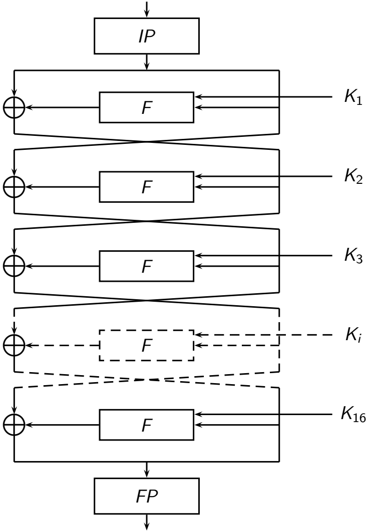
Block Ciphers

- One of the most basic cryptographic algorithms.
- A symmetric key algorithm (both sides hold secret information).
- Is a transformation of blocks of bits (of size n) into new blocks of bits (usually of the same size). Formally: $E : \{0,1\}^n \times \{0,1\}^k \mapsto \{0,1\}^n$ or $E_k : \{0,1\}^n \mapsto \{0,1\}^n$.
- To deal with more (or less) data, some mode of operation is used (ECB, CBC, counter mode, etc.).

The Data Encryption Standard

- Designed by IBM at the mid 70's.
- Feistel block cipher with 16 rounds.
- 64-bit block size, 56-bit key size.
- The round function accepts 32-bit input and 48-bit subkey.

Outline of DES



IP and *FP*

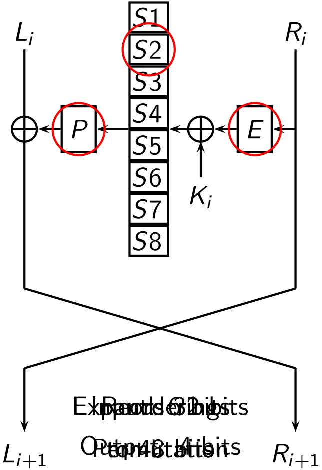
IP

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

FP ($=\text{IP}^{-1}$)

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



DES' F-function (cont.)

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

DES' F-function (cont.)

$S1$

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

$S2$

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

DES' F-function (cont.)

$S3$

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

$S4$

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

DES' F-function (cont.)

$S5$

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

$S6$

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

DES' F-function (cont.)

$S7$

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

$S8$

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

DES' F-function (cont.)

Beware!

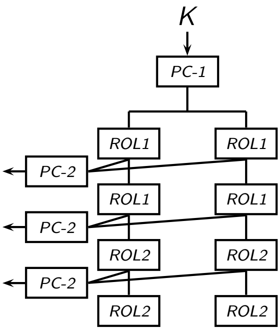
The S-boxes are given (as in the FIPS) in a very confusing manner. The MSB and the LSB of the input determine the row in the table, and the middle 4 bits determine the column. For example, this table shows where the entry corresponding to the input is:

Location of entries in the previous tables

0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62
33	35	37	39	41	43	45	47	49	51	53	55	57	59	61	63

DES' Key Schedule Algorithm

- The key is divided into two registers C and D (28-bit each).
- Each round both registers are rotated to the left (1 or 2 bits).
- 24 bits from C are chosen as the subkey entering $S1, S2, S3, S4$.
- 24 bits from D are chosen as the subkey entering $S5, S6, S7, S8$.

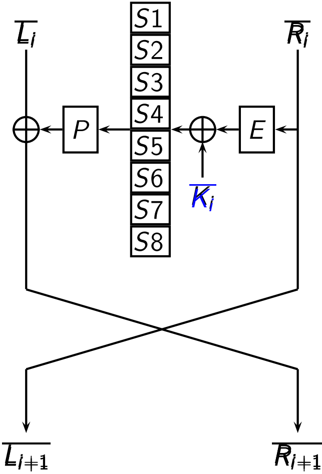


Round	1	2	3	4	5	6	7	8
Rotation	1	1	2	2	2	2	2	2
Round	9	10	11	12	13	14	15	16
Rotation	1	2	2	2	2	2	2	1

DES' Complementation Property

- If the key is bitwise complemented, so are all the subkeys.
  $K \rightarrow K_1, K_2, \ldots, K_{16}$ **and**
  $\overline{K} \rightarrow \overline{K_1}, \overline{K_2}, \ldots, \overline{K_{16}}$
- If the input to the round function is also bitwise complemented, the complementation is canceled.
- In other words, the input to the S-boxes is the same. **And the output of the S-boxes (and the round).**
- **DES's complementation property**:

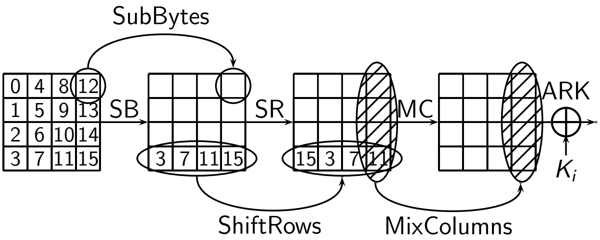
$$DES_K(P) = \overline{DES_{\overline{K}}(\overline{P})}$$



The Advanced Encryption Standard

- Designed by Vincent Rijmen and Joan Daemen, under the name Rijndael and submitted to NIST's competition in 1998.
- The cipher has an SP network structure.
- Block size — 128 bits, Key size — 128, 192, or 256 bits.
- Number of rounds depends on the key length (10/12/14, respectively).
- Several attacks in the related-(sub)key model on AES-192/AES-256.
- For any practical application, still offers sufficient security (but new systems may benefit from using something else).

The AES Round Function



Before the first round, an additional AddRoundKey operation is performed, and in the last round, the MixColumns operation is omitted.

The MixColumns Operation

- MixColumns treats each column of four bytes as four elements over $GF(2^8)$. Then, the column is multiplied by the Matrix:

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}$$

- The field $GF(2^8)$ is constructed over the (irreducible) polynomial `11B`, i.e., $x^8 + x^4 + x^3 + x + 1$.

The SubBytes Operation

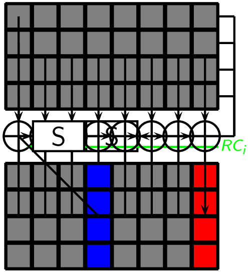
- Given input x, compute $y = x^{-1}$ (over the same field, with $0 \triangleq 0^{-1}$).
- The compute the output as:

$$\begin{bmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

AES' Key Schedule Algorithm

The key schedule for AES with $32 \cdot Nk$-bit key:

- Initialize
  $W[0, \ldots, Nk-1] = K[0, \ldots, Nk-1]$.
- For $i = Nk, \ldots, 4 \cdot (7 + Nk) - 1$ do
  - If $i \equiv 0 \bmod Nk$ then
    $W[i] = W[i - Nk] \oplus$
    $SB(W[i-1] \ggg 8) \oplus RCON[i/Nk]$,
  - Else if $Nk \equiv 8$ and $i \equiv 4 \bmod 8$ then
    $W[i] = W[i-8] \oplus SB(W[i-1])$,
  - Otherwise
    $W[i] = W[i-1] \oplus W[i-Nk]$,
- The first subkey is $W[0, 1, 2, 3]$, the second is $W[4, 5, 6, 7]$, etc.



What is a cryptographic attack?

- Practical attacks — if you can find the key, read the encrypted message without the key, or do any "harmful" operation in practice, this is an attack.
- Close-to-Practical attacks — if the attack is based on solid foundations, you verified a reduced-round version of it, and it just requires some more computation than you have, it seems to be a valid attack.
- Still, there are other attacks (sometimes referred to as *certificational attacks*), either due to time or data requirements.

What is a cryptographic attack? (cont.)

- The most extreme model of certificational attacks is the following rule:

  If the attack on the primitive is better than an attack on an ideal primitive of the same parameters — the attack breaks the primitive.

- For block ciphers this means — better than exhaustive search.
- Hence, we shall (mainly) look at the time complexity of the attack.
- In this course, we shall assume this model.

Remember: **attacks only get better!**

The Ideal Cipher

The following two definitions for the ideal cipher are equivalent:

- The *ideal cipher* is a cipher for which for every key, even if $2^n - 2$ plaintext/ciphertext pairs are known, the adversary has no knowledge concerning the remaining two plaintext/ciphertext pairs.
- An ideal cipher is a set of 2^k random permutations over $\{0,1\}^n$.

The Data Requirements of the Attack

An attack may be applied in different models:

- **Ciphertext-only** — where the adversary has access only to the ciphertext.
- **Known plaintext** — where the adversary can obtain pairs of plaintexts and their corresponding ciphertexts.
- **Chosen plaintext** — where the adversary can choose for which plaintexts (s)he has the knowledge of the corresponding ciphertexts.
- **Chosen ciphertext** — just like chosen plaintext, but with ciphertexts.
- **Adaptive chosen plaintext** — where the adversary may choose what is the next plaintext (s)he wishes for, after seeing an earlier response.
- **Adaptive chosen plaintext and ciphertext** — . . .

Questions?

Thank you for your attention.