# CS557: Cryptography

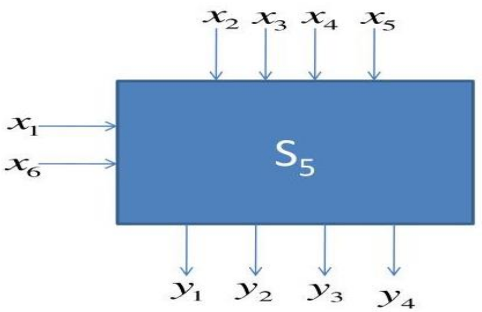
## Modern Ciphers (DES→AES)

S. Tripathy
IIT Patna

- Block Ciphers (DES):
  - Modes of Encryption  (Why?)
    - ECB
    - CBC
    - OFB
    - CFB
    - CTR

# Linear Cryptanalysis of 3 round DES

Pr( $\bar{x}_2 = y_1 \oplus y_2 \oplus y_3 \oplus y_4$ ) = 52/64 >0.8



X[17] ⊕ Y[3,8,14,25]= K[26] ⊕ 1, p= 52/64

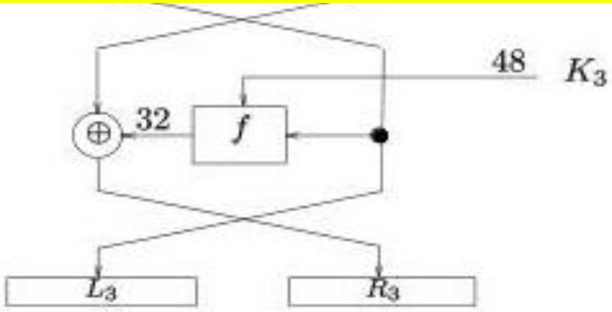
Round 1

## Applying an Attack on DES:

- When attacking the cipher, try to determine key bits for first or last round, then repeat attack on reduced round version of the cipher
- DES has 16 rounds, find round key for 1st or last round, repeat attack for 15 round version …
- If same expanded key bits used in multiple rounds, fill in round key bits as they become known

$P_R[17] \oplus P_L[3,8,14,25] \oplus C_L[3,8,14,25] \oplus C_R[17] =$
$K_1[26] \oplus K_3[26]$

Thus holds with p= $(52/64)^2 + (12/64)^2 = .66$



for each pair compute the bit of the key take the value that occurs more times.

# Matsui’s Per Round Constraints

| Label | Equation | Pr |
|---|---|---|
| A | $X[17] \oplus Y[3,8,14,25]=K[26]$ | 12/64 |
| B | $X[1,2,4,5] \oplus Y[17]=K[2,3,5,6]$ | 22/64 |
| C | $X[3] \oplus Y[17]=K[4]$ | 30/64 |
| D | $X[17] \oplus Y[8,14,25]=K[26]$ | 42/64 |
| E | $X[16,20] \oplus Y[8,14,25]=K[25,29]$ | 16/64 |

Matsui: Linear Cryptanalysis Method for DES Cipher. Eurocrypt, 98.

# Linear Cryptanalysis on DES

Invented by Mitsuru Matsui in 1993.

16-round DES can be attacked using $2^{43}$ known plaintexts - get 26 bits, brute force the remaining 30 bits

$2^{43} = 9 \times 10^{12}$ = 9 trillion known plaintext blocks

Also exploits biases in S-boxes, which were not designed against the attack

A DES key was recovered in 50 days using 12 HP9735 workstations in a lab setting

# Differential Cryptanalysis: Biham and Shamir (1990)

- Was known to IBM team whose design rules provided some resistance
  - Breaks Khafre with 1500 corresponding plain/cipher texts in an hour
  - Breaks 8 round Lucifer in $2^{21}$ steps with 24 texts
  - Breaks FEAL.
  - Breaks 8 round DES.
- DES Results: $2^{47}$ Chosen plaintext attack.

# Security of DES

- DES has: Four weak keys *k* for which $E_k(E_k(m)) = m$ *and* Twelve semi-weak keys which come in pairs $k_1$ and $k_2$ and are such that $E_{k1}(E_{k2}(m)) = m$.

- Exhaustive Key Search attack: Expected number of trials (if k was chosen at random) before success: $2^{56}$

- After proposal of DES two major criticisms
  - Key space is too small (2^56 keys)
  - S-box design criteria have been kept secret
- Exhaustive key search:
  - Relatively easy given today's computer technology
- Analytical Attacks:
  - DES is highly resistant to both differential

    and linear cryptanalysis
- So far there is no known analytical attack which breaks DES in realistic scenarios

# History of Attacks on DES

Year Proposed/ implemented DES Attack

1993: Wiener proposes design of a very efficient key search machine: Average search requires 36h. Cost: $1M

1997: DES Challenge-I broken, 4.5 months of distributed search

1998: DES Challenge II-(1) broken, 39 days (distributed search)

Jul. 1998: DES Challenge II-(2) broken, key search machine Deep Crack: 1800 ASICs with 24 search engines each, Costs: $250,000 15 days average search time

Jan. 1999 DES Challenge III broken in 22h 15min (distributed search assisted by Deep Crack)

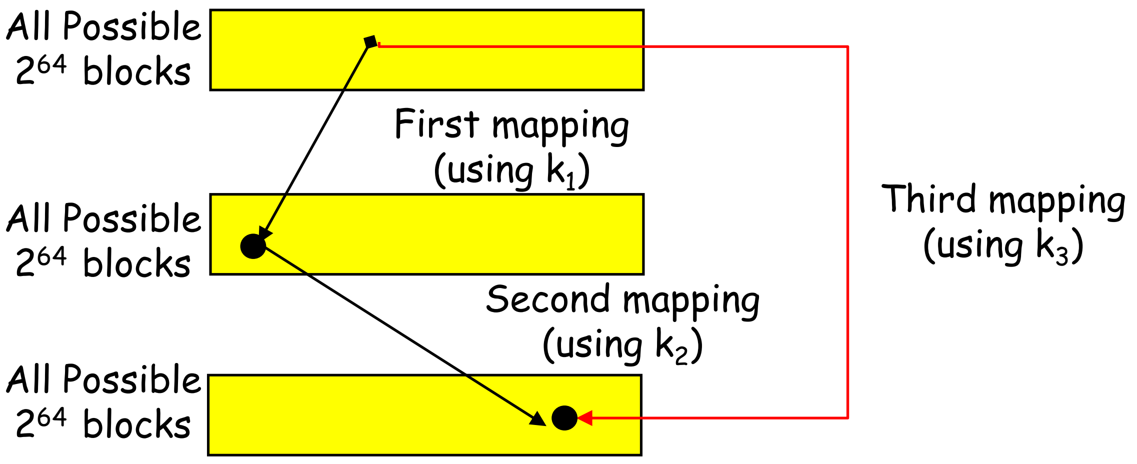
2006- Reconfigurable key search machine COPACOBANA

2008 (Germany), uses 120 FPGAs to break DES in 6.4 days (avg.) at a cost of $10,000.

# Multiple DES

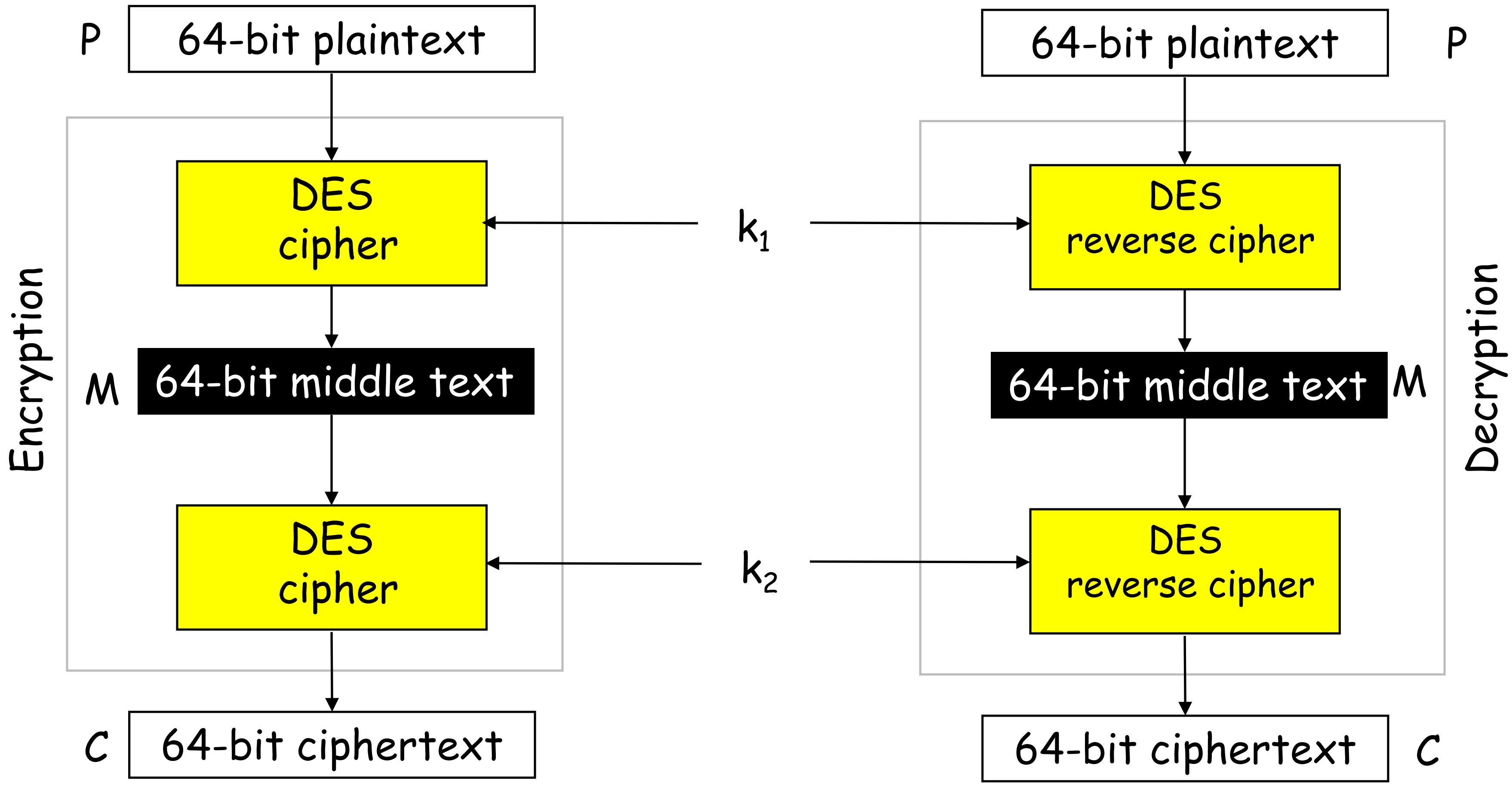
- The major criticism of DES regards its key length. Fortunately DES is not a group.
  - A substitution that maps every possible input to every possible output is a group.
  - Therefore we can use double or triple DES to increase the key size.

Composition of mapping


All Possible $2^{64}$ blocks
First mapping (using $k_1$)
All Possible $2^{64}$ blocks
Third mapping (using $k_3$)
Second mapping (using $k_2$)
All Possible $2^{64}$ blocks

# Double DES

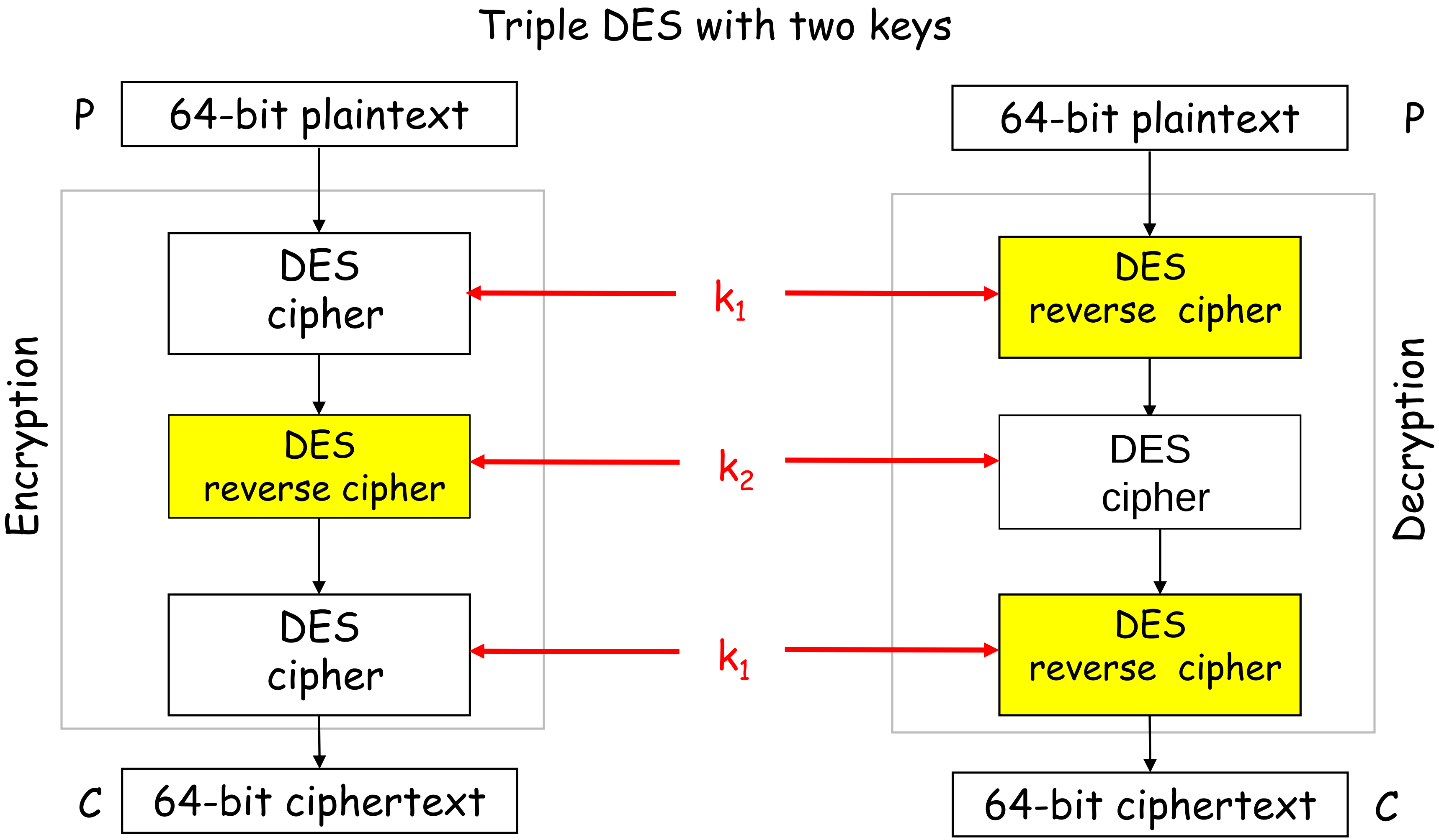
The first approach is to use double DES (2DES)



# Meet-in-the-Middle Attack

- Using a known-plaintext attack called meet-in-the-middle attack proves that double DES improves this vulnerability slightly (to $2^{57}$ tests), but not tremendously (to $2^{112}$).

# Triple DES


Triple DES with two keys
P
64-bit plaintext
Encryption
DES cipher
DES reverse cipher
DES cipher
C
64-bit ciphertext
$k_1$
$k_2$
$k_1$
64-bit plaintext
P
Decryption
DES reverse cipher
DES cipher
DES reverse cipher
64-bit ciphertext
C

# DES and 3-DES

- DES, as the first important block cipher, has gone through much scrutiny. Among the attempted attacks, three are of interest: brute-force, differential cryptanalysis, and linear cryptanalysis.

- Triple DES with Three Keys

  - The possibility of known-plaintext attacks on triple DES with two keys has enticed some applications to use triple DES with three keys. Triple DES with three keys is used by many applications such as PGP

# AES: Advance Encryption Standard

- clear a replacement for DES was needed
  - have theoretical attacks that can break it
  - have demonstrated exhaustive key search attacks
- can use Triple-DES – but slow with small blocks
- NIST announced Call for ciphers in 1997
  - 15 candidates accepted in Jun 98
  - 5 were short-listed in Aug-99
  - Rijndael was selected as the AES in Oct-2000
  - issued as FIPS PUB 197 standard in Nov-2001

# Requirements - NIST

## Security:

- Resistance to cryptanalysis
- Soundness of the mathematical basis
- Randomness of the ciphertext

## Costs:

- System resources (hardware and software) required
- Monetary costs

## Algorithm and implementation characteristics

Simplicity: reduces implementation errors and impacts costs, such as power consumption, number of hardware gates and execution time

- Encryption and decryption using the same algorithm
- Ability to implement the algorithm in both software and hardware
- Use for other cryptographic purposes (hash function, a random bit generator and a stream cipher - such as via CTR mode)

# AES Competetion

| | Rijndael | Serpent | Twofish | MARS | RC6 |
|---|---|---|---|---|---|
| General Security | 2 | 3 | 3 | 3 | 2 |
| Implementation Difficulty | 3 | 3 | 2 | 1 | 1 |
| Software Performance | 3 | 1 | 1 | 2 | 2 |
| Smart Card Performance | 3 | 3 | 2 | 1 | 1 |
| Hardware Performance | 3 | 3 | 2 | 1 | 2 |
| Design Feature | 2 | 1 | 3 | 2 | 1 |
| Total | 16 | 14 | 13 | 10 | 9 |

I Won

- Thanks