مروری برالگوریتمهای رمز متقارن(کلید پنهان)

علی فانیان
a.fanian@cc.iut.ac.ir

فهرست مطالب

- معماری لایه ای امنیت
- اصول الگوریتمهای رمزنگاری
- انواع الگوریتمهای رمز متقارن(کلید پنهان)
- الگوریتمهای رمزنگاری قالبی
- نحوه های بکارگیری رمزهای قطعه ای

فهرست مطالب

- معماری لایه ای امنیت
- اصول الگوریتمهای رمزنگاری
- انواع الگوریتمهای رمز متقارن(کلید پنهان)
- الگوریتمهای رمزنگاری قالبی
- نحوه های بکارگیری رمزهای قطعه ای

معماری لایه ای امنیت

فهرست مطالب

- معماری لایه ای امنیت
- اصول الگوریتمهای رمزنگاری
- انواع الگوریتمهای رمز متقارن(کلید پنهان)
- الگوریتمهای رمزنگاری قالبی
- نحوه های بکارگیری رمزهای قطعه ای

Terminology

plaintext, cleartext: an “unhidden message”

encrypt: transform a message to hide its meaning

ciphertext: encrypted message

cipher: cryptographic algorithm

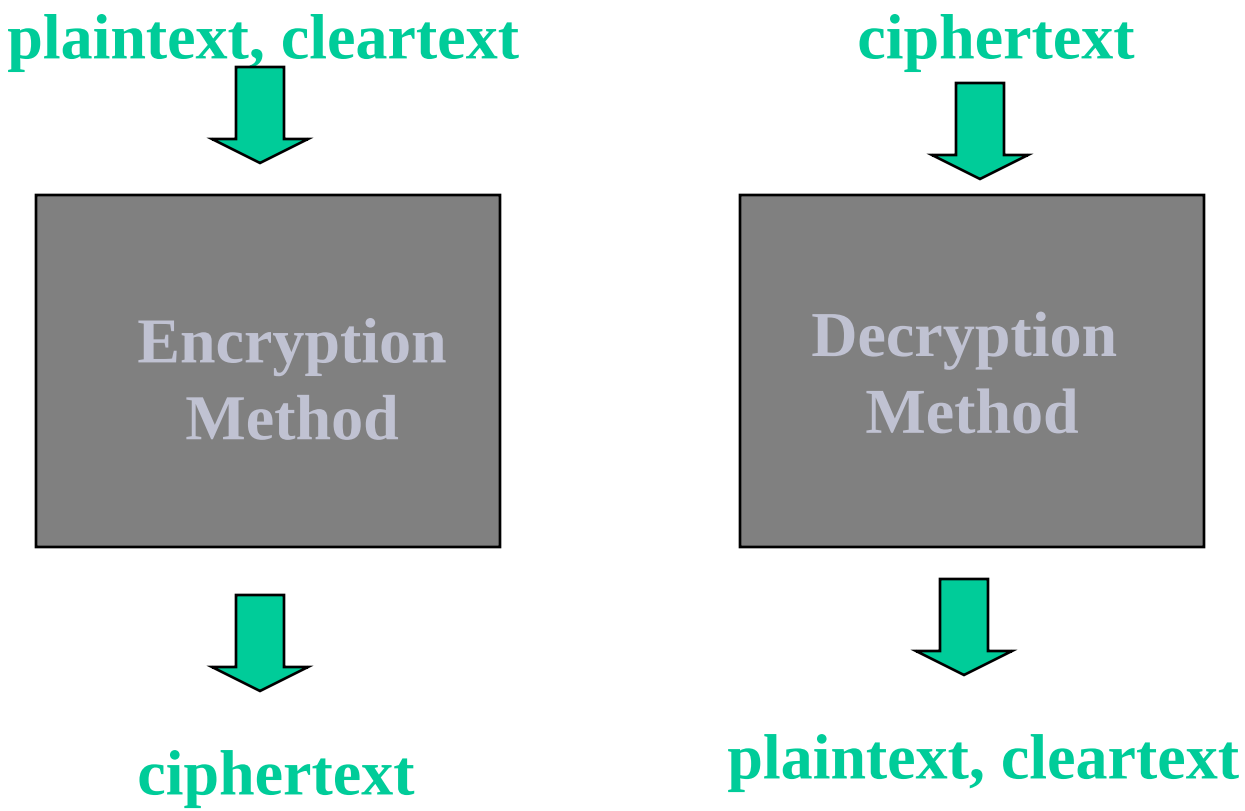
decrypt: recover meaning from encrypted message

cryptography: art/science of keeping message secure

cryptanalysis: art/science of breaking ciphertext

cryptology: study of both cryptography and cryptanalysis

Encryption and Decryption



Common Mathematical Symbols

P plaintext (here is a binary value)

C ciphertext (also binary)

E encryption function

D decryption function

E(P) = C encrypting plaintext yields ciphertext

D(C) = P decrypting ciphertext yields plaintext

D(E(P)) = P decrypting encrypted plaintext yields plaintext

Cryptography Algorithm Type

- Restricted Algorithm
- Key-Based Algorithm

Restricted Algorithm

The security of a restricted algorithm requires keeping the algorithm secret!

Simple Restricted Algorithm

Encryption algorithm

Multiply the plaintext by 2

Decryption algorithm

Divide the ciphertext by 2

plaintext **= SECRET =** 19 5 3 18 5 20

Ciphertext = 38 10 6 35 10 40

Key-Based Algorithm

The security of key-based algorithms is based on the secrecy of the algorithm, the key(s), or both

Simple Key-Based Algorithm

Encryption algorithm

Multiply the plaintext by 2 and add key

Decryption algorithm

Subtract the key and divide the ciphertext by 2

plaintext **= SECRET =** 19 5 3 18 5 20

Key = 3

Ciphertext = 41 13 9 39 13 43

Secret (Symmetric) Key Algorithms

- Decryption key = encryption key
- Key agreed in advance between parties
- Key kept secret
- Like a locked room
  - Need the key to lock up document
  - Need the key to unlock room and get document

Public (Asymmetric) Key Algorithms

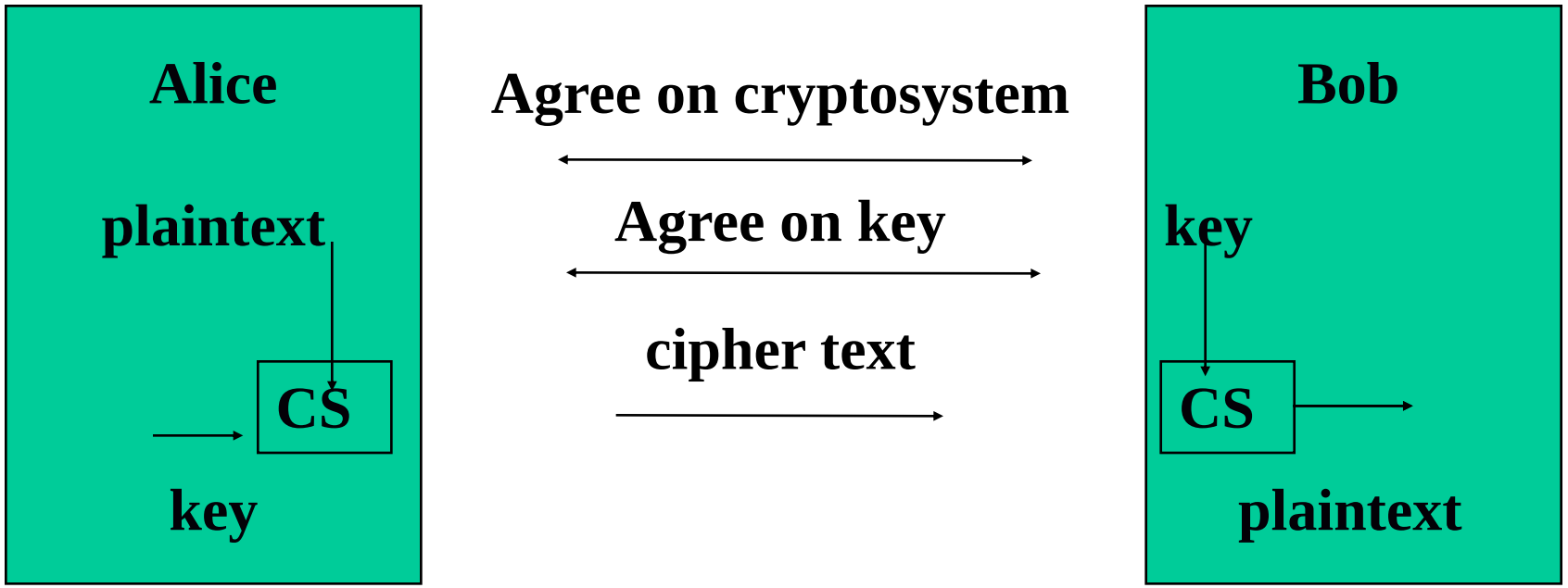
Encryption and decryption keys are different

Encryption key is public (usually)

Decryption key is private

One key locks, the other unlocks

Exchanging Messages with Symmetric Cryptography



Crypto-Attacks

- Adversary goal to break cryptosystem
- Assume adversary knows algorithm, but not key
- two general approaches to attacking a conventional encryption scheme
  - Cryptanalysis : rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext–ciphertext pairs
  - Brute-force attack : The attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained

Crypto-Attacks

- 3 types of attacks:
  - ***ciphertext only***:
    adversary has ciphertext; goal to find plaintext and key
  - ***known plaintext***:
    adversary has ciphertext, corresponding plaintext; goal to find key
  - ***Chosen Text***
    - *Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key*
    - *Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key*

Crypto-Attacks

- **Two definitions are worthy of note.**
  - ***unconditionally secure***
    - ***no matter how much ciphertext is available***
    - ***no matter how much time an opponent has***
    - ***it is impossible for opponent to decrypt the ciphertext***
    - ***there is no encryption algorithm that is unconditionally secure exception of a scheme known as the one-time pad***
  - **computationally secure**
    - **The cost of breaking the cipher exceeds the value of the encrypted information.**
    - **The time required to break the cipher exceeds the useful lifetime of the information.**

Crypto-Attacks

Table 2.2 Average Time Required for Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years

فهرست مطالب

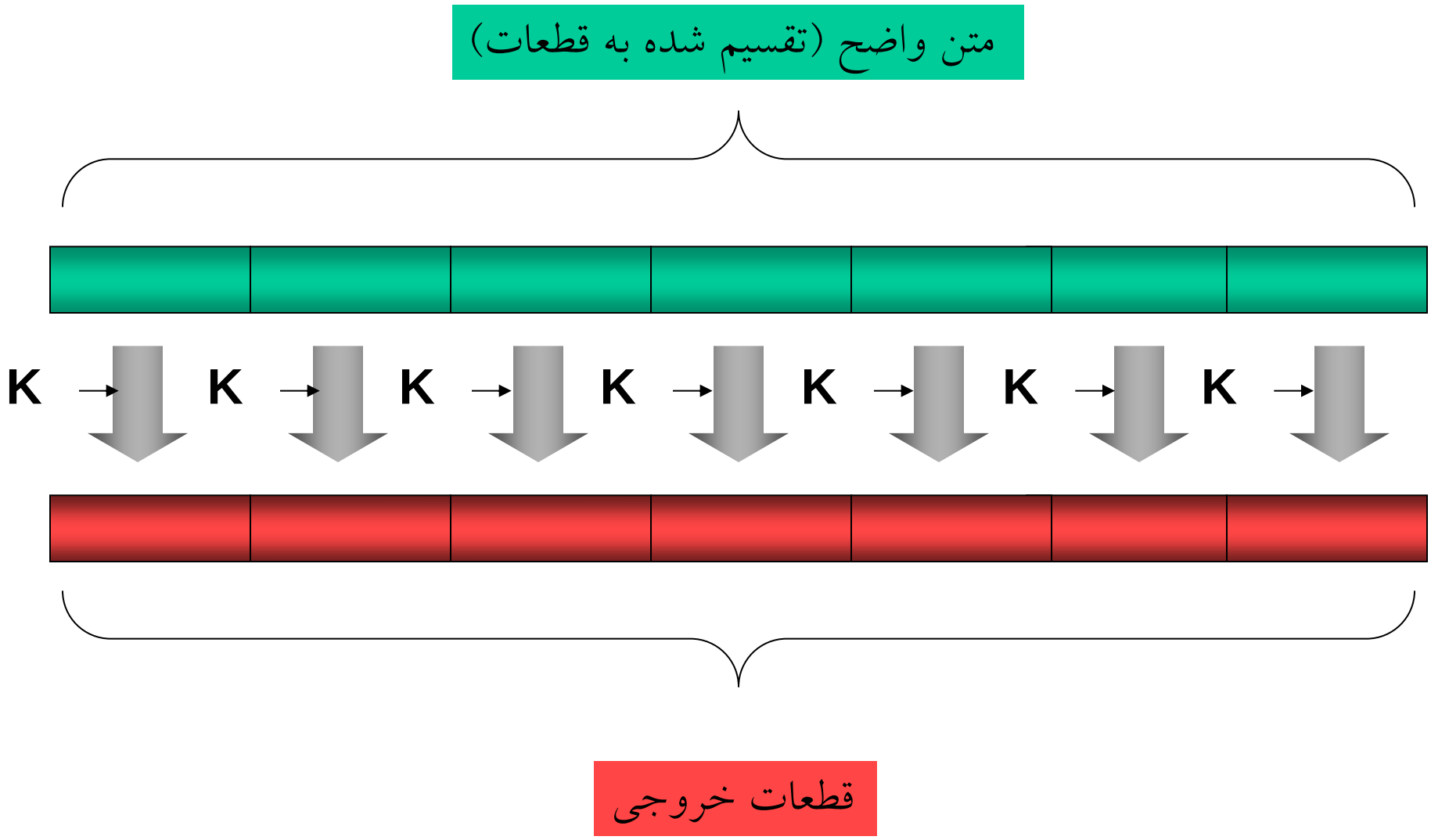
- معماری لایه ای امنیت
- اصول الگوریتمهای رمزنگاری
- انواع الگوریتمهای رمز متقارن(کلید پنهان)
- الگوریتمهای رمزنگاری قالبی
- نحوه های بکارگیری رمزهای قطعه ای

انواع الگوریتمهای رمز متقارن

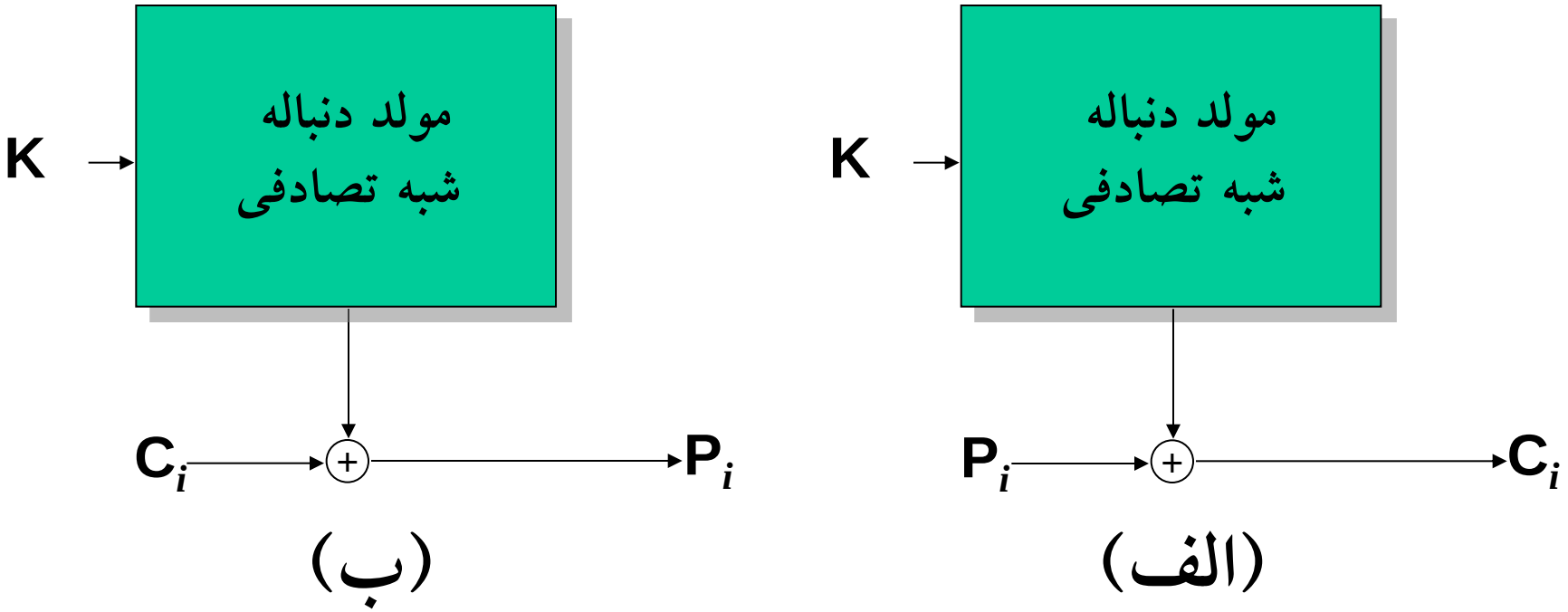
الگوریتمهای رمز متقارن بر دو دسته اند:

- **رمزهای قالبی یا قطعه ای (Block Cipher)**
  - **پردازش پیغام ها بصورت قطعه به قطعه**
  - **اندازه متعارف قطعات ٦٤، ١٢٨ یا ٢٥٦ بیت**
- **رمزهای پی در پی یا دنباله ای (Stream Cipher)**
  - **پردازش پیغام ها بصورت پیوسته (بدون تقطیع)**

رمز قطعه ای

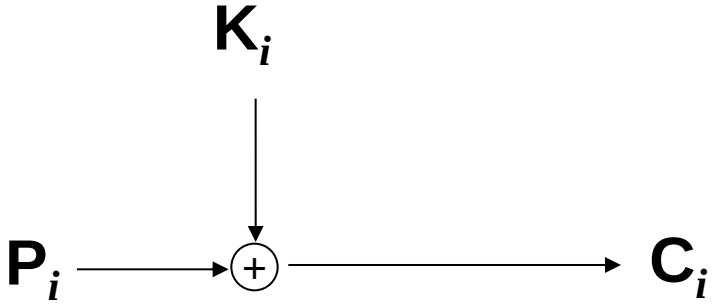


رمز دنباله ای



تابع رمزنگاری کامل(One-Time Pad)

- ایده : برای رمزکردن یک داده به طول **n** کلیدی به طول **n** هزینه کنیم.



- یعنی داشتن هر تعداد متن نمونه رمزشده کمکی به تحلیلگر نمی کند.
- امنیت این روش به تصادفی بودن کلید بستگی دارد.
  - در صورت تصادفی بودن کلید امنیت الگوریتم غیر قابل شکست است.

رمز دنباله ای

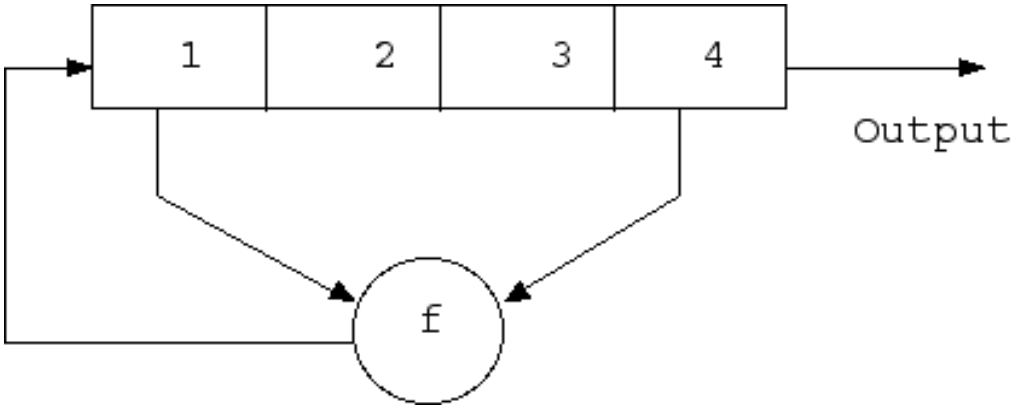
چند الگوریتم نمونه:

-Physical processes

-LSFR (**Linear Feedback Shift Register)**

-BBS(**Blum-Blum-Shub)**

Linear Feedback Shift Register



Linear shift feedback register with 4 bit register

فهرست مطالب

- معماری لایه ای امنیت
- اصول الگوریتمهای رمزنگاری
- انواع الگوریتمهای رمز متقارن(کلید پنهان)
- الگوریتمهای رمزنگاری قالبی
- نحوه های بکارگیری رمزهای قطعه ای

اصول رمزهای قطعه ای

- نگاشت قطعات متن واضح به قطعات متن رمزشده باید برگشت پذیر (یک به یک) باشد.
- الگوریتم قطعات ورودی را در چند مرحله ساده و متوالی پردازش میکند. به این مراحل دور میگوییم.
- هر دور عموماً مبتنی بر ترکیب اعمال ساده ایی همچون جایگزینی و جایگشت استوار است.

دو بلوک پایه برای عملیات رمز گذاری

- جانشینی Substitution
  - جایگیزینی یک سمبل با سمبل دیگر
  - ممکن است هم طول نباشند
- جابگشت Permutation
  - ترتیب قرار گرفتن حروف در متن اصلی جابجا می‌شود

استانداردهای رمزهای قطعه ای آمریکا :

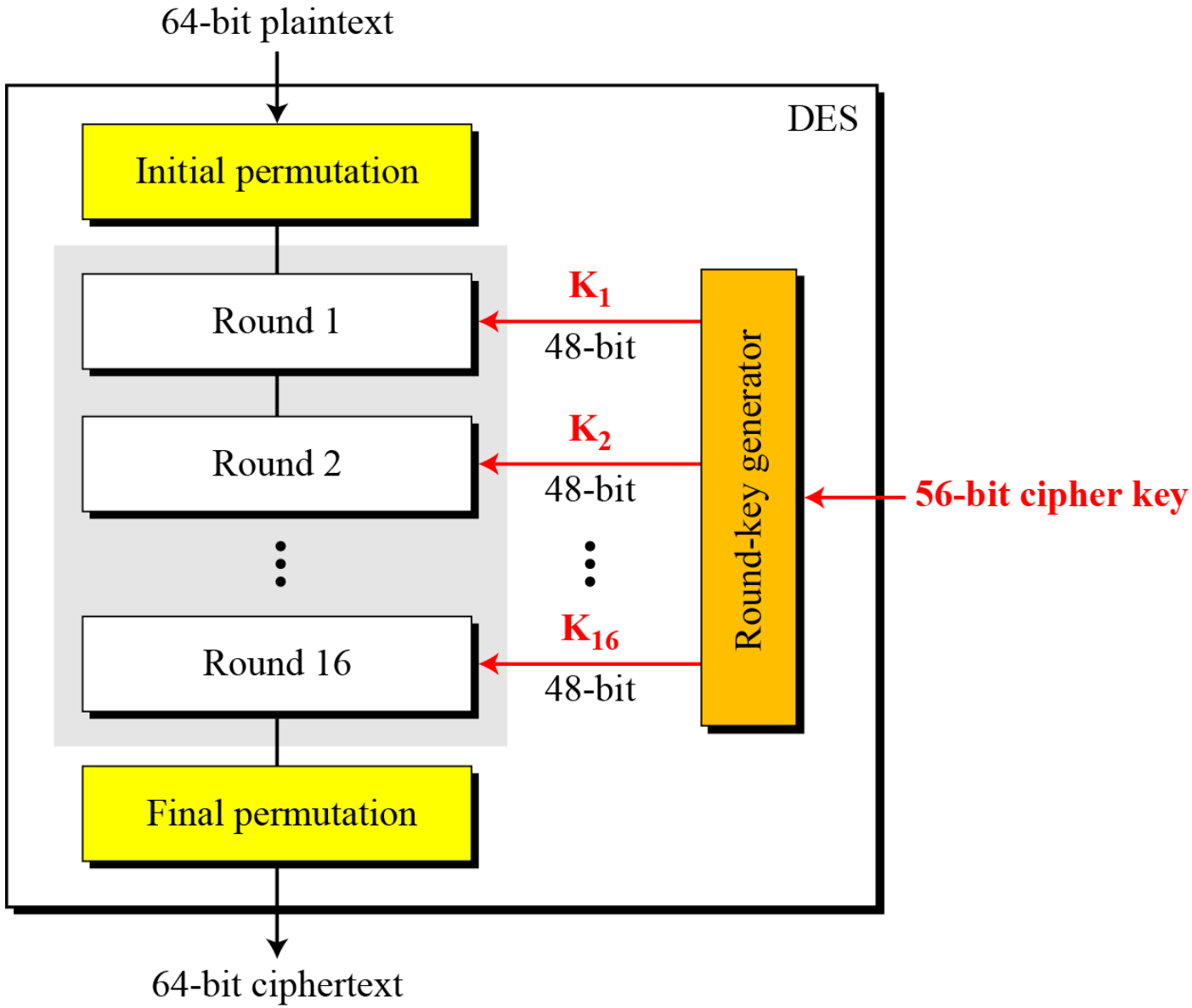
- رمزهای قطعه ای استاندارد
  - استاندارد رمزگذاری داده **DES**
  - استاندارد رمزگذاری پیشرفته **AES**
- تحت نظارت

National Institute of Science and Technology (NIST)

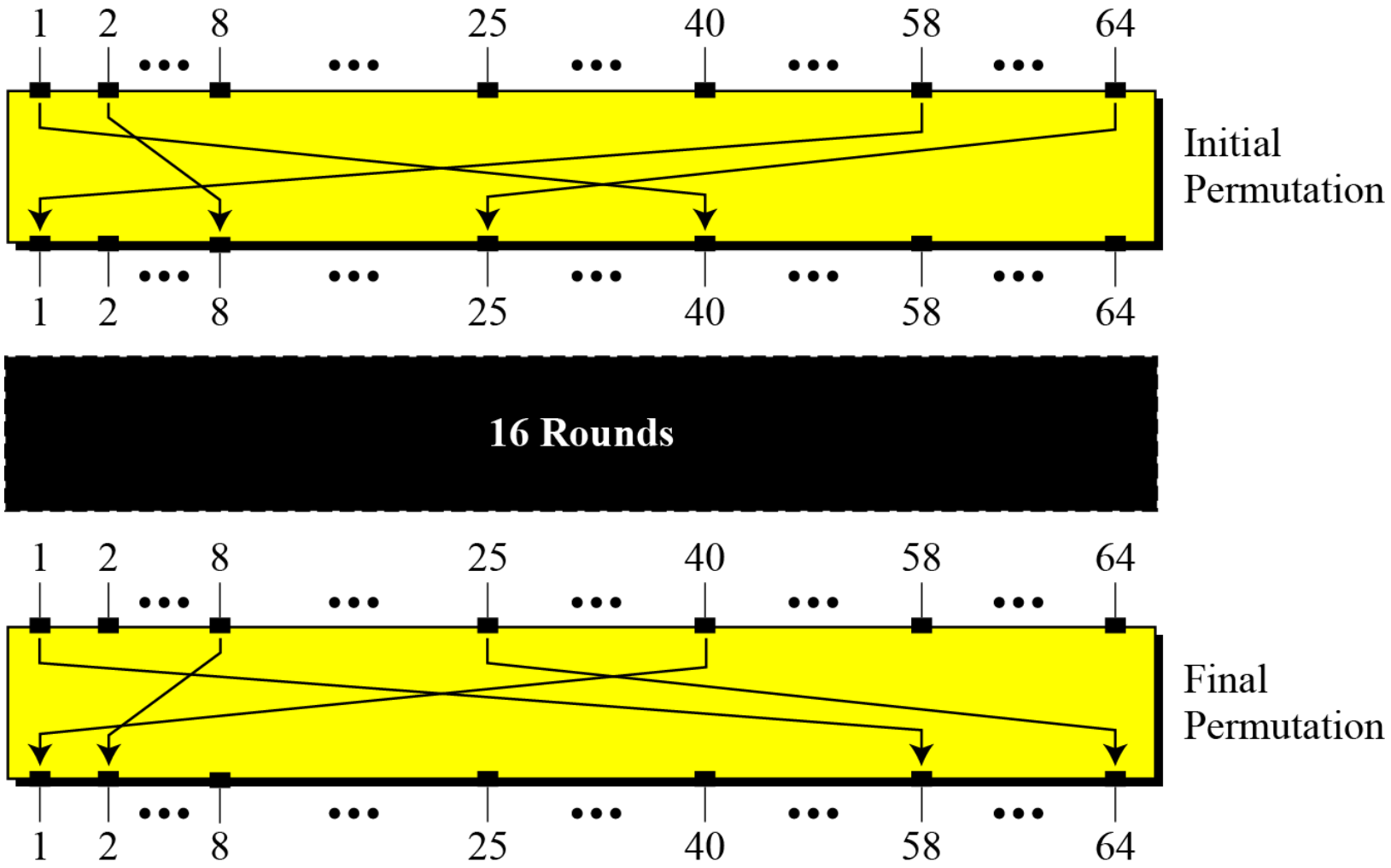
استاندارد رمزگذاری داده DES

- مرور
  - در سال ۱۹۷٤ توسط IBM تولید شد
    - پس از انجام تغییراتی توسط NSA (National Security Agency) ، در سال ۱۹۷٦ NIST آن را پذیرفت.
  - اساس الگوریتم ترکیبی از عملیات جانشینی و جایگشتی می‌باشد.
  - مشخصات:
    - طول کلید ٥٦ بیت
    - طول قالبهای ورودی و خروجی : ٦٤ بیت
    - تعداد دورها: ١٦ دور
  - الگوریتمهای رمزگذاری و رمزگشایی عمومی هستند, ولی مبانی ریاضی و اصول طراحی آنها فاش نشد.
  - در گذشته بسیار پر استفاده بود و هنوز هم از رده خارج نشده است.

استاندارد رمزگذاری داده DES

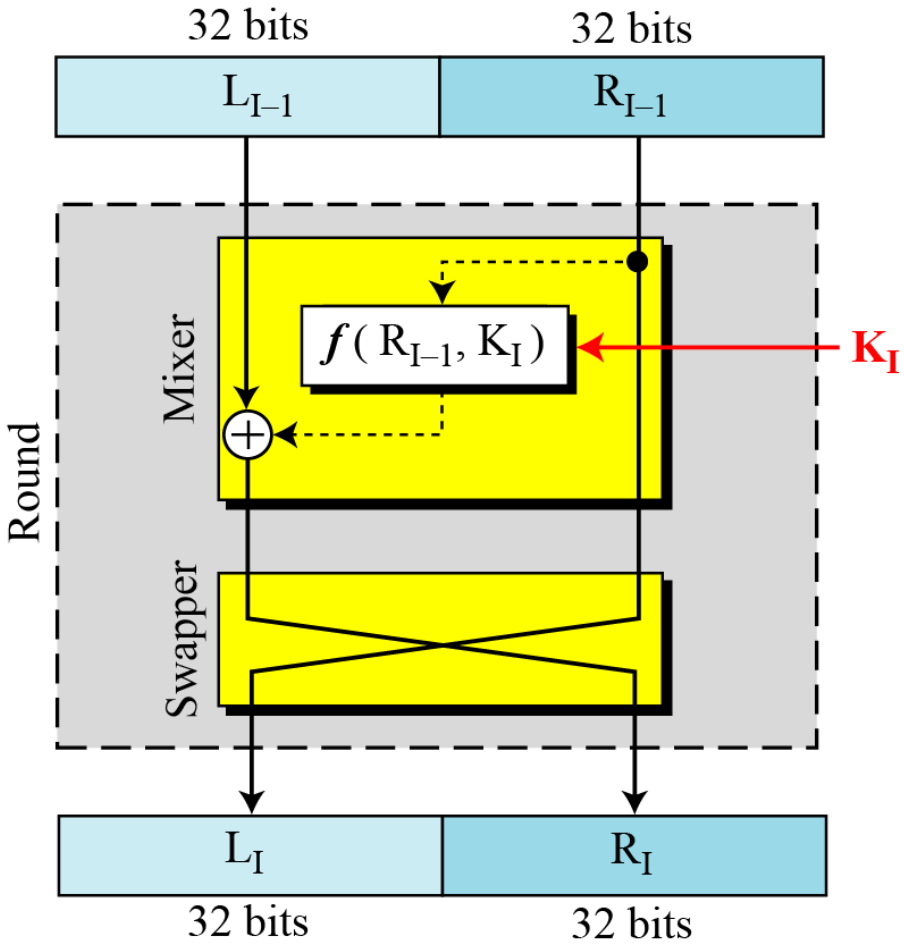


Initial and final permutation steps in DES



DES uses 16 rounds.

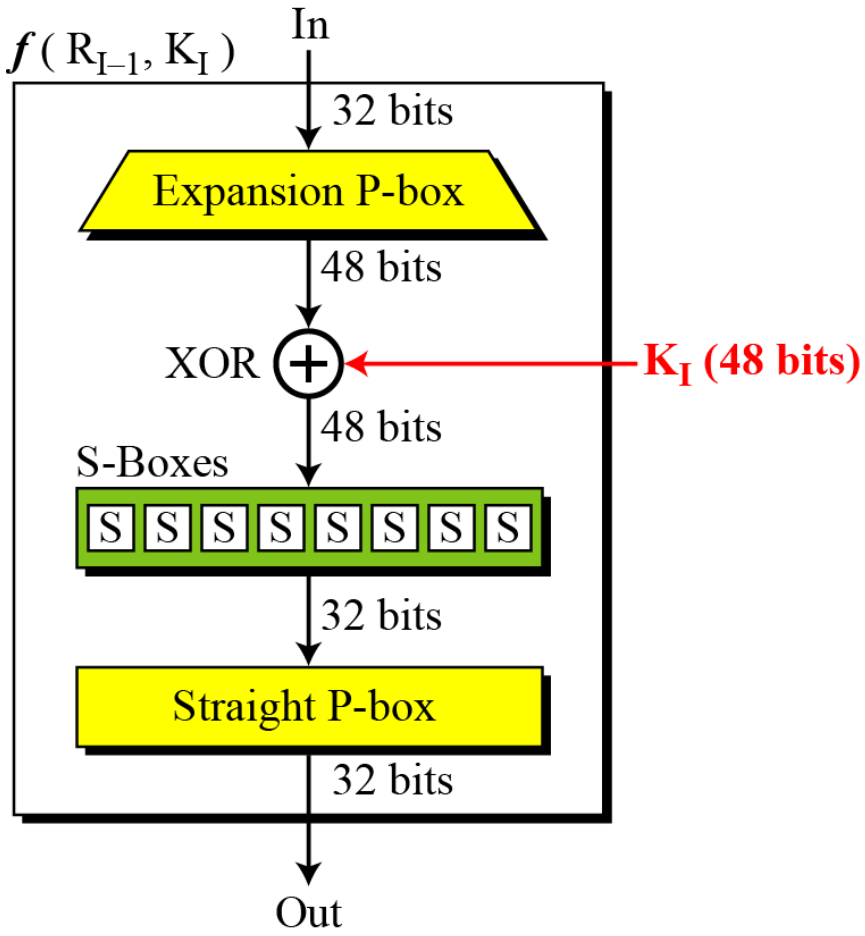
A round in DES (encryption site)



DES Function

The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits to produce a 32-bit output.

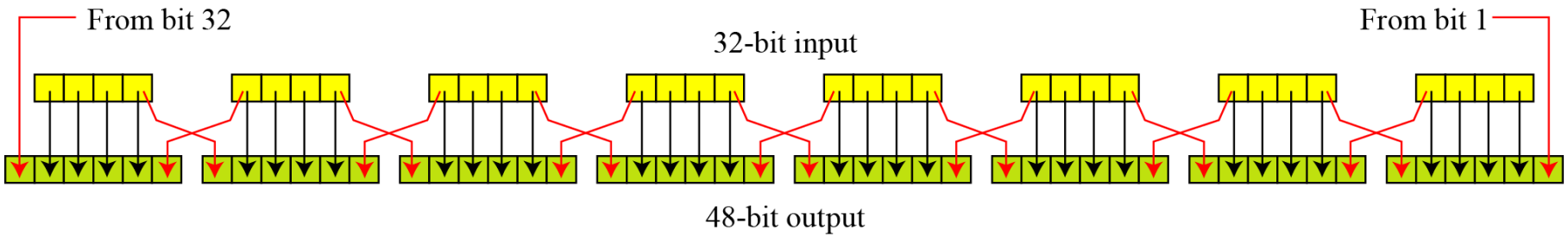
DES function



Expansion P-box

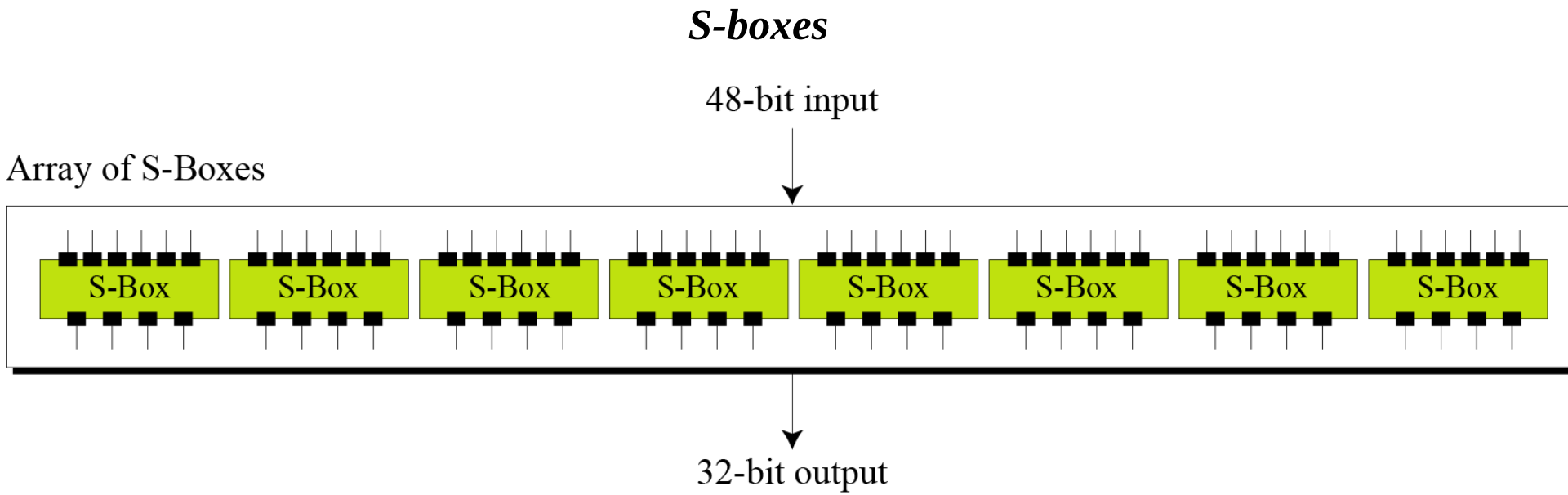
Since R_{I-1} is a 32-bit input and K_I is a 48-bit key, we first need to expand R_{I-1} to 48 bits.

Expansion permutation

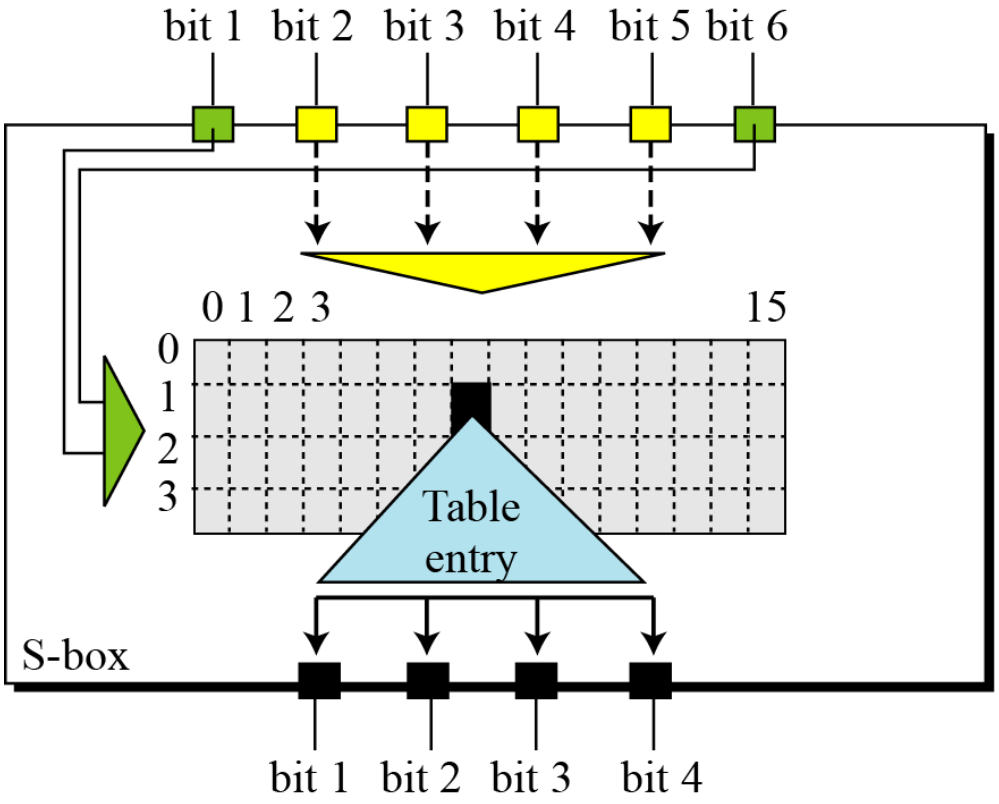


S-Boxes

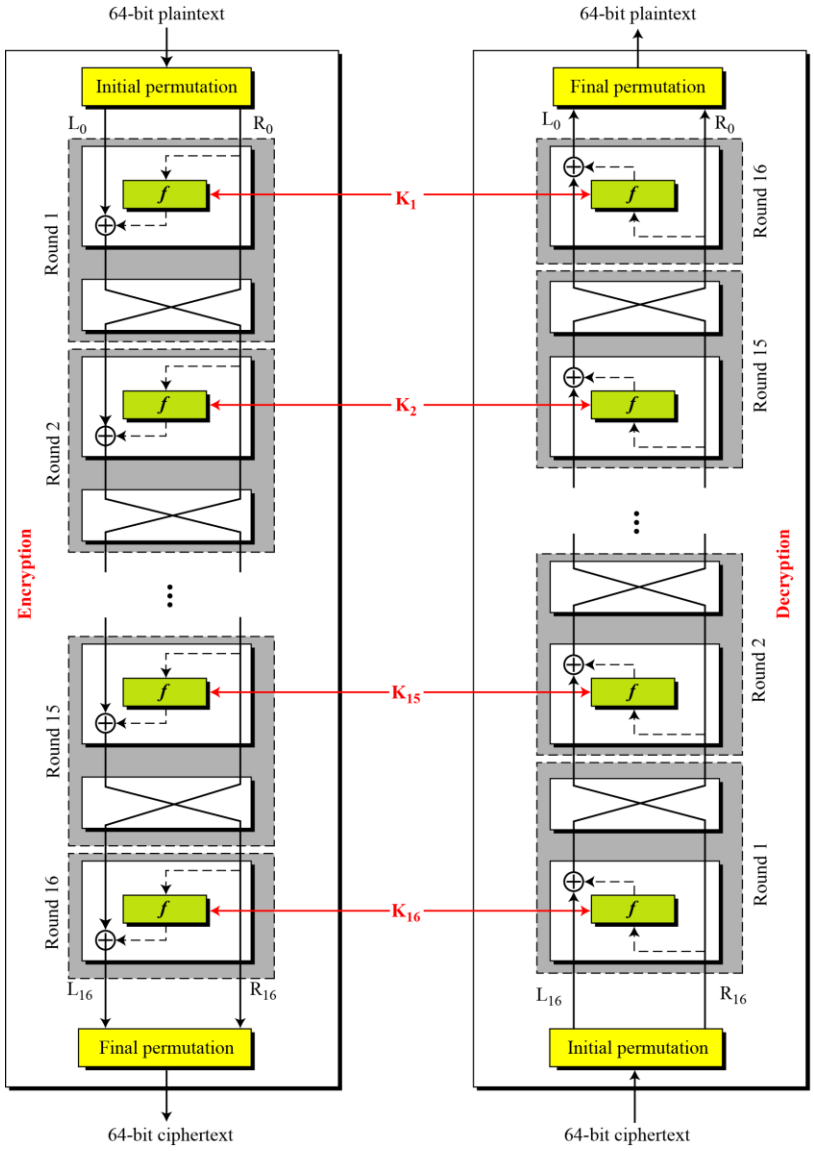
The S-boxes do the real mixing (confusion). DES uses 8 S-boxes, each with a 6-bit input and a 4-bit output.



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

DES cipher and reverse cipher for the first approach



DES باید از رده خارج شود

- در ژانویه ۱۹۹۹ این الگوریتم توسط حمله جستجوی جامع فضای کلید در ۲۳ ساعت شکسته شد!
  - بیش از ۱۰۰۰ کامپیوتر بر روی اینترنت هر یک بخش کوچکی از کار جستجو را انجام دادند.
- به الگوریتمهای امن تر با طول کلید بالاتر نیاز داریم.
- DES طراحی شفاف و روشن ندارد.

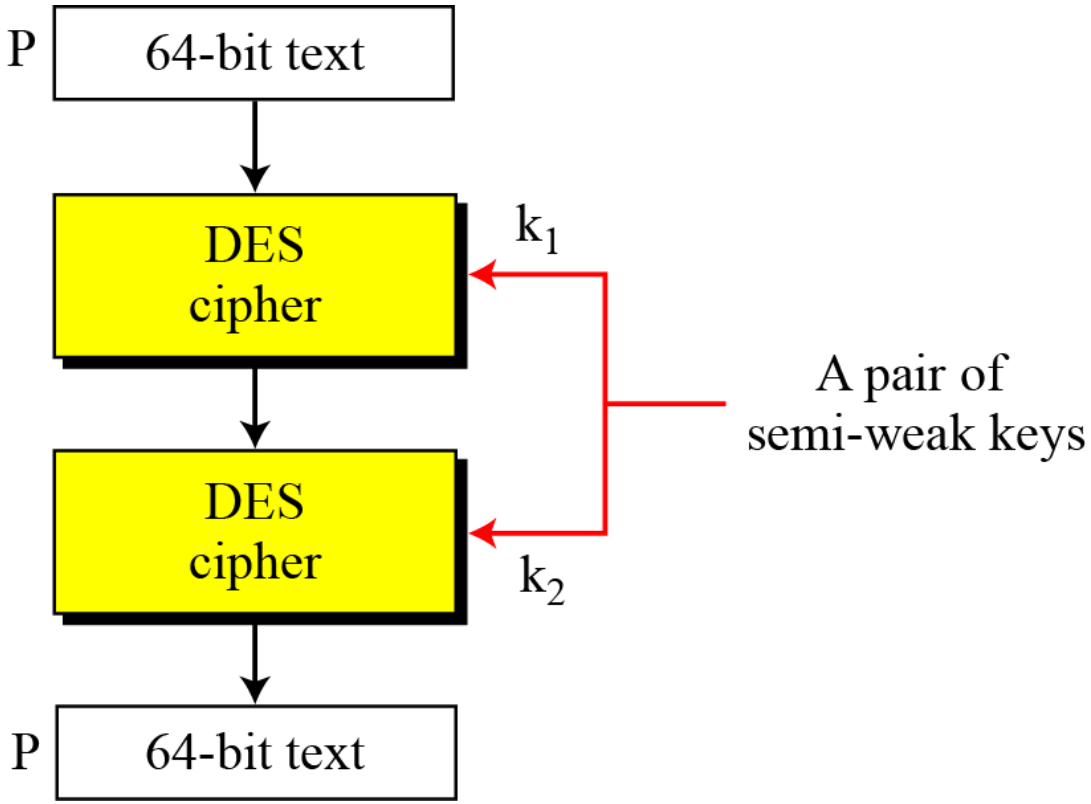
2DES and 3DES

- **مسئله :**
  - **آسیب پذیری DES در مقابل حمله آزمون جستجوی کامل**

- **راه حل :**
  - **استفاده از الگوریتم های رمزنگاری دیگر**
  - **پیچیده کردن الگوریتم DES از طریق اضافه کردن مراحل رمزنگاری و افزایش طول کلید**

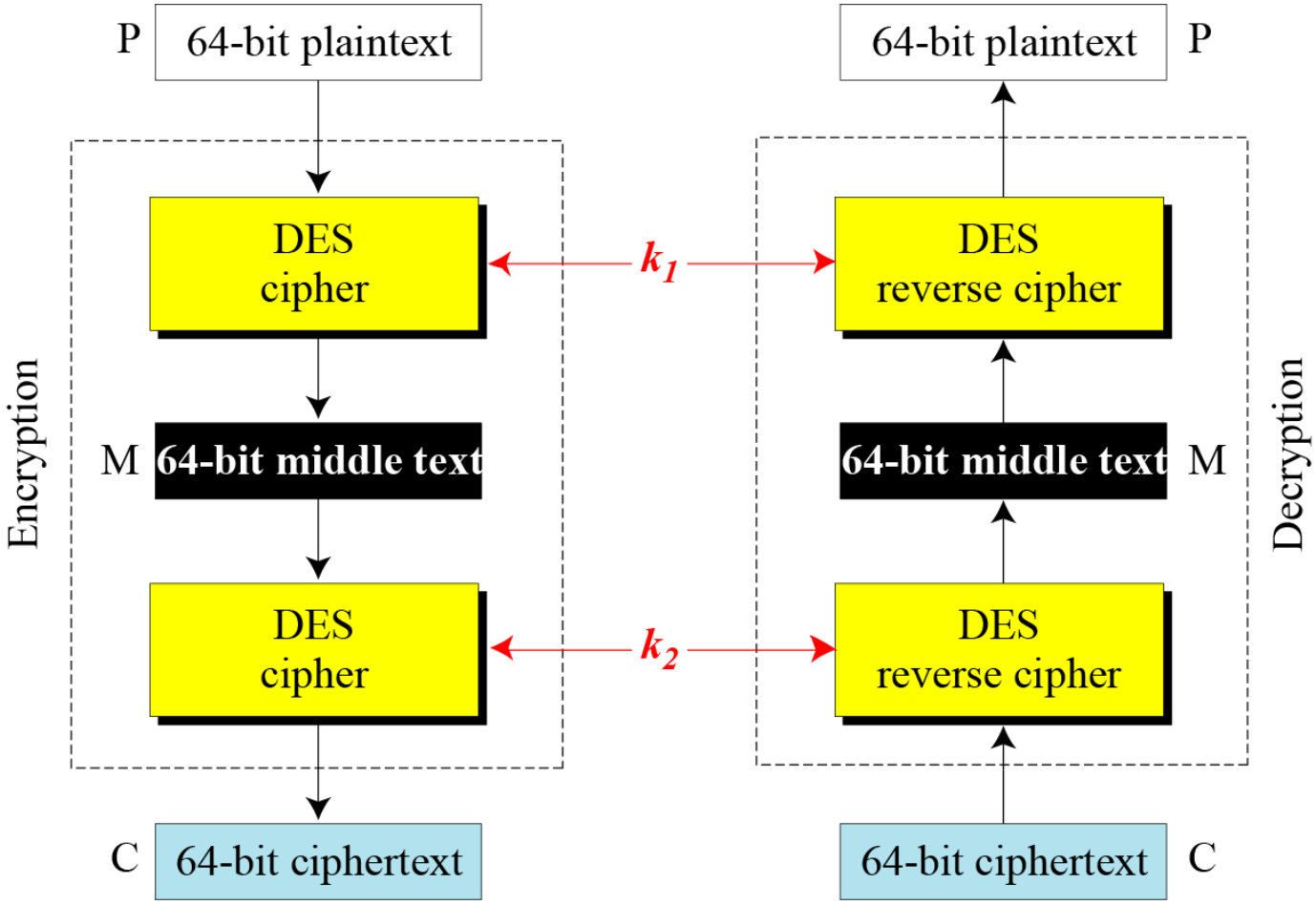
2DES

A pair of semi-weak keys in encryption and decryption



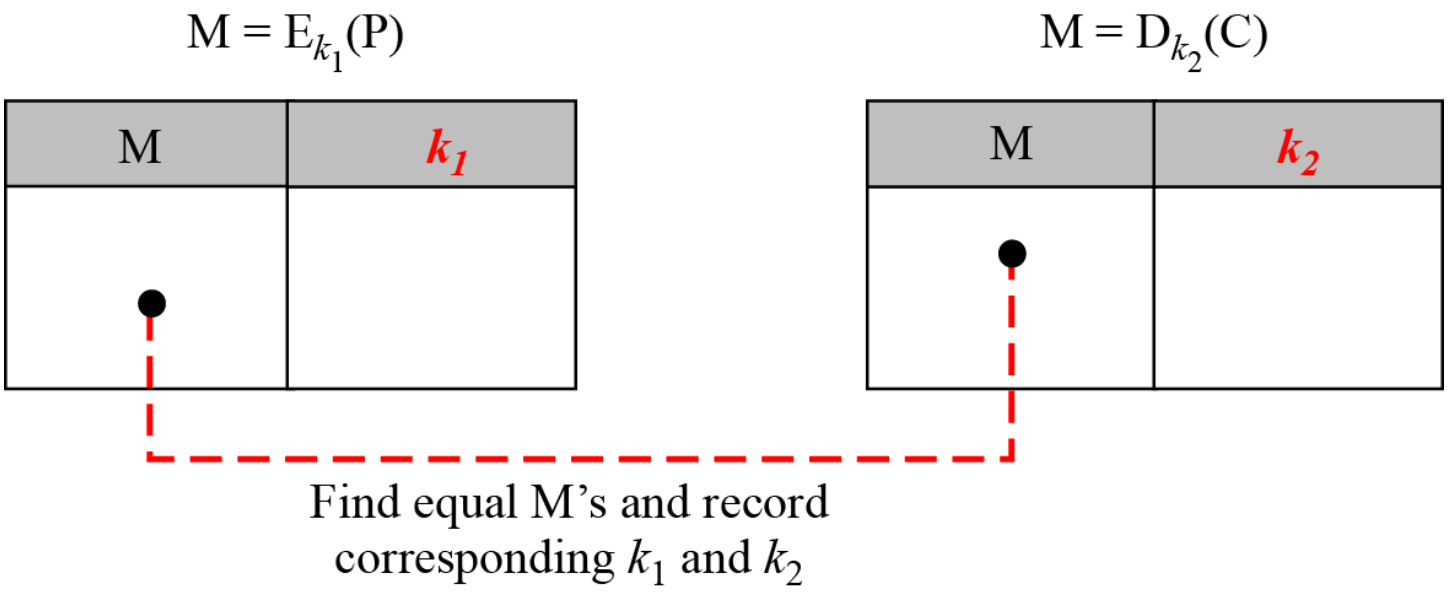
Meet-in-the-Middle Attack

However, using a known-plaintext attack called meet-in-the-middle attack proves that double DES improves this vulnerability slightly (to 2^{57} tests), but not tremendously (to 2^{112}).


P
64-bit plaintext
DES cipher
M
64-bit middle text
DES cipher
C
64-bit ciphertext
Encryption
k_1
k_2
64-bit plaintext
P
DES reverse cipher
64-bit middle text
M
DES reverse cipher
64-bit ciphertext
C
Decryption

Continued

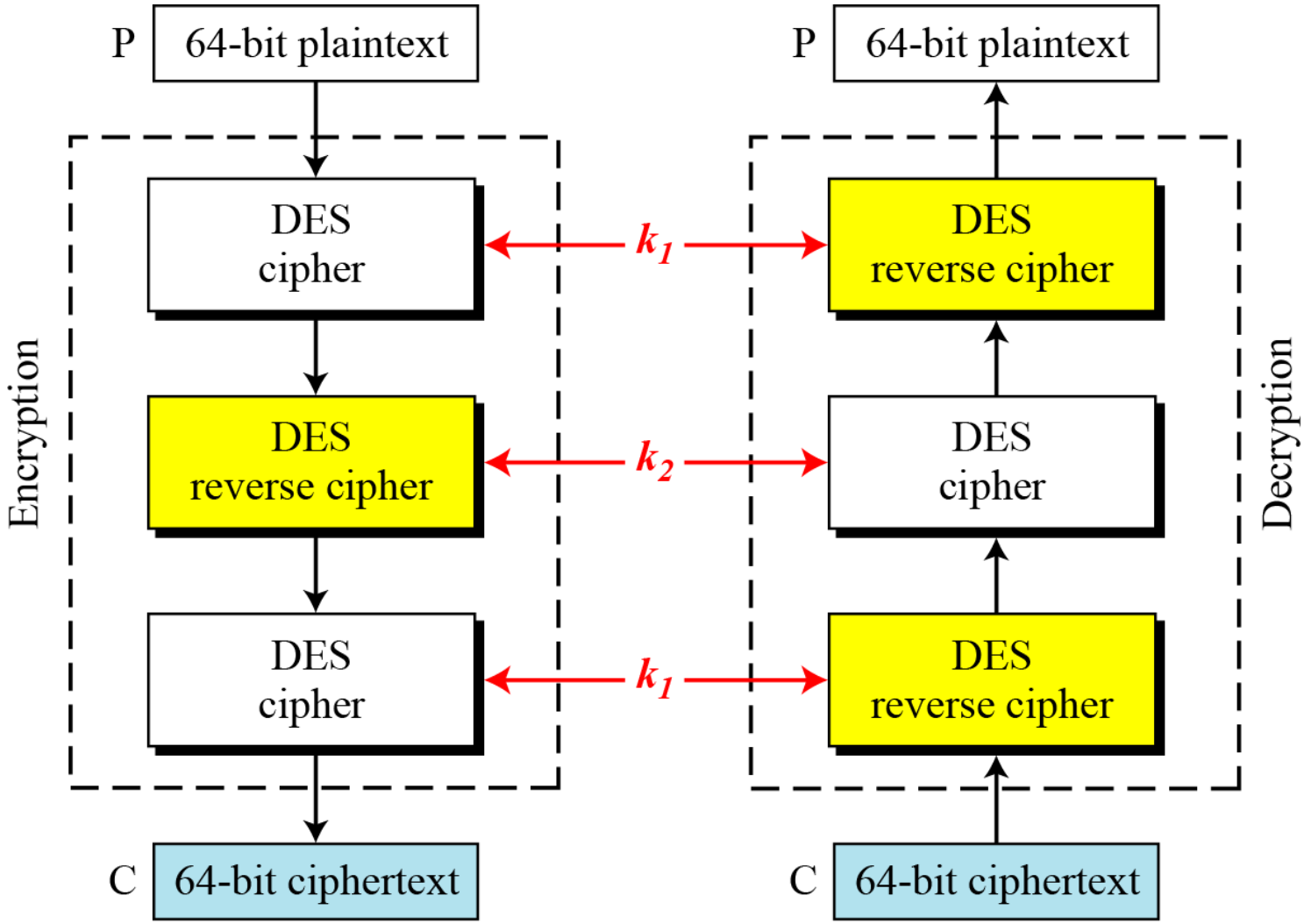
Tables for meet-in-the-middle attack



3DES

- استفاده از الگوریتم 3DES
  - از دو مرحله رمزنگاری و یک مرحله رمزگشایی با سه کلید مجزا استفاده می شود
  - فضای کلید به ۱۶۸ بیت گسترش می یابد
  - در صورت استفاده از یک کلید یکسان،3DES با DES مطابقت می کند
  - نسبت به الگوریتمهای دیگر مانند Blowfish و RC5 سرعت کمتری دارد
  - تا کنون حمله ای علیه آن گزارش نشده است

Triple DES with two keys



استاندارد رمزگذاری پیشرفته AES

- NIST در سال ۱۹۹۷ مسابقه ای دو مرحله ای برای طراحی استاندارد جدید برگزار کرد.
  - تمام طراحی ها باید بر اساس اصول کاملاً روشن انجام شوند.

- در سال ۲۰۰۰ رایندال(Rijndael) به عنوان برنده اعلام شد
  - استاندارد رمزگذاری پیشرفته AES

فینالیست های مسابقه AES

- ***MARS***
- ***RC6***
- ***Rijndael***
- ***Serpent***
- ***Twofish***

- مقاله زیر اطلاعات بیشتر درباره مقایسه فینالیست ها ارائه می دهد:

A Performance Comparison of the Five AES Finalists

B. Schneier and D. Whiting

فهرست مطالب

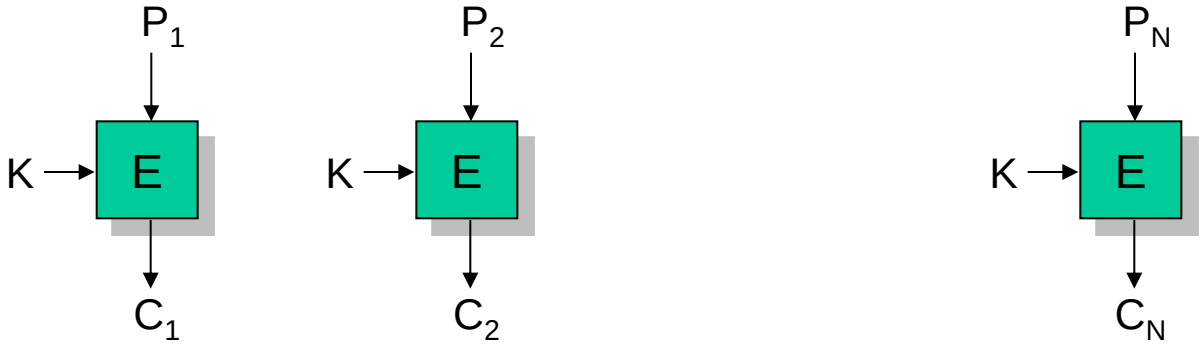
- معماری لایه ای امنیت
- اصول الگوریتمهای رمزنگاری
- انواع الگوریتمهای رمز متقارن(کلید پنهان)
- الگوریتمهای رمزنگاری قالبی
- نحوه های بکارگیری رمزهای قطعه ای

نحوه های بکارگیری رمزهای قطعه ای

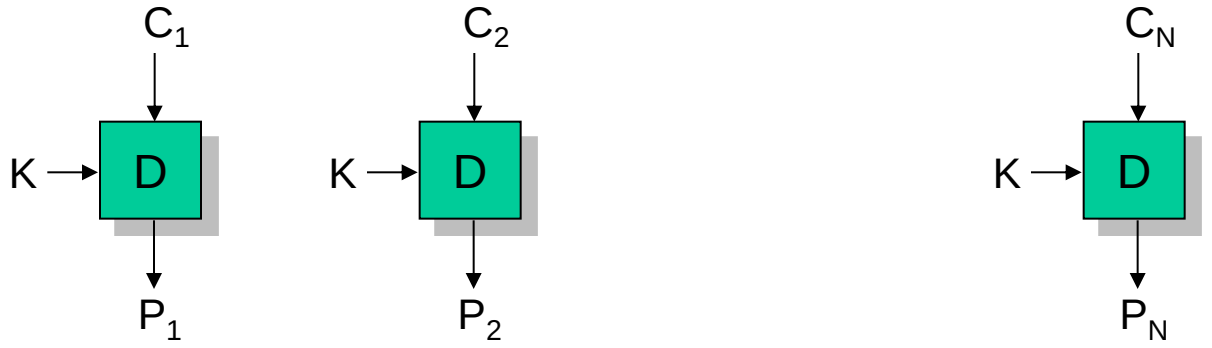
- **ECB: Electronic Code Book**
- **CBC: Cipher Block Chaining**
- **CFB: Cipher Feed Back**
- **OFB: Output Feed Back**
- **CTR: CounTeR mode**

نحوه بکارگیری ECB

- رمز نگاری:



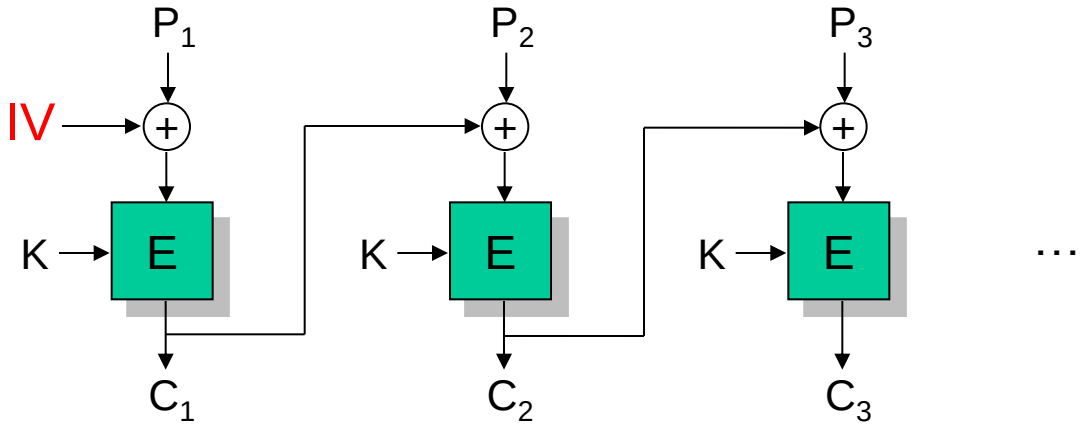
- رمز گشایی:



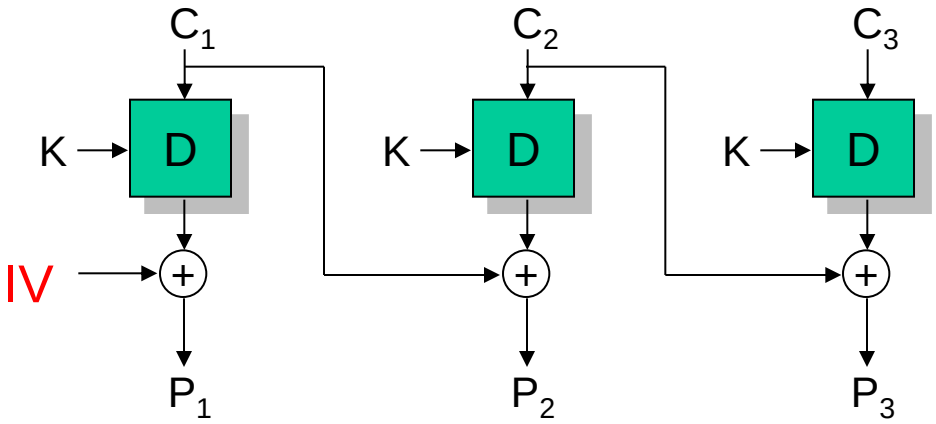
- اشکال اساسی: هر متن واضح به ازاء کلید ثابت همیشه به یک متن رمز شده نگاشته میشود.
  - دشمن میتواند دریابد که پیامهای یکسان ارسال شده اند.

نحوه بکارگیری CBC

- رمز نگاری:



- رمز گشایی:



مد کاری CBC

- این مد از یک مقدار دهی اولیه تصادفی (IV)بهره می گیرد

- مقدار IVدر هر بار رمزگذاری به صورت تصادفی تغییر می کند
- بهتر است IVنیز رمز شده ارسال گردد

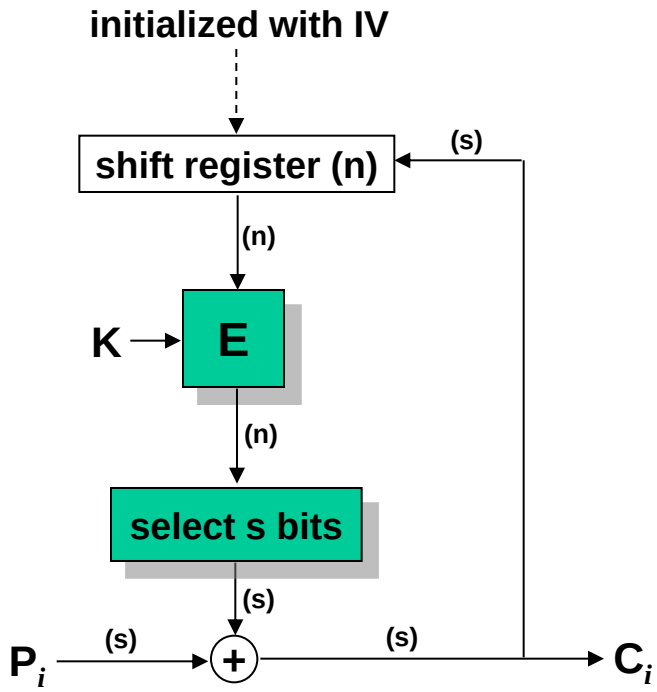
- هر متن آشکار به ازاء کلید ثابت هر بار به یک متن رمز شده متفاوت نگاشته می شود

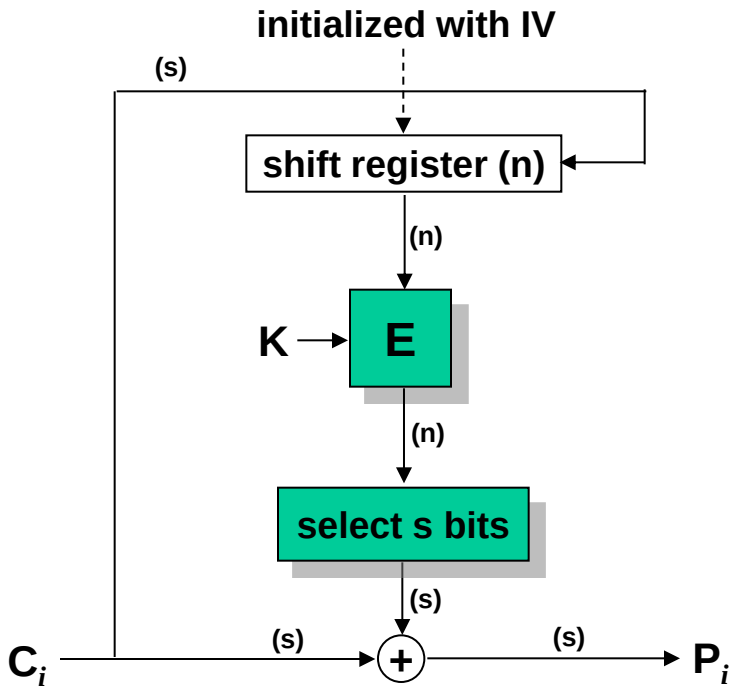
نحوه بکارگیری CBC

- **ملزومات امنیتی:**
  - **IV باید کاملاً غیر قابل پیش بینی و غیر قابل دستکاری باشد**
- **رمزنگاری:**
  - **عملیات رمزنگاری قابل موازی سازی نیست.**
  - **مقدار IV و متن واضح باید در دسترس باشند.**
- **رمزگشایی:**
  - **عملیات رمزگشایی قابل موازی سازی است.**
  - **مقدار IV و متن رمزشده باید در دسترس باشند.**
- **طول پیام:**
  - **در برخی موارد ممکن است وادار به افزایش طول پیام بشویم.**
    - **طول پیام باید مضربی از طول قطعه باشد.**
- **پیاده سازی:**
  - **رمز گشایی و رمز نگاری، هر دو باید پیاده سازی شوند.**

نحوه بکارگیری CFB

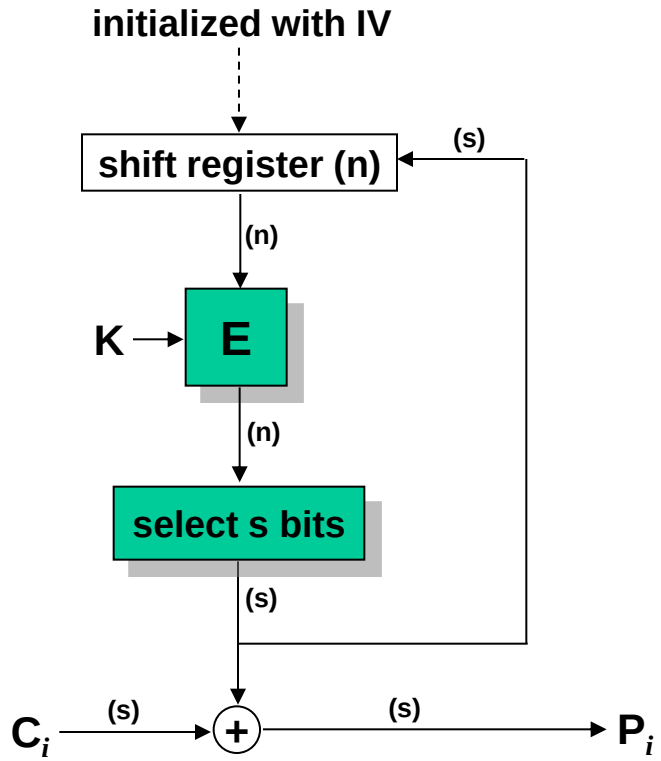
- رمزنگاری
- رمزگشایی



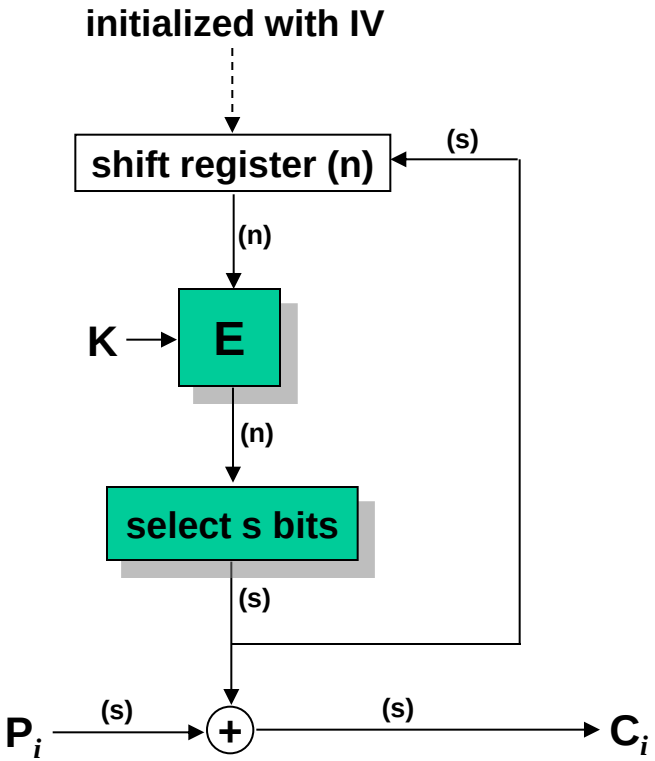


نحوه بکارگیری OFB

- رمزگشایی



- رمز نگاری

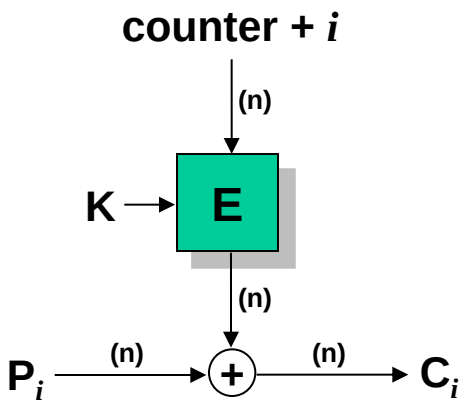


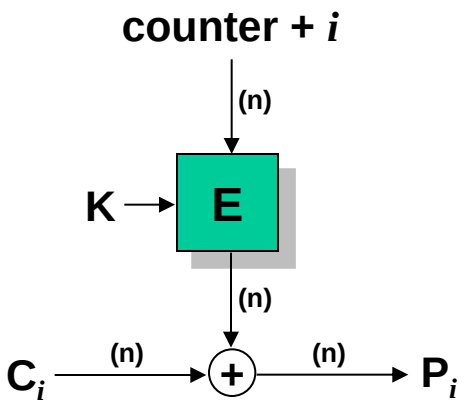
مقایسه CFB و OFB

- موارد استفاده CFB و OFB
  - رمز جریانی
  - کاربردهای بلادرنگ
- عیب CFB : انتشار خطای انتقال
  - OFB این عیب را برطرف می کند

نحوه بکارگیری CTR

- رمزگشایی
- رمز نگاری





مقایسه کاربرد انواع مدهای کاری

مد کاری	کاربرد
EBC (Electronic Code Book)	ارسال مقادیر کوچک مانند کلید
CBC (Cipher Block Chaining)	ارسال قطعه-گرای هر گونه داده احراز صحت
CFB (Cipher Feed Back)	ارسال جریانی هر گونه داده احراز صحت
OFB (Output Feed Back)	ارسال جریانی بر روی کانال نویزی (مانند ارتباطات ماهواره‌ای)
CTR (Counter)	ارسال قطعه-گرای هر گونه داده مناسب برای ارسال با سرعت بالا

لغت نامه

Authentication	احراز اصالت
Brute Force	جستجوي كامل
AES	استاندارد رمزگذاري پيشرفته
DES	استاندارد رمزگذاري داده
Padding	افزايش طول پيام
Provable Security	امنيت قابل اثبات
Differential cryptanalysis	تحليل تفاضلي
linear cryptanalysis	تحليل خطي
Substitution	جانشيني
Permutation	جايگشت
NSA: National Security Agency	
Timing Attack	حمله زماني

Meet-in-the-Middle attack	حمله ملاقات در ميانه
Round	دور
Symmetric Encryption Scheme	رمزنگاري متقارن
Stream Cipher	رمزهاي پي درپي(دنباله اي)
Block Cipher	رمزهاي قالبي(قطعه اي)
Symmetric Cipher	*رمزهاي متقارن*
Key Schedule	زمان بندي كليد
plaintext	متن واضح
Confidentiality	محرمانگي
parallelization	موازي سازي
MAC: Message authentication code	كد احراز اصالت پيام