Information Systems Security

Lecture 3

Symmetric cryptography

Dr. En. Bader Ahmad

References

1. **Cryptography and Network Security**, By W. Stallings. Prentice Hall, 2003.

2. **Handbook of applied Cryptography** by A. Menezes, P. Van Oorschot and S. Vanstone. 5th printing, 2001
   http://www.cacr.math.uwaterloo.ca/hac

3. **Cryptography: A Very Short Introduction (Very Short Introduction S.)**, by Fred Piper and Sean Murphy, Oxford University Press, 2002.

Outline

1. Cryptography
2. Symmetric Cipher systems
3. Stream Cipher
   - Vernam Cipher
   - One-time pad
4. Block cipher
   - DES
   - Triple DES
   - AES
5. Modes of operation
   - ECB
   - CBC

1. Cryptography

- **Cryptography** is a means of providing information security.
- **Cryptography** is the study of mathematical techniques related to aspects of information security such as:
  - confidentiality,
  - integrity,
  - authentication, and
  - non-repudiation

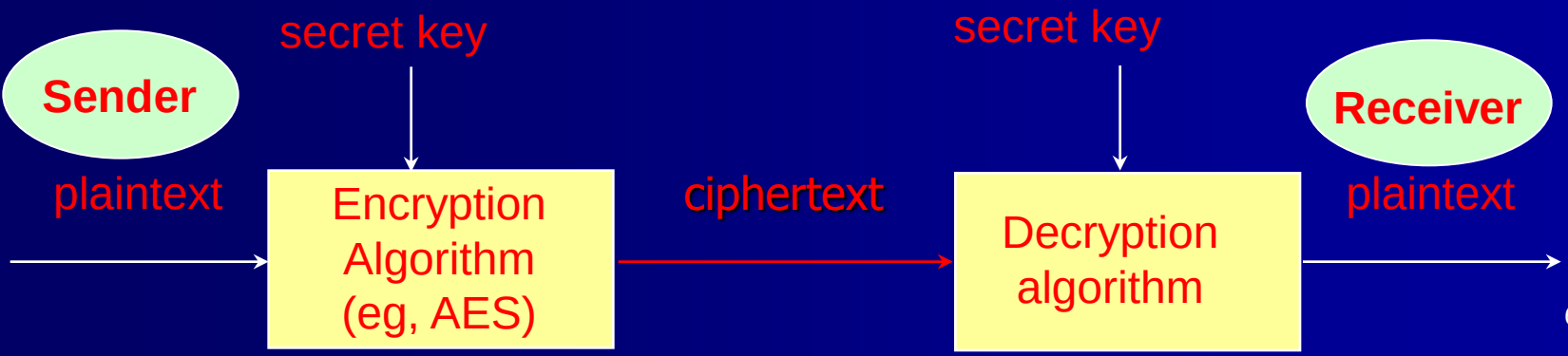
  - which form the main objectives of ISS

Cryptography

- **Cryptanalysis**: the study of mathematical techniques for attempting to defeat cryptographic techniques.
- **Cryptanalyst**: is the one who engages in cryptanalysis.
- **Cryptology**: the study of cryptanalysis and cryptography.
- Cryptosystem (Cryptographic system): is a general term referring to a set of cryptographic primitives used to provide information security services.
  - Also called a ***cipher***.

A cipher model

- A (Symmetric) cipher model consists of:
  - Plaintext, *m*: the original intelligible message fed into the encryption algo.
  - Encryption algo., *E*: performs various substitutions and transformation on *m*.
  - Secret key, *K*: an input to *E*, and a value independent of *m*.
  - Ciphertext, *C*: scrambled message produced as output of *E*. it depends on *m* and *K*.
  - Decryption algo., *D*: the reverse of *E*. it takes *C* and *K* and produces *m*.



Symmetric-key systems

- ***Symmetric*** cipher
  - Encryption key and decryption key are exactly the same, or
  - Decryption key is easily obtained from the encryption key.
- All practical cipher systems prior to the 1980's were symmetric cipher systems.
- The study of symmetric cipher systems is often referred to as ***symmetric cryptography.***
  - Also referred to as ***conventional cryptography***, ***single-key cryptography***, or ***secret-key cryptography***.

Public-key systems

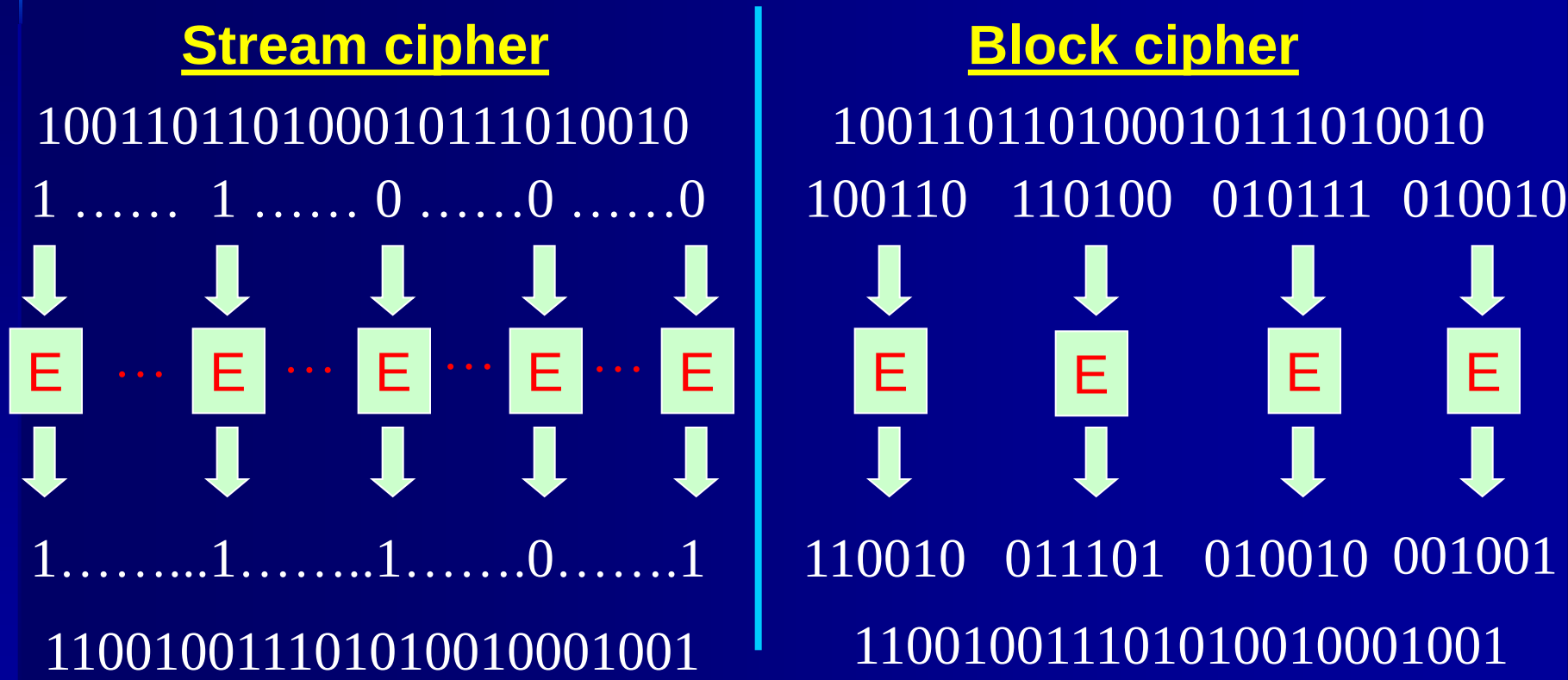
- In ***public-key cipher systems***
  - Computationally infeasible to determine the decryption key from the encryption key.
- Encryption key and decryption key must be different.
  - Public key cipher systems are sometimes referred to as ***asymmetric cipher systems***.
- The study of public key cipher systems is often referred to as ***public-key*** **or** ***asymmetric cryptography***.

Cryptography

- Cryptographic techniques are divided into 3 types:
  - Symmetric-key Cryptography
    - Symmetric-key ciphers
      - Block cipher
      - Stream cipher
    - Message Authentication Code (MACs)
  - Public-key Cryptography
    - Asymmetric-key ciphers
      - Integer Factorization
      - Discrete logarithm
    - Signatures
    - Key Agreement
  - Keyless Cryptography
    - Hash (message digest) functions

2. Symmetric ciphers

- There are two classes: Block cipher and Stream cipher.

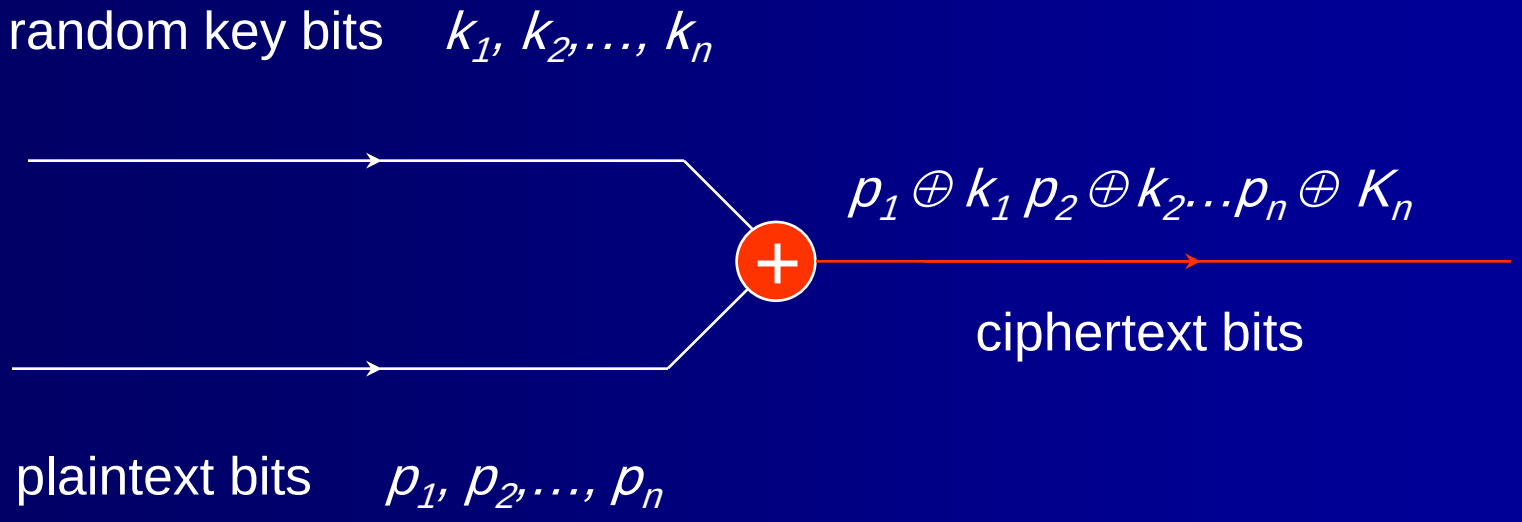


3. Stream Ciphers

- A ***stream cipher*** is an encryption scheme which treats the plaintext symbol-by-symbol (e.g., bit or character)
  - A ***keystream*** is a sequence of symbols $e_1e_2e_3\ldots \in K$ (the key space for a set of encryption transformations)
  - A an alphabet of definition of q symbols
  - Encryption: E_e is a simple substitution cipher with block length 1, where e $\in$ K, $E_e = E_{e_1}(m_1)\, E_{e_2}(m_2) \ldots = c_1c_2\ldots$
    - Plaintext $m = m_1 m_2..$ and ciphertext $c = c_1c_2\ldots$
  - Decryption: $D_d = D_{d_1}(c_1)\, D_{d_2}(c_2) \ldots = m_1m_2\ldots$, $d_i = e_i^{-1}$
- The security stream ciphers depends on the changing keysteam rather than the encryption function (may be simple, e.g., XOR).

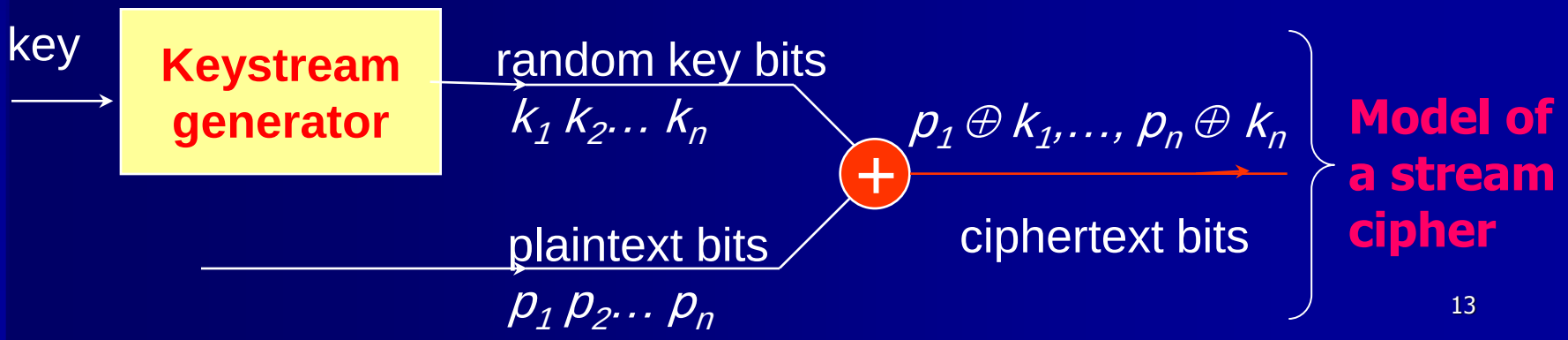
Vernam Cipher

- ***Vernam Cipher*** A stream cipher defined on the alphabet $A=\{0,1\}$
- The keystream is a binary string ($k=k_1 \ldots k_t$) of the same length as the plaintext m ($=m_1 \ldots m_t$)
- Encryption $c_i=m_i \oplus k_i$, Decryption $m_i=c_i \oplus k_i$



One-time pad

- If the key string is randomly chosen and never used again then Vernam cipher is called a ***one-time pad***
- One-time pad's drawback: The keystream must be as long as the plaintext.
  - This increases the difficulty of key distribution and key management
- Solution: generate the key stream pseudorandomly (*i.e.*, keystream generated from a smaller secret key).



Properties of stream ciphers

- Advantages:
  - No error propagation: a ciphertext digit is modified during transmission doesn't affect the decryption of other ciphertext digits
  - Easy for implementation
  - Fast
- Drawbacks:
  - Requirement for synchronization: sender and receiver must be synchronized
    - *ie*, they must use the same key and operate on the same position (digit),
    - if synchronization is lost due to digit insertion or deletion then re-synchronization is required.
- They are suitable for applications where errors are intolerable.
  - GSM and phone networks.
- A Modern Stream cipher: RC4 (1987).

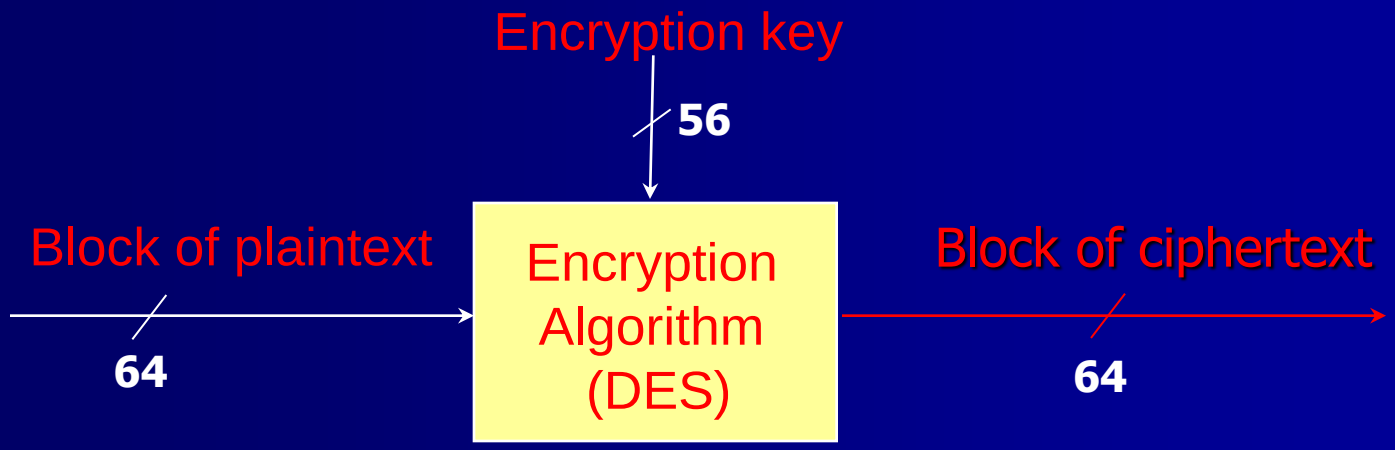
4. Block ciphers

- A ***block cipher*** is an encryption scheme which breaks up the plaintext message into blocks of a fixed length and produces ciphertext blocks of the same length.
- Block ciphers encrypt one block at a time, using a complex encryption function
- Examples
  - DES: operates on blocks of 64 bits
  - AES: operates on blocks of 128 bits
- Block ciphers can be used in various modes (***modes of operation***).

Data Encryption Standard

- Adopted in 1977 by the National Bureau of Standards (US), nowadays NIST
  - FIPS 46
- Most commonly used block cipher
  - 3-DES variant
  - financial sector
- DES is essentially unbroken
  - DES exhaustive key search just becoming feasible
  - DES techniques are basis for other block ciphers
- 1999: DES should only be used for legacy systems and 3DES should replace it
- 2004: Withdrawn
- We will use DES to illustrate the principles of modern symmetric ciphers

Data Encryption Standard

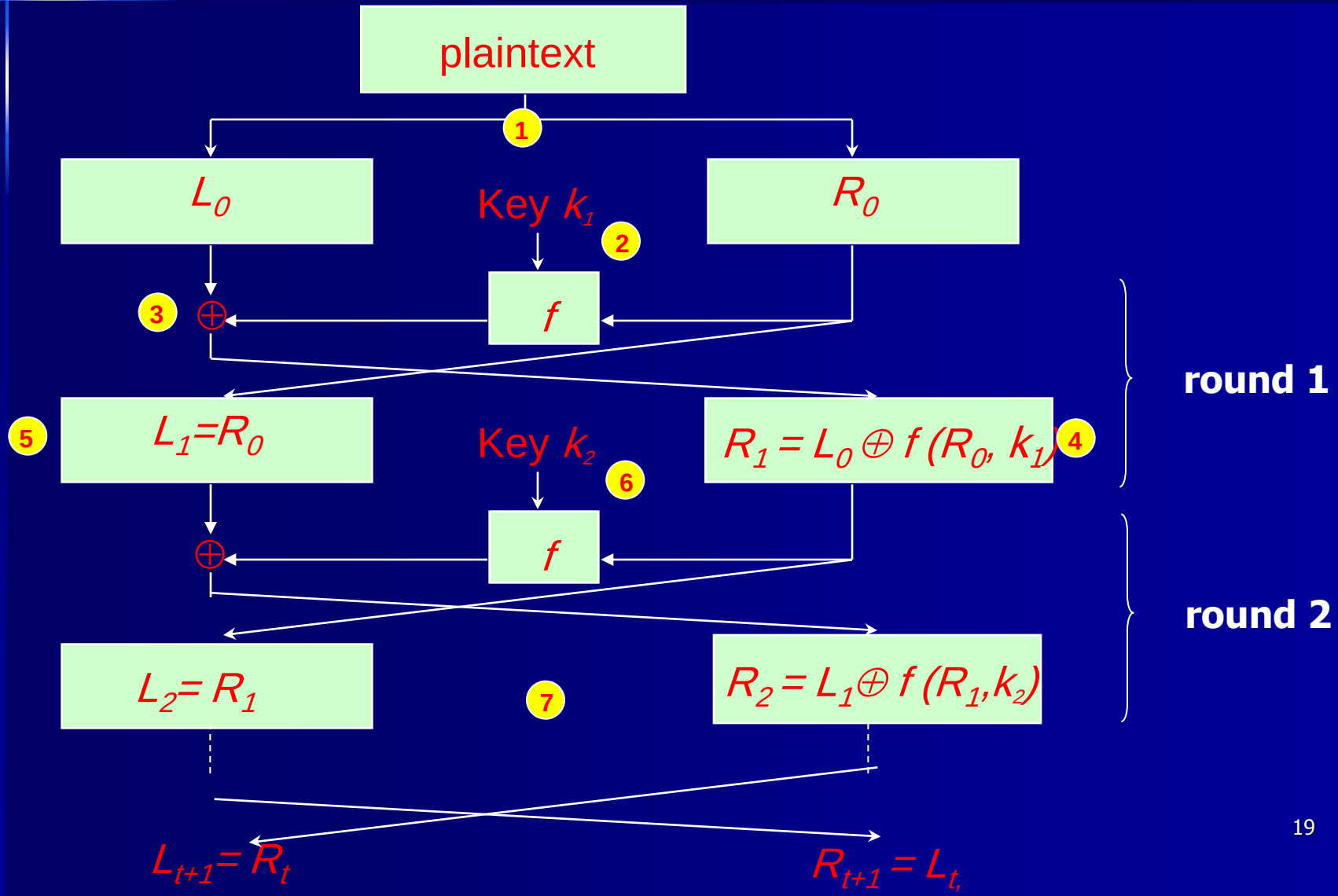


- DES design is based on two general concepts:
  - product cipher: combination of two or more operations (transposition, translation (e.g., XOR), arithmetic operations, modular multiplication, simple substitutions.)
  - Feistel Concept:

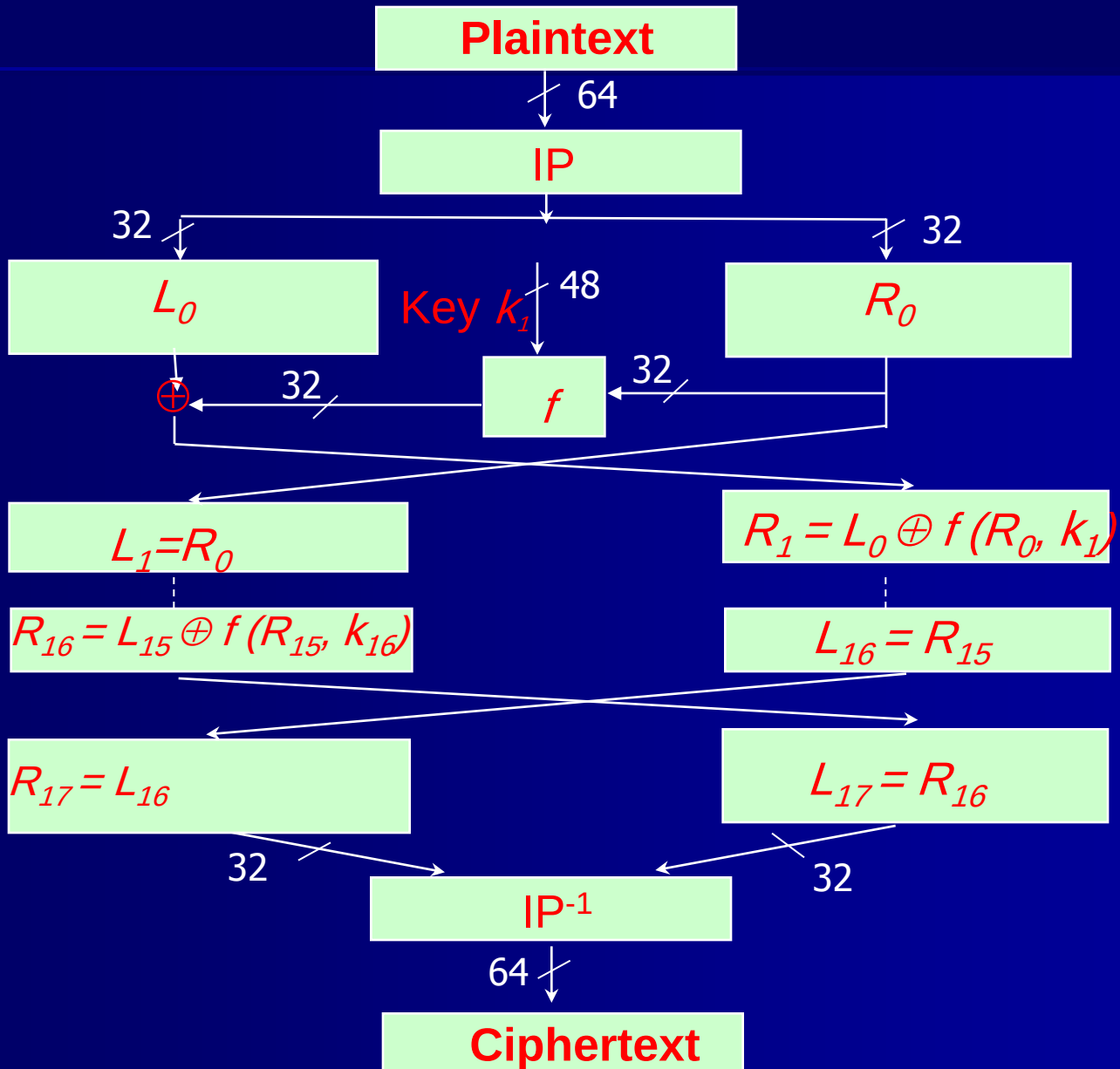
Feistel principle

- An ***iterated block cipher*** is a block cipher involving the sequential repetition of an internal function called ***round function***. Parameters include : r, number of rounds, n block size and k, the input key from which r subkeys k_i (*round keys*) are derived.
- A ***Feistel Cipher*** is an iterated cipher mapping a $2t$-bit plaintext (L_0, R_0), for t-bit blocks L_0 and R_0, to a ciphertext (R_r, L_r), through an r-round process ($r \geq 1$) for each $1 \leq i \leq r$, round i maps $(L_{i-1}, R_{i-1}) \rightarrow (L_i, R_i)$ as follows:
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$
- Decryption is achieved by the same r-round process but with subkeys in reverse order.

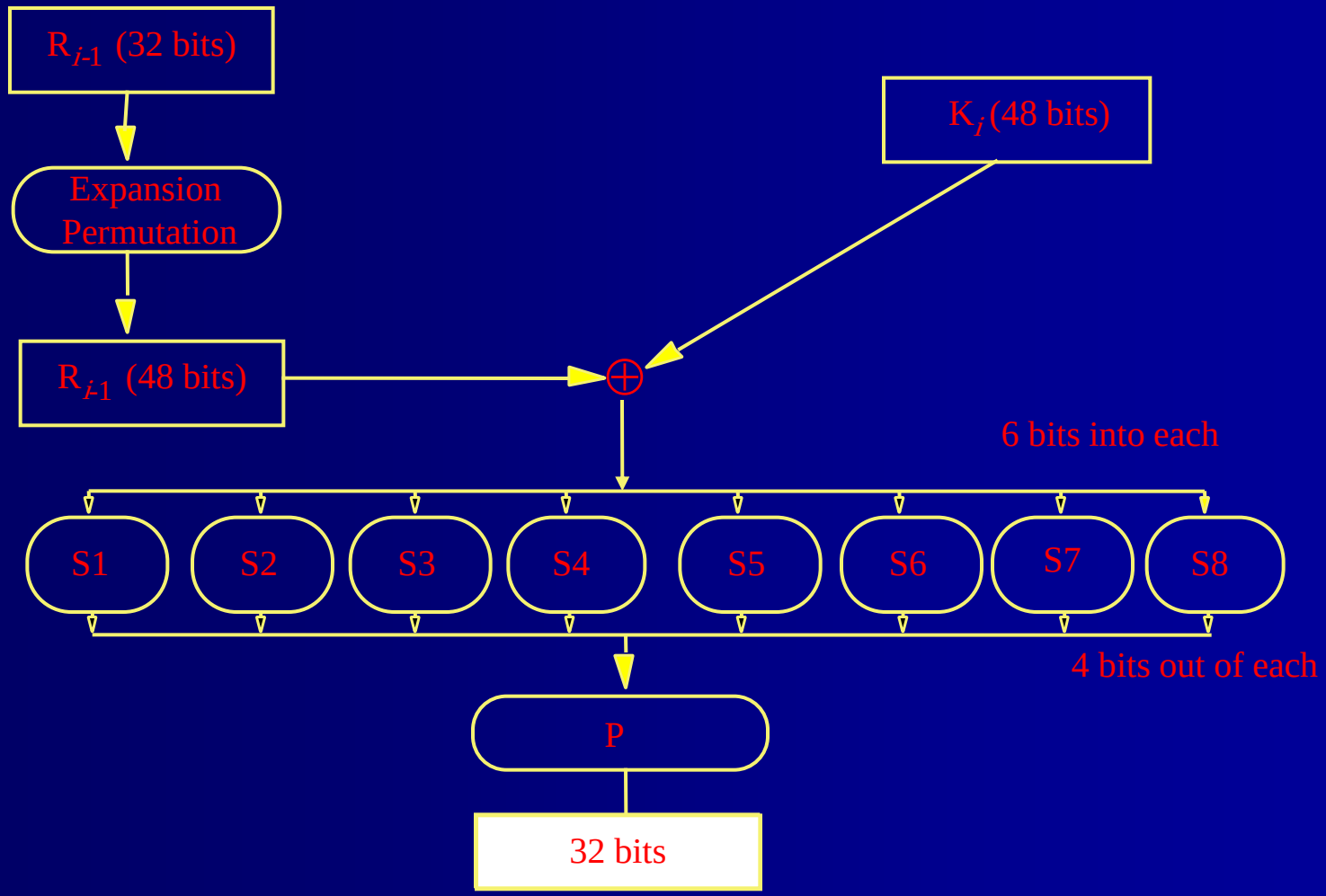
Feistel principle



DES Encryption (ch 7 ,[2])



DES's *f* function



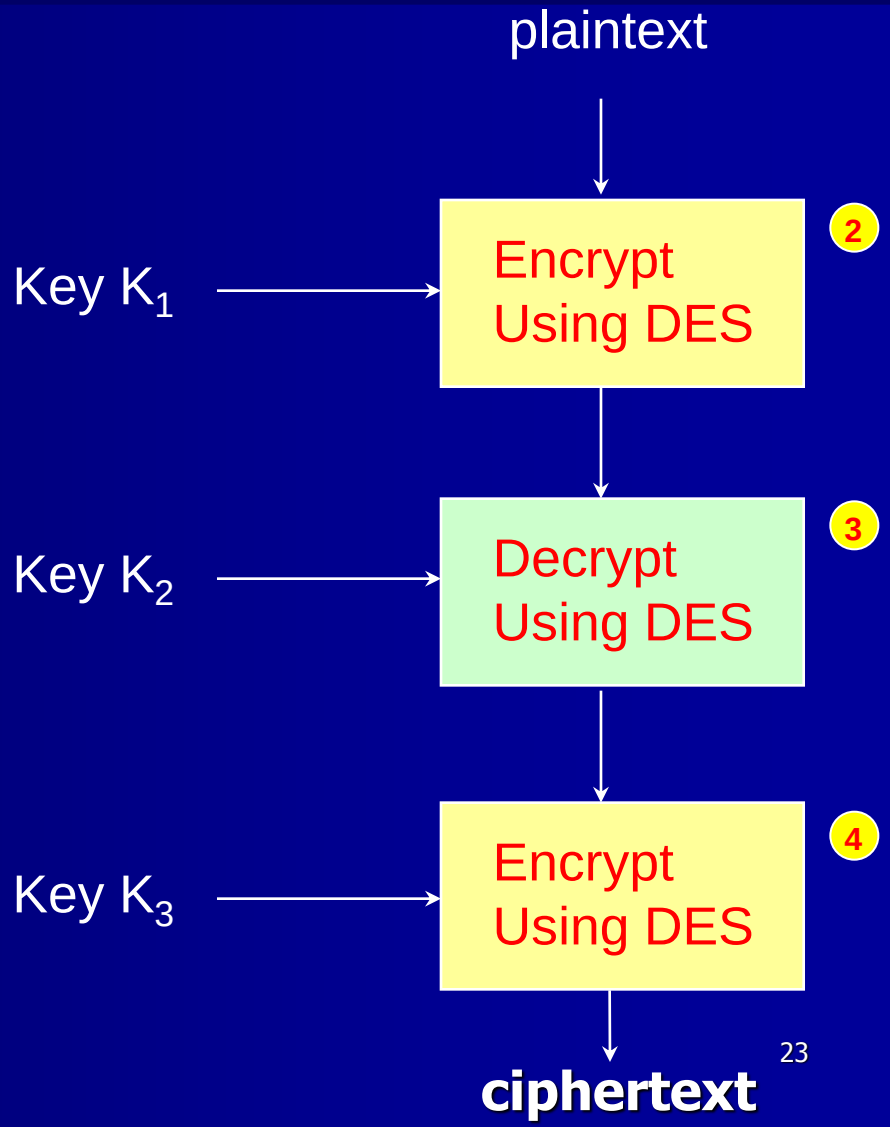
DES properties

- DES has 4 weak keys and six pairs of semi-weak keys
  - A DES weak key is a key k such that $E_k(E_k(x))=x$ for all x
  - A pair of DES semi weak keys is a pair (K_1,K_2) with $E_{k_1}(E_{k_2}(x))=x$ Tables 7.5 and 7.6, of weak and semi-weak keys on pp. 258 of [2].

- DES Today
  - A DES key can be found by anyone determined enough.
    - In 1998 Electronic Frontier Foundation managed to break DES (using DES Cracker, costing < $250,000) in less than 3 days.
  - Differential and linear cryptanalysis provide academic attacks on DES.
  - However, DES is still in use in many applications.
  - 3DES or AES are commonly recommended instead of DES.

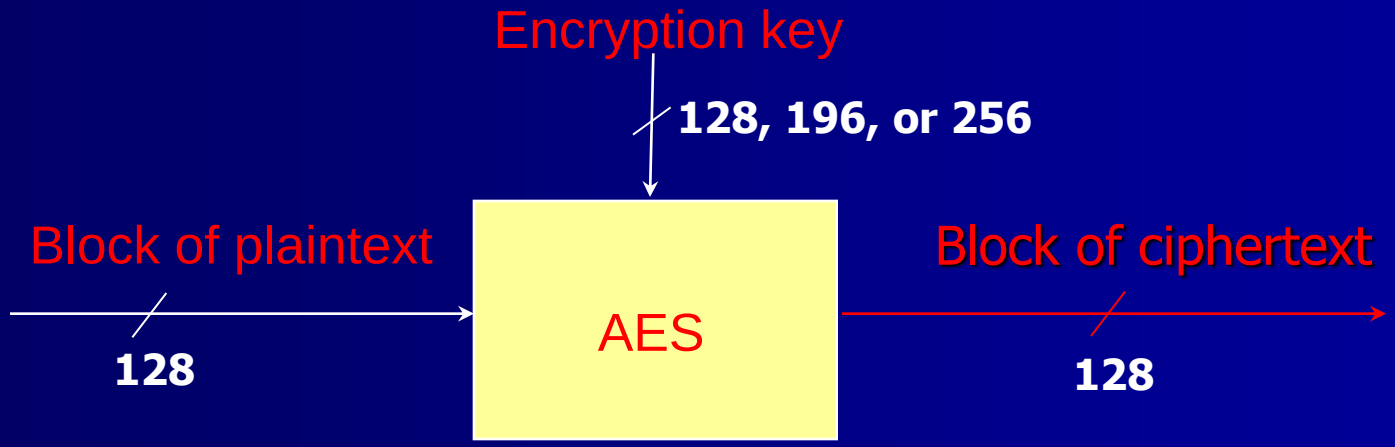
Triple DES

- Key =k_1 k_2k_3
- Key are longer (192 bits)
- Three times slower than DES



Advanced Encryption Standard

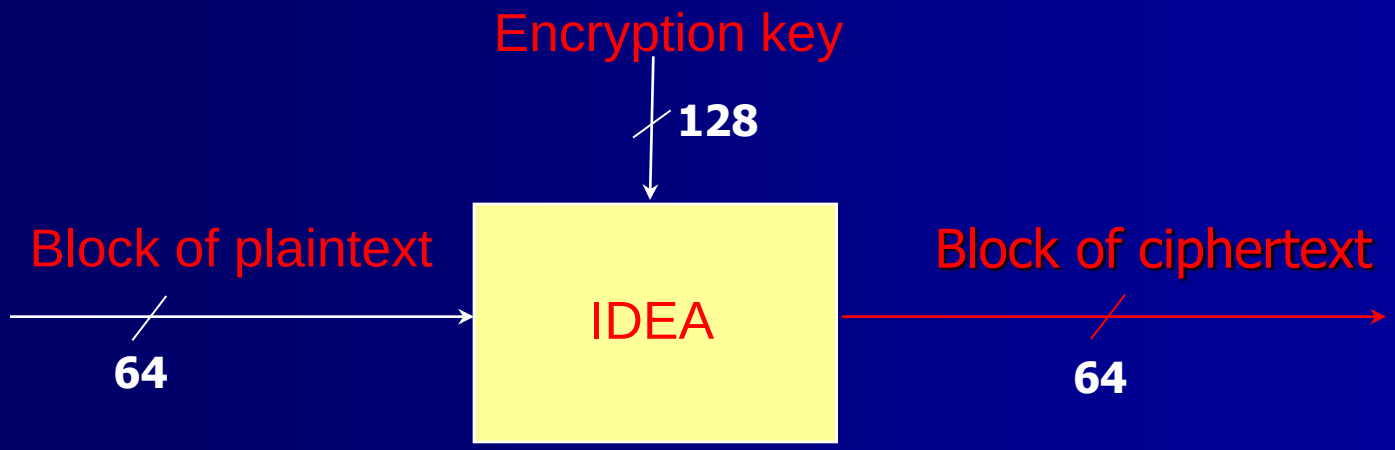
- In November 2001 the USA NIST announced *Rijndael* algorithm as the AES to replace DES as a FIPS 197
- Became effective in May 2002
- AES is a symmetric encryption algorithm
- Block size 128, rounds 10, 12, or 14 depending on the key size (128, 192, or 256)



- AES will probably be worldwide used very soon
- No known attack

Other Block ciphers

- IDEA (International Data Encryption Algorithm)
  - Published in 1991
  - Operates on 64-bit blocks, and 128-bit key and produces blocks of 64 bits



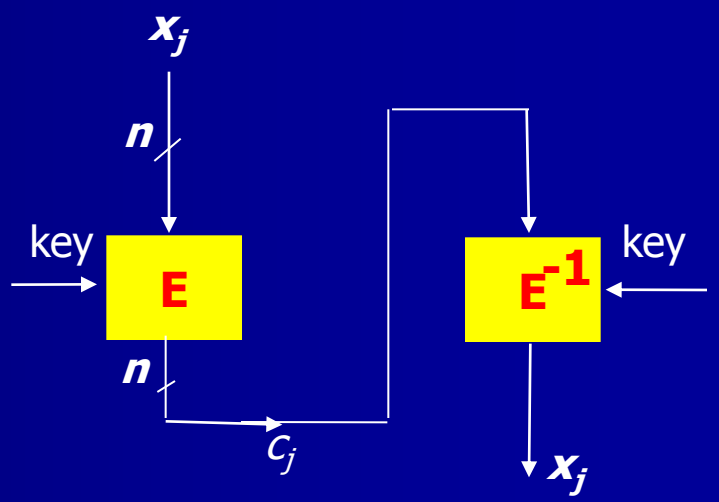
- Other ciphers: FEAL, SAFER, RC5, MARS, RC6, Serpent, Twofish....

5. Modes of operation

- FIPS 81 specifies four modes for DES.
  - ECB -Electronic Code Book.
  - CBC -Cipher Block Chaining.
  - CFB -Cipher Feedback.
  - OFB -Output Feedback.

1. Electronic CodeBook (ECB):

- Identical plaintext blocks (under the same key) result in identical ciphertext.
- Chaining dependency: blocks are enciphered independently of other blocks.
- Error propagation: one or more bit errors in a single ciphertext affect decipherment of that block only.
- ECB is not recommended for messages longer than one block, or if keys are reused for more than one-block message.
- Security of ECB may be improved by inclusion of random padding bits in each block.

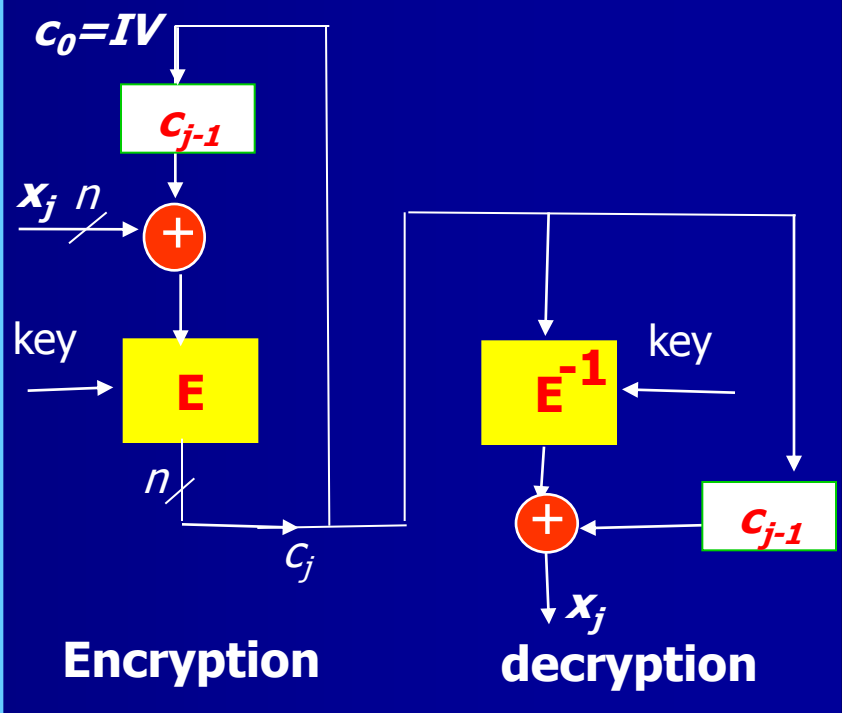


Electronic CodeBook (ECB)

6. Modes of operation

2. Cipher-Block Chaining (CBC):

- Identical plaintexts: identical ciphertext blocks result when the same plaintext is enciphered under the key and *IV*.
- Chaining dependency: a ciphertext c_j depends on x_j and all preceding plaintext blocks ⇒ rearranging the order of ciphertext blocks affects decryption.
- Error propagation: a single bit error in ciphertext block c_j affects decipherment of c_j and c_{j+1}.
- Error recovery: CBC is *self-synchronizing* in the sense that if an error occurs in block c_j, c_{j+2} is correctly recovered.
- *IV* is not secret but needs integrity.

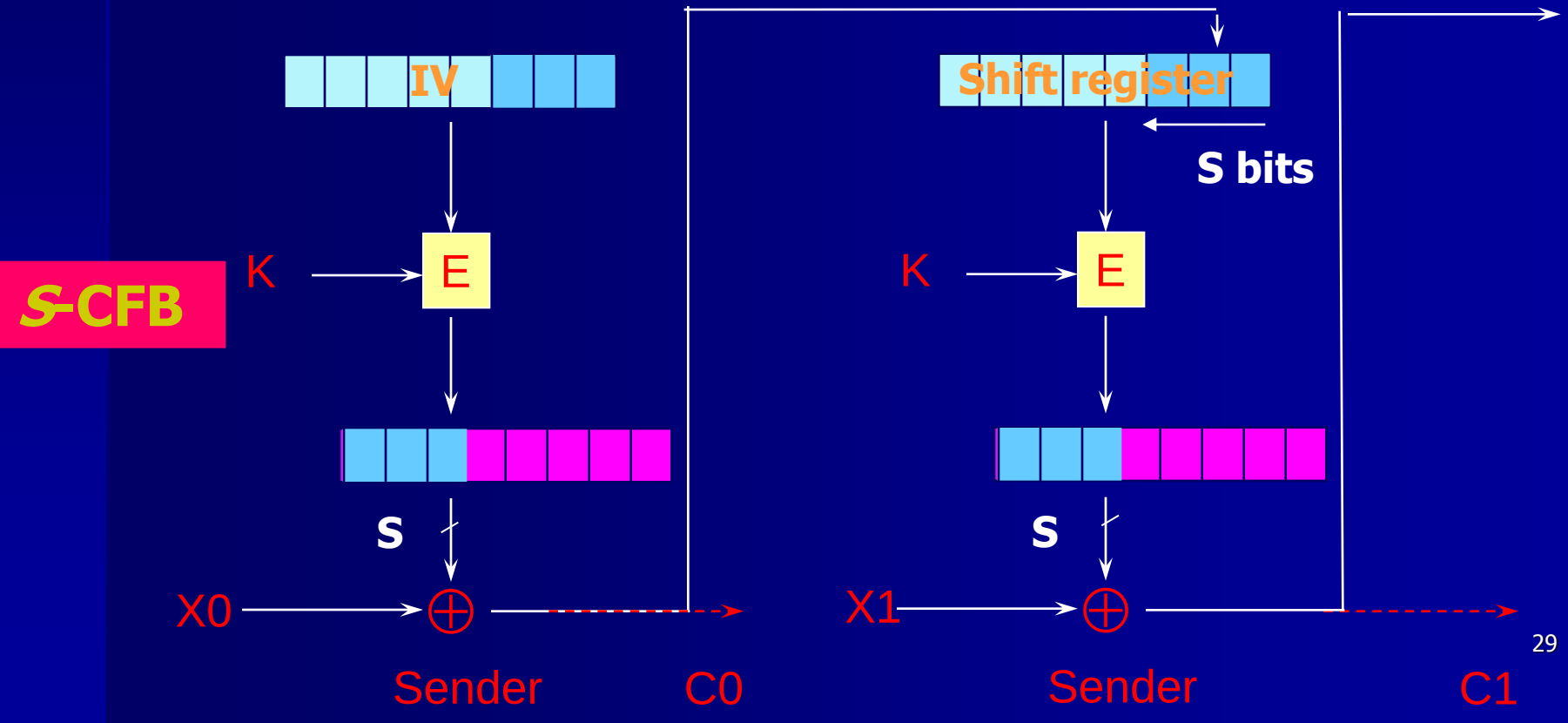


Cipher-Block Chaining (CBC)

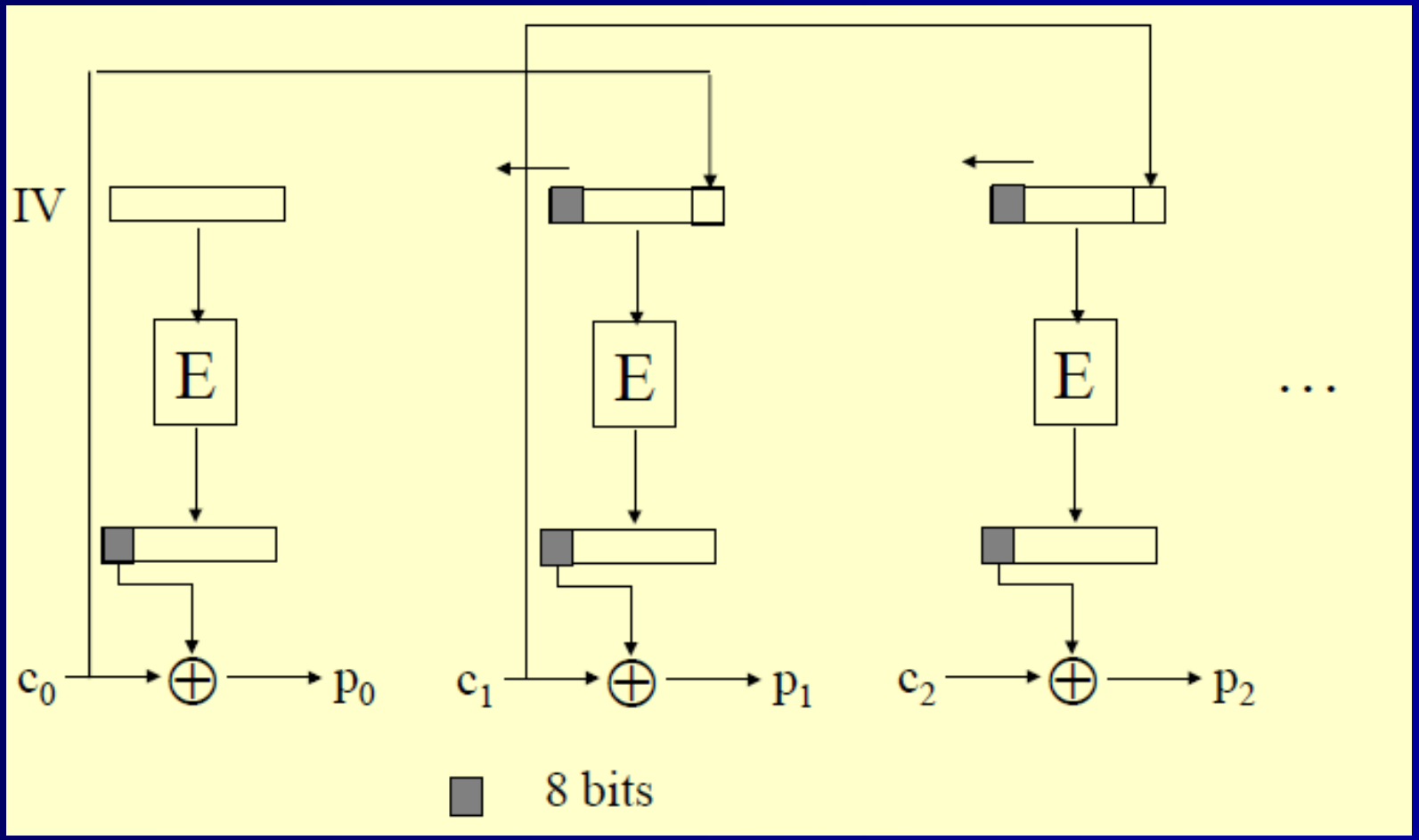
Modes of operation

3. Cipher FeedBack Mode (CFB):

- ***Self-synchronizing*** stream cipher for symbols of size up to block size.
- CFB turns block cipher into stream cipher, but not as efficient as a dedicated stream cipher.



CFB Decryption



Properties of block ciphers

- Block ciphers do propagate errors (to a limited extent), but are quite flexible and can be used in different ways in order to provide different security properties.
- The properties of cryptographic algorithms are not only affected by algorithm design, but also by the ways in which the algorithms are used. Different modes of operation can significantly change the properties of a block cipher.
- The security of block ciphers mainly depends on the complexity of the encryption function whereas thus of stream ciphers depend on the keystream randomness.
- They can be used to provide confidentiality, data integrity, or user authentication, and can even be used to provide the keystream generator for stream ciphers


Questions?