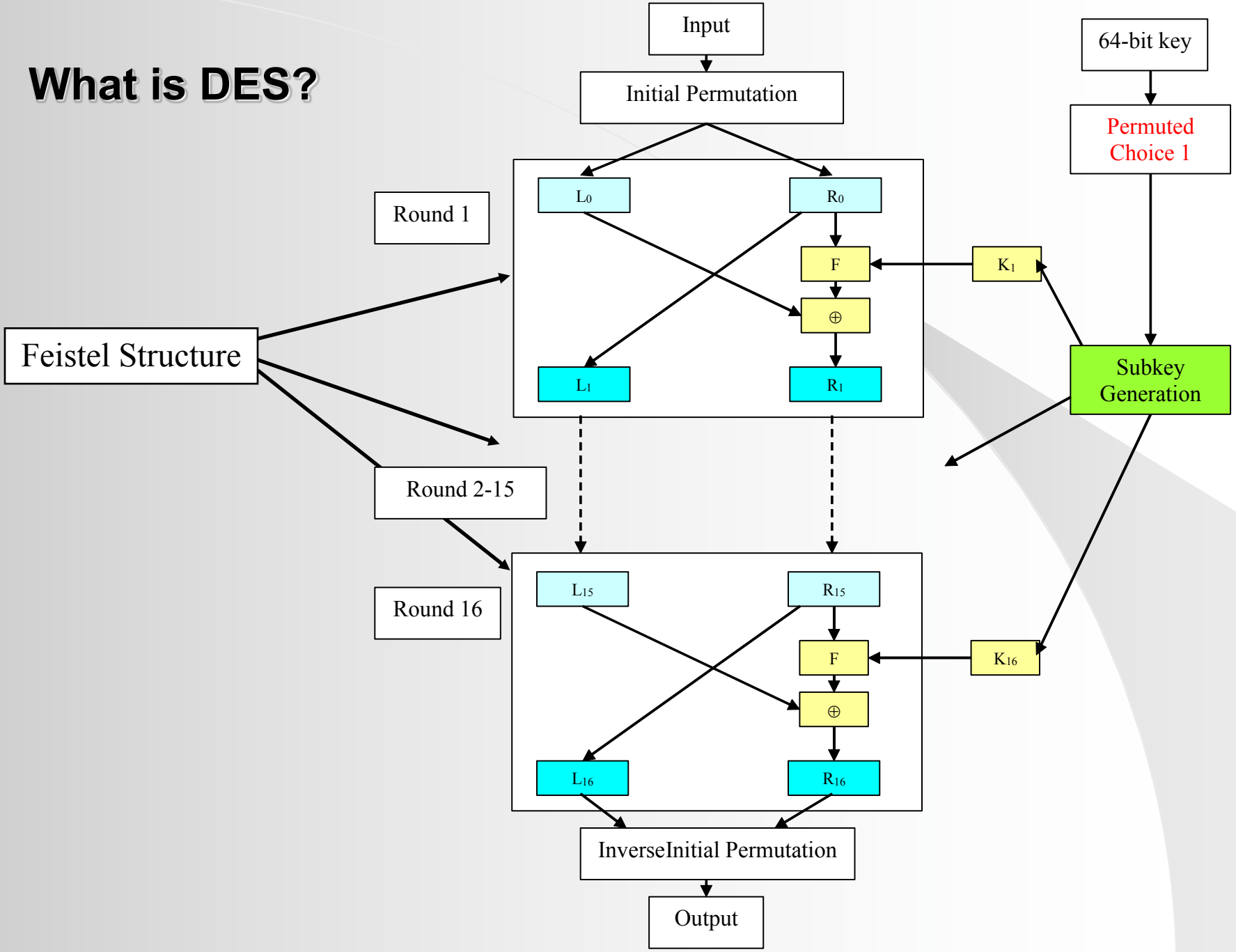
COMP 3355
Modern Cryptography

K.P. Chow
University of Hong Kong

Modern Cryptography – DES and AES

- DES (Data Encryption Standard)
  - A block cipher with 56-bit key (64-bit including parity bits), 64-bit block
  - Most commonly used block cipher
  - The same hardware can be used for both encryption and decryption based on the "Feistel" network structure
  - Designed to facilitate hardware implementation
- In 1999, NIST issued a new standard requiring "Triple DES" to be used
- As of 26 Nov 2001, AES, a standardization of Rijindael, adopted as the Federal Information Processing Standard FIPS01

What is DES?

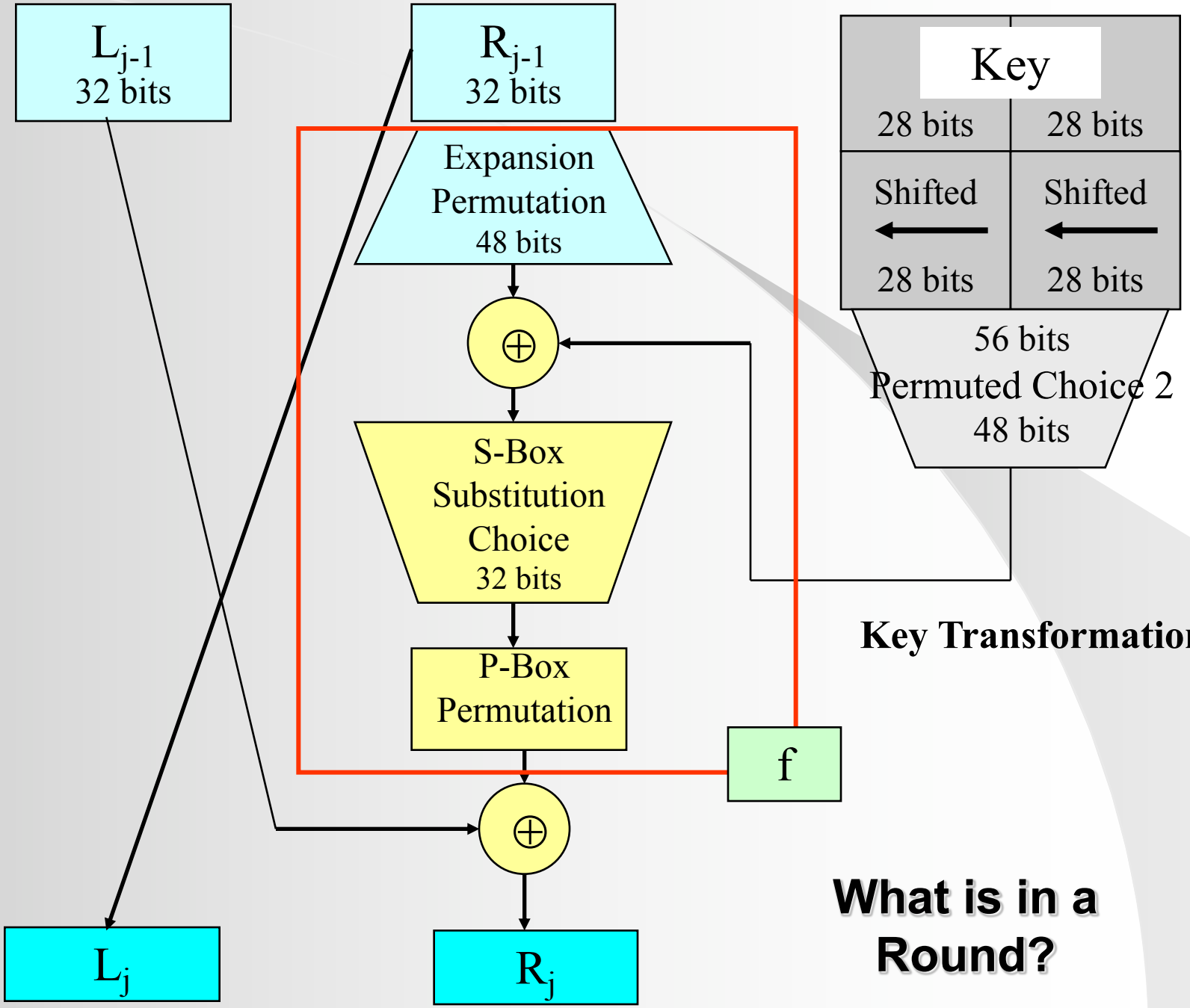

Input
Initial Permutation
64-bit key
Permuted Choice 1
Round 1
L0
R0
F
K1
⊕
Feistel Structure
L1
R1
Subkey Generation
Round 2-15
Round 16
L15
R15
F
K16
⊕
L16
R16
InverseInitial Permutation
Output

Feistel Structure

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

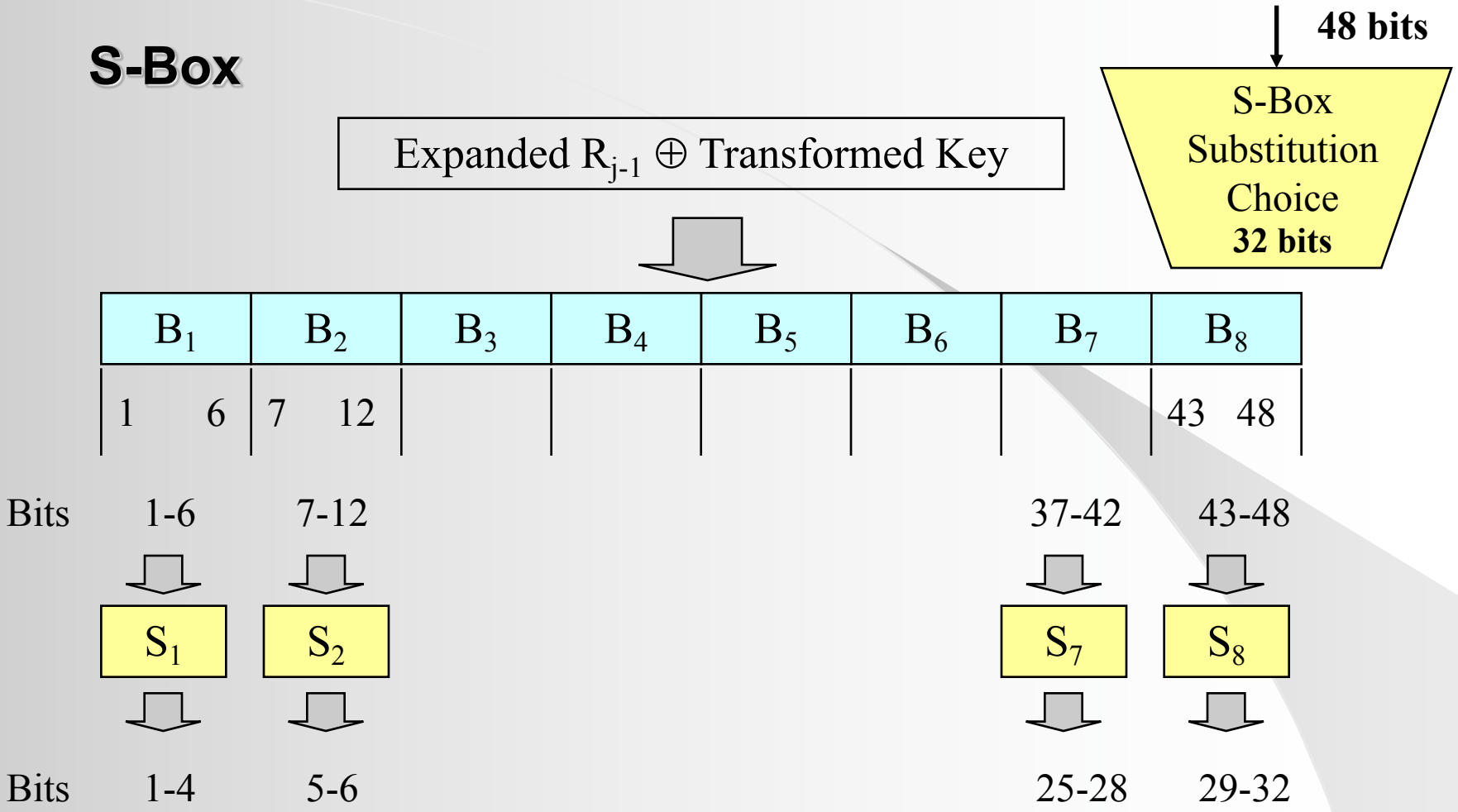
How about the inverse?

- Inverse is the same:
- $R_i = L_{i+1}$
- $L_i = R_{i+1} \oplus f(K_i , L_{i+1})$


L_{j-1}
32 bits
R_{j-1}
32 bits
Key
28 bits
28 bits
Shifted
Shifted
28 bits
28 bits
56 bits
Permuted Choice 2
48 bits
Expansion
Permutation
48 bits
S-Box
Substitution
Choice
32 bits
P-Box
Permutation
f
L_j
R_j
Key Transformation
What is in a Round?

Substitution: S-box
Permutation: P-box

S-Box


48 bits
S-Box
Substitution
Choice
32 bits
Expanded R_{j-1} ⊕ Transformed Key
B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8
1 6
7 12
43 48
Bits 1-6 7-12 37-42 43-48
S_1 S_2 S_7 S_8
Bits 1-4 5-6 25-28 29-32

S-Box – S1 to S8

S_1

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

S_2

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

S_3

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

S_4

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

S_5

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

S_6

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

S_7

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

S_8

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

P-Box

P-Box Permutation

- All 32-bits from the S-box substitution are permuted by a straight permutation P
- The permutation P is as follow:

Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
From Input Bit	16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10

Bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
From Input Bit	2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

S-box Design Criteria

- The criteria for the design of the substitutions (S-boxes), fixed permutation (P-box), and key schedule were not published by the designers at the beginning (rumor about possible backdoor)
- In 1994, Coppersmith of IBM published the design criteria of S-boxes:
  - The S-boxes were carefully tuned to increase resistance against differential cryptanalysis
  - No S-box is a linear or affine function of its input: the 4 output bits cannot be expressed as a system of linear equations of the 6 input bits
  - Changing 1 bit in the input of an S-box results in changing at least 2 output bits: the S-boxes diffuse their information well throughout their outputs
  - The S-boxes were chosen to minimize the difference between the number of 1s and 0s when any single input bit is held constant: holding a single bit constant as a 0 or 1 and changing the bits around it should not lead to disproportionately many 0s or 1s in the output

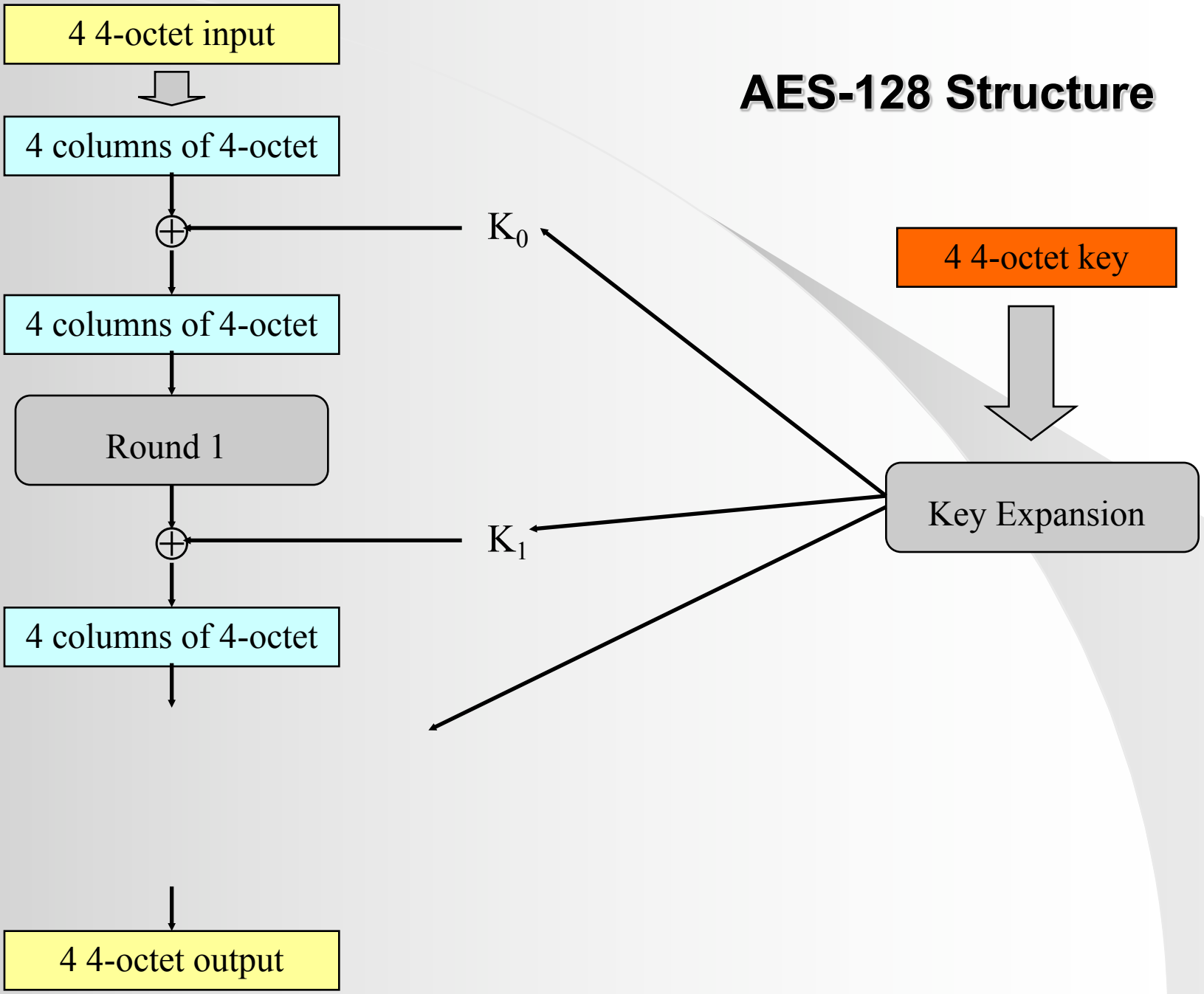
Key Search Machine

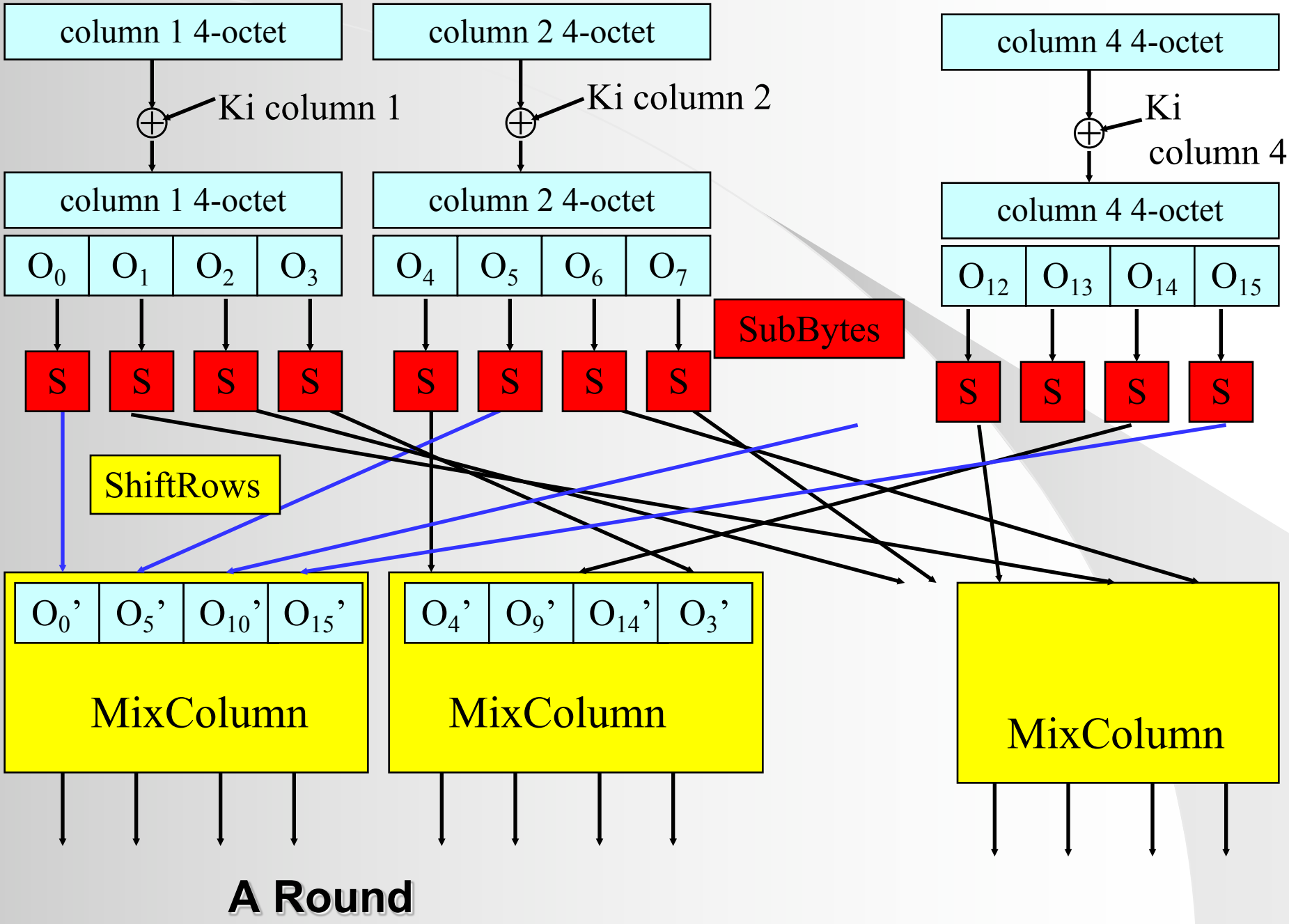
- The Electronic Frontier Foundation (EFF) had designed "Deep Crack", an ASIC-based specialized machine (1800 ASIC chips, 40MHz clock) in 1998
  - Total Cost: US$220,000
  - EFF also made the entire design documents publicly available:
    - **"Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design" by Electronic Frontier Foundation, John Gilmore (Ed), Publisher:** O'Reilly & Associates; May 98
  - With the design, it only costs US$150,000 to replicate a machine (in 1998)
  - Average time of search: 4.5 days/key

Advanced Encryption Standard (AES)

- On Jan 2, 1997, NIST announced a contest to select a new encryption standard to be used for protecting sensitive, non-classified, U.S. government information
- 21 submissions from all over the world, 5 selected as the final candidates in Aug 1999: Rijndael, Serpent, MARS, Twofish, RC6
- 26 Nov 2001, AES (a standardization of Rijndael) became the Federal Information Processing Standard (FIPS01)
- Rijndael is NOT a Feistel cipher
- AES mandates a block size of 128 bits and a choice of key size from 128, 192, 256 bits (called AES-128, AES-192, AES-256)

AES-128 Structure




column 1 4-octet
column 2 4-octet
column 4 4-octet
Ki column 1
Ki column 2
Ki
column 4
column 1 4-octet
column 2 4-octet
column 4 4-octet
O0 O1 O2 O3
O4 O5 O6 O7
O12 O13 O14 O15
SubBytes
S S S S S S S S S S S S
ShiftRows
O0' O5' O10' O15'
O4' O9' O14' O3'
MixColumn
MixColumn
MixColumn

A Round

Diffusion and Confusion in AES

- Diffusion: changes in the plaintext should affect many parts of the ciphertext
  - By permutations in ShiftRows and MixColumns
- Confusion: difficult to predict when changing one character in the plaintext will do to the ciphertext (relationships are lost)
  - By substitutions (S-Box) in SubBytes

AES Algebraic Structure – S-Box

- AES has a simple algebraic structure: it is possible to write an AES encryption as a simple closed algebraic formula over the finite field with 256 elements
- The S-Box can be represented by the following algebraic form, while the look up table is an easy and faster representation of the algebraic structure

$$\begin{vmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{vmatrix} \times \begin{vmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{vmatrix} \otimes \begin{vmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{vmatrix}$$

AES Algebraic Structure – Mix Column

$$\begin{vmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{vmatrix} = \begin{vmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 01 & 03 \\ 03 & 01 & 01 & 02 \end{vmatrix} \otimes \begin{vmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{vmatrix}$$

- MixColumn is a matrix-multiplication operation
  - $\otimes$ means to perform matrix multiplication with the $\bullet$ operator and XOR instead of addition
  - It guarantees that the original plaintext bit pattern becomes highly diffused over several rounds
  - It also ensures there is very little correlation between the inputs and the outputs

Cryptographic Hash Function

- Compression: for any size of input x, the output length of y=h(x) is small
- Efficiency: easy to compute h(x) for any input x
- One-way: Given any value y, it is computationally infeasible to find a value x such that h(x) = y
- Collision resistance
  - Given x and h(x), it is infeasible to find $y \neq x$ such that h(x) = h(y)
  - It is infeasible to find x and y, with $y \neq x$, such that h(x) = h(y)
- Common used cryptographic hash function: MD5, SHA-1, SHA-256

Diffusion Property of SHA-256

Example 20.3: The Diffusion Capabilities of Secure Hash Algorithm—SHA-256 That Can Be Applied to Protect the Integrity of Files

The input to SHA-256 is the following plaintext:

```
 Phishing Explained
 Phishing scams are typically fraudulent e-mail messages appearing
to come from legitimate sources like your bank, your Internet Service
Provider, eBay, or PayPal, for example. These messages usually direct
you to a fake web site and ask you for private information (e.g.,
                                                 perpetrators then
                                                 ssage may not be
                                                 aking the bait."
                                                 rm. They contain
                                                 JST click on the
                                                 ne, be wary. Fake
                                                 r" or "Attention
                                                  If the URL dis-
                                                 same as the text
                                                 a fake. Sometimes
```

/6nUwxfi8JFrSCXe7J6ZUmyHZk1ZcWSFP5OiyAFkPNc =

The corresponding digest in binary format is listed as follows:

```
1010110001010110011110011101000000111010000111101101110100101001 0110
1111101101000100001001 [illegible] 1101100100110111 10001
00110011011001010100110 1 [illegible] 11000000011011 0001011
1010011011111111110101 1 [illegible]
```

Text first "P" to "Q"

A single character change i[illegible]nificant change in the corresponding digest. For example, changing the first character from P to Q, i.e., from Phishing to Qhishing, results in the following digest from SHA-256 encoded in BASE64 format:

rZo6V2mYL9pI06fZjNMb711eQVpIAAiCWfvhomaUC/A =

The corresponding digest in binary format is listed as follows:

```
1010010011001011100010110101000100101100110011111010000001001011 0110
111001011000101100000100110011100110010110011100100000100001 01000101
0100001101111101010010110110111111111111101110111110110100110 00000
1000001111001011101100110010110101111111010000010000
```

Basic Structure of SHA-1

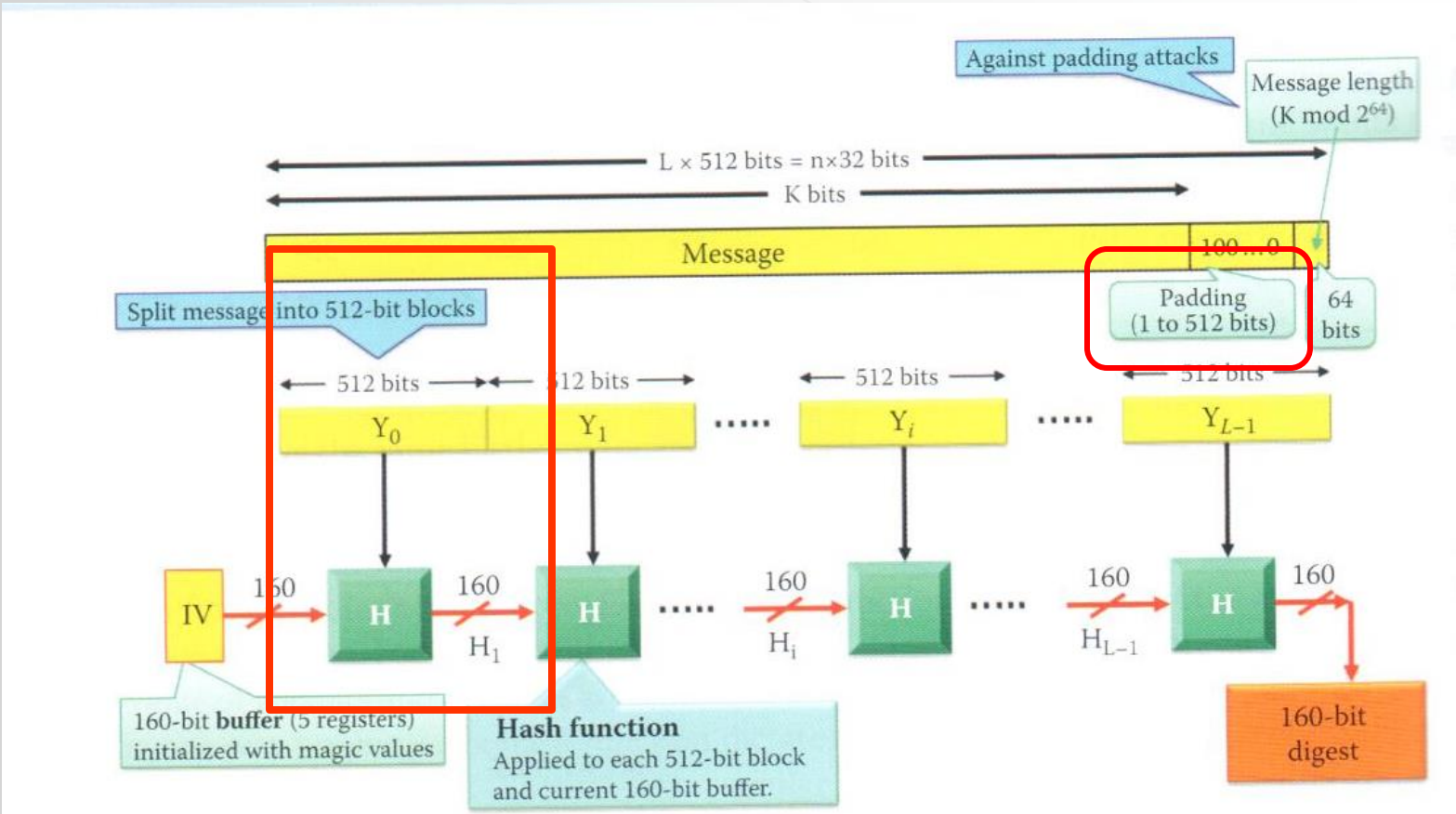


FIGURE 20.6 The basic structure for SHA-1.

HMAC

- Hash Message Authentication Code (HMAC)
- The use of a shared secret key that provides authentication in addition to integrity protection
- Some features
  - Faster than encryption in software
  - Use of any hash function is permitted in any export product from US
  - Used in IPsec and TLS

HMAC Structure

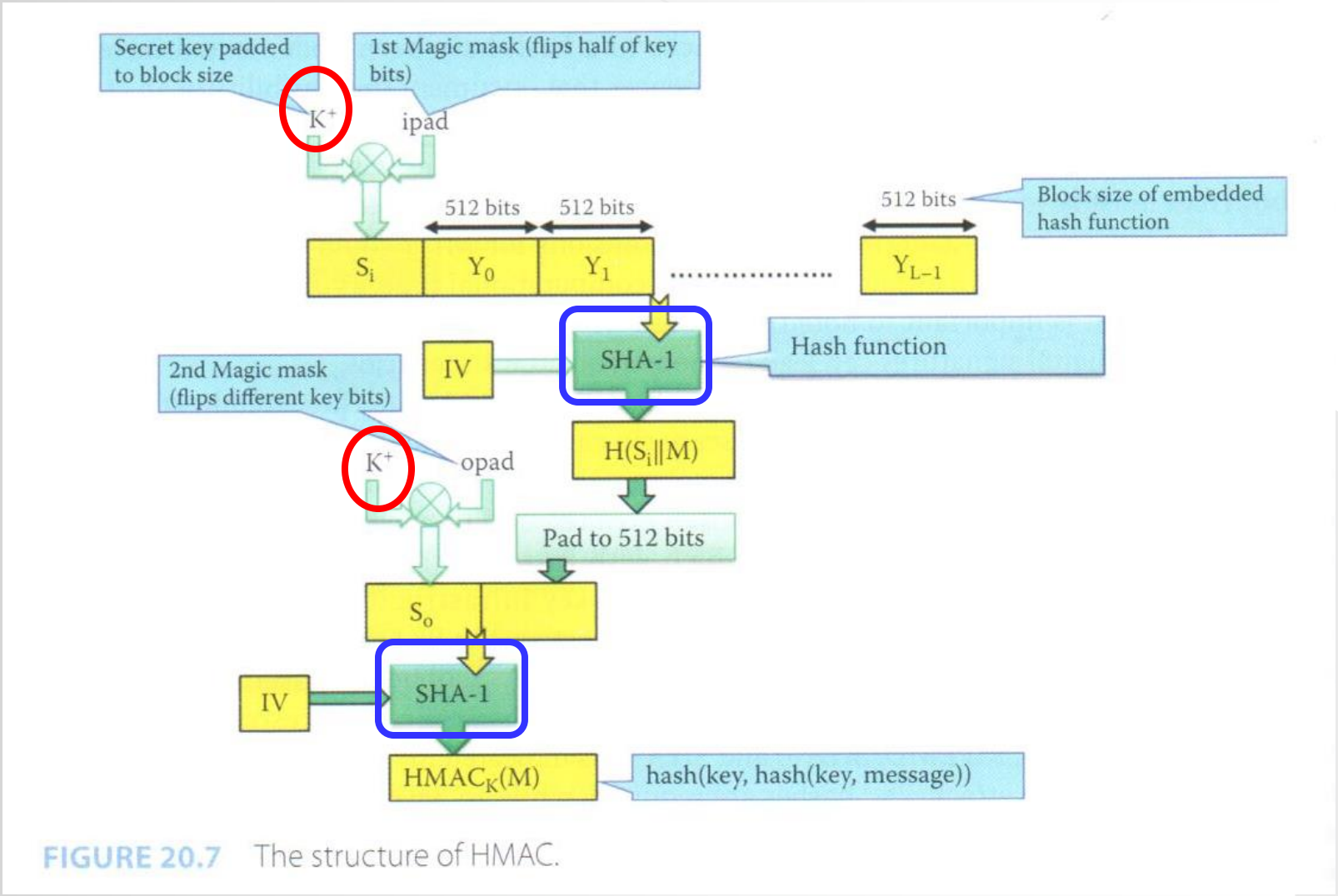


FIGURE 20.7 The structure of HMAC.