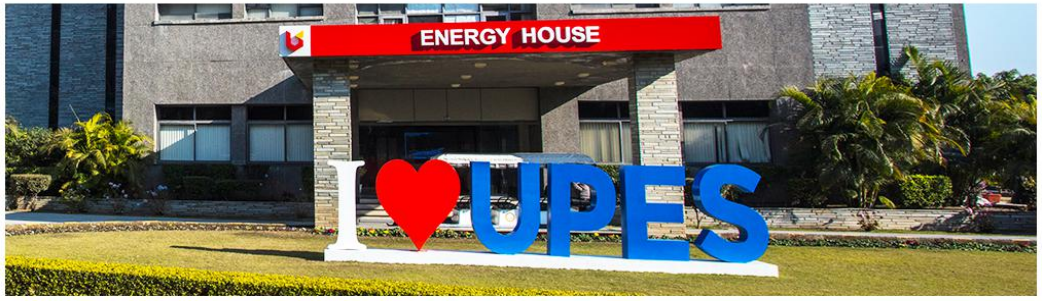
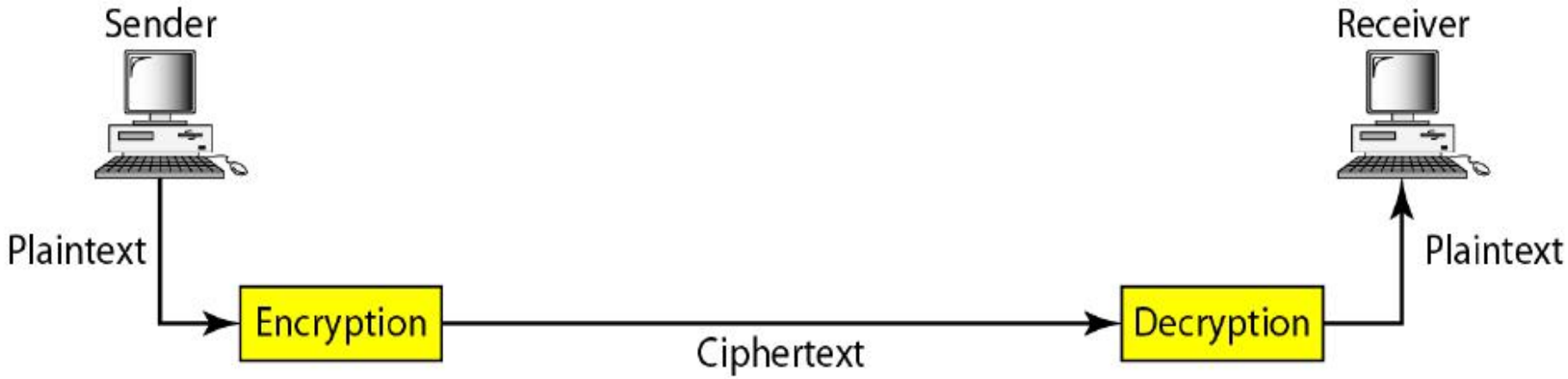
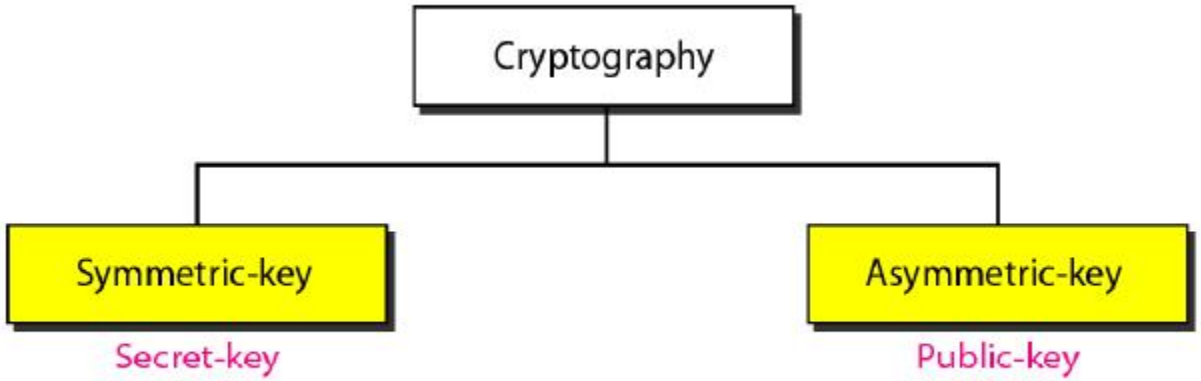


UPES

UNIVERSITY WITH A PURPOSE

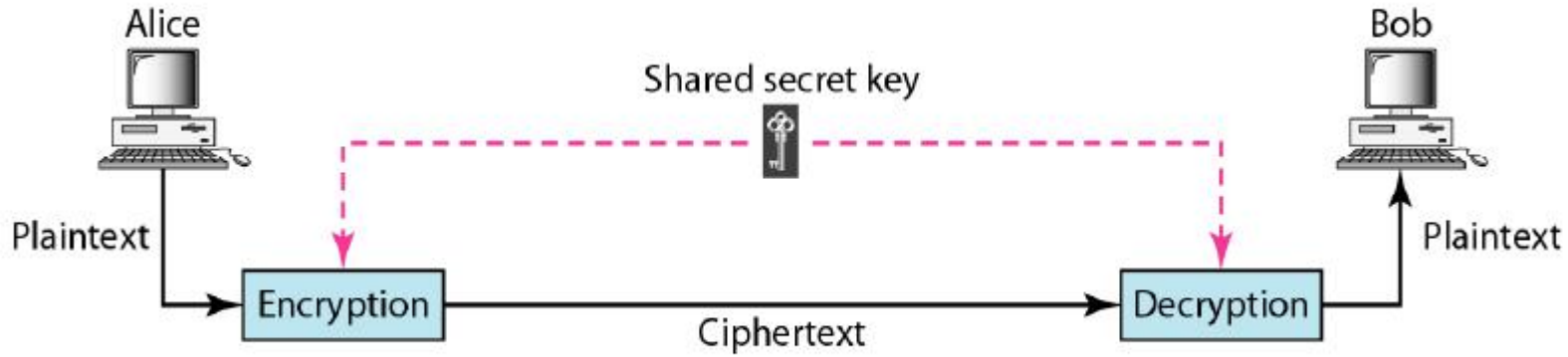
Cryptography

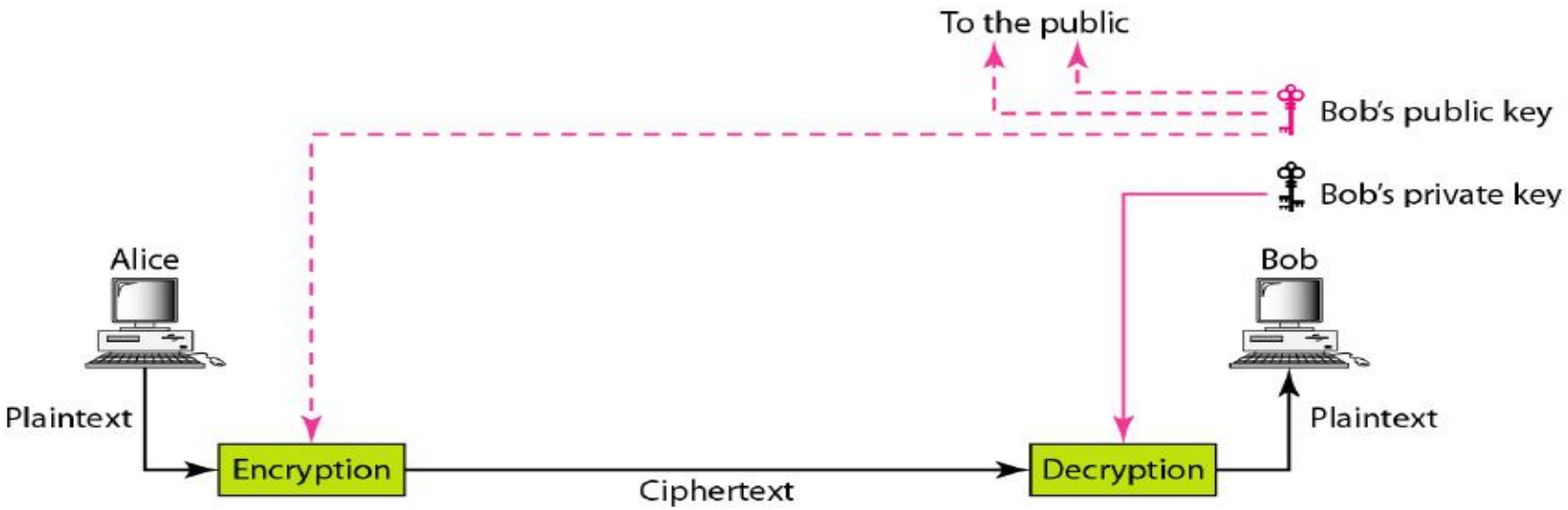




UPES
UNIVERSITY WITH A PURPOSE

Symmetric vs. Asymmetric Key Cryptography





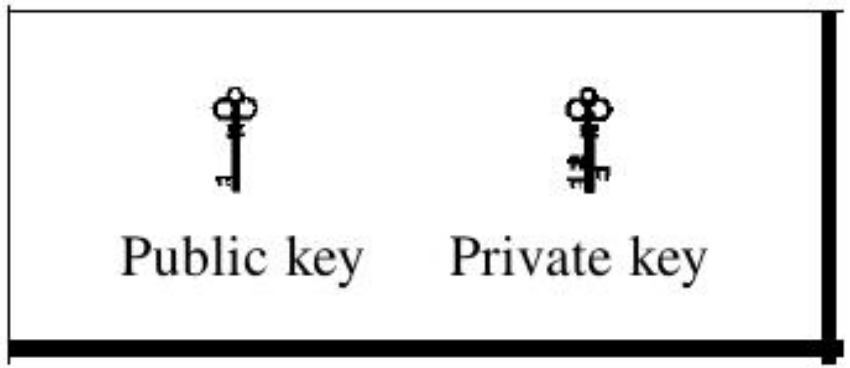
UPES
UNIVERSITY WITH A PURPOSE

Symmetric vs. Asymmetric Key Cryptography (contd...)

- In symmetric·key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared.
- In public-key encryption/decryption, the public key that is used for encryption is different from the private key that is used for decryption.
  - The public key is available to the public; the private key is available only to an individual.

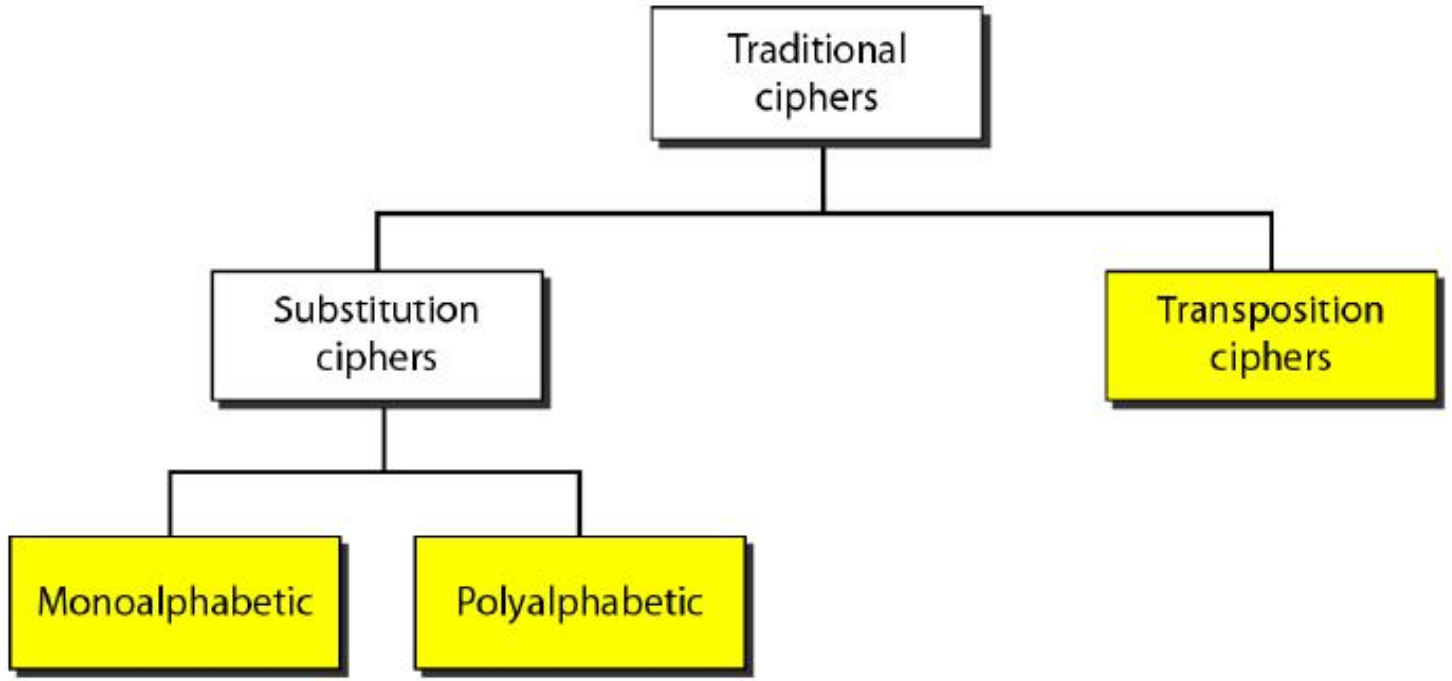
Symmetric vs. Asymmetric Key Cryptography (contd...)

Symmetric-key cryptography



Asynunetric-key cryptography

SYMMETRIC-KEY CRYPTOGRAPHY



Substitution Ciphers

- A substitution cipher replaces one symbol with another.
  - In a monoalphabetic cipher, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text.
  - In a polyalphabetic cipher, each occurrence of a character can have a different substitute.

Substitution Ciphers (contd...)

Q1. Using key=5, obtain the Caesar shift cipher for the message, “HAPPY DIWALI IN ADVANCE.”

Q2. Using a key sequence, 5 7 13 17, obtain the Caesar shift for the message, “UNIVERSITY OF PETROLEUM AND ENERGY STUDIES”.

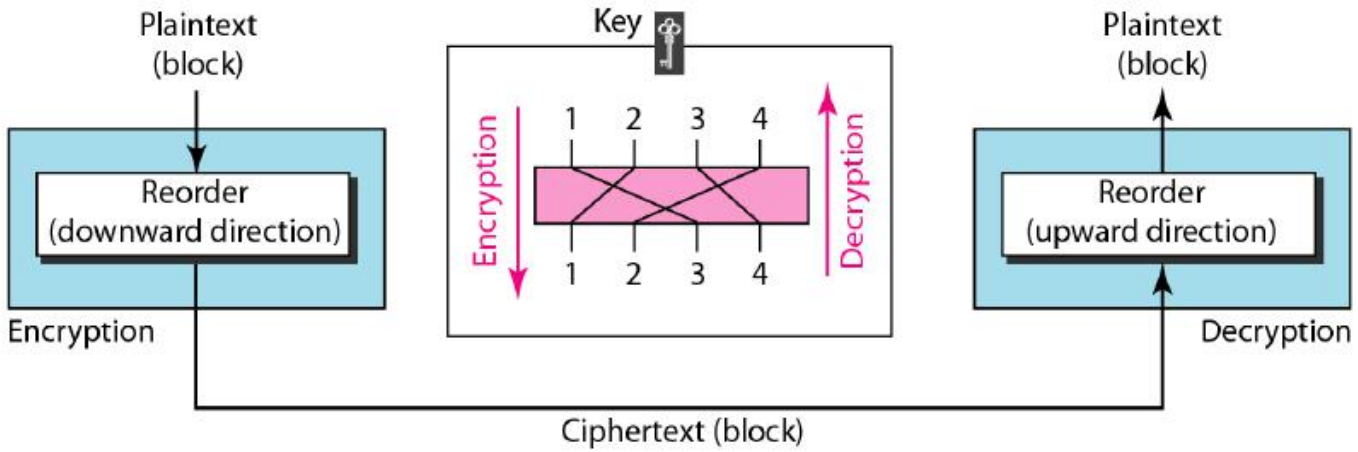
Transposition Ciphers

A transposition cipher reorders (permutes) symbols in a block of symbols.

A possible key:

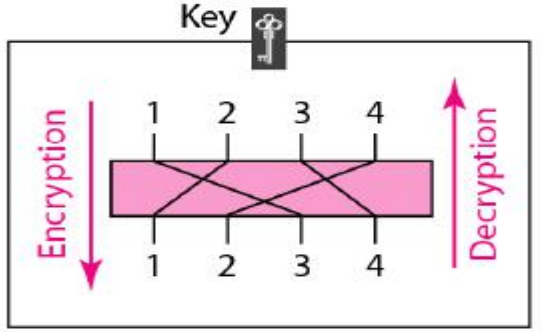
Plaintext: 2 4 1 3

Ciphertext: 1 2 3 4



UPES
UNIVERSITY WITH A PURPOSE

Q: Encrypt the message “HELLO MY DEAR,” using the key shown below:



Ans: First, remove the spaces in the message. Divide the text into blocks of four characters. Add a bogus character Z at the end of the third block. The result is HELL OMYD EARZ.

Create a three-block ciphertext ELHLMDOYAZER.

UPES
UNIVERSITY WITH A PURPOSE

Steganography

- Steganography is the practice of concealing information within another message or physical object to avoid detection.
- Steganography can be used to hide virtually any type of digital content, including text, image, video, or audio content.
- That hidden data is then extracted at its destination.
- Content concealed through steganography is sometimes encrypted before being hidden within another file format. If it isn't encrypted, then it may be processed in some way to make it harder to detect.

Steganography (contd...)

As a form of covert communication, steganography is sometimes compared to cryptography. However, the two are not the same since steganography does not involve scrambling data upon sending or using a key to decode it upon receipt.

How steganography works

- One of the most prevalent techniques is called ‘least significant bit’ (LSB) steganography. This involves embedding the secret information in the least significant bits of a media file.

- Another steganography technique is the use of word or letter substitution. This is where the sender of a secret message conceals the text by distributing it inside a much larger text, placing the words at specific intervals. While this substitution method is easy to use, it may also make the text look strange and out of place since the secret words might not fit logically within their target sentences.

- Other steganography methods include hiding an entire partition on a hard drive or embedding data in the header section of files and network packets. The effectiveness of these methods depends on how much data they can hide and how easy they are to detect.

Types of steganography

- Text steganography
- Image steganography
- Video steganography
- Audio steganography
- Network steganography

Types of Steganography (contd...)

- Text steganography
  - Text steganography involves hiding information inside text files. This includes changing the format of existing text, changing words within a text, using context-free grammars to generate readable texts, or generating random character sequences.

- Image steganography
  - This involves hiding information within image files. In digital steganography, images are often used to conceal information because there are a large number of elements within the digital representation of an image, and there are various ways to hide information inside an image.

Types of Steganography (contd...)

- Audio steganography
  - Audio steganography involves secret messages being embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a more difficult process compared to others.

- Video steganography
  - This is where data is concealed within digital video formats. Video steganography allows large amounts of data to be hidden within a moving stream of images and sounds. Two types of video steganography are:
    - Embedding data in uncompressed raw video and then compressing it later
    - Embedding data directly into the compressed data stream

Types of Steganography (contd...)

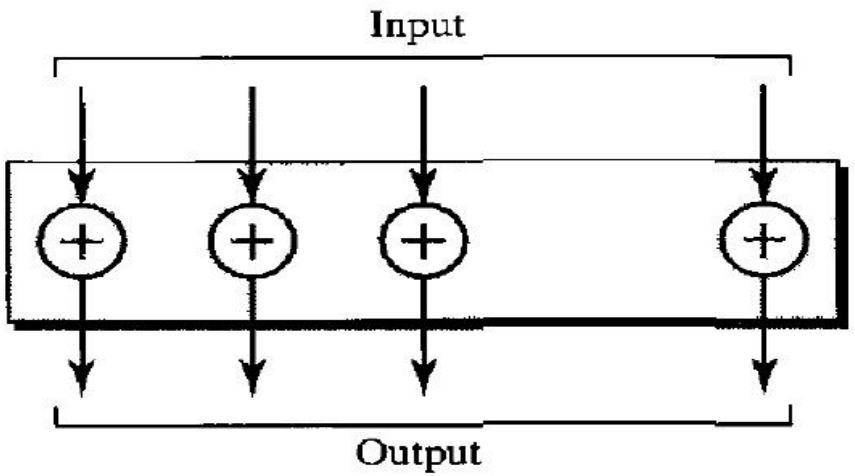
- Network steganography
  - Network steganography, sometimes known as protocol steganography, is the technique of embedding information within network control protocols used in data transmission such TCP, UDP, ICMP, etc.

Block Ciphers

- Block ciphers process messages into blocks, each of which is then en/decrypted; whereas, stream ciphers process messages a bit or byte at a time when en/decrypting
- Operates on a single chunk (“block”) of plaintext, e.g. 64 bits for DES
- Same key is reused for each block (can use short keys)
- Result should look like a random permutation As if plaintext bits were randomly shuffled.
- Modern block ciphers are widely used to provide encryption of quantities of information, and/or a cryptographic checksum to ensure the contents have not been altered.

Simple Modern Block Ciphers

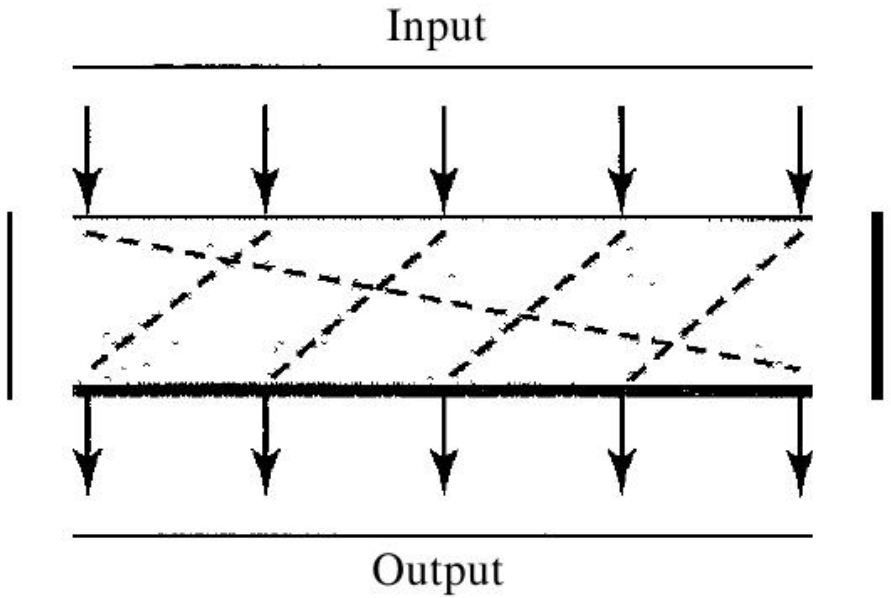
- **XOR Cipher**
  - It uses the exclusive-or operation
  - The size of the key the plaintext, and the ciphertext are all the same.
  - XOR ciphers have a very interesting property: the encryption and decryption are the same.



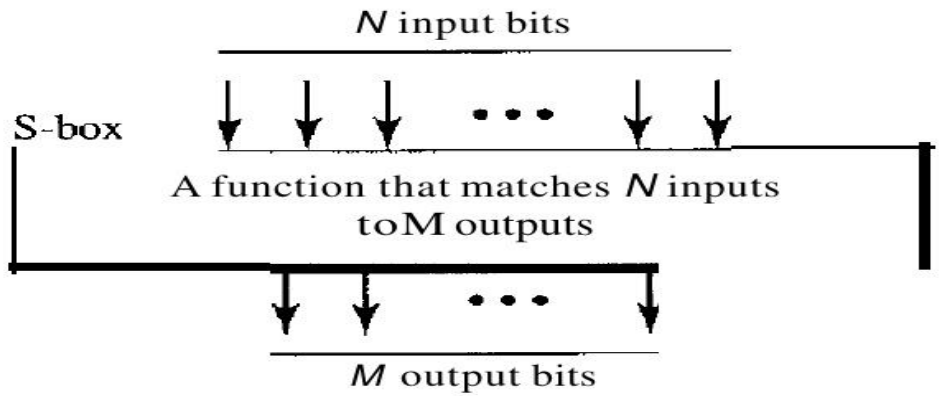
UPES
UNIVERSITY WITH A PURPOSE

- **Rotation Cipher**
  - The input bits are rotated to the left or right.
  - The rotation cipher can be keyed or keyless.
  - In keyed rotation, the value of the key defines the number of rotations; in keyless rotation the number of rotations is fixed.
  - The rotation cipher can be considered a special case of the transpositional cipher using bits instead of characters.
  - The rotation cipher has an interesting property. If the length of the original stream is N, after N rotations, we get the original input stream.
  - In other words, the number of rotations must be between 1 and N-1.

- **Rotation Cipher (contd...)**
  - The decryption algorithm for the rotation cipher uses the same key and the opposite rotation direction.
  - If we use a right rotation in the encryption, we use a left rotation in decryption and vice versa.

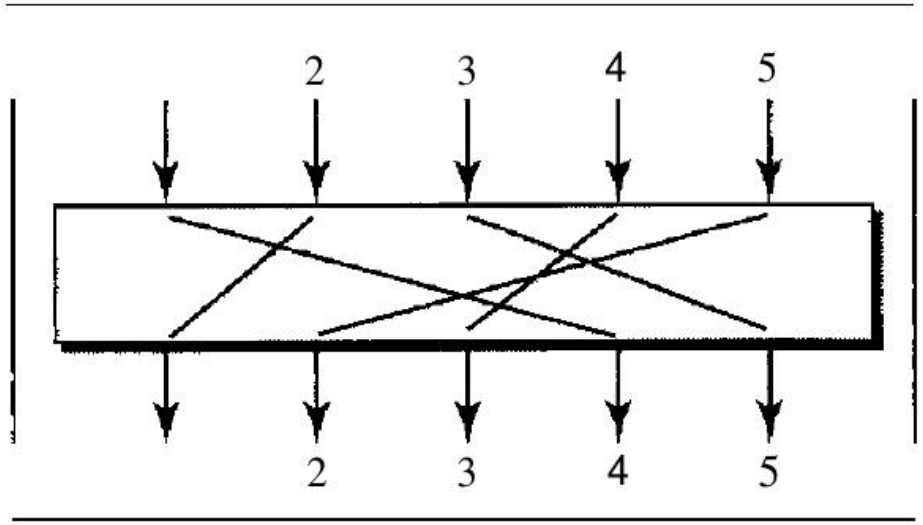


- **Substitution Cipher: S-box**
  - The input to an S-box is a stream of bits with length N; the result is another stream of bits with length M. And Nand M are not necessarily the same.
  - Is used as an intermediate stage of encryption or decryption.
  - The function that matches the input to the output may be defined mathematically or by a table.

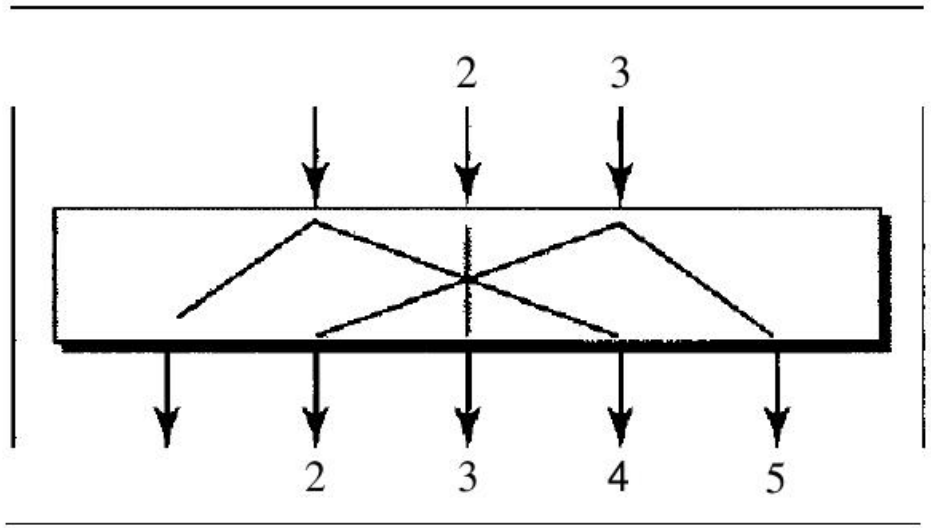


UPES
UNIVERSITY WITH A PURPOSE

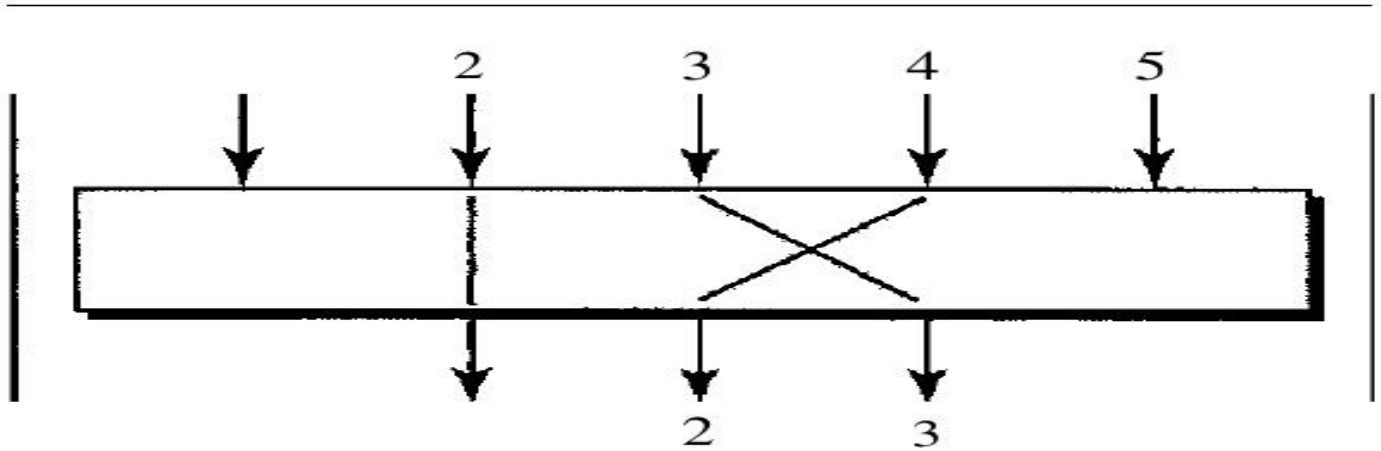
- Transposition Cipher: P-box
  - A P-box (permutation box) for bits parallels the traditional transposition cipher for characters.
  - It performs a transposition at the bit level; it transposes bits.
  - There are three types of permutations in P-boxes: the straight permutation, expansion permutation, and compression permutation.



a. Straight



b. Expansion

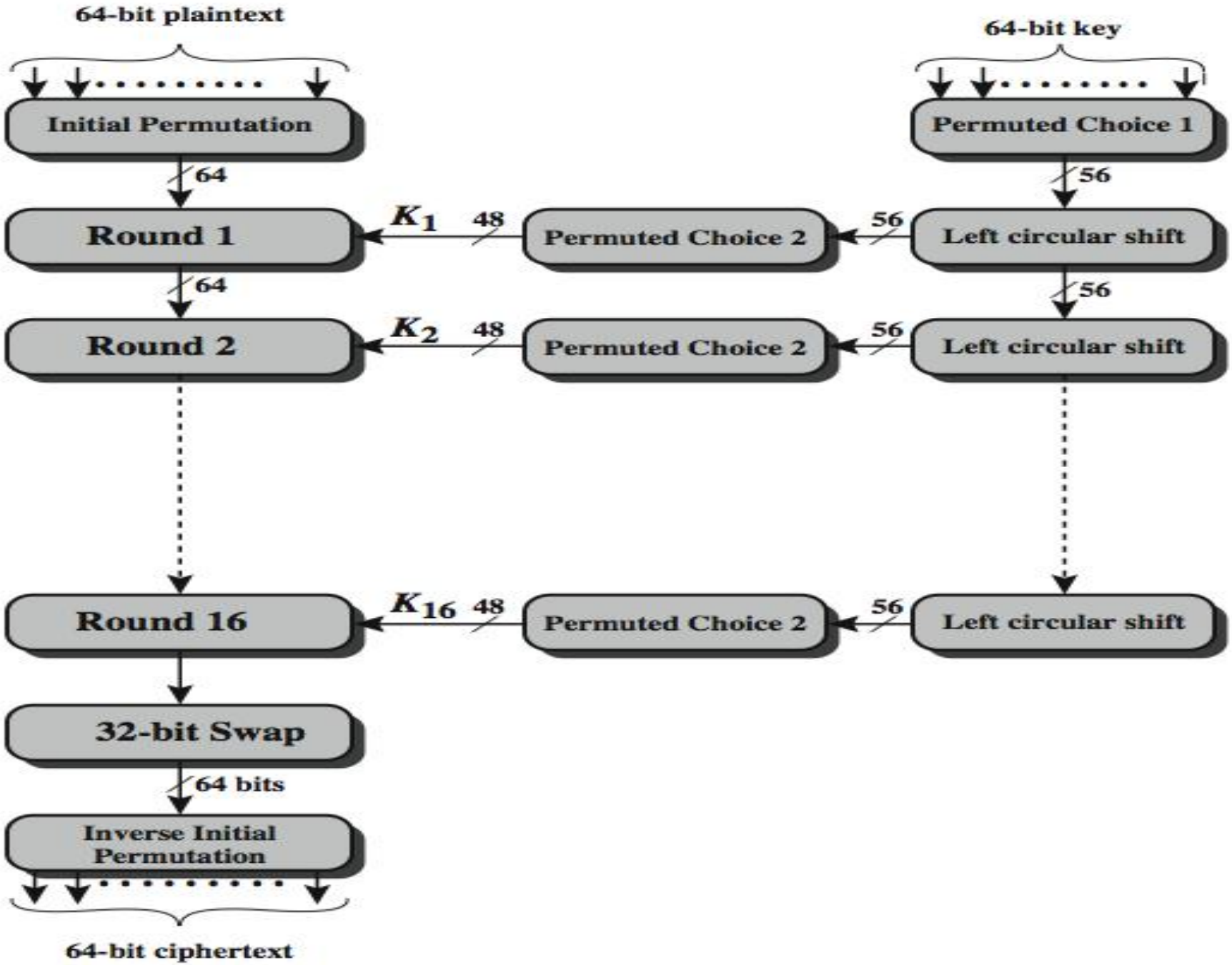


c. Compression

UPES
UNIVERSITY WITH A PURPOSE

Data Encryption Standard (DES)

- Symmetric-key cipher
- Block cipher
- It divides the plaintext into blocks and use the same key to encrypt and decrypt the blocks.
- DES has been the de-facto standard until AES has come into existence, which is now the formal standard.
- Are the round ciphers because it involves multiple rounds, where each round is a complex cipher made up of the simple ciphers described above.
- The key used in each round is a subset or variation of the general key called the round key, viz. K_1 K_2, ..., K_N.



Initial Permutation (IP)

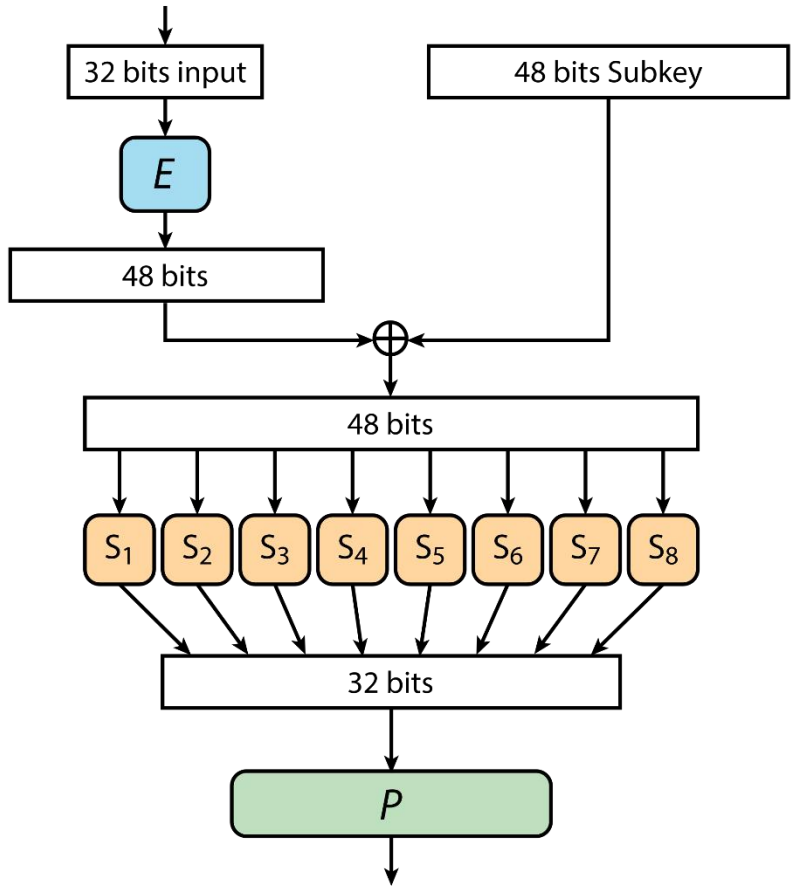
- first step of the data computation
- IP reorders the input data bits
- even bits to LH half, odd bits to RH half
- quite regular in structure (easy in h/w)
- no cryptographic value

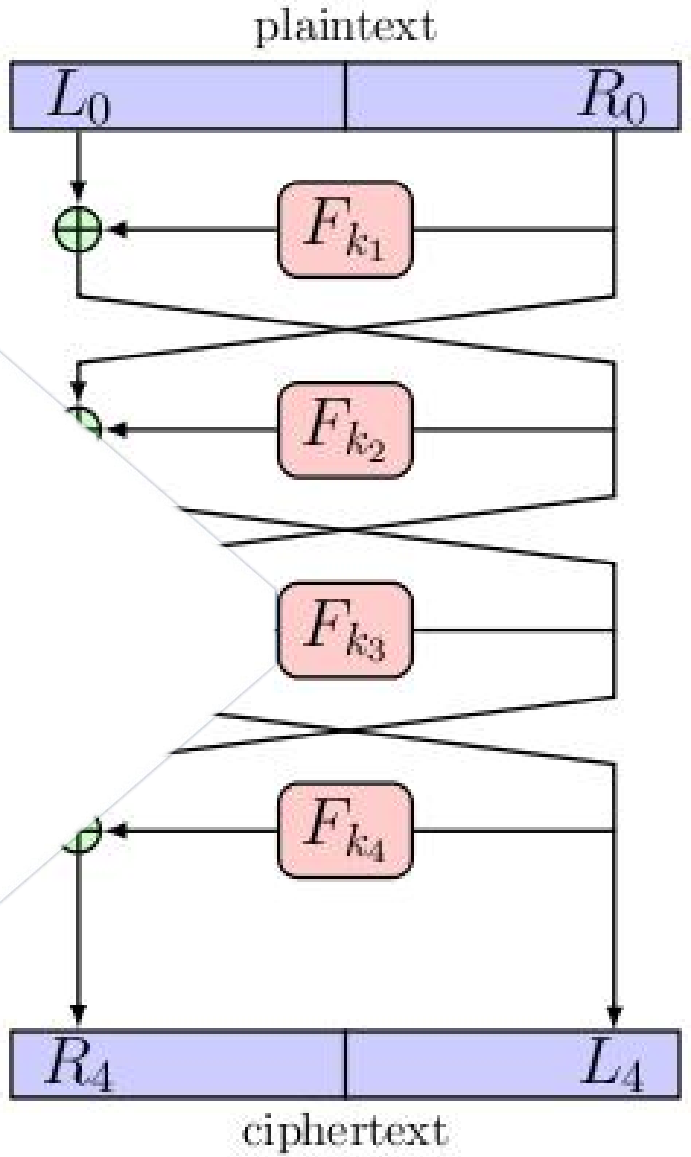
DES Round Function

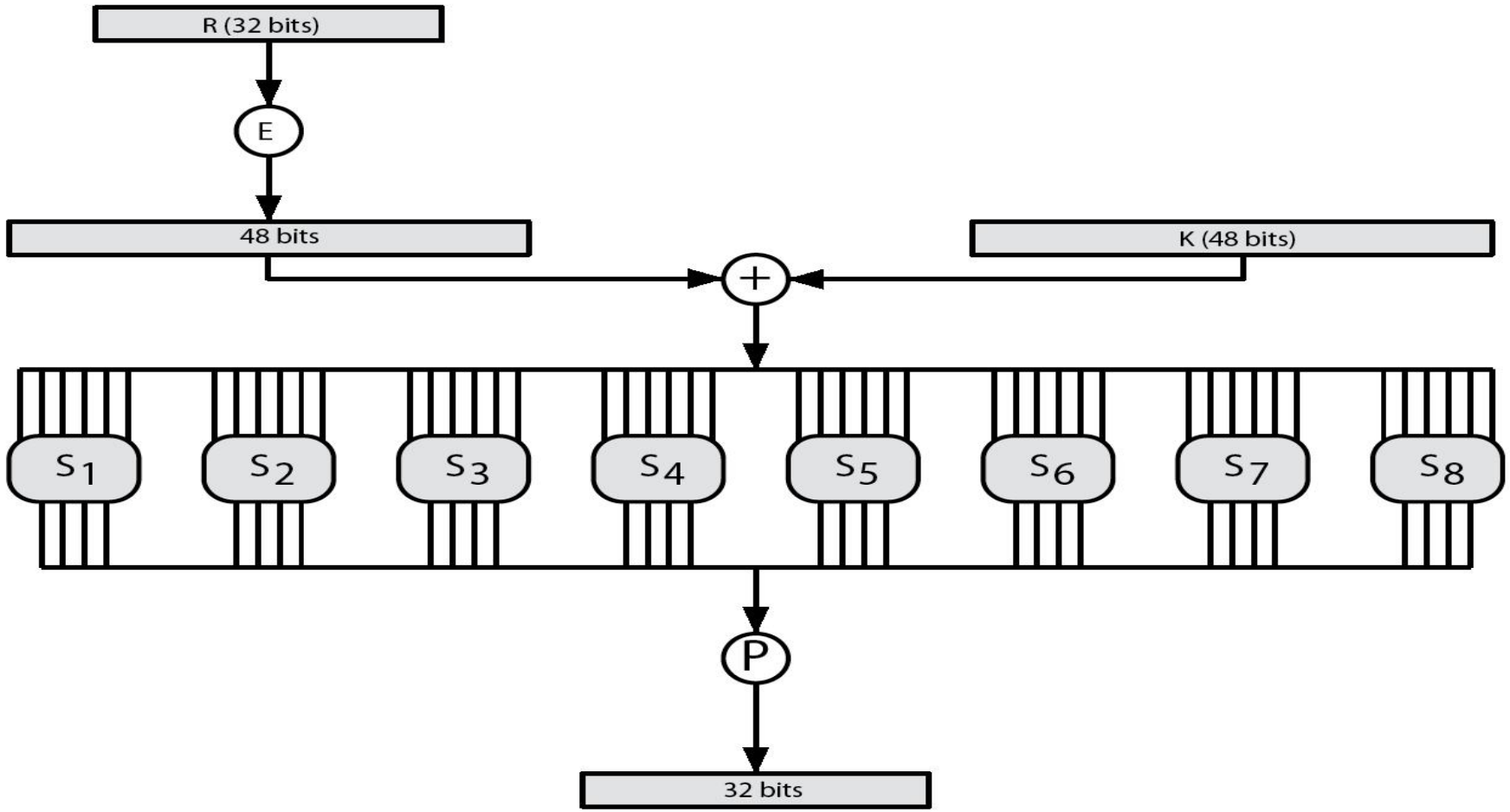
- uses two 32-bit L & R halves
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus \mathrm{F}(R_{i-1}, K_i)$
- F takes 32-bit R half and 48-bit subkey:
  - expands R to 48-bits using perm E
  - adds to subkey using XOR
  - passes through 8 S-boxes to get 32-bit result
  - finally permutes using 32-bit perm P

DES round function

$F(K_i,\ X)$

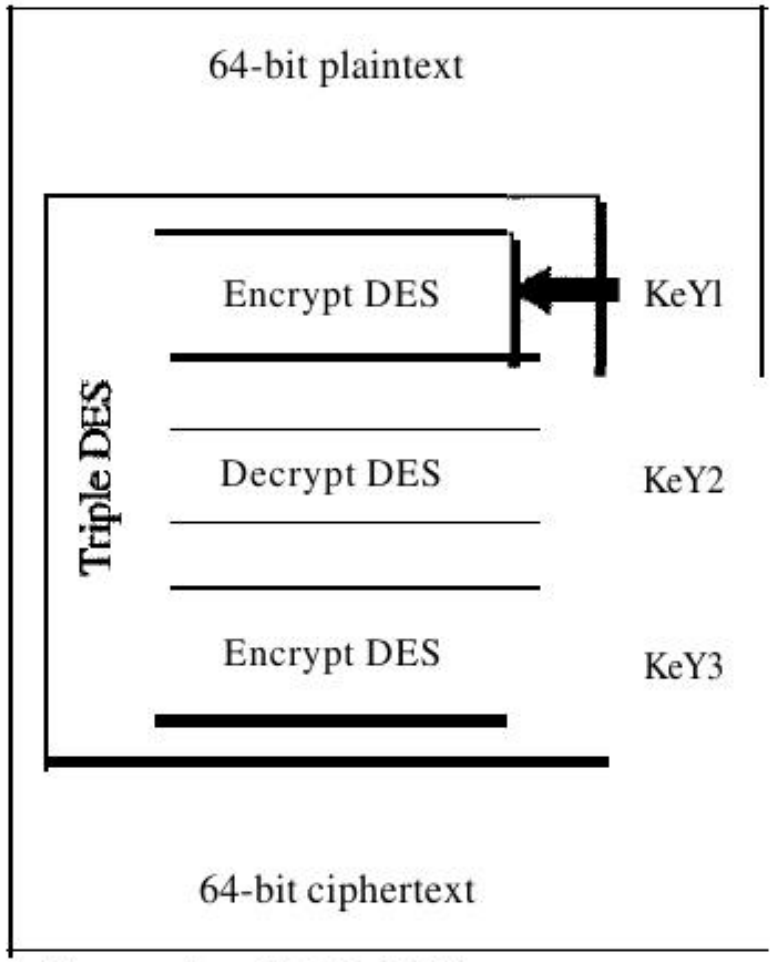




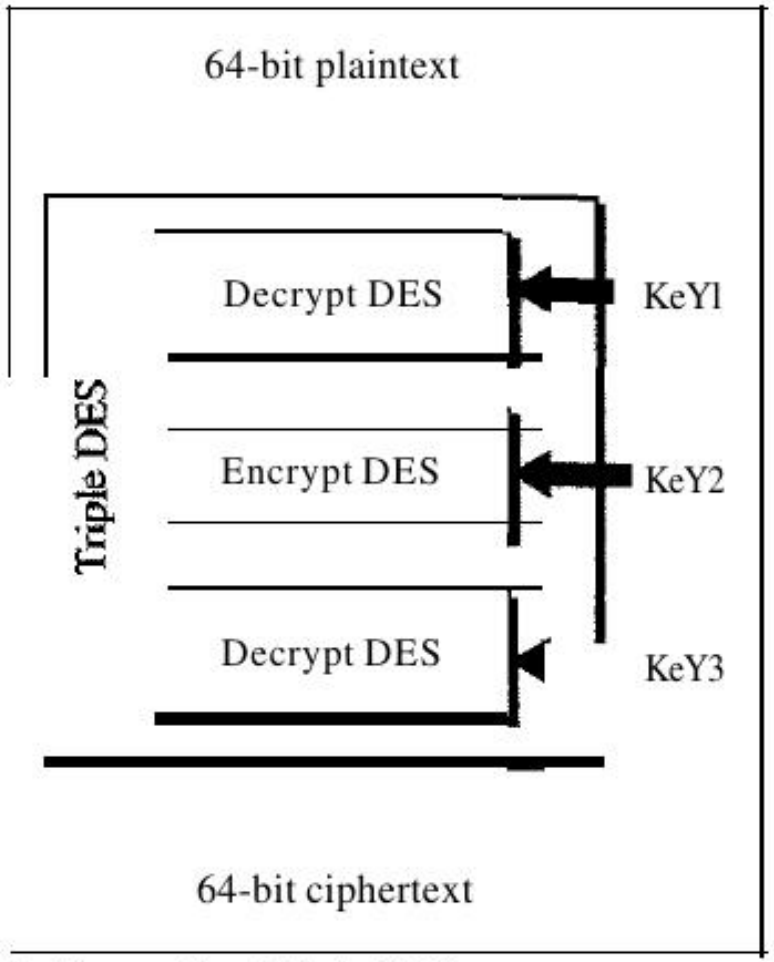


UPES
UNIVERSITY WITH A PURPOSE

Triple-DES



a. Encryption Triple DES



b. Decryption Triple DES

UPES
UNIVERSITY WITH A PURPOSE

Advanced Encryption Standard (AES)

- The Advanced Encryption Standard (AES) was designed because DES's key was too small.
- AES is a very complex round cipher.
- AES is designed with three key sizes: 128, 192, or 256 bits.

Size ofData Block	*Number ofRounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

UPES
UNIVERSITY WITH A PURPOSE

UPES
UNIVERSITY WITH A PURPOSE

UPES
UNIVERSITY WITH A PURPOSE

THANK YOU

UPES

UNIVERSITY WITH A PURPOSE