

مروری بر الگوریتمهای رمز متقارن (کلید پنهان)

علی فانیان

a.fanian@iut.ac.ir

معماري لايه اي امنيت

کاربرد امنيتي

پروتکل امنيتي

الگوریتم ها

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

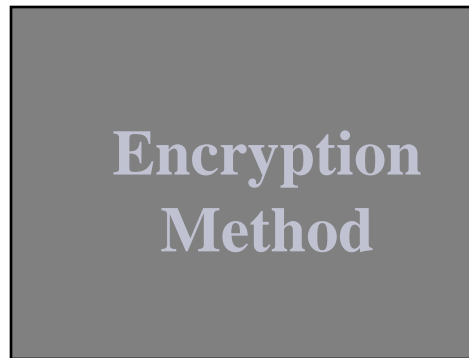
cryptography: art/science of keeping message secure

cryptanalysis: art/science of breaking ciphertext

cryptology: study of both cryptography and cryptanalysis

Encryption and Decryption

plaintext, cleartext



ciphertext

ciphertext



plaintext, cleartext

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

Type of cryptography Algorithm

- Symmetric Algorithm
- Asymmetric Algorithm

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



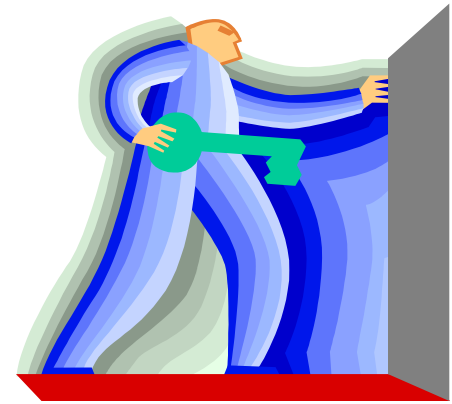
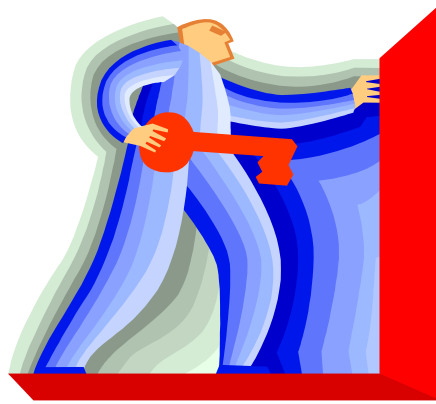
Public (Asymmetric) Key Algorithms

Encryption and decryption keys are different

Encryption key is **public** (usually)

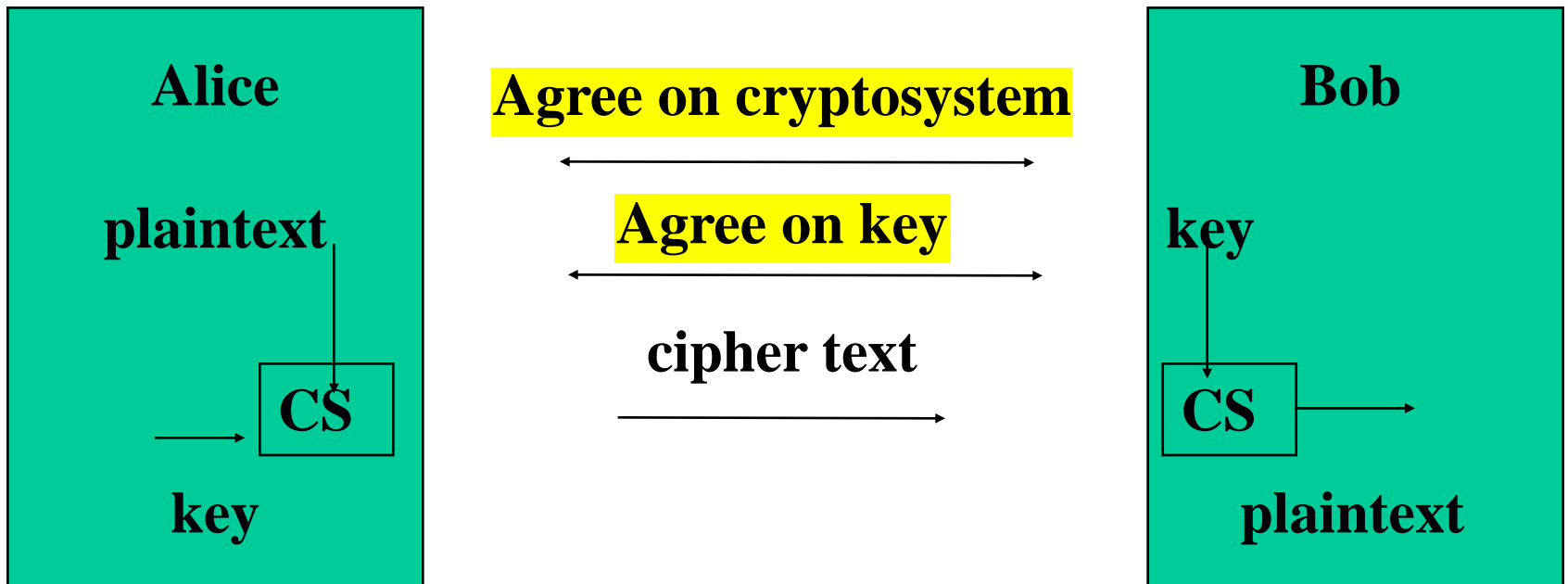
Decryption key is **private**

One key locks, the other unlocks



Symmetric Key Algorithms

Exchanging Messages with Symmetric Cryptography



Crypto-Attacks

Table 2.2 Average Time Required for Exhaustive Key Search

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

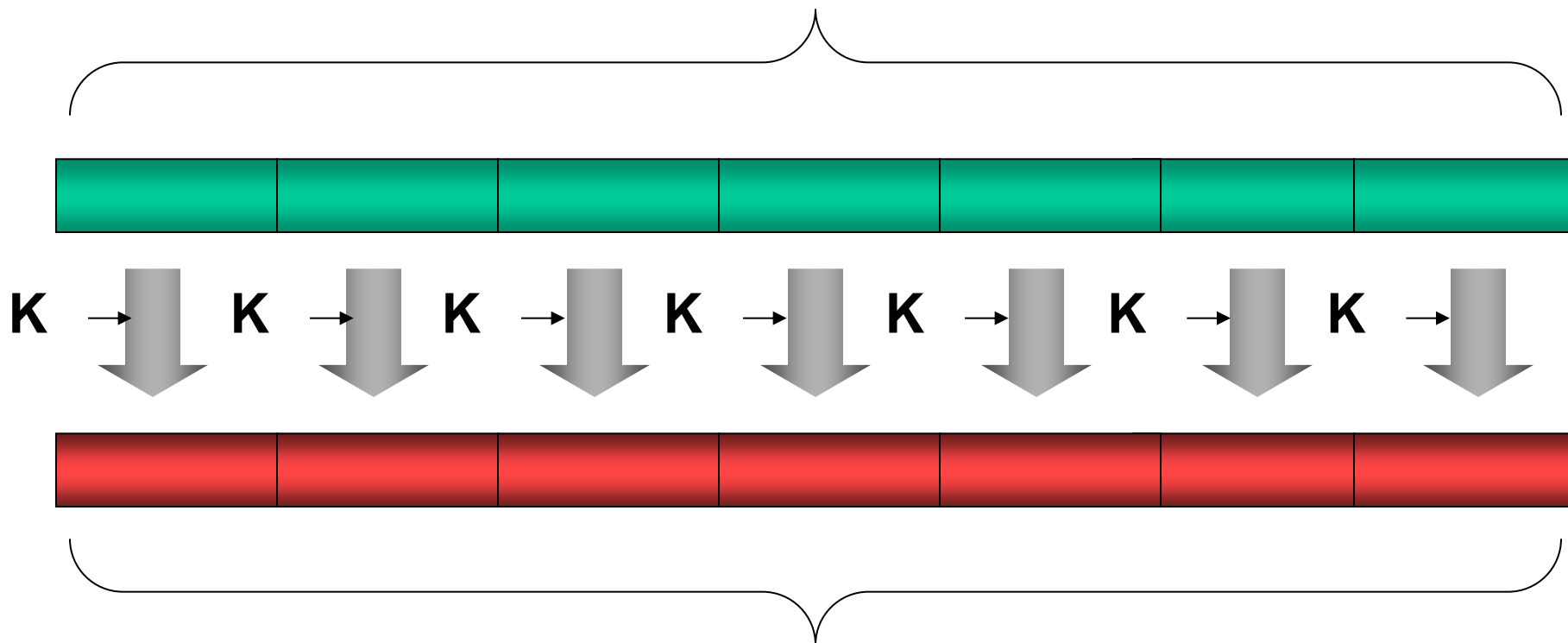
- اندازه متعارف قطعات ۶۴، ۱۲۸ یا ۲۵۶ بیت

- رمزهای پی در پی یا دنباله ای (Stream Cipher)

- پردازش پیغام ها بصورت پیوسته (بدون تقطیع)

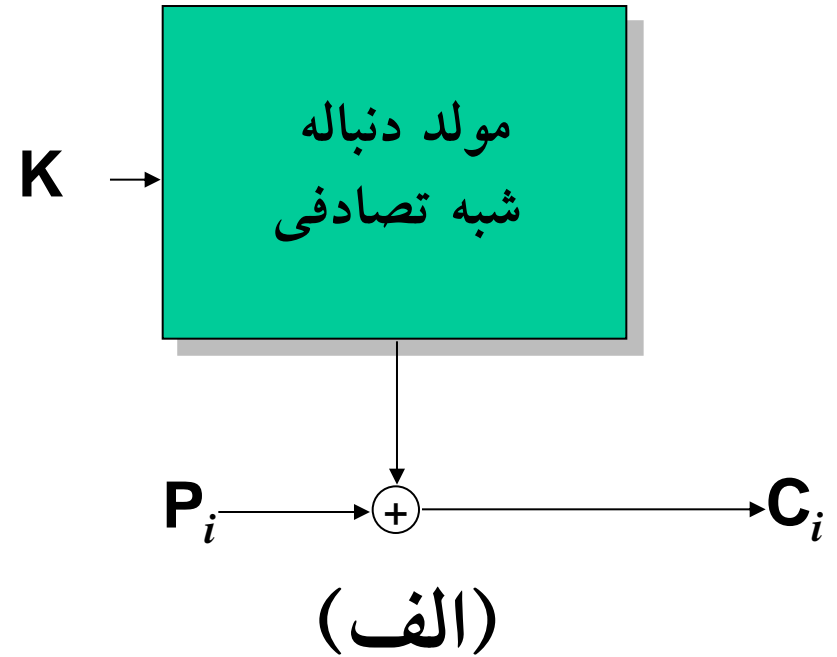
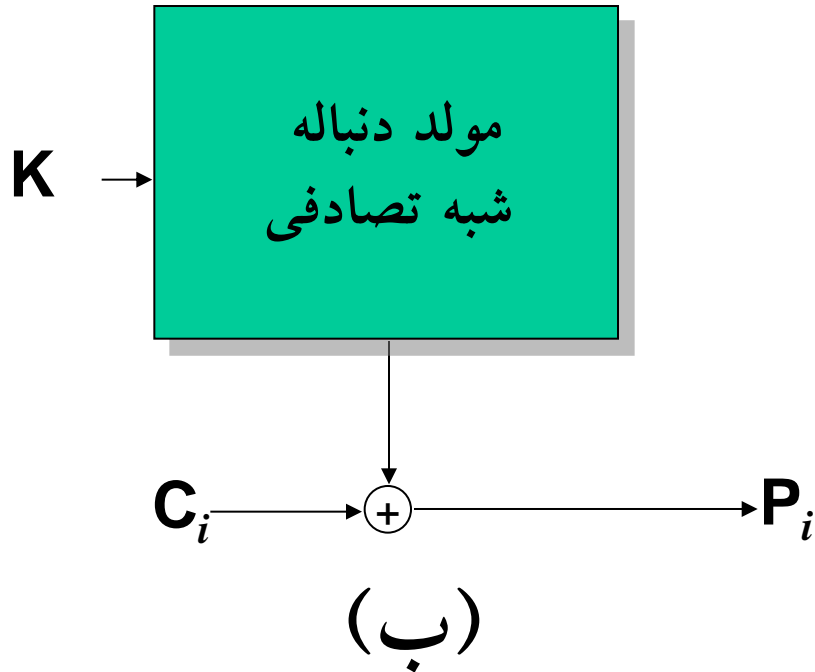
رمز قطعه ای

متن واضح (تقسیم شده به قطعات)



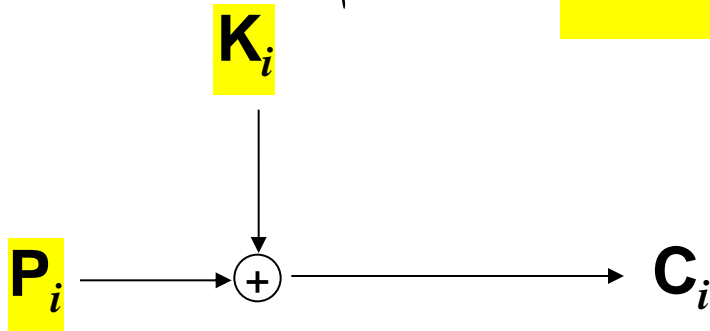
قطعات خروجی

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 رمز شده 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

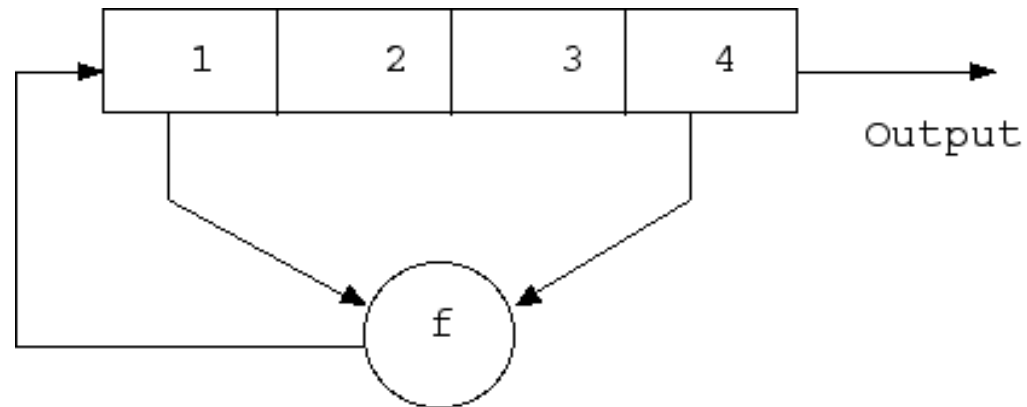
چند الگوریتم نمونه:

-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 رمز شده 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**

- جایگزینی یک سمبل با سمبل دیگر

- ممکن است هم طول نباشند

- **جابگشت Permutation**

- ترتیب قرار گرفتن حروف/بیتها در متن اصلی جابجا می شود

استانداردهای رمزهای قطعه ای آمریکا :

- رمزهای قطعه ای استاندارد

- استاندارد رمزگذاری داده **DES**

- استاندارد رمزگذاری پیشرفته **AES**

- تحت نظارت

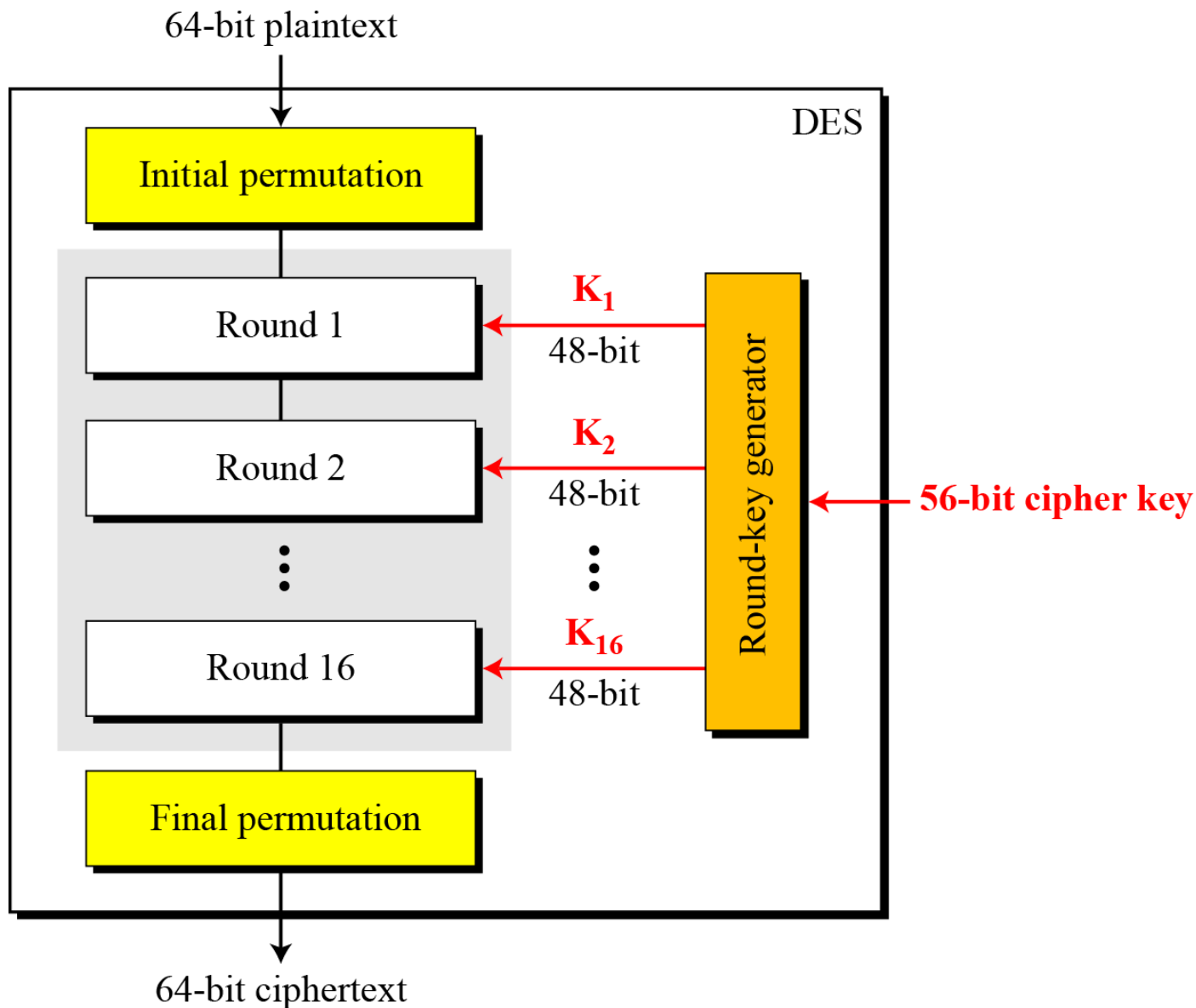
National Institute of Science and Technology (NIST)

استاندارد رمزگذاری داده DES

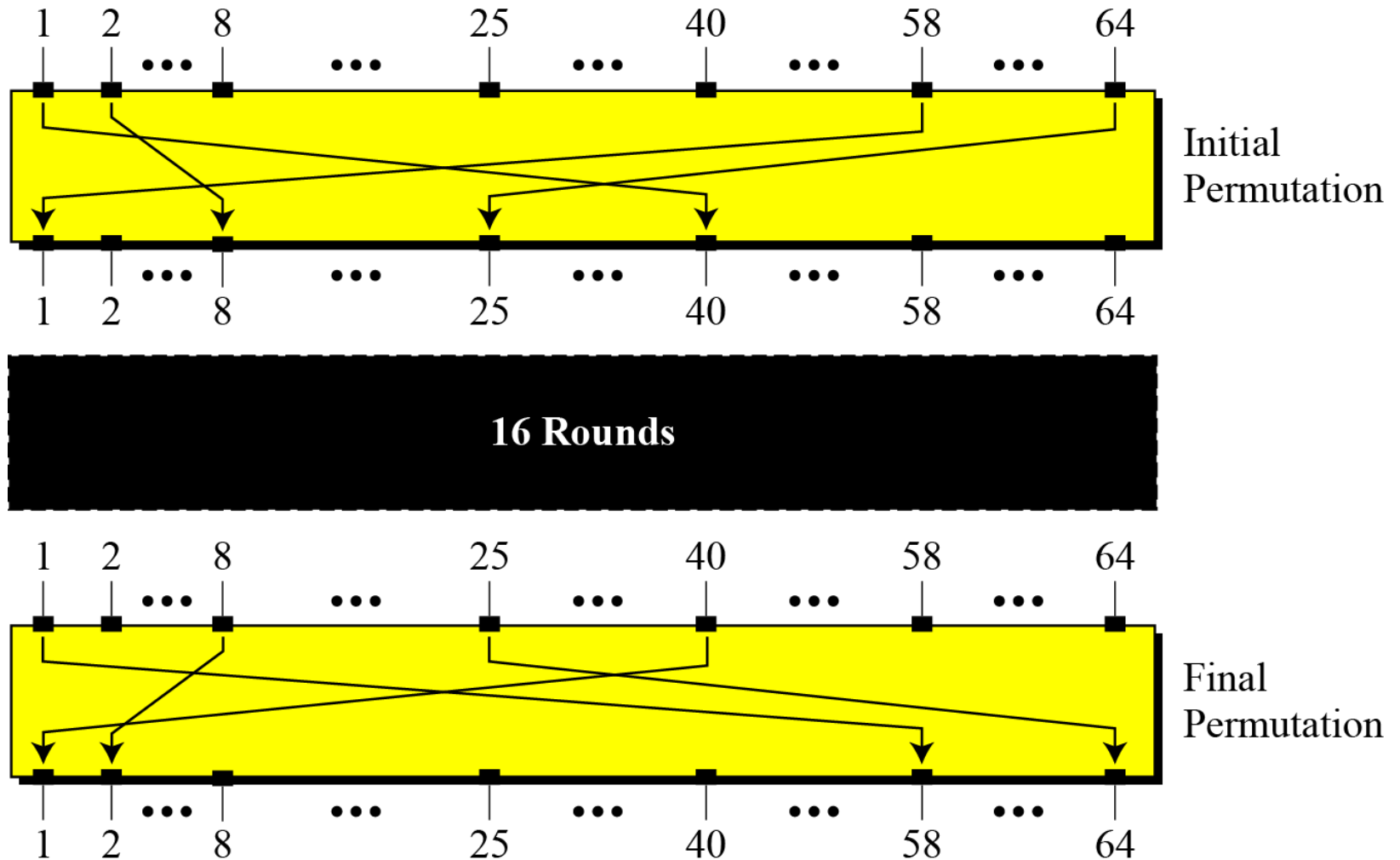
• مرور

- در سال ۱۹۷۴ توسط IBM تولید شد
- پس از انجام تغییراتی توسط NSA (National Security Agency)، در سال ۱۹۷۶ NIST آن را پذیرفت.
- اساس الگوریتم ترکیبی از عملیات **جانشینی و جایگشتی** می باشد.
- مشخصات:
 - طول کلید ۵۶ بیت
 - طول قالبهای ورودی و خروجی : ۶۴ بیت
 - تعداد دورها: ۱۶ 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**

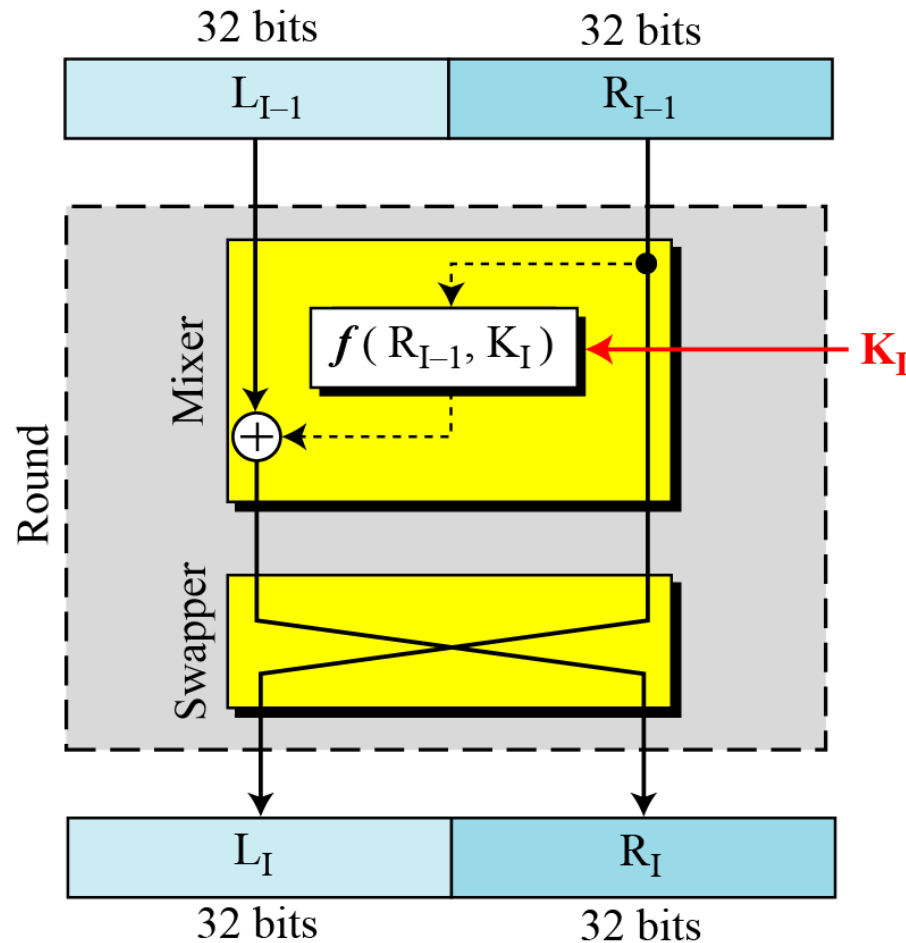


Initial and final permutation steps in DES



DES uses 16 rounds.

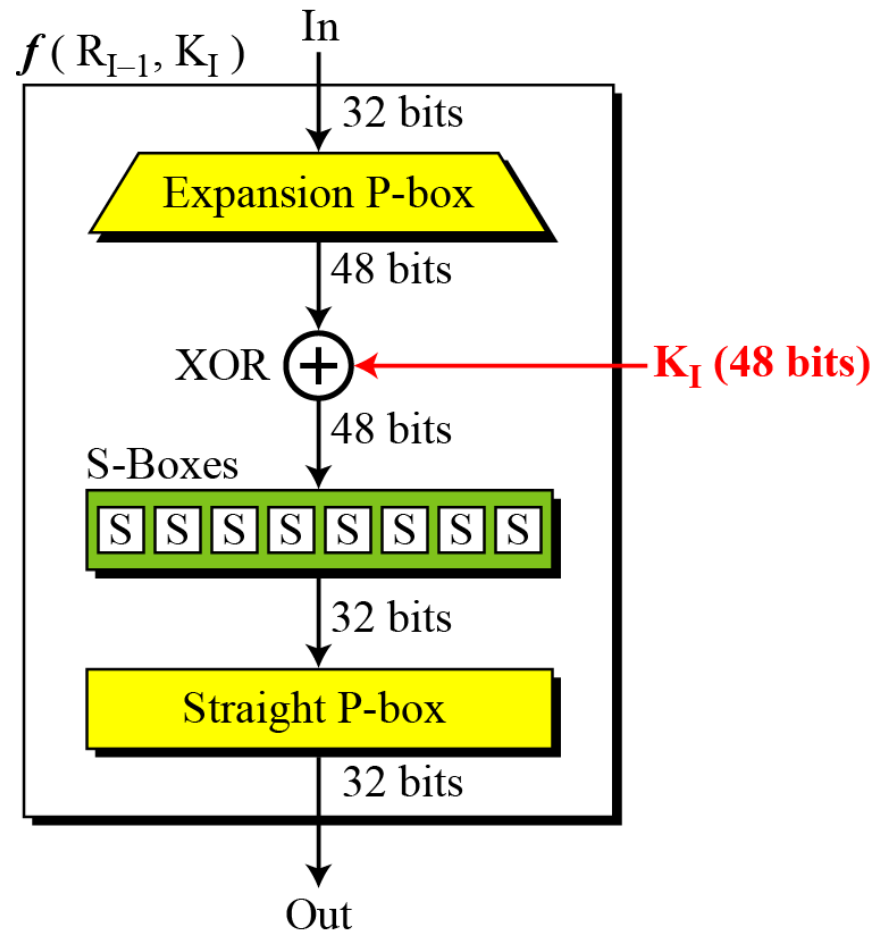
*A round in DES
(encryption site)*



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.

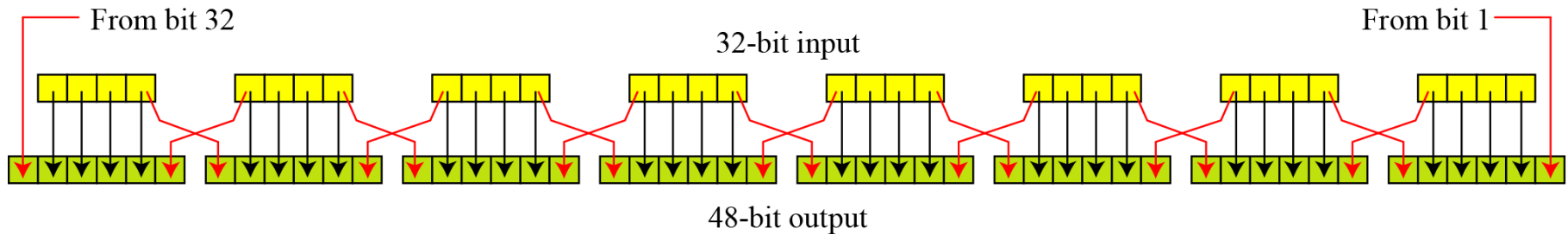
DES function



Expansion P-box

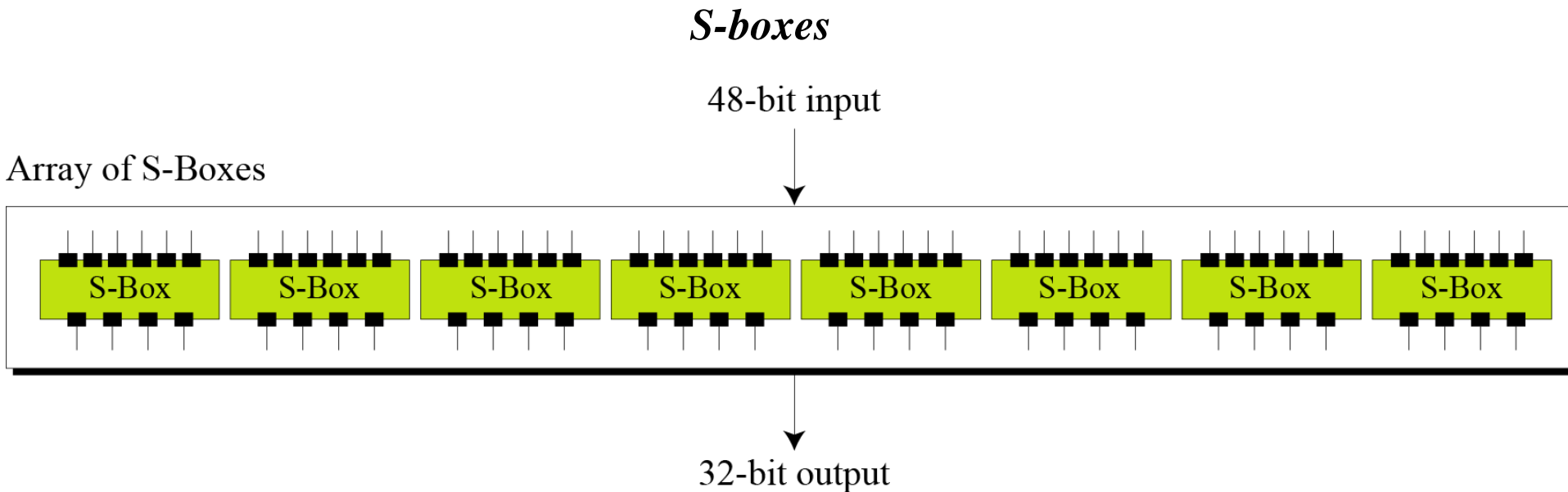
Since R_{I-1} is a 32-bit input and K_I is a 48-bit key, we first need to expand R_{I-1} to 48 bits.

Expansion permutation

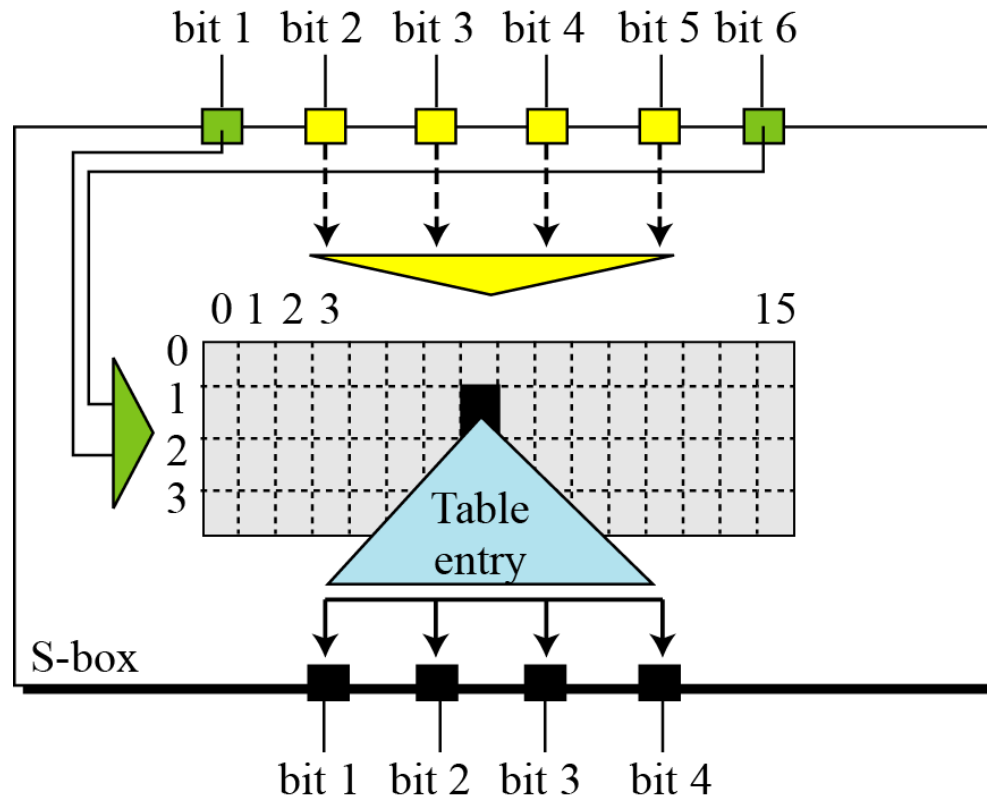


S-Boxes

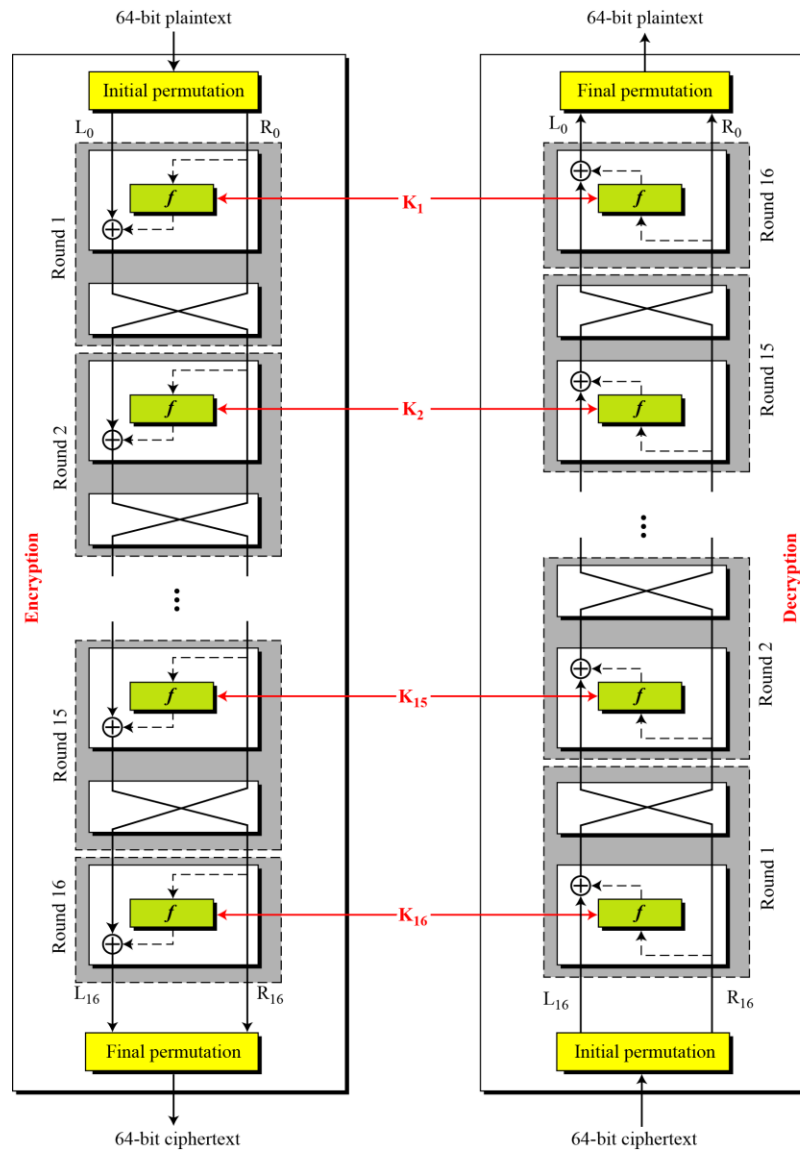
*The S-boxes do the real mixing (**confusion**). DES uses **8 S-boxes**, each with a **6-bit input** and a **4-bit output**.*



S-box rule



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

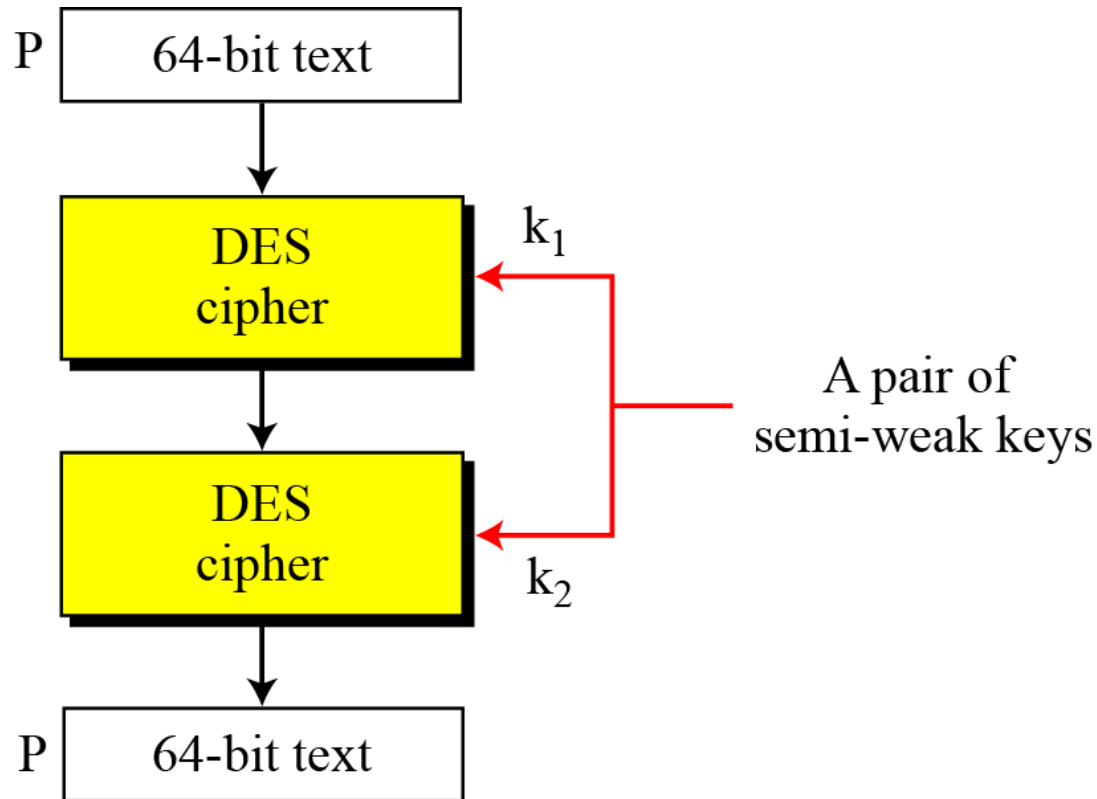
- راه حل :

- استفاده از الگوریتم های رمزنگاری دیگر

- پیچیده کردن الگوریتم DES از طریق اضافه کردن مراحل رمزنگاری و افزایش طول کلید

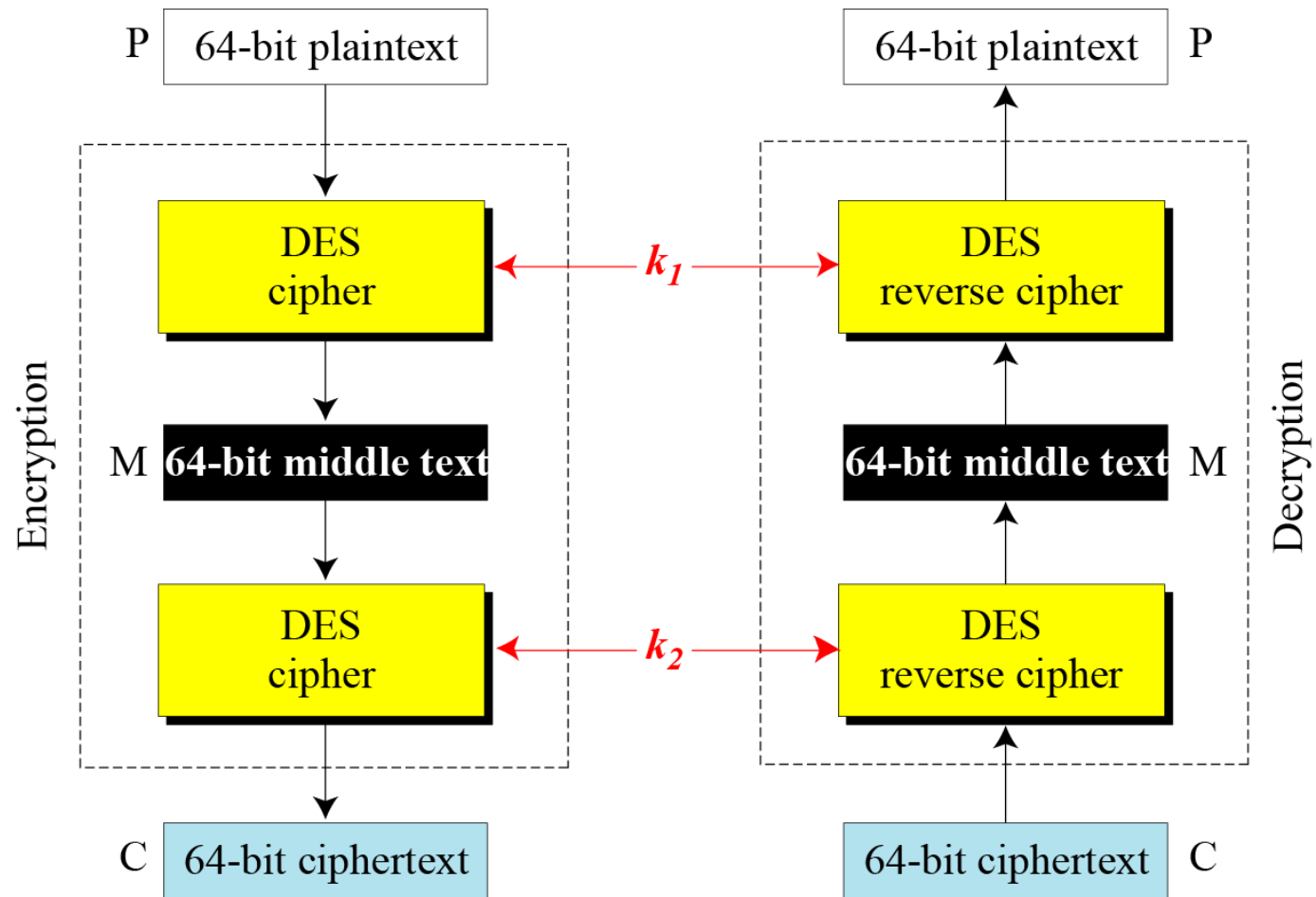
2DES

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}).*



Tables for meet-in-the-middle attack

$$M = E_{k_1}(P)$$

M	k_1
●	

$$M = D_{k_2}(C)$$

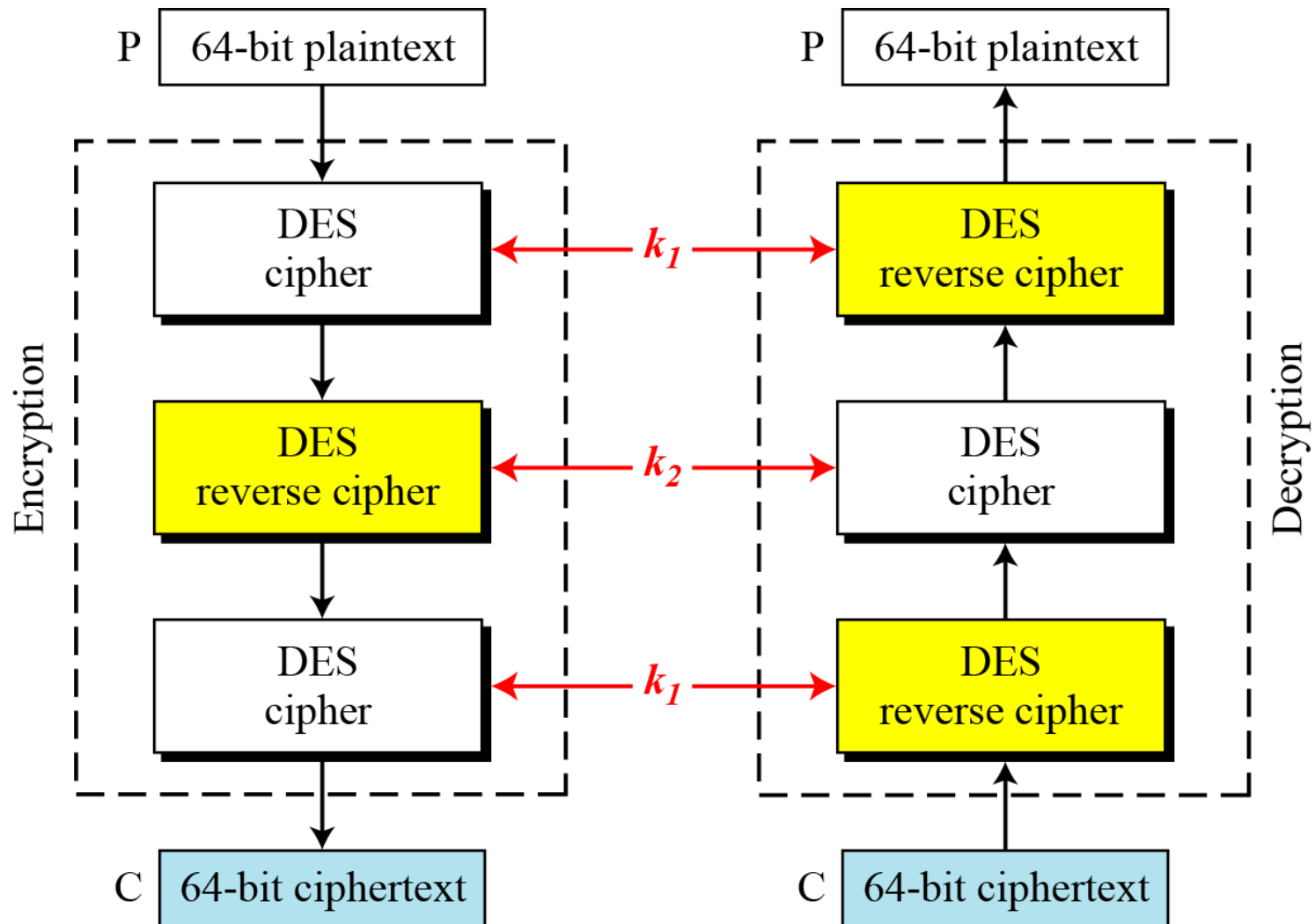
M	k_2
●	

Find equal M's and record
corresponding k_1 and k_2

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 رایندهال (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

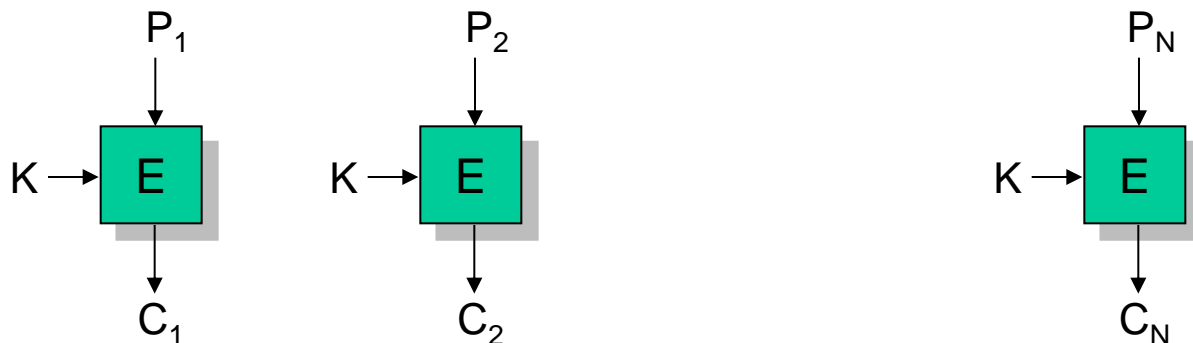
- معماری لایه ای امنیت
- اصول الگوریتمهای رمزنگاری
- انواع الگوریتمهای رمز متقارن (کلید پنهان)
- الگوریتمهای رمزنگاری قالبی
- نحوه های بکارگیری رمزهای قطعه ای

نحوه های بکارگیری رمزهای قطعه ای

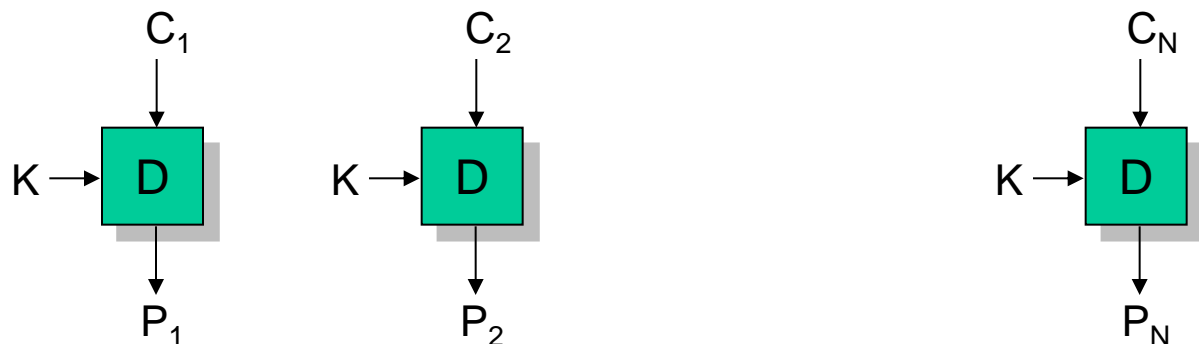
- **ECB: Electronic Code Book**
- **CBC: Cipher Block Chaining**
- **CFB: Cipher Feed Back**
- **OFB: Output Feed Back**
- **CTR: CounTeR mode**

نحوه بکارگیری ECB

- رمز نگاری:



- رمز گشایی:

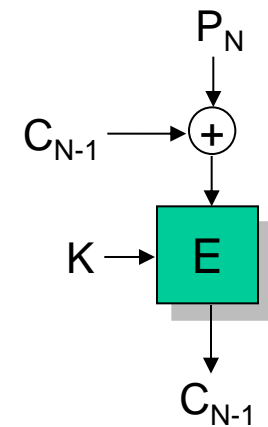
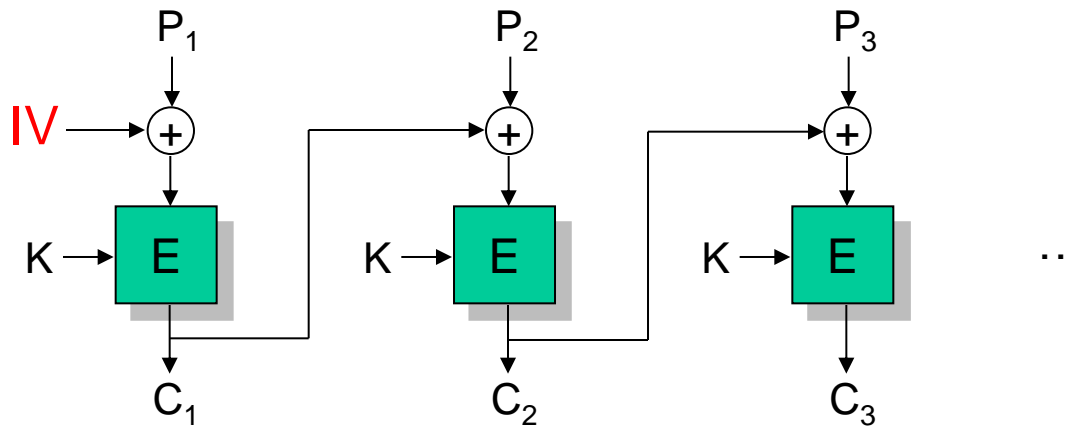


- اشکال اساسی: هر متن واضح به ازاء کلید ثابت همیشه به یک متن رمز شده نگاشته میشود.

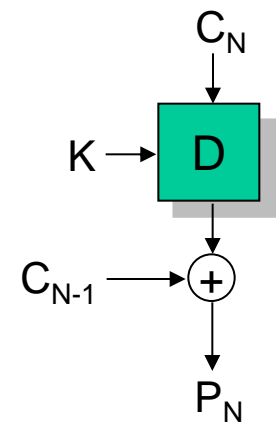
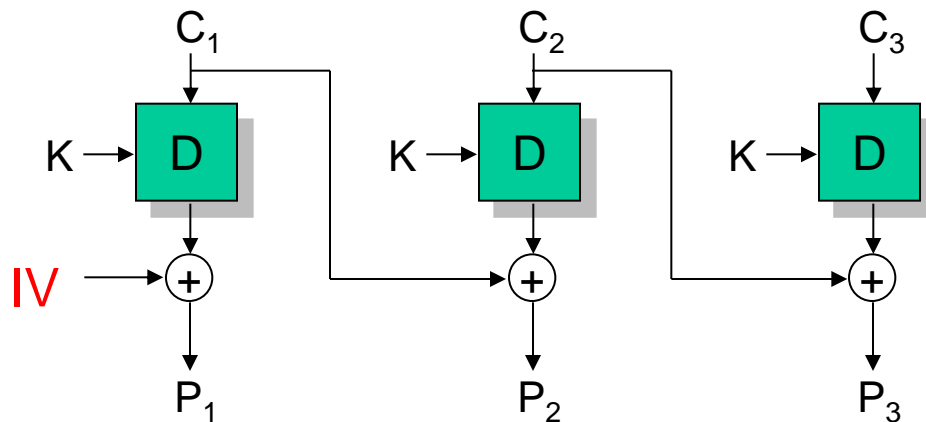
– دشمن میتواند دریابد که پیامهای یکسان ارسال شده اند.

نحوه بکارگیری CBC

- رمز نگاری:



- رمز گشایی:



مد کاری CBC

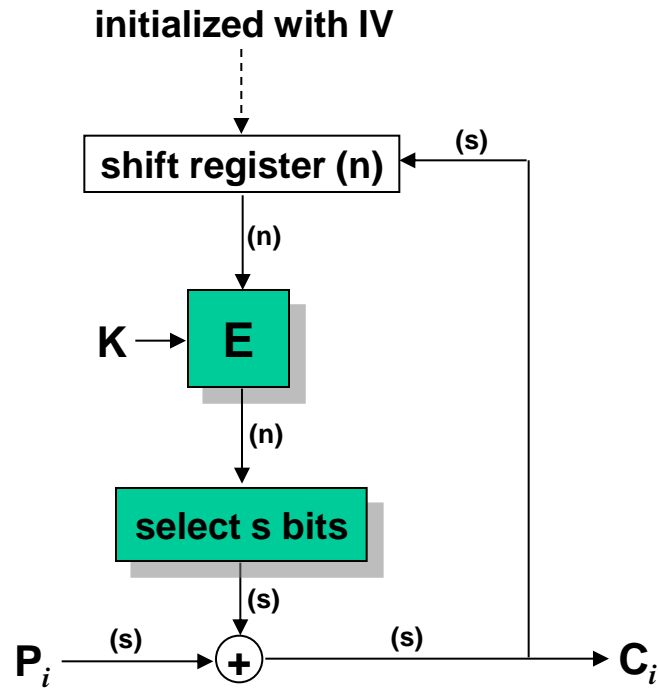
- این مد از يك مقدار دهی اولیه تصادفی (IV) بهره می گیرد
- مقدار IV در هر بار رمزگذاری به صورت تصادفی تغییر می کند
- بهتر است IV نیز رمز شده ارسال گردد
- هر متن آشکار به ازاء کلید ثابت هر بار به يك متن رمز شده متفاوت نگاشته می شود

نحوه بکارگیری CBC

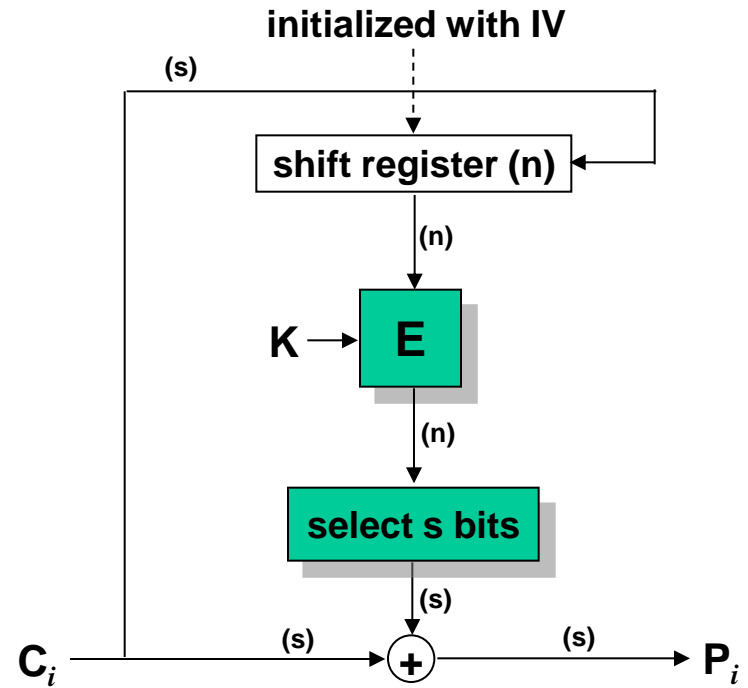
- ملزومات امنیتی:
 - IV باید کاملاً غیر قابل پیش بینی و غیر قابل دستکاری باشد
- رمزنگاری:
 - عملیات رمزنگاری قابل موازی سازی نیست.
 - مقدار IV و متن واضح باید در دسترس باشند.
- رمزگشایی:
 - عملیات رمزگشایی قابل موازی سازی است.
 - مقدار IV و متن رمز شده باید در دسترس باشند.
- طول پیام:
 - در برخی موارد 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

• رمز نگاری

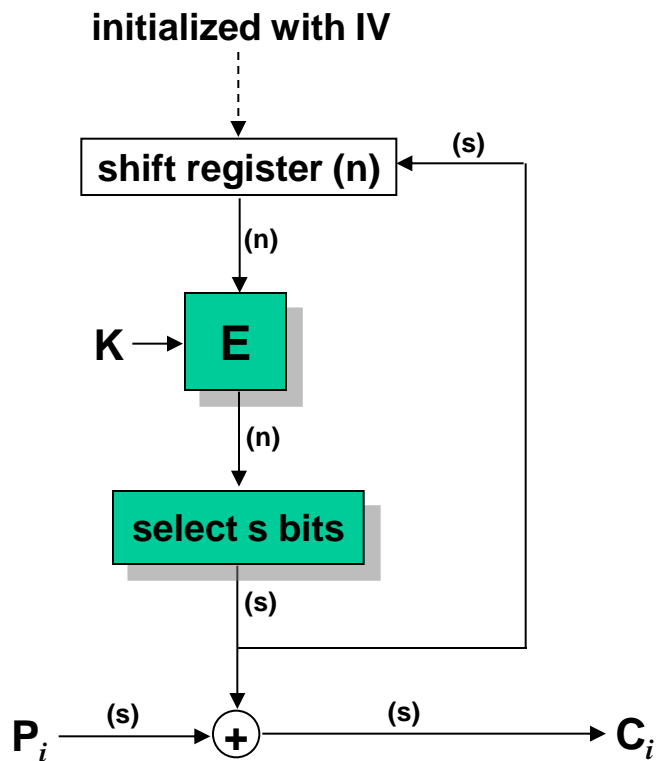


• رمز گشایی

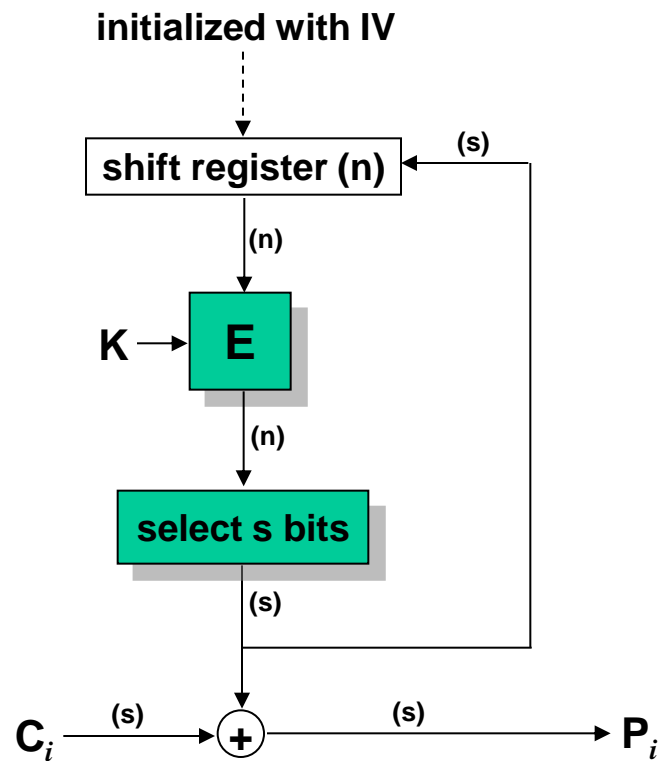


نحوه بکارگیری OFB

• رمز نگاری



• رمز گشایی

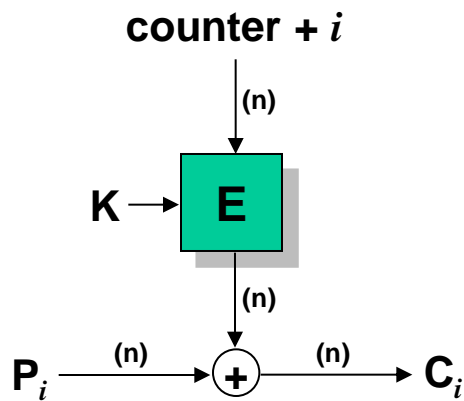


مقایسه OFB و CFB

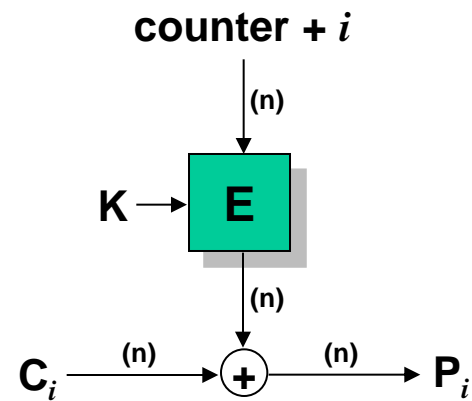
- موارد استفاده OFB و CFB
 - رمز جریانی
 - کاربردهای بلادرنگ
- عیب CFB : انتشار خطای انتقال
 - OFB این عیب را برطرف می کند

نحوه بکارگیری CTR

• رمز نگاری



• رمز گشایی



مقایسه کاربرد انواع مدهای کاری

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