Block ciphers (DES)

Hyoungshick Kim

Department of Software

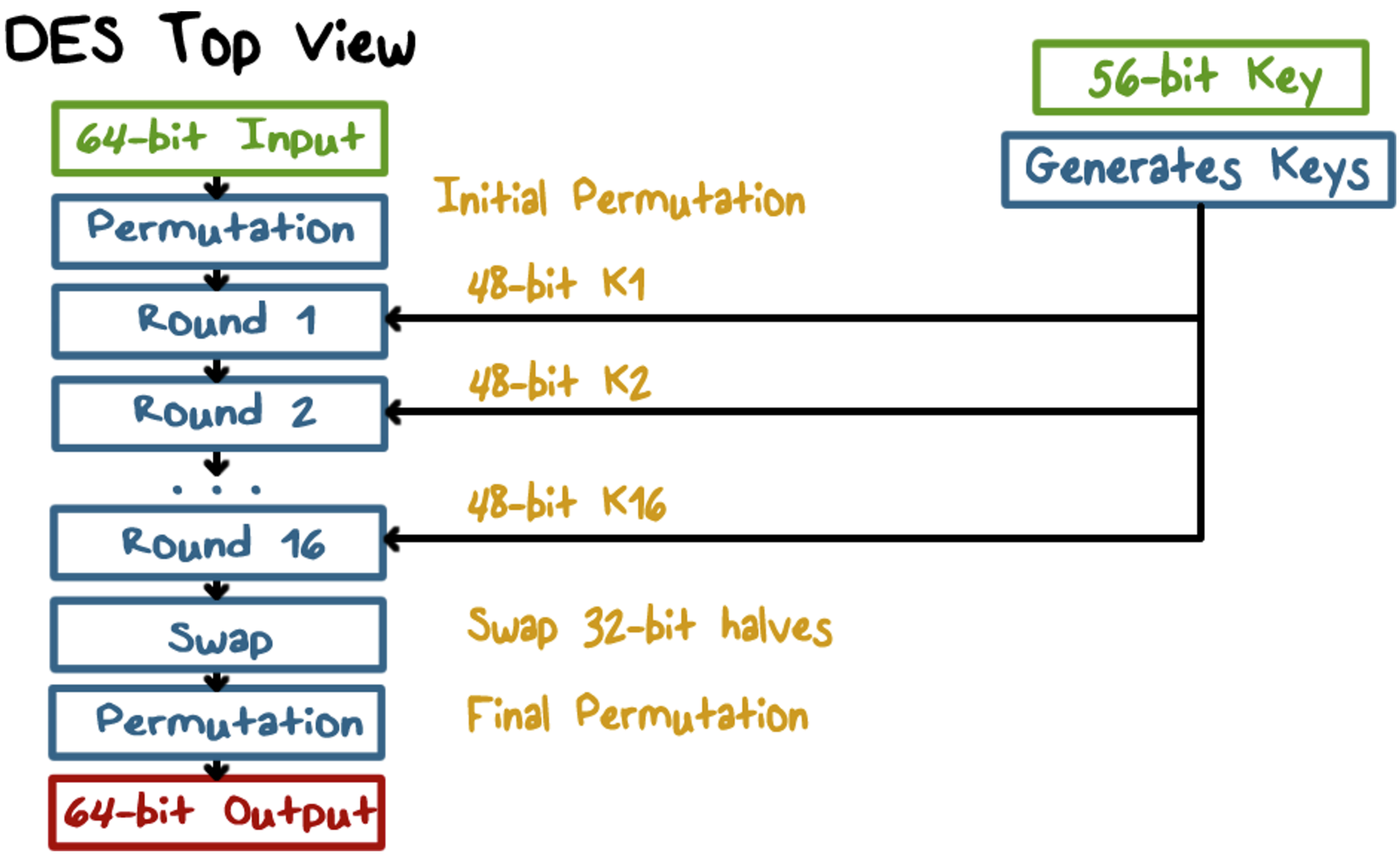
College of Software

Sungkyunkwan University

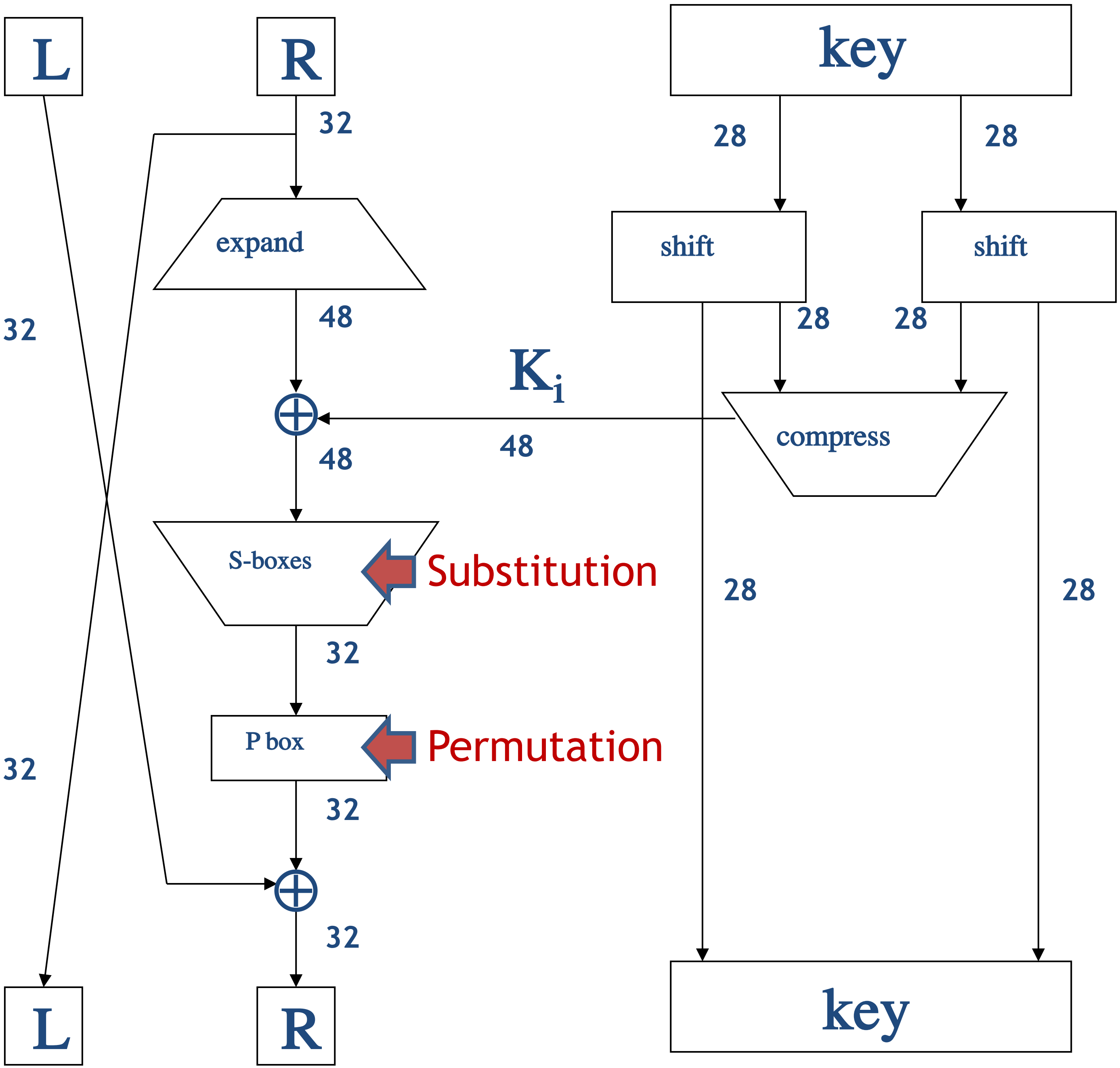
Data Encryption Standard (DES)

- DES was standardized in 1977; it’s widely used in banking, and assorted embedded stuff
- Based on IBM’s Lucifer cipher
- DES is a Feistel cipher with…
  - 64 bit block length
  - 56 bit key length
  - 8 bit parity
  - 16 rounds
  - 48 bits of key used each round (subkey)
- Each round is simple (for a block cipher)

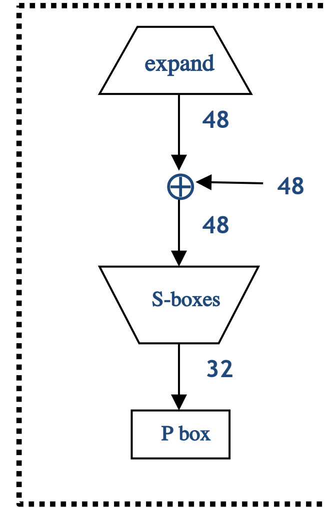
Overview of DES

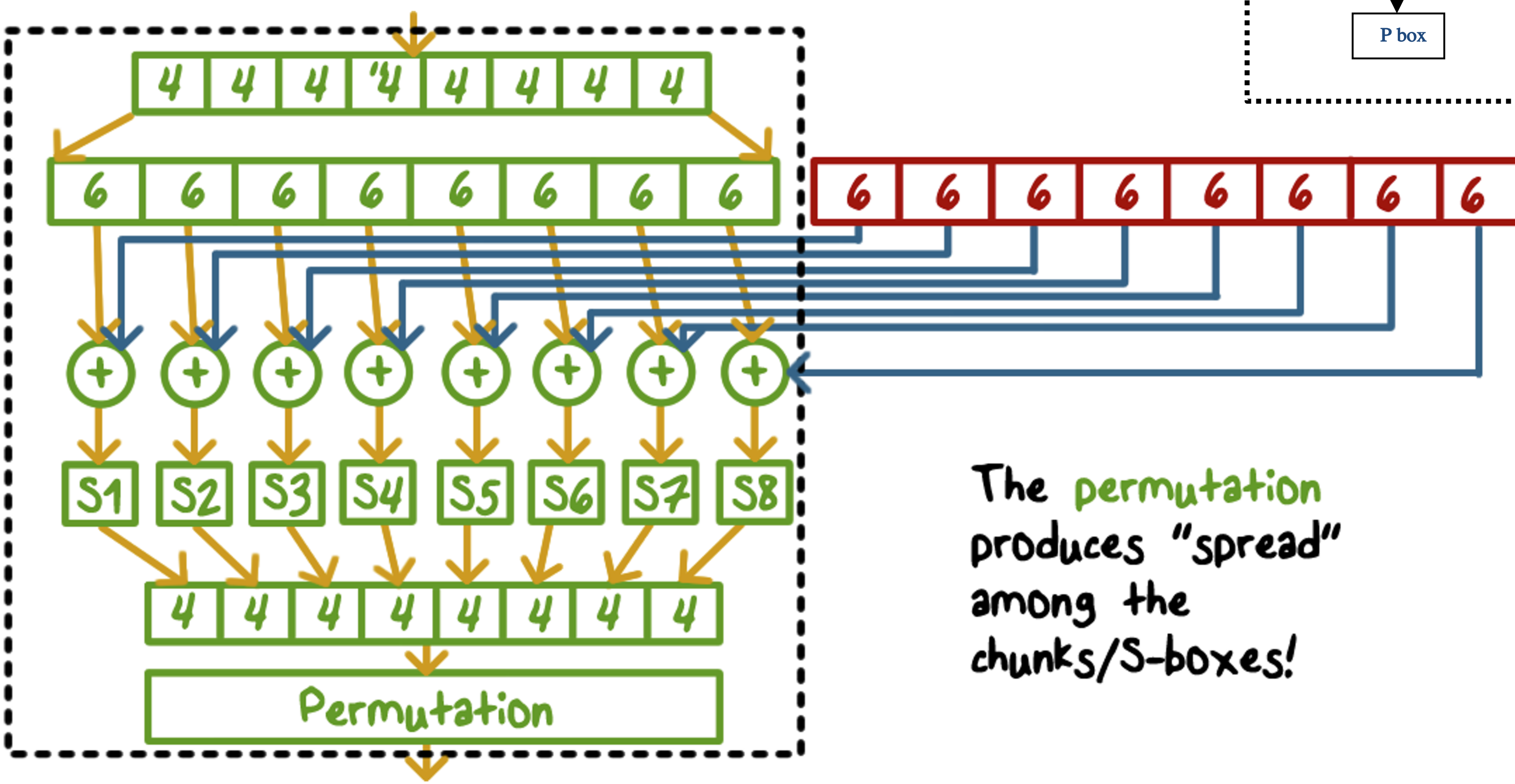


One round of DES



Mangler function

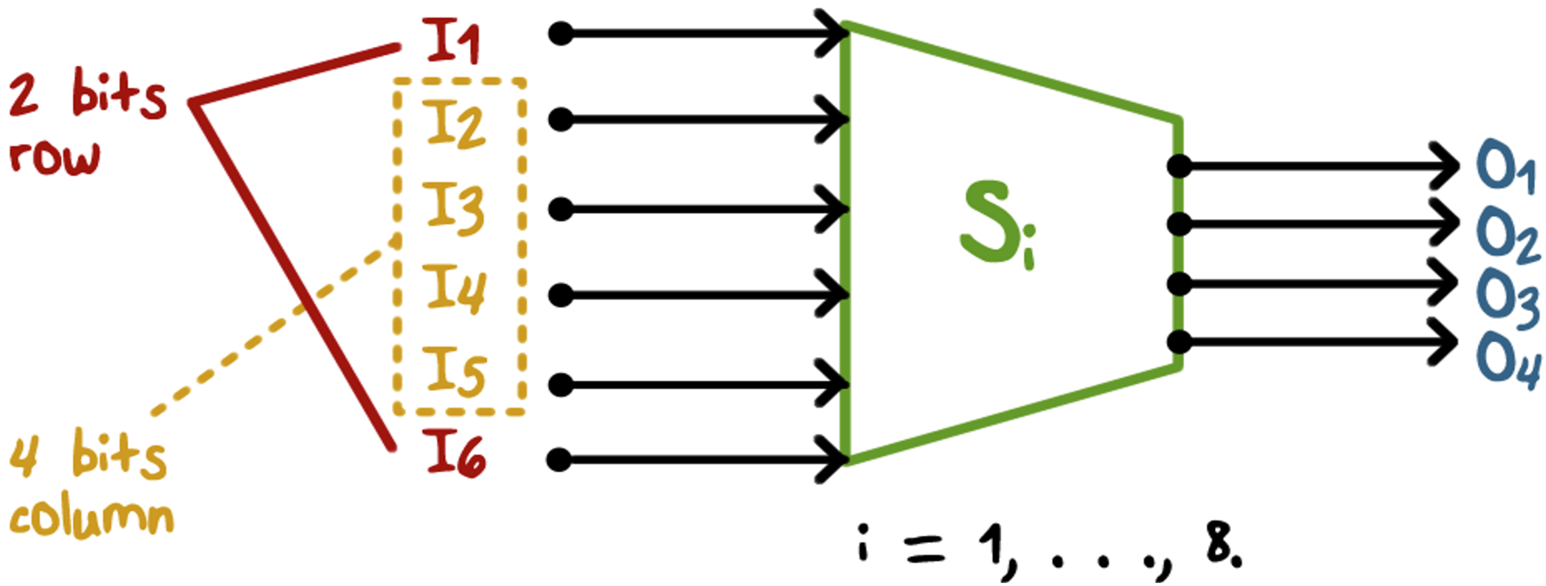




The permutation produces "spread" among the chunks/S-boxes!

S-box

- 48 bits => 32 bits. (8*6 => 8*4)
- 2 bits used to select amongst 4 substitutions for the rest of the 4-bit quantity



Quiz

For the given input, determine the output.

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Input: 011011

Output: 1001

Security of DES

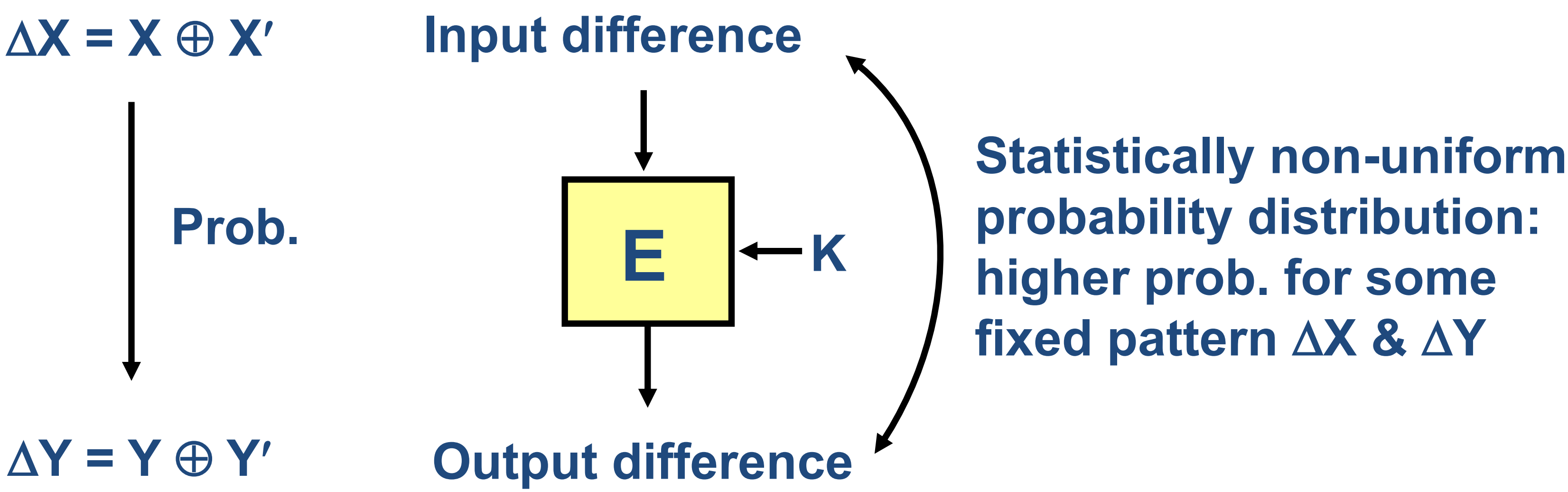
- Security depends heavily on S-boxes
  - Everything except for S-boxes in DES is linear
- Thirty+ years of intense analysis has revealed no “back door”
- Shortcut attacks exist but are not important:
  - differential cryptanalysis (2^{47} chosen texts)
  - linear cryptanalysis (2^{41} known texts)
- 56-bit key is too small – key search is the real vulnerability!
  - COPACOBANA (120 FPGAs, 10,000$) broke DES in 7 days.
  - In 2012, a system (48 FPGAs) broke DES in 26 hours.

Avalanche effect

- Key desirable property of an encryption algorithm
- Where a change of one input or key bit results in changing approx half of the output bits
- If the change were small, this might provide a way to reduce the size of the key space to be searched
- DES exhibits strong avalanche

Differential cryptanalysis

- E. Biham and A. Shamir : Crypto90, Crypto92
- It is called ‘differential’ because the attacker studies how a small change in the plaintext block affects the encrypted block

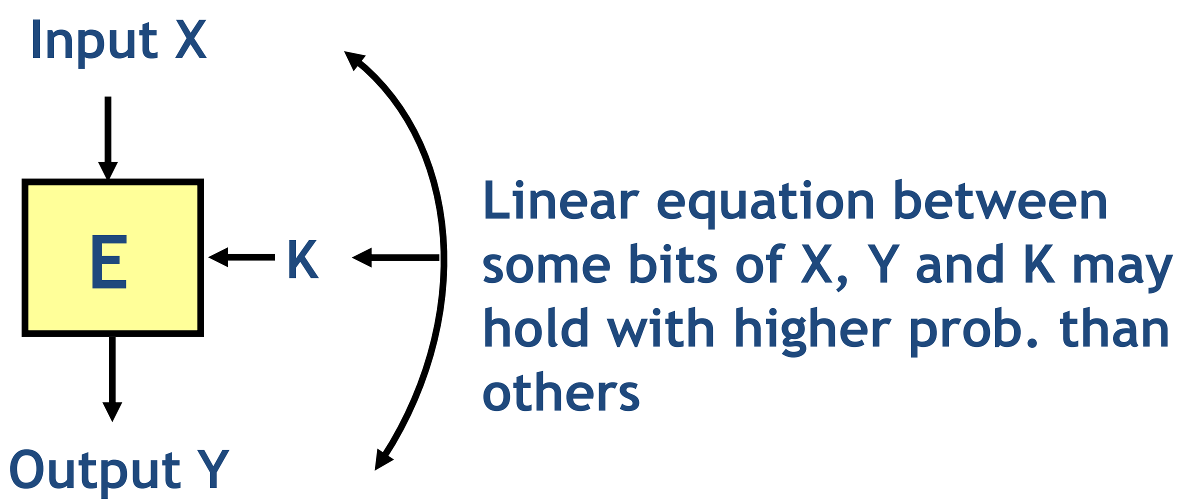


“Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag, 1993

* http://cs.ucsb.edu/~koc/ccs130h/notes/dc1.pdf

Linear cryptanalysis

- Matsui : Eurocrypt93, Crypto94
- Look for correlations between key, cipher input and output



"Linear Cryptanalysis Method for DES Cipher", Eurocrypt 93

Key space against brute-force search

- Consider brute-force search of key space; assume one key can be tested per clock cycle
- Desktop computer $\approx 2^{57}$ keys/year
- Supercomputer $\approx 2^{80}$ keys/year
- Supercomputer since Big Bang $\approx$ 2^{112} keys
- Modern key space: 2^{128} keys or more

Key length recommendation

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

NIST recommendation (2016)

(https://www.keylength.com/en/4/)

3DES

- Let $E : K \times M \longrightarrow M$ be a block cipher
- Define **3E**: $K^3 \times M \longrightarrow M$ as

$$\mathbf{3E}\big((k_1, k_2, k_3), m\big) = E\big(k_1, D(k_2, E(k_3, m))\big)$$

- Q. Why should we use **EDE** rather than **EEE**?
- key-size = $3 \times 56 = 168$ bits. But, $3 \times$ slower than DES.
- There exists a simple attack in time $\approx 2^{118}$

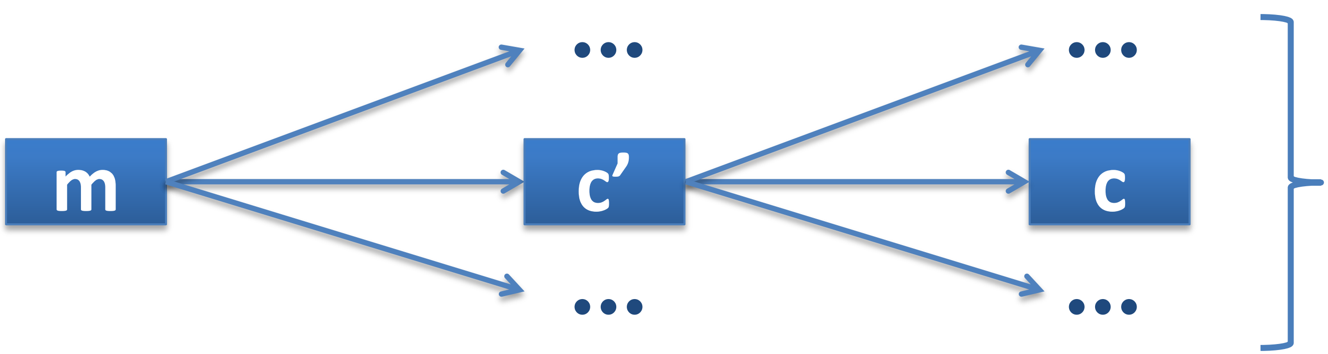
Q. What if $k_1 = k_2 = k_3$? **DES**

How about 2DES?

Define $2E(\,(k_1,k_2),\, m) = E(k_1\,,\, E(k_2\,,\, m)\,)$

$$m \rightarrow E(k_2,\cdot) \rightarrow E(k_1,\cdot) \rightarrow c$$

key-len = 112 bits



$c' = c$?

2^{112}

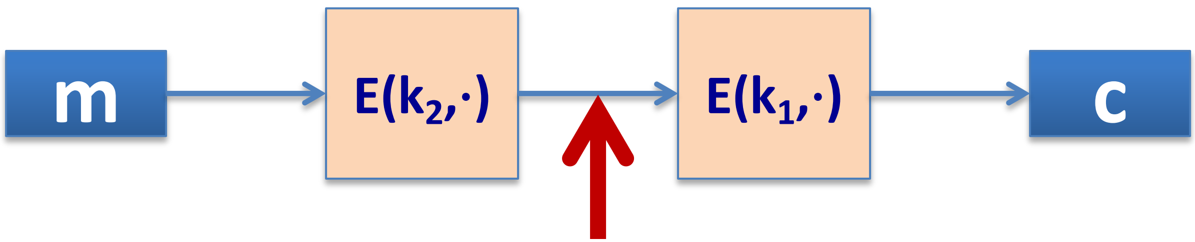
Why?

$2^{56} \times 2^{56}$

It looks good, right?

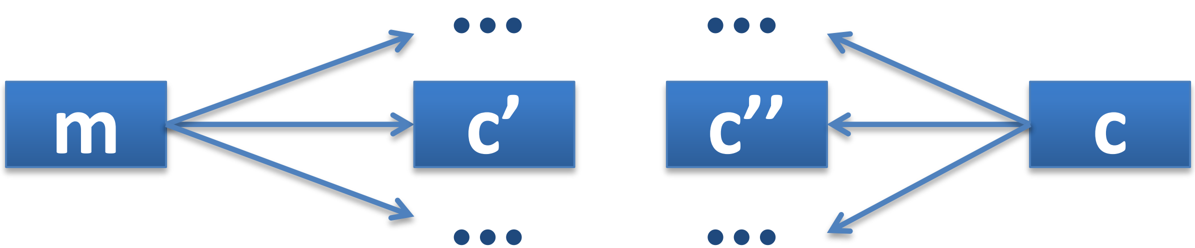
Meet in the middle attack (1)

- Define $2E(\,(k_1,k_2),\, m) = E(k_1\,,\, E(k_2\,,\, m)\,)$



key-len = 112 bits

Idea: key found when c' = c'': $E(k_i, m) = D(k_j, c)$



$2^{56} + 2^{56}$

$\approx 2^{57}$

Why?

Meet in the middle attack (2)

- Define $2E((k_1,k_2), m) = E(k_1 , E(k_2 , m))$

$$m \rightarrow E(k_2,\cdot) \rightarrow E(k_1,\cdot) \rightarrow c$$

key-len = 112 bits

Assumption: the attacker knows a pair of (m, c).

1. build table and then sort on 2nd column. Q. Why?

2. For all k all $k \in \{0,1\}^{56}$ do: test if D(k, c) is in the 2nd column. If so then **$E(k^i, m) = D(k, c)$** → **k_2: k^i and k_1: k**

$k^0 = 00…00$	$E(k^0 , m)$
$k^1 = 00…01$	$E(k^1 , m)$
$k^2 = 00…10$	$E(k^2 , m)$
⋮	⋮
$k^N = 11…11$	$E(k^N , m)$

2^{56} entries

Same attack on 3DES: Time = 2^{112} , space ≈ 2^{56}

Questions?


Sungkyunkwan
Campus
established
Sciences
campus
university
University
School
Suwon
Seoul
Natural
Graduate
English
constructed
Korean
edit
Social
Global
Building
Institute
Humanities
Professors
Confucian
Korea
schools
Science
Academic
ASLE-Korea
Administration
located
Joseon
Engineering
Education
Anniversary
Advanced
also
two
four