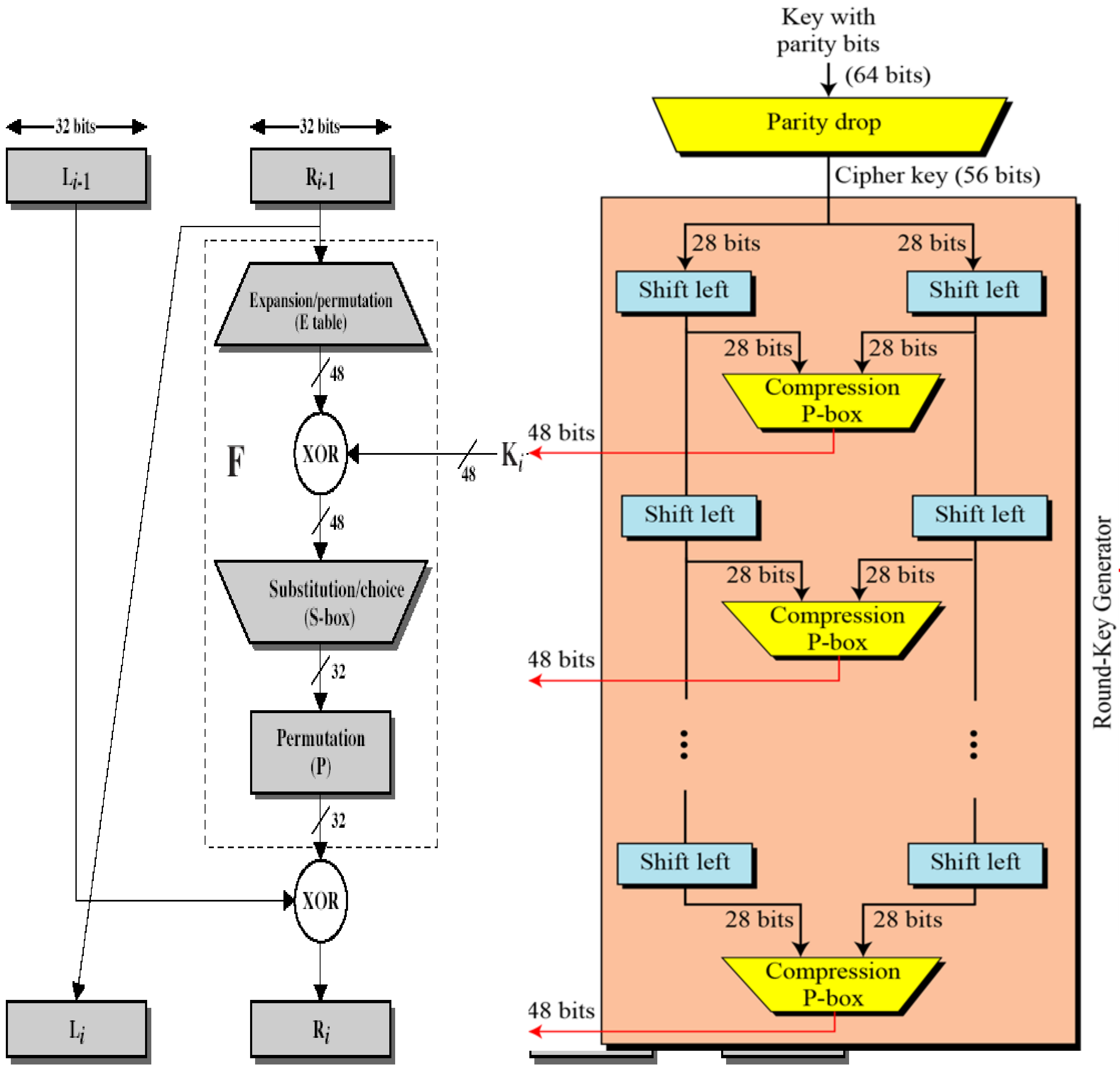
CS557: Cryptography

Block Cipher (Cryptanalysis)

S. Tripathy
IIT Patna

Previous Classes

- Modern Cipher
  - Block cipher
    - DES



– 56-bit cipher key

Avalanche Effect

- DES exhibits strong avalanche
  - let us encrypt two plaintext blocks (with the same key) that differ only in one bit and observe the differences in the number of bits in output

EX.: **Key** K = "08192A3B4C5D6E7F",

M_1 = "0000000000000000" M_2 = "0000000000000001"

Hamming distance $d_H(M_1, M_2) = 1$

C_1 = "25DDAC3E96176467" C_2 = "1BDD183F1626FB43"

$d_H(C_1, C_2) = 22$

- Encrypt a plaintext block with two different keys that differ only in one bit and observe the differences in the number of bits in output

EX2.: The plain text message M= ABCDEFABCDEFABCD

Key K1 = "0123456789ABCDEF", k2 ="8123456789ABCDEF"

$d_H(k_1, k_2) = 1$

C_1 = "CDE872D4A471346F" C_2 = "1B73FE8BC0B88606"

$d_H(C_1, C_2) = 35$

Weak Keys

- DES has:
  - Four weak keys k for which $E_k(E_k(m)) = m$.
  - Ex.: 01010101 01010101 dropping parity bits bcecome all 0s
  - Twelve semi-weak keys which come in pairs k_1 and k_2 and are such that $E_{k1}(E_{k2}(m)) = m$.
  - Ex.: 011F011F010E010E and 1F011F010E010E01
  - Weak keys are due to “key schedule” algorithm

DES Attacks: Exhaustive Search

- Suppose we know plain/cipher text pair (p,c)

```
for(k=0;k<2^56;k++) {
  if(DES(k,p)==c) {
  printf("Key is %x\n", k);
  break;
  }
}
```

- Complementary property DES(**k'**, **x'**)=DES(**k**, **x**)'
- Expected number of trials (if k was chosen at random) before success: 2^{55}

Cryptanalysis

– Modern Ciphers
  - Cryptanalysis
    – Linear Cryptanalysis
    – Differential Cryptanalysis

- Linear cryptanalysis first defined on Feal by Matsui and Yamagishi, 1992.
  - Matsui later published a linear attack on DES.

- Differential cryptanalysis originally defined on DES
  - Eli Biham and Adi Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer Verlag, 1993.

Ref: LDC Tutorial (will upload in course link)

A Tutorial on Linear and Differential Cryptanalysis By H.M. Hey

*https://www.engr.mun.ca/~howard/PAPERS/**ldc_tutorial**.pdf*

Linear Cryptanalysis

Notation

- P = plaintext
- p_i = i^{th} bit of P
- C = Ciphertext
- c_i = i^{th} bit of C
- K = Key (initial or expanded)
- k_i = i^{th} bit of K
- $\oplus_{i=1,n}\, p_i = p_1 \oplus p_2 \oplus \;\; \dots \oplus p_n$

- X,Y,Z are subsets of bits (notation on next slide only)

Linear Cryptanalysis

Attack Overview

- Obtain linear approximation(s) of the cipher relating P,K,C

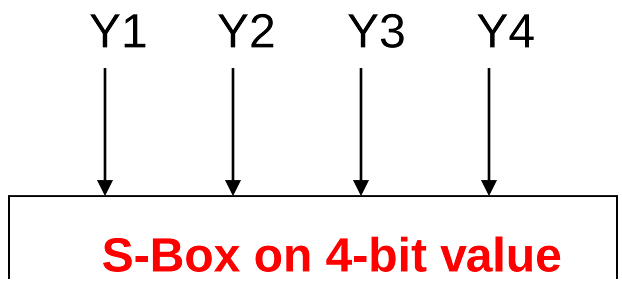
$$\bigoplus_{i\in X,}\ p_i \oplus_{j\in Y} c_j = \bigoplus_{g\in Z} k_g$$

  which occur with probability pr = $\frac{1}{2} + e$ for max bias $-\frac{1}{2} \leq e_i \leq \frac{1}{2}$.

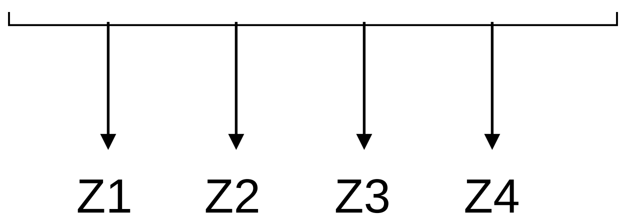
- Encrypt random P's to obtain C's and compute k_g's.
  - Known plaintext attack

- Guess remaining key bits via exhaustive search.

Example S-Box



input	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
output	E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7



$Y2 \oplus Y3 = Z1 \oplus Z3 \oplus Z4$ in 12 of the 16 input, output pairs

$12/16 = \frac{1}{2} + \frac{1}{4}$ and the bias is $\frac{1}{4}$

$Y1 \oplus Y4 = Z2$ in $\frac{1}{2}$ of the pairs, so there is no bias

$Y3 \oplus Y4 = Z1 \oplus Z4$ in 2 of the 16 pairs, so the bias is -3/8

$2/16 = \frac{1}{2} - 3/8$

Finding Linear Relationships

General form of linear relationship:

$a1Y1 \oplus a2Y2 \oplus a3Y3 \oplus a4Y4$

$= b1Z1 \oplus b2Z2 \oplus b3Z3 \oplus b4\ Z4$

$ai, bi \in \{0,1\}$

Summarize all equations in a table Only need to do once

Finding Linear Relationships

b1b2b3b4

a1a2a3a4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
2	0	0	-2	-2	0	0	-2	-2	0	0	2	2	0	0	-6	2
3	0	0	0	0	0	0	0	0	2	-6	-2	-2	2	2	-2	-2
4	0	2	0	-2	-2	-4	-2	0	0	-2	0	2	2	-4	2	0
5	0	-2	-2	0	-2	0	4	2	-2	0	4	-2	0	-2	-2	0
6	0	2	-2	4	2	0	0	2	0	-2	2	4	-2	0	0	-2
7	0	-2	0	2	2	-4	2	0	-2	0	2	0	4	2	0	2
8	0	0	0	0	0	0	0	0	-2	2	2	-2	2	-2	-2	6
9	0	0	-2	-2	0	0	-2	-2	-4	0	-2	2	0	4	2	-2
A	0	4	-2	2	-4	0	2	-2	2	2	0	0	2	2	0	0
B	0	4	0	-4	4	0	4	0	0	0	0	0	0	0	0	0
C	0	-2	4	-2	-2	0	2	0	2	0	2	4	0	2	0	2
D	0	2	2	0	-2	4	0	2	-4	-2	2	0	2	0	0	2
E	0	2	2	0	-2	-4	0	2	-2	0	0	-2	-4	2	-2	0
F	0	-2	4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

# of times equation holds: $a1Y1 \oplus a2Y2 \oplus a3Y3 \oplus a4Y4 = b1Z1 \oplus b2Z2 \oplus b3Z3 \oplus b4\,Z4$

Piling-Up Lemma

Matsui

- If $Pr(V_i = 0) = \frac{1}{2} + e_i$
  - $Pr(V_1 \oplus V_2 \oplus \dots \oplus V_n = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} e_i$
- V_i's are independent random variables
- e_i is the bias $-\frac{1}{2} \leq e_i \leq \frac{1}{2}$

Use to combine linear equations if view each as independent random variable

Linear Bounds

- Bound a linear equation holds across q rounds: $0 < p \leq 1$
- Cipher has nq rounds
- Estimate upper bound $\leq p^n$
- 2^b possible plaintexts
- Round key bits, output of a round/input to next round not independent
- If $p^n \leq 2^{-b}$, no attack