Information Security
CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Secure Communication and Storage

- **Vulnerable components**
  - Channels
  - Processes (clients, servers)

- **Security properties:**
  - Authentication
  - Authorization
  - Confidentiality
  - Integrity
  - Availability

Types of cryptographic functions

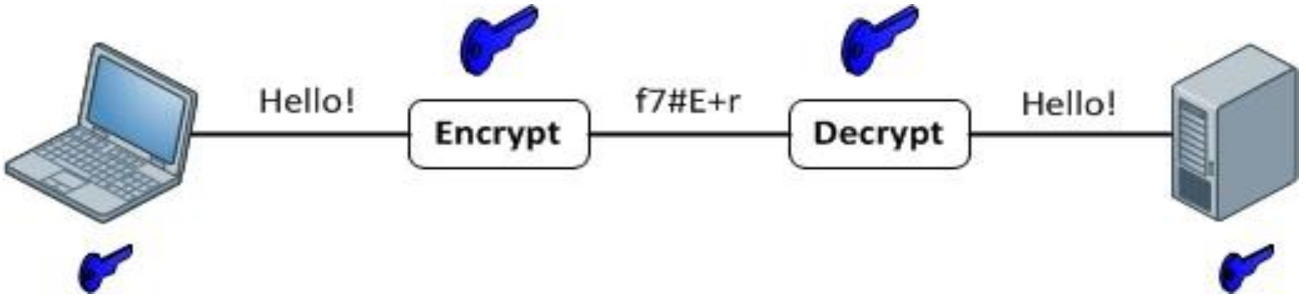
- Secret/symmetric key cryptographic function
  - Uses 1 key
  - Fast computation
- Public/Asymmetric key cryptographic function
  - Uses 2 keys
  - Slow computation
- Hash functions
  - Uses no keys
  - Very fast computation

Key terms

- Plaintext
  - Readable message or data that needs to be protected
- Encryption Algorithm
  - Algorithm to perform various substitutions and transformations on the plaintext
- Secret key
  - Used as input to the algorithm, transformations depend on the key
- Ciphertext
  - Scrambled message produced as output
- Decryption Algorithm
  - Produces the original plaintext

Symmetric/secret key encryption

- Also called conventional cryptography
- Sender and receiver must both know the secret key
- Uses techniques like confusion and diffusion to encrypt/decrypt data



Symmetric encryption uses

- Transmitting over secure channel
- Secure storage on insecure media

- Authentication
  - Strong authentication: prove the knowledge of a secret without revealing it

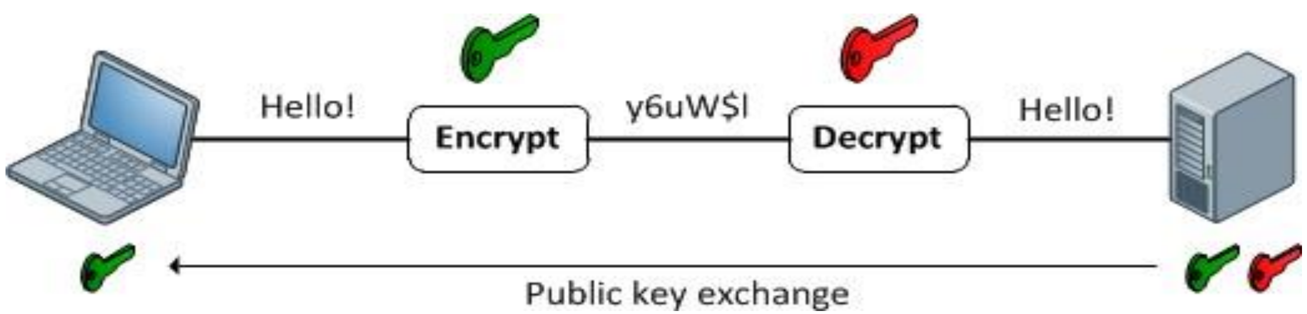
- Integrity check
  - Checksum vs cryptographic checksum
  - Message Authentication Code (MAC)/MIC

Problems with symmetric cryptography

- No mechanism of sharing the key.
- Impersonation problem.
  - If Alice and bob share a key. Imagine Trudy shares the same key with Alice for secure communication. Trudy may act as alice and talk to bob.
- Difficult key management

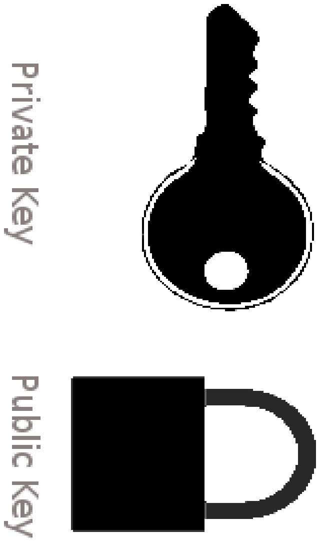
PUBLIC KEY CRYPTOGRAPHY

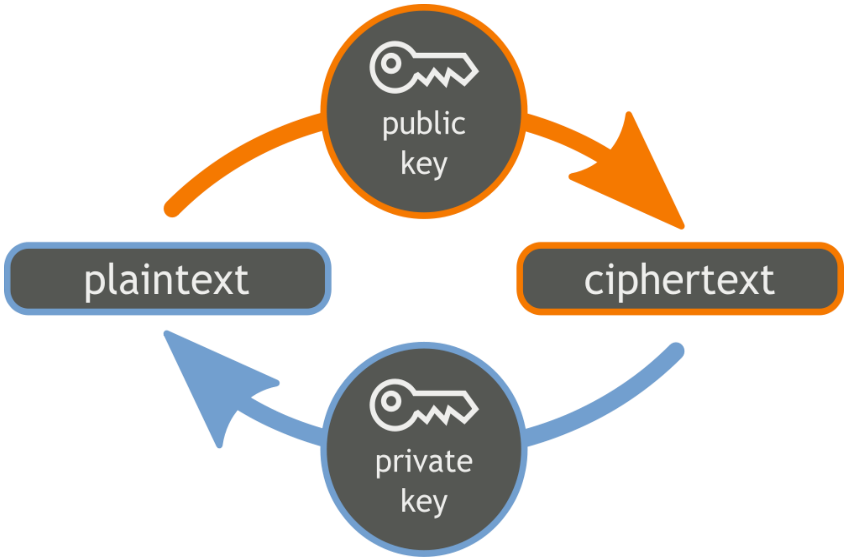
- Also called Asymmetric cryptography
- Rather newer form of cryptography – invented in 1975.
- Two keys – Public Key & Private Key
- Based on hard mathematical problems



Public key encryption

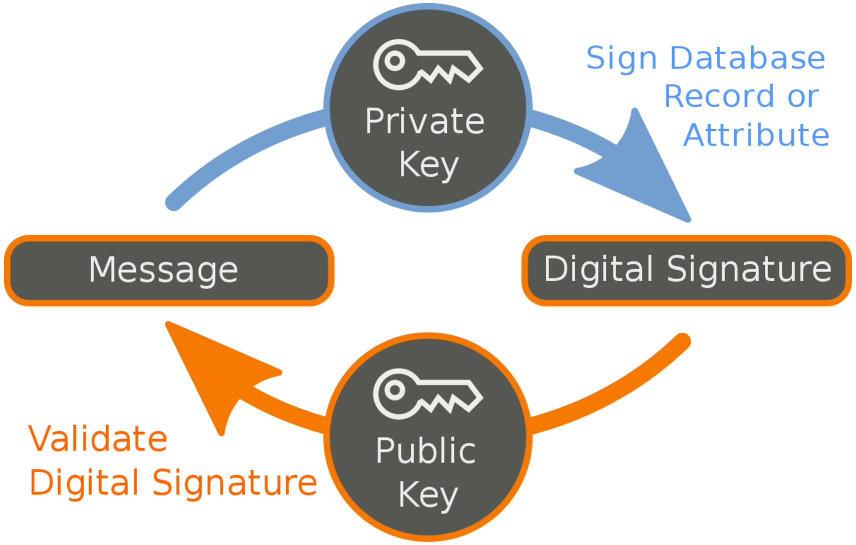
- **The private key can unlock (decrypt) what is locked (encrypted) with the public key and vice versa**





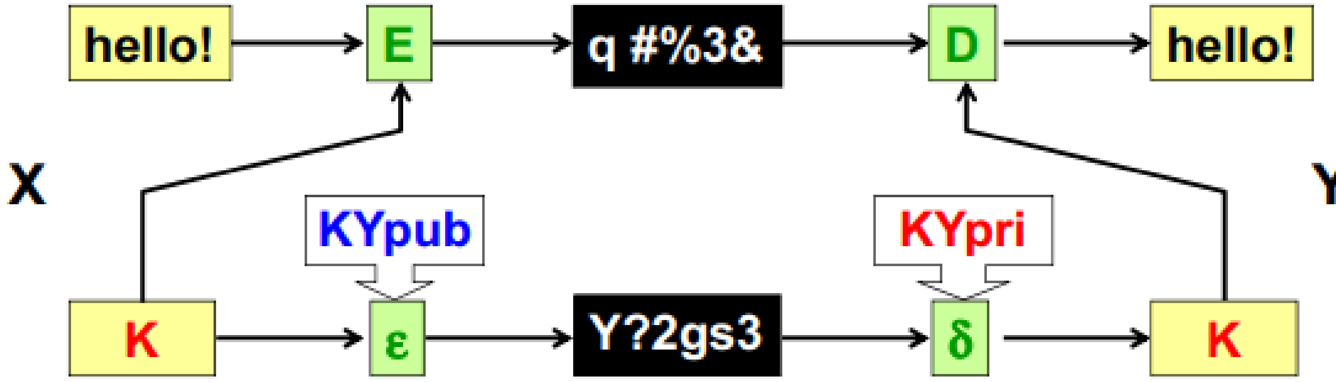
Digital signature

- Scheme for proving the authenticity and origin of a message.
- Recipient is sure of the origin of the message
- Sender can not deny having sent
- the message(non-repudiation)



Using PKC to share secret key

- **The key(K – which is the secret key NOT the private key) is encrypted using the Public key of Y so that the key(K) is shared between X and Y only. Then that K is used for encryption of data(hello!)**



Public Key Cryptography Uses

- Used primarily for Symmetric key exchange
- Transmitting over an insecure channel
- Secure storage on insecure media
- Authentication
- Easy key management
- Digital signatures
  - Non-repudiation
  - Data integrity

Symmetric Encryption

E, D: Algorithms **k: secret key**

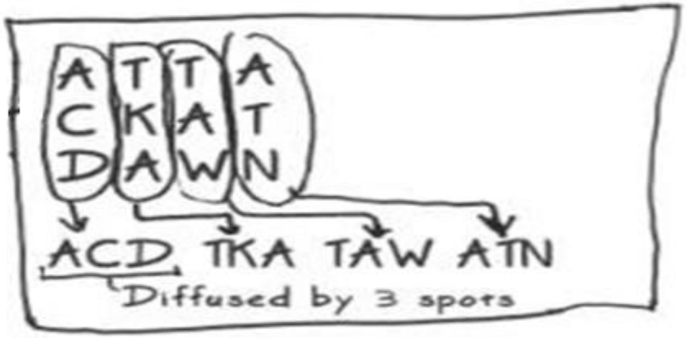
m: plaintext **c: ciphertext**

Encryption algorithm Should be publicly known

Early days techniques

- Confusion
  - Replacing of some bit strings with other bit strings
  - Also called substitution or Caesar's cipher

- Diffusion
  - Changing order of bit strings
  - Also called permutation/transposition



Question

What is the size of key space in the substitution cipher assuming 26 letters?

$$|\mathcal{K}| = 26$$

$$|\mathcal{K}| = 26!$$

$$|\mathcal{K}| = 2^{26}$$

$$|\mathcal{K}| = 26^2$$

Breaking of Substitution Cipher

(1) Use frequency of English letters

E, T, A

(1) Use frequency of pairs of letters (di-grams)

an , in , the

Example

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYY
FVUFOFEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCU
BOYNRVNIWNCPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZ
PUKBZPUNVPWPCYVFZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUN
VNIPUBRNCHOPYXPUBNCUBOYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCY
VFZIXUPUNFCPWZPUKBZPUNVR

B	36
N	34
U	33
P	32
C	26

➔ E

➔ T

➔ A

NC	11
PU	10
UB	10
UN	9

Di-grams

➔ IN

➔ AT

UKB	6
RVN	6
FZI	4

Tri-grams

➔ THE

Vigenere Cipher

- **Idea:** Uses Caesar's cipher with various different shifts, in order to hide the distribution of the letters.
- A key defines the shift used in each letter in the text
- A key word is repeated as many times as required to become the same length

Plain text: I a t t a c k
Key: 2 3 4 2 3 4 2
Cipher text: K d x v d g m

(key is "234")

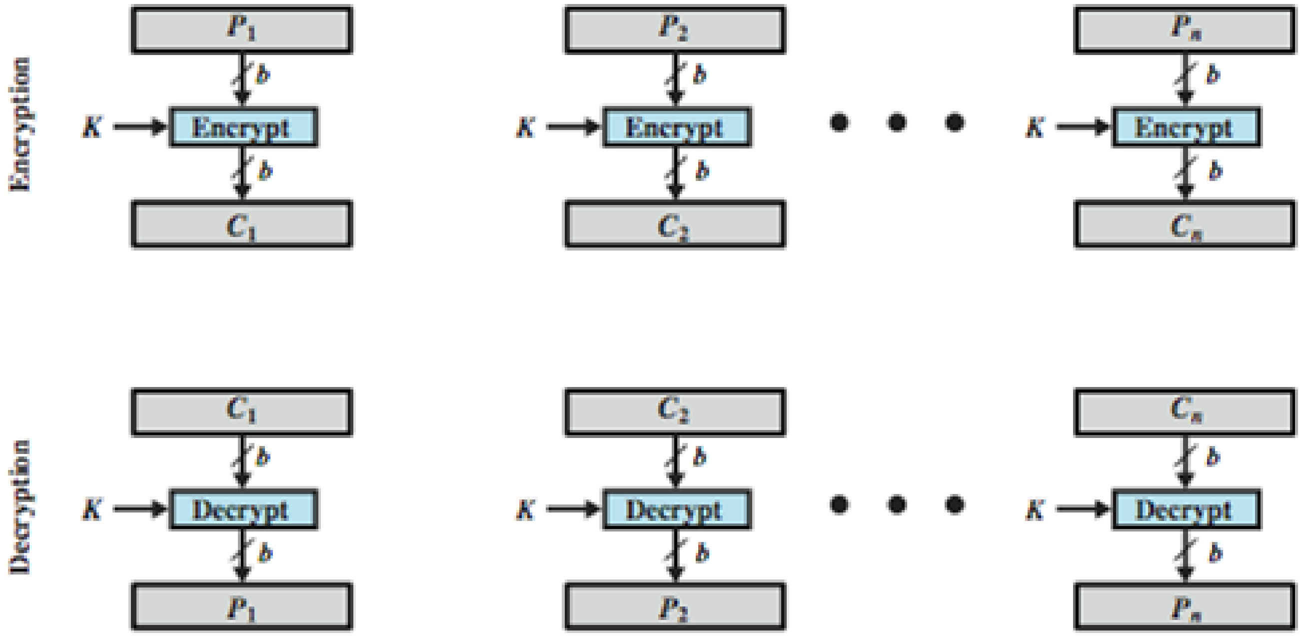
Breaking of Vigenere Cipher

- **Find repeated strings in the ciphertext. Their distance is expected to be a multiple of the length. Compute the gcd of (most) distances.**
- **For example:**
  - **Plaintext: TOBENOTORTOBE**
  - **Keyword: 1231231231231**
  - **Ciphertext: UQEFPRUQUUQEF**

Diagraph	First Position	Second Position	Distance	Factors
UQ	1	7	6	3
UQ	7	10	3	3
EF	3	12	9	3
QE	2	11	9	3

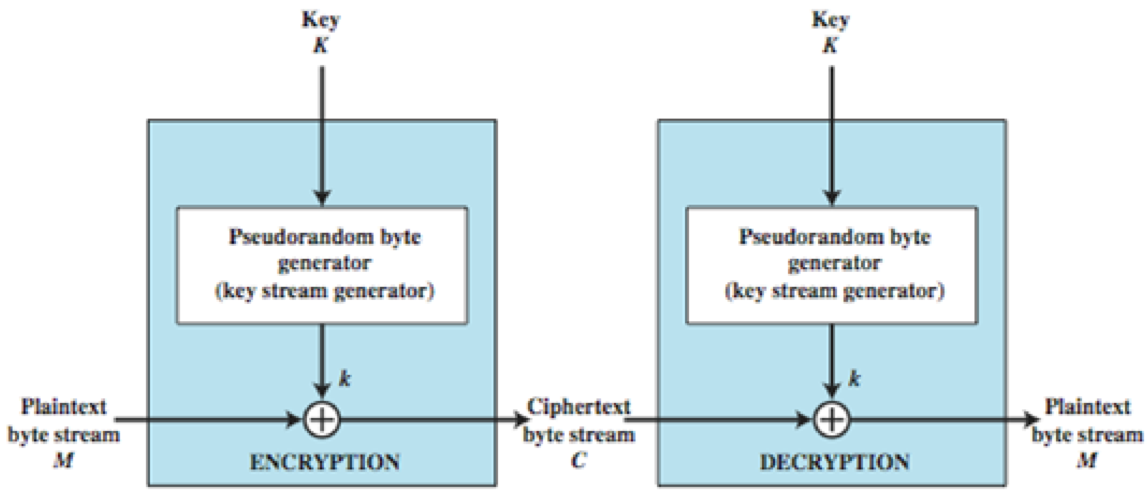
Block Cipher

- Processes the plaintext input in fixed-size blocks
- produces a block of cipher text of equal size for each plaintext block.



Stream Cipher

- Processes the input elements (typically 1 byte at a time) continuously, producing output one element at a time
- With a properly designed pseudorandom number generator, a stream cipher can be as secure as block cipher of comparable key length.
- The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers.
- The advantage of a block cipher is that you can reuse keys.



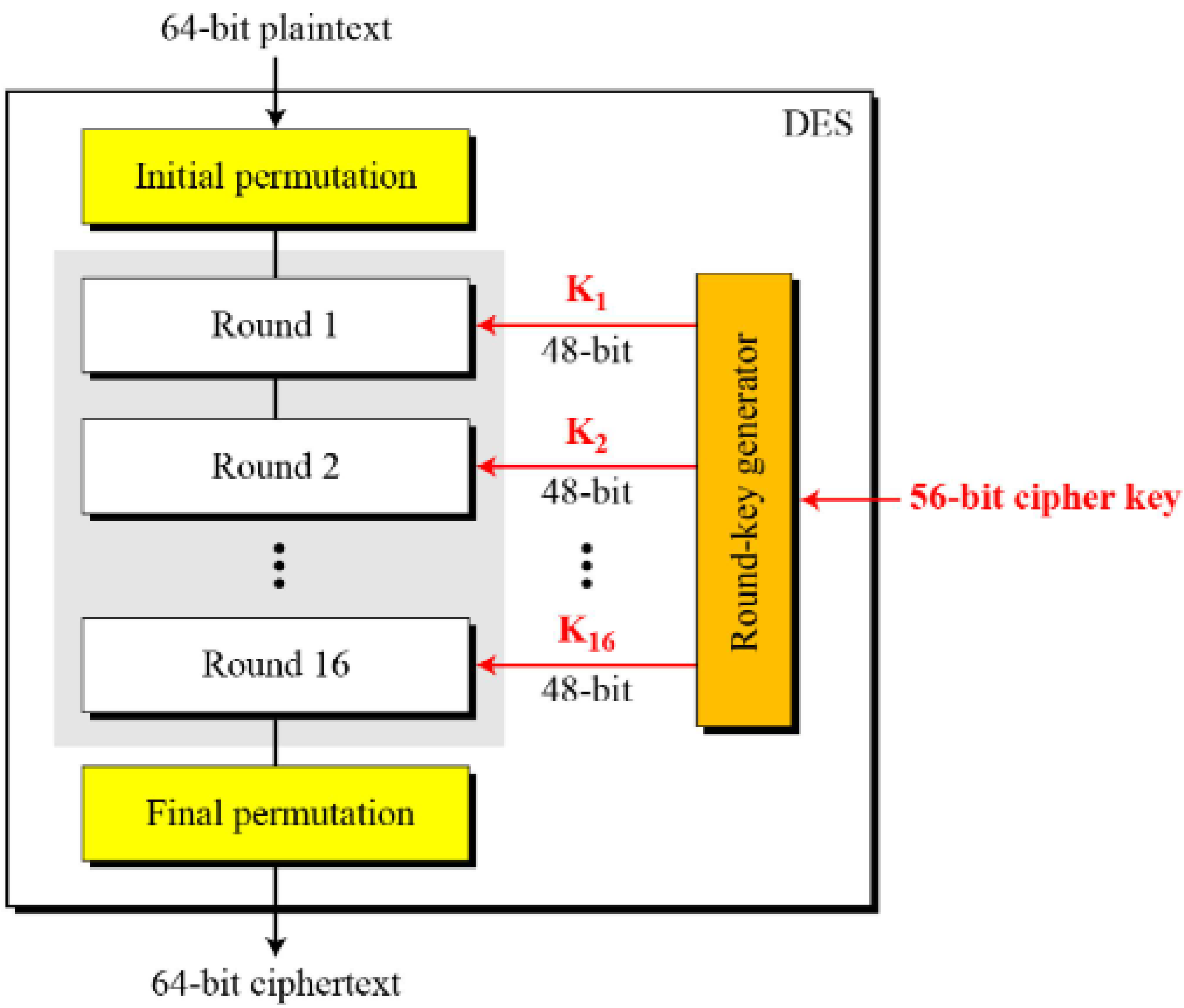
Data Encryption Standard (DES)

- **Data Encryption Standard (DES) is the most widely used encryption scheme**
  - **uses 64 bit plaintext block and 56 bit key to produce a 64 bit cipher text block**
  - **concerns about algorithm & use of 56-bit key**

- **Concerns**
- **The first concern refers to the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm.**

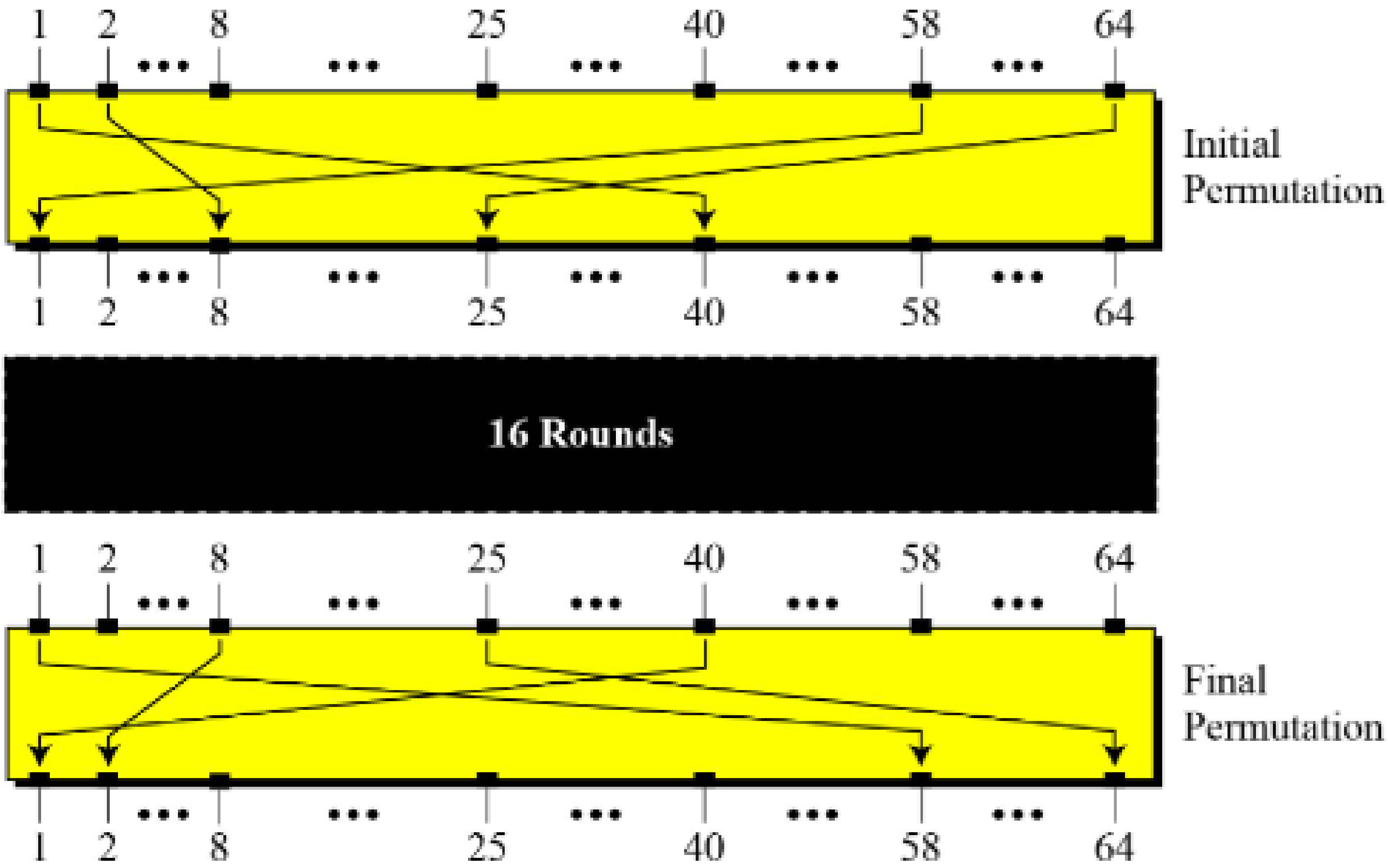
- **A more serious concern is key length. With a key length of 56 bits, there are 2^{56} possible keys, which is approximately 7.2×10^{16} keys which can be broken easily.**

DES



64-bit plaintext
DES
Initial permutation
Round 1
Round 2
Round 16
Final permutation
K_1
48-bit
K_2
48-bit
K_{16}
48-bit
Round-key generator
56-bit cipher key
64-bit ciphertext

Initial and final permutation steps

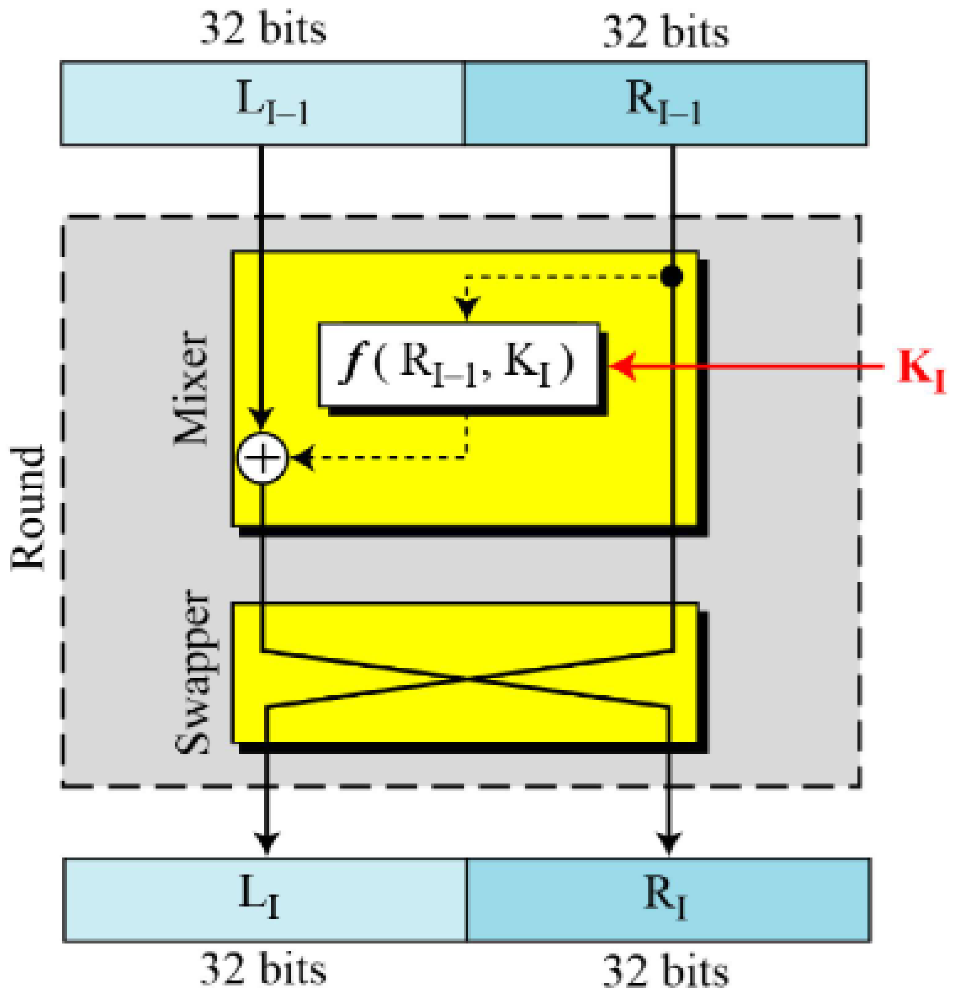


Initial and final permutation tables

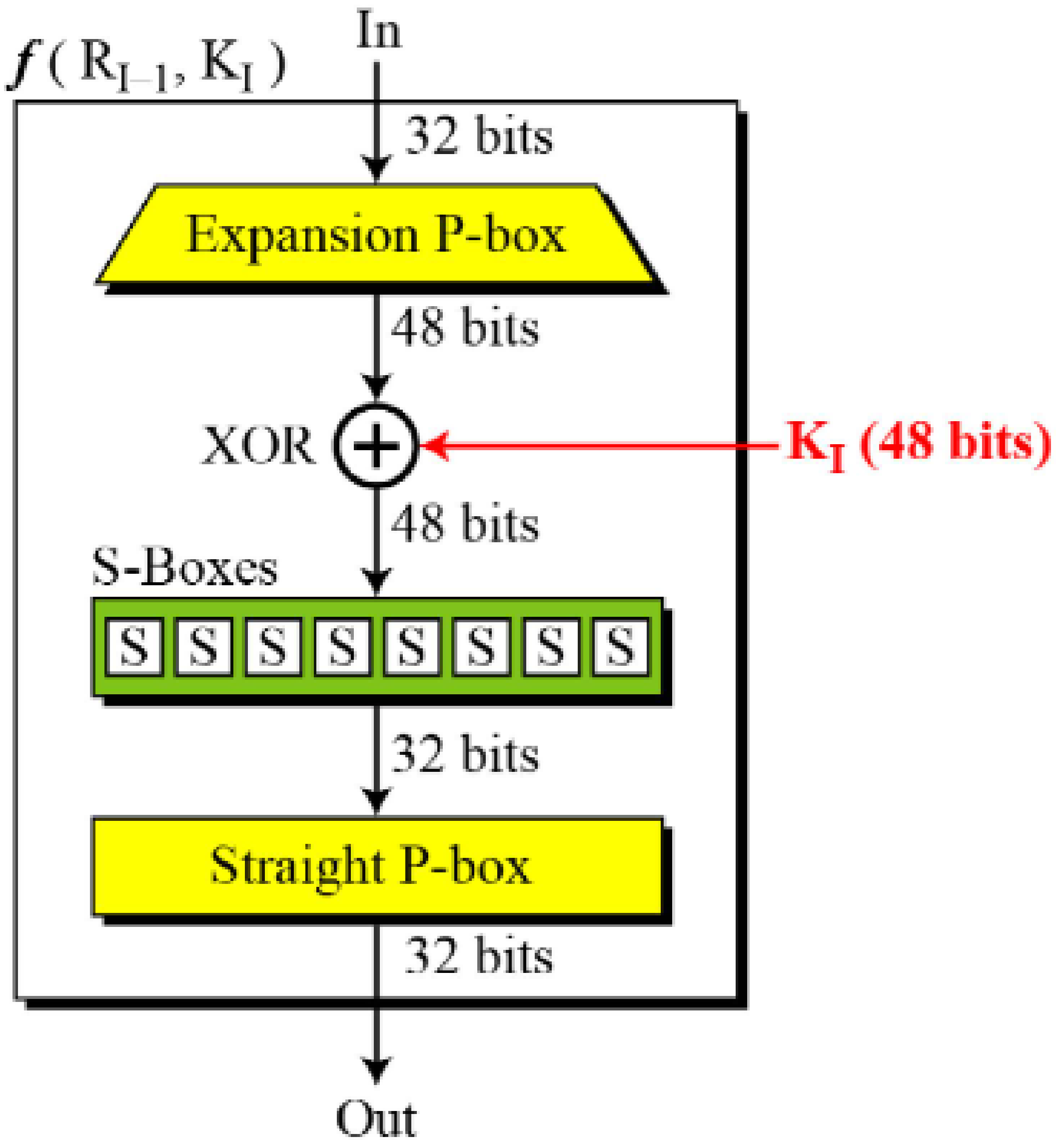
Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

A round in DES (Feistel cipher)

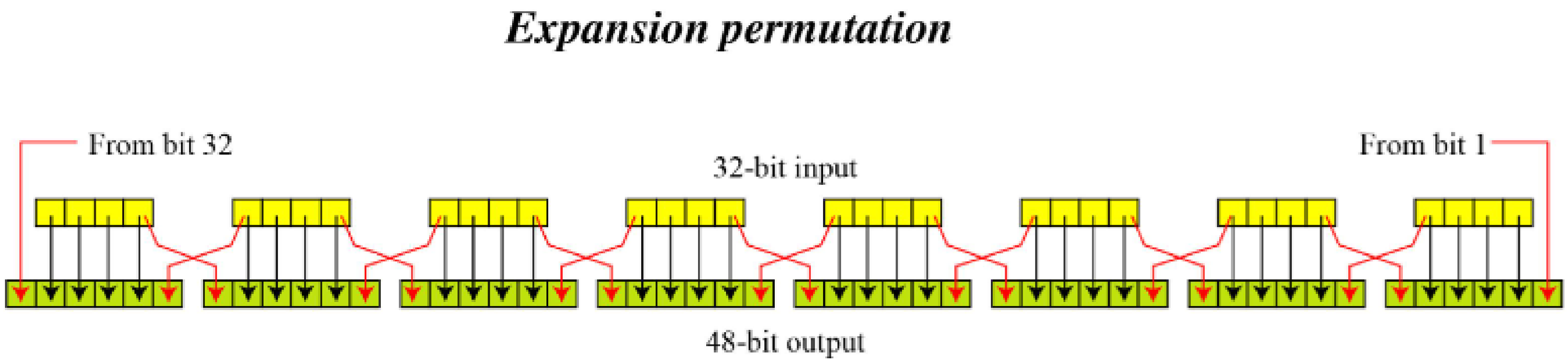
A round in DES (encryption site)



DES function



Expansion mechansim

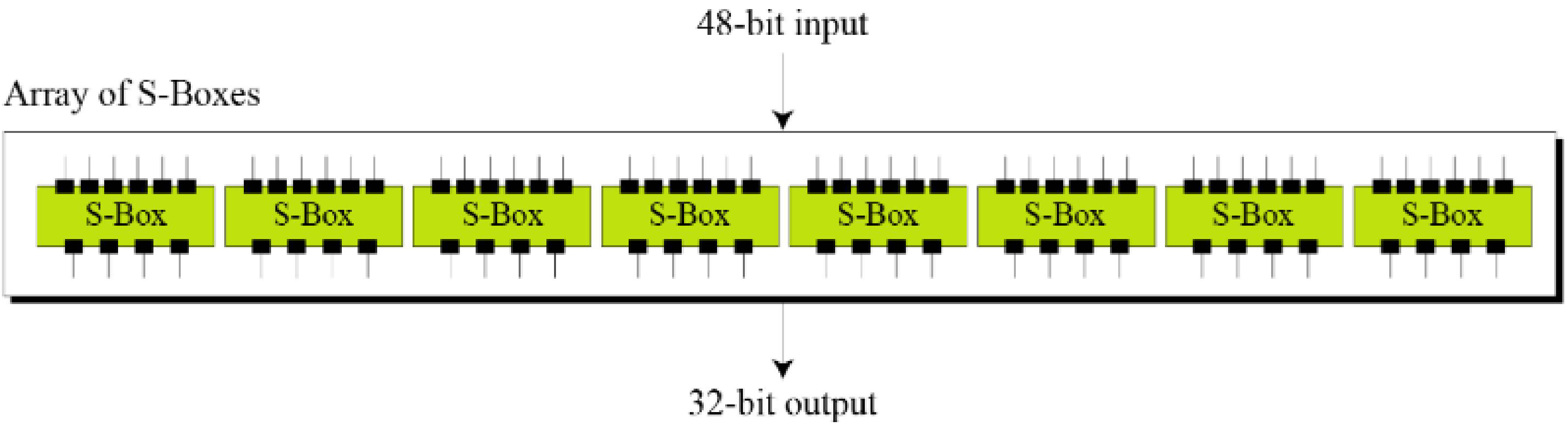


Expansion table

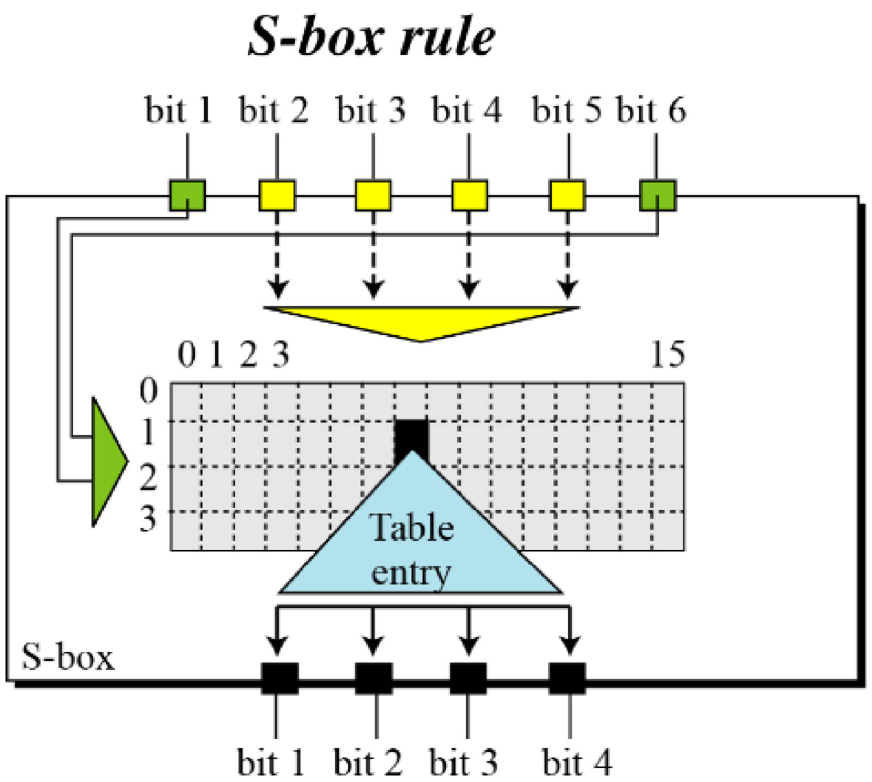
Expansion P-box table

32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	31	31	32	01

S-box



48-bit input
Array of S-Boxes
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
S-Box
32-bit output



S-box rule
bit 1 bit 2 bit 3 bit 4 bit 5 bit 6
0 1 2 3
15
0
1
2
3
Table entry
S-box
bit 1 bit 2 bit 3 bit 4

S-box

S-box 1

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

- **If input to s-box 1 is 100011. What would be the output?**

Triple-DES

- repeats basic DES algorithm three times
- using either two or three unique keys
  - key size of 112 or 168 bits.

- much more secure but also much slower
- key size of 112 or 168 bits.

Advanced Encryption Algorithm (AES)

- Because of the drawbacks of 3DES, it was not a reasonable candidate for long-term use and there was need for a better replacement to DES
- NIST called for proposals in 1997
  - efficiency, security, HW/SW suitability, 128, 256, 256 keys
- selected Rijndael in Nov 2001
- symmetric block cipher
- uses 128 bit data & 128/192/256 bit keys
- now widely available commercially