



یاد‌الامن والامان

امنیت داده و شبکه

مفاهیم رمز و رمزگاری متقاضی

مرتضی امینی - سیدمهدی خرازی

نیمسال اول ۱۴۰۴-۱۴۰۳



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای رمزنگاری



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای رمزنگاری



تعریف اولیه

□ **Plaintext:** the original message

□ متن آشکار: پیام اصلی رمز نشده

□ **Ciphertext:** the coded message

□ متن رمز: پیام رمز شده

□ **Cipher:** algorithm for transforming plaintext to ciphertext

□ رمز: الگوریتم تبدیل متن آشکار به متن رمز

□ **Key:** info used in cipher known only to sender/receiver

□ کلید: اطلاعی که در رمز مورد استفاده قرار می‌گیرد و فقط فرستنده و/یا گیرنده پیام آن را می‌دانند.



تعریف اولیه

- **Encipher (encrypt):** converting plaintext to ciphertext
 - رمزگذاری: تبدیل متن آشکار به متن رمز
- **Decipher (decrypt):** recovering plaintext from ciphertext
 - رمزگشایی: استخراج متن آشکار از متن رمز



تعریف اولیه

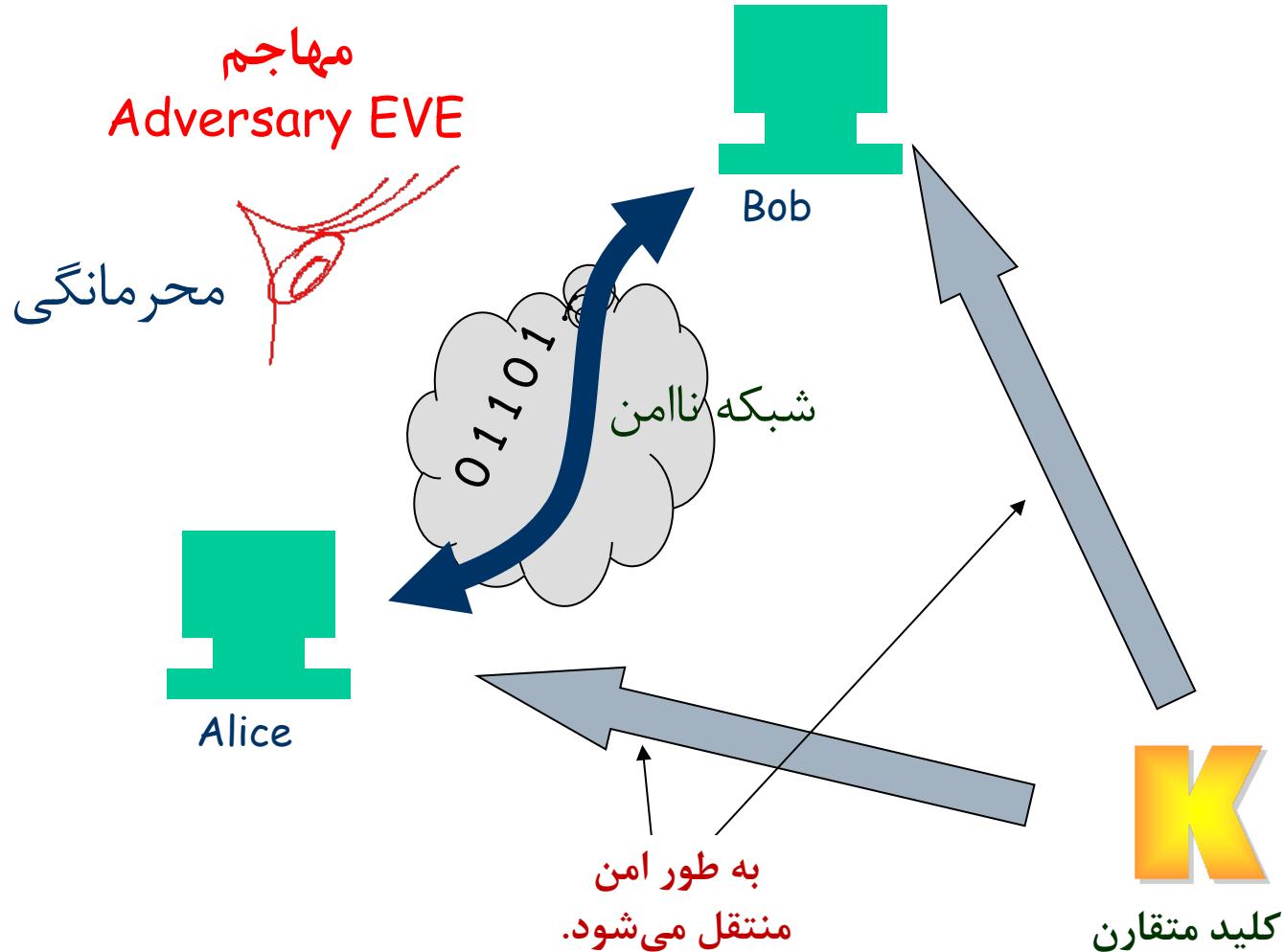
- **Cryptography:** study of encryption principles/methods
رمزنویسی: علم اصول و روش‌های رمزگذاری □
- **Cryptanalysis (codebreaking):** the study of principles/methods of deciphering ciphertext *without* knowing key
تحلیل رمز: علم اصول و روش‌های رمزگشایی متن رمز بدون اطلاع از کلید □
- **Cryptology:** the field of both cryptography and cryptanalysis
رمزنگاری: علم حاصل از ترکیب رمزنویسی و تحلیل رمز □



رمزنگاری متقارن (Symmetric)

- معادل با رمزنگاری معمولی / رمزنگاری کلید خصوصی / رمزنگاری تک کلیدی
- فرستنده و گیرنده از یک کلید مشترک استفاده می‌کنند.
- تمام رمزنگاری‌های کلاسیک از نوع متقارن هستند.
- تنها نوع رمزنگاری تا قبل از دهه ۷۰

مدل رمزگاری متقارن





نیازمندی‌های رمزنگاری

□ دو نیازمندی برای استفاده امن از رمزنگاری متقاضی:

- یک الگوریتم رمزنگاری قوی
- یک **کلید سری** که تنها فرستنده و گیرنده از آن آگاه هستند.

$$C = E_K(P)$$

$$P = D_K(C)$$

□ فرض بر آن است که **الگوریتم برای همه مشخص** است.

□ بنابراین نیاز به یک کانال امن برای توزیع کلید است.



ابعاد رمزنگاری

□ آعمال مورد استفاده برای رمزگذاری

- جانشینی (Substitution): جایگزینی هر عنصر با عنصری دیگر
- جایگشت (Transposition): جابجایی عناصر رمزشده

□ روش پردازش متن آشکار

- **بلوکی (قالبی):** بلوکی از عناصر متن پردازش و رمز می‌شوند.
- **جريانی:** عناصر متن به طور پیوسته به ورودی داده شده و در هر لحظه یک عنصر رمز شده خارج می‌شود.



حملات تحلیل رمزنگاری

□ هدف از حمله:

- استخراج کلید
- استخراج متن آشکار از متن رمزشده

□ نحوه حمله:

- بررسی خصوصیات الگوریتم رمز
- بررسی مجموعه‌ای از متن‌های آشکار و رمزشده آنها



انواع حملات تحلیل رمز نگاری

نوع حمله	اطلاعات در اختیار تحلیلگر رمز
ciphertext only	<ul style="list-style-type: none">• الگوریتم رمز• متن رمز
known plaintext	<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• یک یا چند جفت متن آشکار و رمز شده آن
chosen plaintext	<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• متن آشکار انتخاب شده توسط تحلیلگر و متن رمز معادل آن
chosen ciphertext	<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• متن رمز انتخاب شده توسط تحلیلگر و متن آشکار حاصل از رمزگشایی آن
chosen text	<ul style="list-style-type: none">• الگوریتم رمز• متن رمز• متن آشکار انتخاب شده توسط تحلیلگر و متن رمز معادل آن• متن رمز انتخاب شده توسط تحلیلگر و متن آشکار حاصل از رمزگشایی آن



جستجوی تمام حالات (Brute Force Search)

ابتداً ترین حمله

فرض بر این است که متن آشکار قابل شناسایی است.

DES →
AES →
3DES →
Substitution code →

Key size (bits)	Number of alternative keys	Time required at 1 decryption / μs	Time required at 10^6 decryption / 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
AES →	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
3DES →	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
Substitution code →	$26! = 4 \times 10^{26}$ characters (permutation)	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years



امنیت مطلق - امنیت محاسباتی

□ امنیت مطلق

- مستقل از قدرت محاسباتی در دسترس، متن رمز شده اطلاع کافی برای تعیین قطعی متن آشکار یا کلید ارائه نکند (و بنابراین الگوریتم رمز مستقل از مدت زمانی که مهاجم در اختیار دارد قابل شکستن نباشد).

□ امنیت محاسباتی

- با داشتن منابع محاسباتی **محدود** (مانند زمان)، رمز قابل شکستن نباشد.



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای رمزنگاری



رمزهای کلاسیک

مبتنی بر دو روش اصلی:

جاگشت

- جابجایی بین حروف متن اصلی
- شکست رمز سخت تر.

جانشینی

- جانشینی یک حرف با حرف دیگر
- تک الفبایی
- چند الفبایی
- حملات شناخته شده با استفاده

از توزیع فرکانس تکرار حروف



ایده‌های تحلیل رمز کلاسیک

□ حملات Brute Force

■ جستجوی همه حالات (کلیدهای ممکن)

□ حملات تحلیل فرکانسی

■ فراوانی حروف (a b c d e f ...)

■ فراوانی ترکیبات حروف (th, nt)

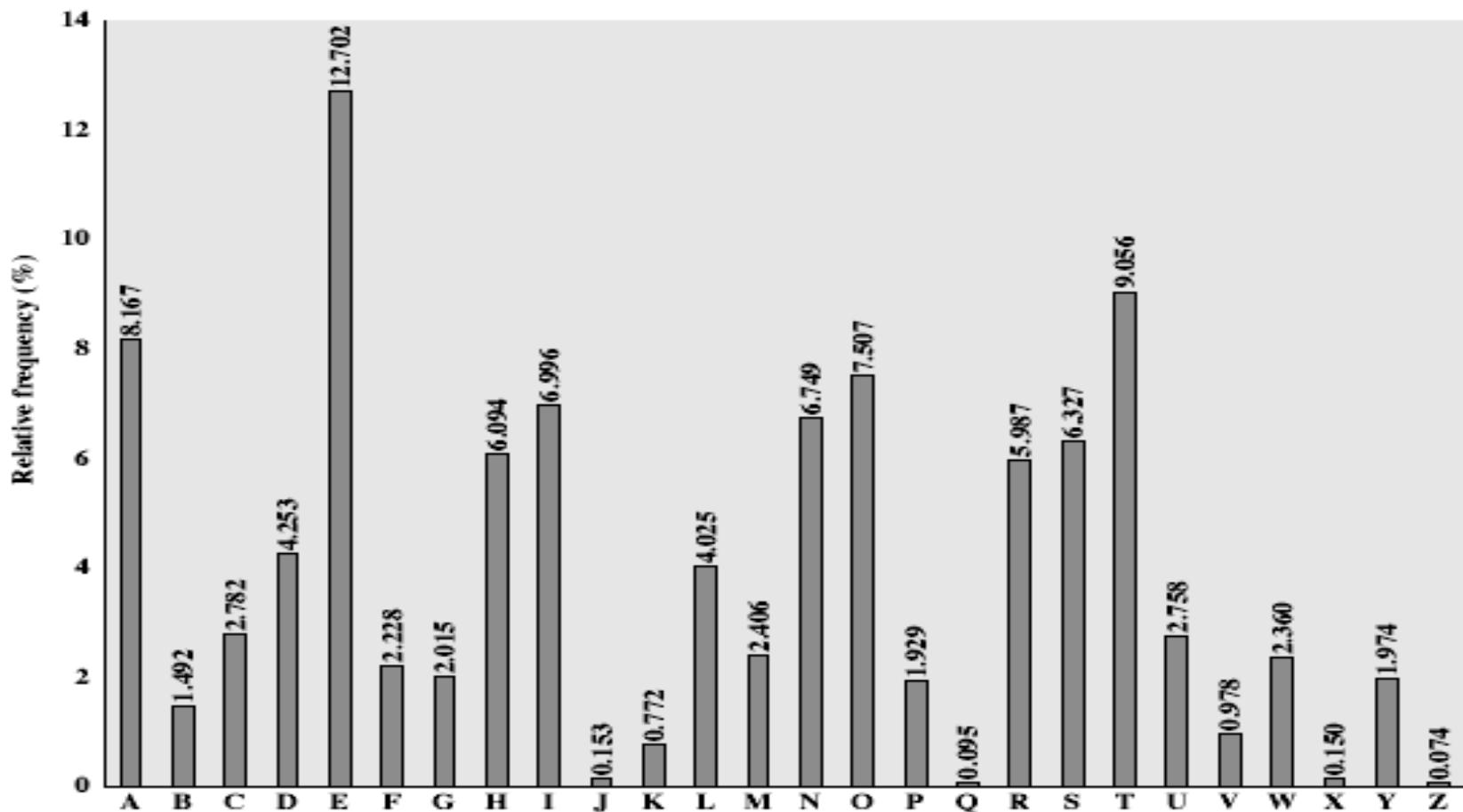
■ حروف ابتدا و انتهای کلمه (th___, ___nt, ___gh)

■ نظم موجود در گرامر زبان



تحلیل فرکانسی

فراوانی حروف انگلیسی در متن





رمز جانشینی تک الفبایی

• هر حرف با حرف دیگری در الفبا جایگزین می شود.

Plain: a b c d e f g h i j k l m n o p q r s t u v w x y z

Cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

نمونه ها:

- Playfair Cipher
- Hill Cipher

(جهت مطالعه این دو الگوریتم به کتاب مرجع درس مراجعه شود)



تحليل رمز جانشينی تک الفبايی

□ حمله Brute-Force

■ تعداد کلیدهای ممکن $26^{1026} = 4 \times 10^{26!}$ ← اجرای حمله غیرممکن

□ امكان حمله فرکانسي

■ با مقایسه نمودار فراوانی حروف در متن رمز شده با نمودار استاندارد فراوانی حروف، می‌توان تناظر احتمالی حروف را پیدا کرد.



رمز جانشینی چندالفایی

□ خصوصیات

- استفاده از مجموعه‌ای از جانشینی‌های تک الفبایی مختلف بصورت متوالی.
- کلید نمایانگر این است که چه ترتیبی از قواعد جانشینی باید به کار برده شود.
- همچنان می‌توان از فرکانس یا توزیع حروف برای شکست رمز استفاده کرد.

□ نمونه‌ها:

- جانشینی **Vigenere** (جهت مطالعه به کتاب مرجع درس مراجعه شود)



مثال رمز چندالفایی: جانشینی ۲۱۳

کلید



۲

Plain: send another catapult

abcdefghijklmnopqrstuvwxyz

حروف به ترتیب به
رمزکننده‌های تک الفایی برای
رمز شدن داده می‌شوند.

۱

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

۳

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

Cipher: ufqf bqqukgs fcudrvov



ماشینهای روتور (Rotor Machines)

- ماشین روتور یک پیاده‌سازی الکترونیکی-مکانیکی از رمزچندالفبایی محسوب می‌شود.
- در این روش، داده‌ها از داخل تعدادی سیلندر که در مقابل هم قرار گرفته‌اند، عبور می‌کنند. هر سیلندر یک رمز تک الفبایی را انجام می‌دهد.
- به ازای هر حرف از ورودی، سیلندر اول به اندازه یک حرف می‌چرخد با یک دور گردش کامل هر روتور، روتور بعدی به اندازه یک حرف جابجا می‌شود.
- دوره تناوب ماشین روتور با افزایش تعداد روتورها افزایش می‌یابد (2^n).
- آلمان‌ها اعتقاد داشتند که ماشین روتور طراحی شده توسط آنها (با نام Enigma) غیرقابل شکست است، ولی متفقین توانستند رمز آن را کشف کنند و بسیاری از اطلاعات سری آنها را فاش کنند.

Direction of motion

Direction of motion

→ A	24	21
→ B	25	3
→ C	26	15
D	1	1
E	2	19
F	3	10
G	4	14
H	5	26
I	6	20
J	7	8
K	8	16
L	9	7
M	10	22
N	11	4
O	12	11
P	13	5
Q	14	17
R	15	9
S	16	12
T	17	23
U	18	18
V	19	2
W	20	25
X	21	6
Y	22	24
Z	23	13

Fast rotor

Medium rotor

Slow rotor

(a) Initial setting

A

B →

C

D

E →

F

G

H

I →

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

A

B →

C

D

E →

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

A

B →

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

A

B →

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

A

B →

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

A

B →

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z

A

B →

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

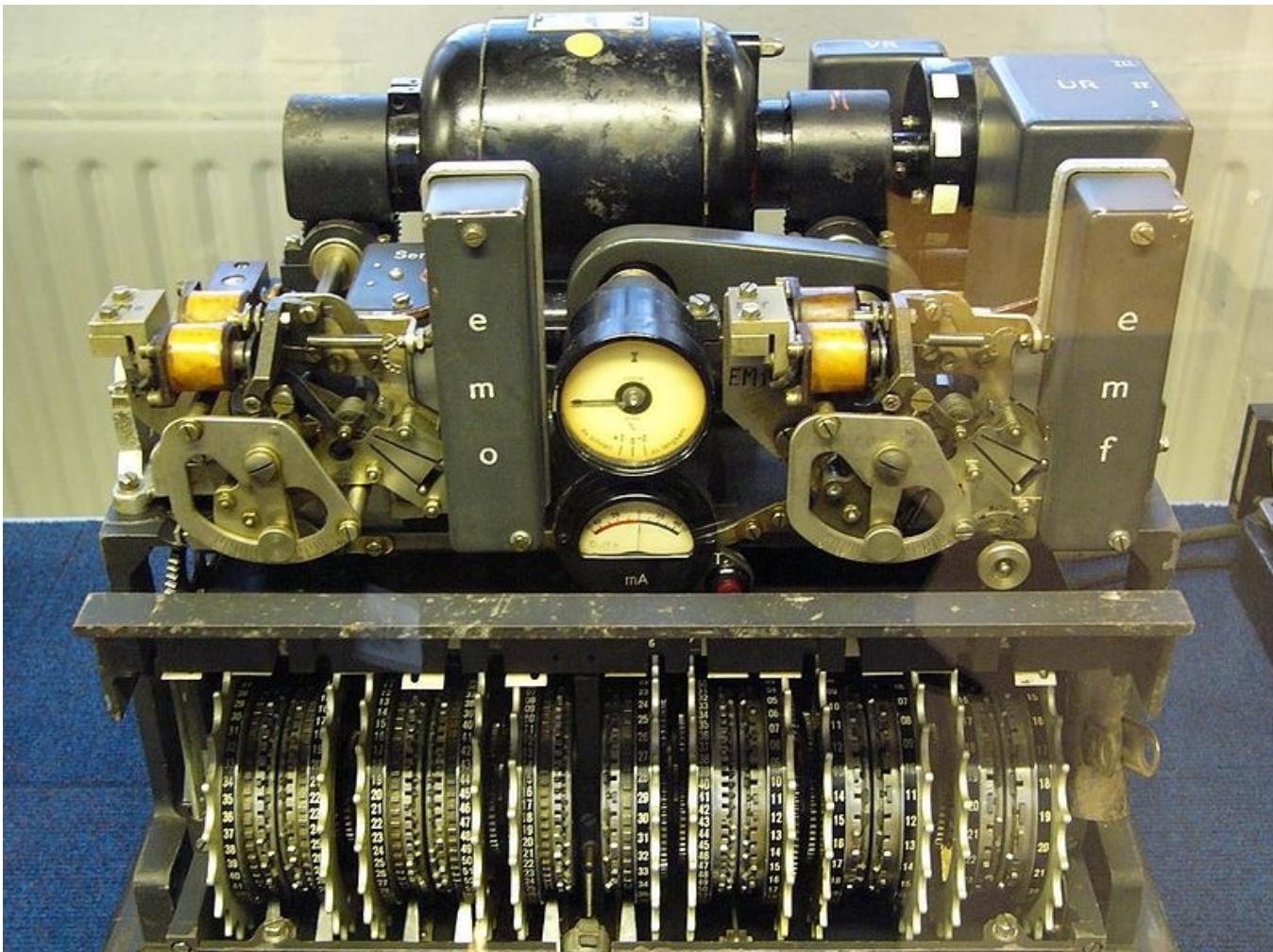
Y

Z

(a) Initial setting

(b) Setting after one keystroke

ماشینهای روتور





رمز One-Time Pad

- اگر از کلید **کاملاً تصادفی** به اندازه متن آشکار استفاده شود، رمز حاصله امن خواهد بود.
- این نوع کلید Pad نام دارد.
- در One-Time Pad از هر کلید فقط یک بار می‌شود استفاده کرد.

$$C_i = P_i \oplus K_i$$

□ رمزگذاری:

\oplus means XOR

$$P_i = C_i \oplus K_i$$

□ رمزگشایی:



تحلیل رمز One-Time Pad

- این رمز، از **امنیت مطلق** برخوردار است، چرا که هیچ رابطه‌ای بین متن آشکار و متن رمز شده وجود ندارد.
- یعنی می‌توان بین هر متن آشکار و هر متن رمز شده، یک کلید رمز متناظر پیدا کرد.
- مشکل این روش:
 - تولید کلید تصادفی به تعداد زیاد
 - توزیع کلید (نیاز به ارسال کلید برای هر متن به اندازه خود آن)



رمز جایگشتی

- جابجایی حروف در متن اصلی بدون تغییر حروف الفبا
- امکان استفاده ترکیبی از آن با رمز جانشینی
- ایده اصلی مورداستفاده در رمزنگاری متقارن مدرن



رمز جایگشت ستونی

- متن را بصورت سطري بنويسيم و بصورت ستوني بخوانيم.
- **کليد:** تعداد ستونها (در اينجا 5)

43125

SEND*
ANOTH
ER*SE
T****

SAETENR*NO**DTS**HE*

- **کليد:** ترتيب نوشتن ستونها (در اينجا 43125)

NO**DTS*ENR*SAET*HE*

- مى توان برای امنیت بیشتر چند بار جایگشت را انجام داد.



تحلیل رمز جایگشتی

- با تحلیل رمز جایگشتی مشخص می‌شود که:
- فراوانی حروف در متن رمزشده تفاوتی با فراوانی متن اصلی ندارد.
- تحلیلگر نمی‌تواند از نمودارهای فراوانی (اجرایی حمله تحلیل فرکانسی) استفاده کند.



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای رمزنگاری



الگوریتم‌های مدرن رمز متقارن

□ رمزهای متقارن را می‌توان با دو روش عمدی تولید کرد:

■ رمزهای بلوکی یا قالبی (Block Cipher)

- پردازش پیغام‌ها بصورت قطعه به قطعه
- اندازه متعارف مورد استفاده برای قطعات ۶۴، ۱۲۸ یا ۲۵۶ بیتی است.

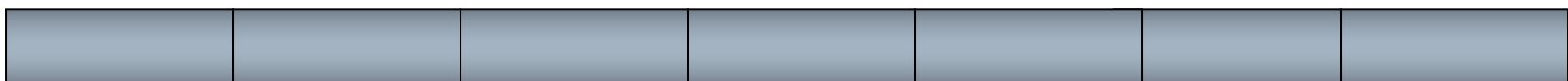
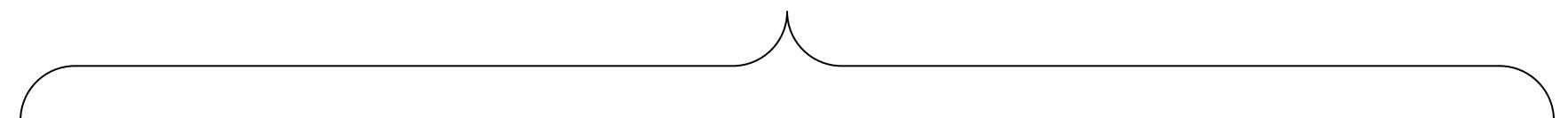
■ رمزهای جریانی (Stream Cipher)

- پردازش پیغام‌ها بصورت پیوسته



رمزهای بلوکی یا قالبی

متن آشکار (تقسیم شده به بلوک‌ها یا قطعات)



بلوک‌های خروجی



اصول رمزمایی بلوکی

- اغلب مبتنی بر ساختار رمز فیستل هستند.
- نگاشت قطعات متن آشکار به قطعات متن رمزشده باید (برای ممکن بودن رمزگشایی) برگشتپذیر باشد.
- ایده رمز محصولی (Product Cipher): الگوریتم رمز، قطعات ورودی را در چند مرحله ساده و متوالی پردازش می‌کند. به این مراحل دور می‌گوییم.
- هر دور عموماً مبتنی بر ترکیب اعمال ساده‌ای همچون جایگزینی و جایگشت و XOR استوار است.



شانون و رمز جانشینی و جایگشت

- شانون ایده استفاده از شبکه آعمال جانشینی و جایگشت را در سال ۱۹۴۹ مطرح کرد.
- پایه رمזה‌های مدرن بر اساس این دو عمل است:
 - جانشینی (S-box)
 - جایگشت (P-box)
- این دو عمل، گمراه‌کنندگی (Confusion) و پراکندگی (Diffusion) پیام موردنظر و کلید را موجب می‌شوند.



گمراه‌کنندگی و پراکندگی

- الگوریتم‌های رمز باید خصوصیات آماری پیام اصلی (متن آشکار) را به طور کامل مخفی کنند.
- گمراه‌کنندگی (Confusion): رابطه بین متن رمزشده و کلید تا حد امکان پیچیده باشد.
- پراکندگی (Diffusion): ساختار آماری متن آشکار بر روی حجم وسیعی از متن‌های رمزشده ممکن پراکنده شود.

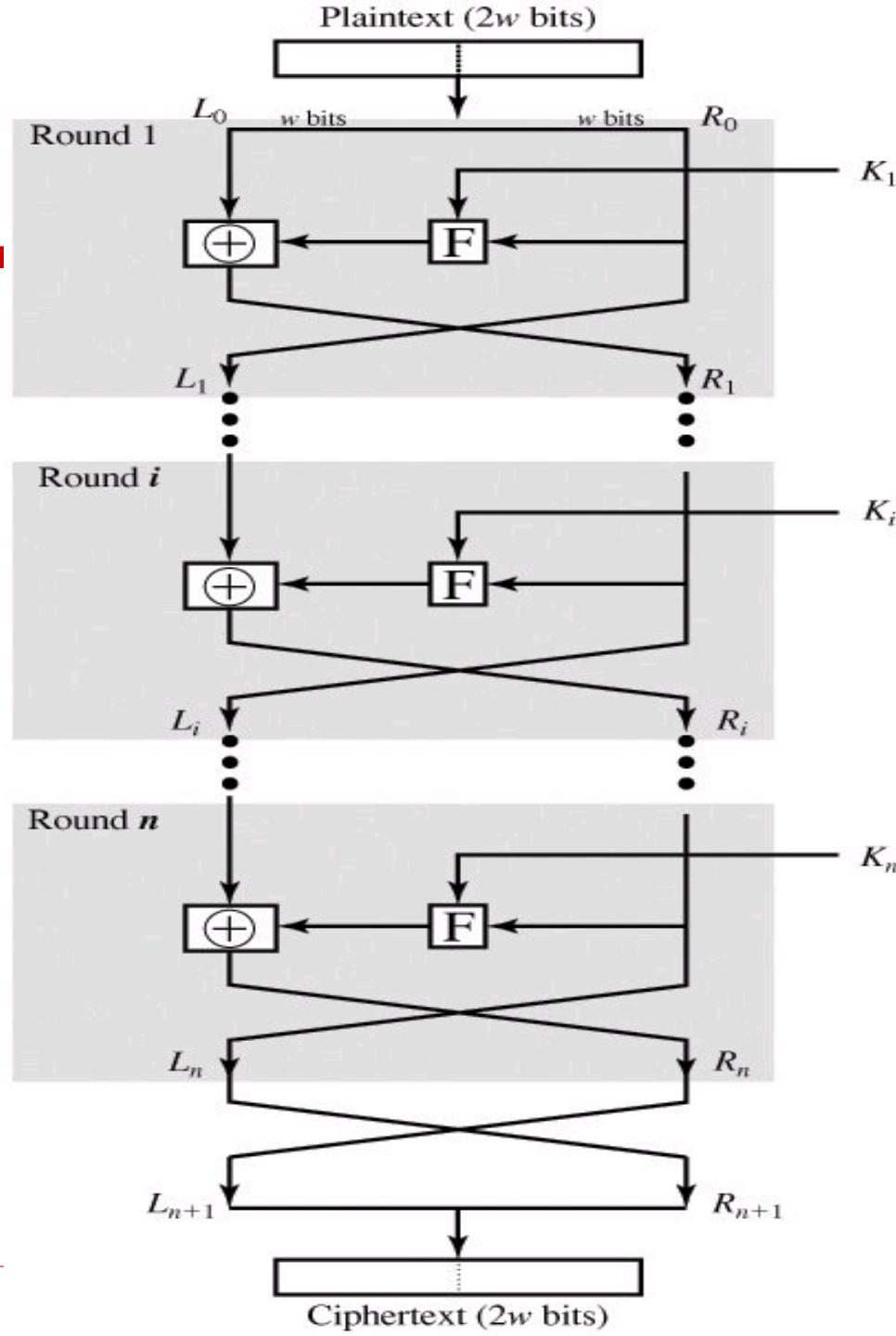


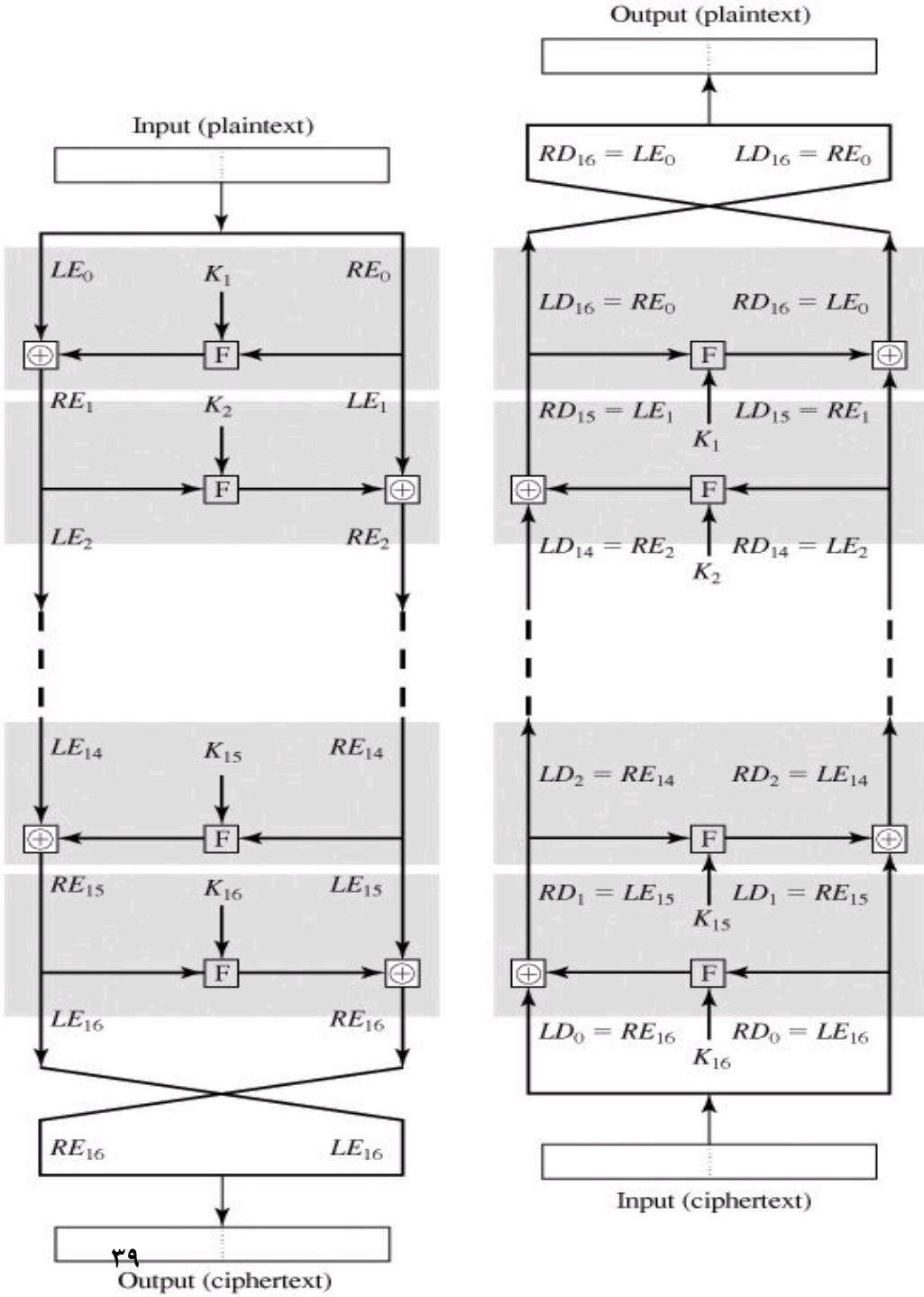
ساختار رمزهای فیستل

- معمولاً الگوریتم‌های رمزنگاری از ساختاری تبعیت می‌کنند که توسط فیستل در سال ۱۹۷۳ IBM پیشنهاد شد.
- مبتنی بر رمز محصولی برگشت‌پذیر
- مبتنی بر مفهوم شبکه جانشینی و جایگشت
- هر قطعه ورودی را به دو نیمه تقسیم می‌کند:
 - پردازش در طی چند مرحله (دور)
 - انجام جانشینی بر روی نیمه چپ
- جانشینی بر اساس تابع دور حاصل از زیرکلید هر دور و نیمه راست
- جایگشت با معاوضه دو نیمه



ساختار مرز پیشل





رمزگذاری و رمزگشایی در ساختار
رمز فیستل یکسان است.

□ نیازی به برگشت‌پذیر بودن
تابع F نیست.



ساختار رمزهای فیستل

رمزهای فیستل به انتخاب پارامترهای زیر بستگی دارند.

- طول قطعه (بلوک): ۶۴ بیت تا ۱۲۸ بیت
- طول کلید: ۶۴ بیت یا کمتر در حال حاضر کافی نیست.
- تعداد دورها: معمولاً ۱۶ دور
- الگوریتم تولید زیر کلیدها
- هر چه پیچیده‌تر باشد، تحلیل هم سخت‌تر می‌شود.
- تابع دور (F : Round Function): هر چه پیچیده‌تر تحلیل سخت‌تر
- سرعت رمزگذاری/رمزگشایی
- سادگی بررسی و درک درستی عملکرد



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای رمزنگاری



استانداردهای رمزهای بلوکی آمریکا

□ رمزهای قالبی استاندارد

■ استاندارد رمزگذاری داده **DES** (نامن و از رده خارج)

■ استاندارد رمزگذاری پیشرفته **AES** (پر کاربرد امروزی)

□ تحت نظرارت

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، در سال ۱۹۷۶ NIST آن را پذیرفت.
- اساس الگوریتم ترکیبی از عملیات جایگزینی و جایگشت است.

□ مشخصات

- طول کلید ۵۶ بیت
- طول قطعه‌های ورودی و خروجی : ۶۴ بیت
- تعداد دورها: ۱۶ دور
- الگوریتم‌های رمزگذاری و رمزگشایی عمومی هستند، ولی مبانی ریاضی و اصول طراحی آنها فاش نشد.



استاندارد رمزگذاری داده DES

قطعه ۶۴ بیتی متن آشکار



دور ۱

دور ۲

دور ۱۵

دور ۱۶

زیر کلید دور

زیر کلید دور

زیر کلید دور

زیر کلید دور

تولید زیر کلیدهای ۴۸
بیتی از کلید اصلی ۵۶
بیتی برای هر دور



کلید ۵۶ بیتی

قطعه ۶۴ بیتی متن رمزنگاری شده



DES امن نیست!

- کلید ۵۶ بیتی دارای کل فضای حالت $2^{56} = 7.2 * 10^{16}$
- حمله آزمون جامع هرچند مشکل ولی امکان‌پذیر است.
- در ژانویه ۱۹۹۹ این الگوریتم توسط آزمون 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 امن‌تر با طول کلید بیشتر نیاز داریم.
- علاوه بر این، DES طراحی شفاف و روشن ندارد.



الگوریتم 3DES و 2DES

□ مسئله:

■ آسیب‌پذیری DES در مقابل حمله آزمون جامع

□ راه حل:

■ پیچیده کردن الگوریتم DES از طریق اضافه کردن مراحل

رمزنگاری و افزایش طول کلید

■ یا استفاده از الگوریتم‌های رمزنگاری مناسب دیگر



الگوریتم 2DES

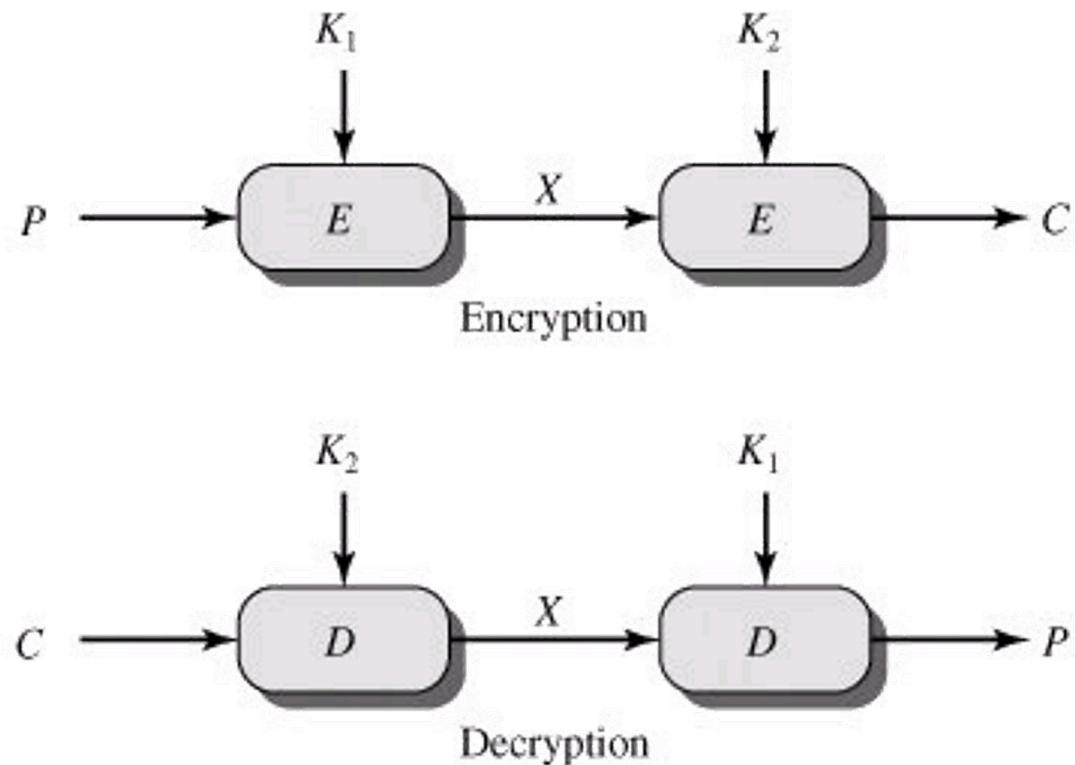
□ افزایش قدرت DES با رمزگذاری چند مرحله‌ای با DES و استفاده از کلیدهای متعدد

2DES

$$C = E(K_2, E(K_1, P))$$

$$P = D(K_1, D(K_2, C))$$

طول کلید = ۱۱۲ بیت





تحليل الگوریتم رمز 2DES

□ حمله ملاقات در میانه (Meet-in-the-Middle)

$$\square C = E(K_2, E(K_1, P))$$

$$\square X = D(K_2, C) = E(K_1, P)$$

با داشتن یک زوج (P, C) ,

□ P را با 2^{56} کلید ممکن برای K_1 رمزگذاری کن و مقادیر X را (در یک جدول درهمساز یا Hash Table) ذخیره کن.

□ C را با 2^{56} کلید ممکن برای K_2 رمزگشایی کن و مقادیر حاصله با مقادیر ذخیره شده مقایسه کن.

□ در صورت تطابق، درستی زوج کلید یافت شده را چک کن.

□ پیچیدگی محاسباتی انجام عملیات فوق $O(2^{56})$ است و البته نیاز به $O(2^{55})$ فضای ذخیرهسازی دارد.



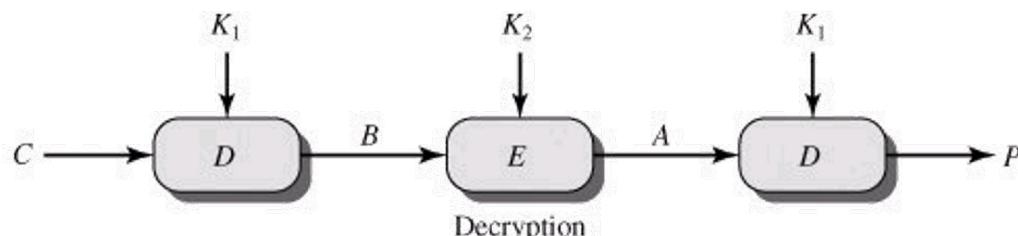
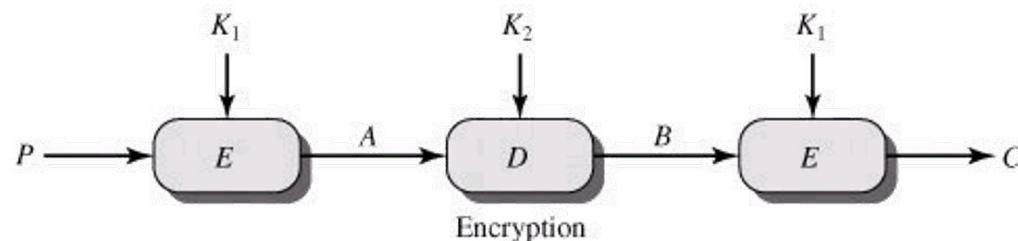
الگوریتم 3DES با دو کلید

□ حل مشکل 2DES با سه مرحله رمزگذاری با DES

□ امکان بهره‌گیری از DES به صورت زیر:

$$C = E(K_1, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_1, C)))$$





الگوریتم 3DES با سه کلید

استفاده از سه کلید مختلف

$$C = E(K_3, D(K_2, E(K_1, P)))$$

طول کلید = ۱۶۸ بیت

استفاده در برخی برنامه‌های تحت اینترنت

PGP

S/MIME



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای رمزنگاری



استاندارد رمزگذاری پیشرفته AES

□ NIST در سال ۱۹۹۷ مسابقه‌ای دو مرحله‌ای برای طراحی استاندارد جدید برگزار کرد.

- تمام طراحی‌ها باید بر اساس اصول کاملاً روشن انجام شوند.
- سازمانهای دولتی آمریکا حق هیچ گونه دخالتی در طراحی الگوریتم ندارند.

ارایه شده توسط:
Vincent Rijmen
Joan Daemen

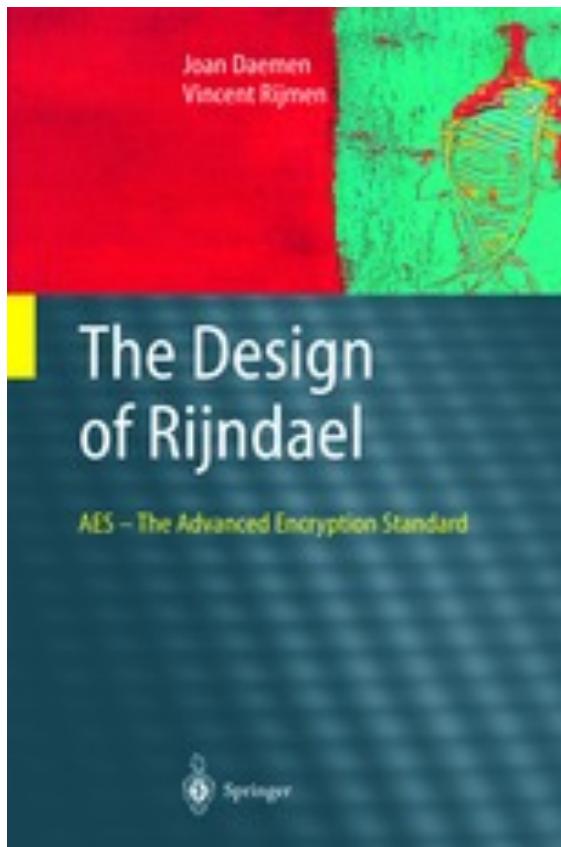
□ در سال ۲۰۰۰ راینداال (Rijndael) به عنوان برنده اعلام شد.

- استاندارد جدید تحت عنوان استاندارد رمزگذاری پیشرفته AES مورد قبول واقع شد.



اصول طراحی Rijndael

- J. Daemen and V. Rijmen. **The Design of Rijndael**. Springer-Verlag Berlin, 2002.



Joan Daemen
(1965 –)



Vincent Rijmen
(1970 –)



مشخصات استاندارد AES

۲۵۶	۱۹۲	۱۲۸	طول کلید
۱۲۸	۱۲۸	۱۲۸	طول قطعه ورودی و خروجی
۱۴	۱۲	۱۰	تعداد دور
۱۲۸	۱۲۸	۱۲۸	طول کلید هر دور

در الگوریتم اصلی Rijndael طول قطعه می تواند ۱۲۸، ۱۹۲ و یا ۲۵۶ بیت باشد، ولی در استاندارد **FIPS PUB 197** طول آن به ۱۲۸ بیت محدود شده است.



نحوه کار AES-128

- مبتنی بر ساختار رمز **فیستل** نیست و کل قطعه داده پردازش می‌شود.
- الگوریتم زمان بندی **کلید** نقش تهیه **کلید** (۱۲۸ بیتی) برای هر دور بر اساس کلید اصلی را بر عهده دارد.
- برخلاف DES و بسیاری از رمزهای دیگر، آعمال لازم بر روی بایتها انجام می‌شود نه **بیتهایها**.



نحوه کار AES-128

□ متن آشکار ورودی به صورت ستونی در ماتریس حالت ذخیره می‌شود.

Input = 32 43 f6 a8 88 5a 30 8d
31 31 98 a2 e0 37 07 34

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34



مراحل رمزگذاری AES-128

- در هر دور ۴ عمل بر روی ماتریس حالت اعمال می‌شود.
- جایگزینی بایتهای جایگزینی درایه‌های ماتریس حالت با استفاده از یک s-box
- شیفت سطروی
- ترکیب ستونها: ترکیب خطی ستونها با استفاده از ضرب ماتریسی
- اضافه نمودن کلید دور: جمع مبنای دو ماتریس حالت با کلید دور
- هر چهار عمل برگشت‌پذیر بوده، لذا هر دور برگشت‌پذیر است.



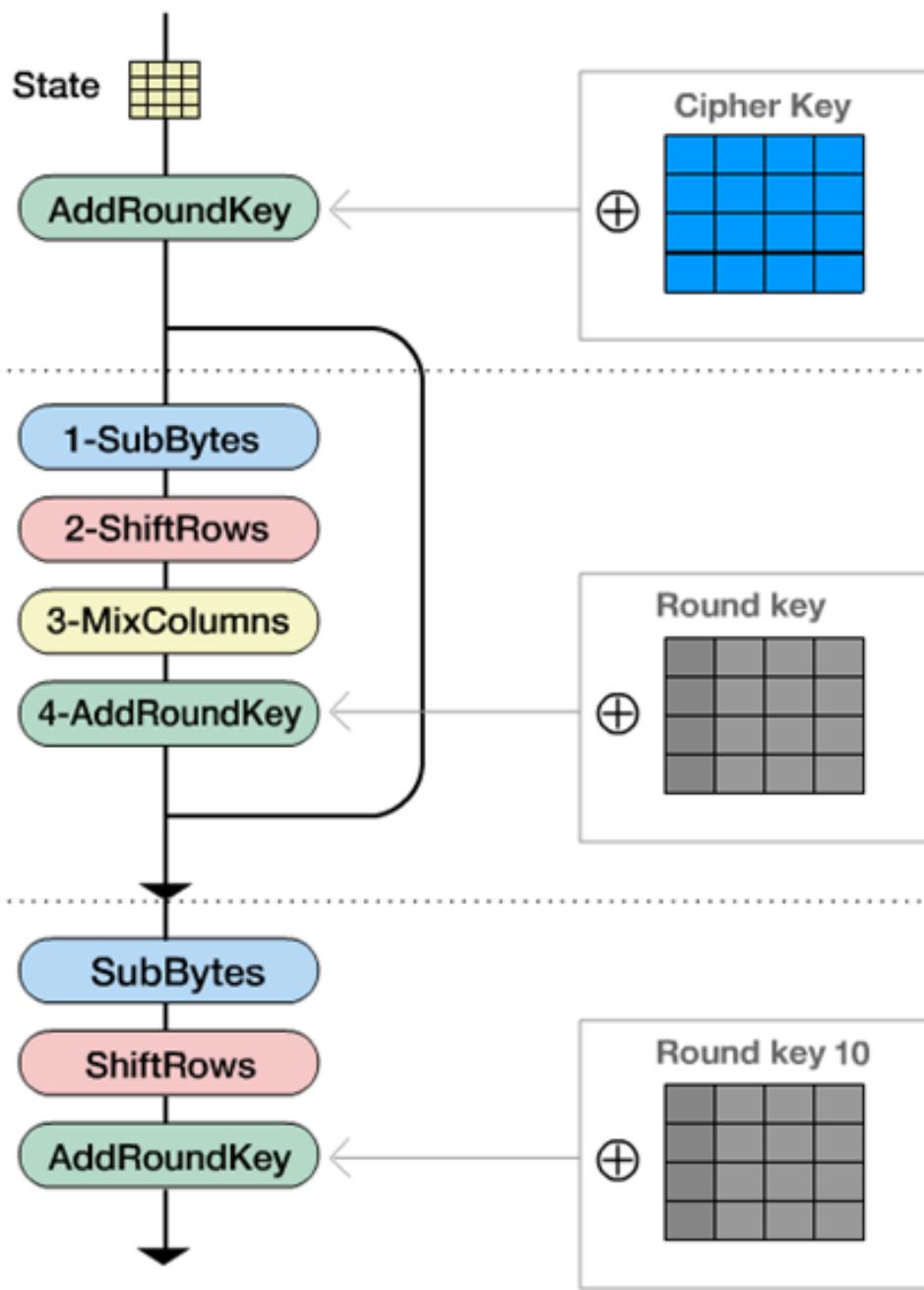
initial
round

ROUND
1..9

9
rounds

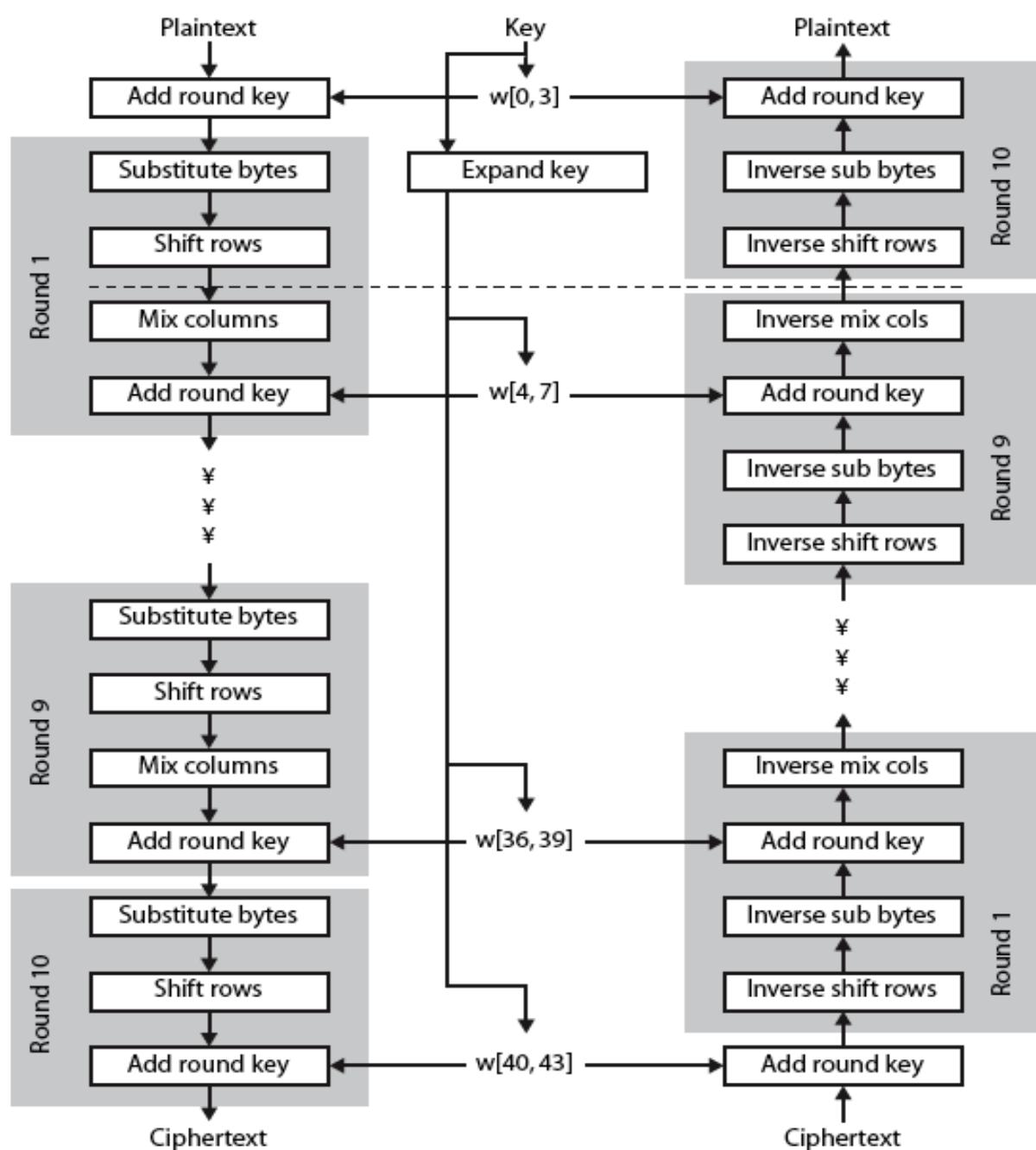
دزگذاری در AES

final
round





رمزگذاری و رمزگشایی در AES





جایگزینی بایتها (S-box) در AES

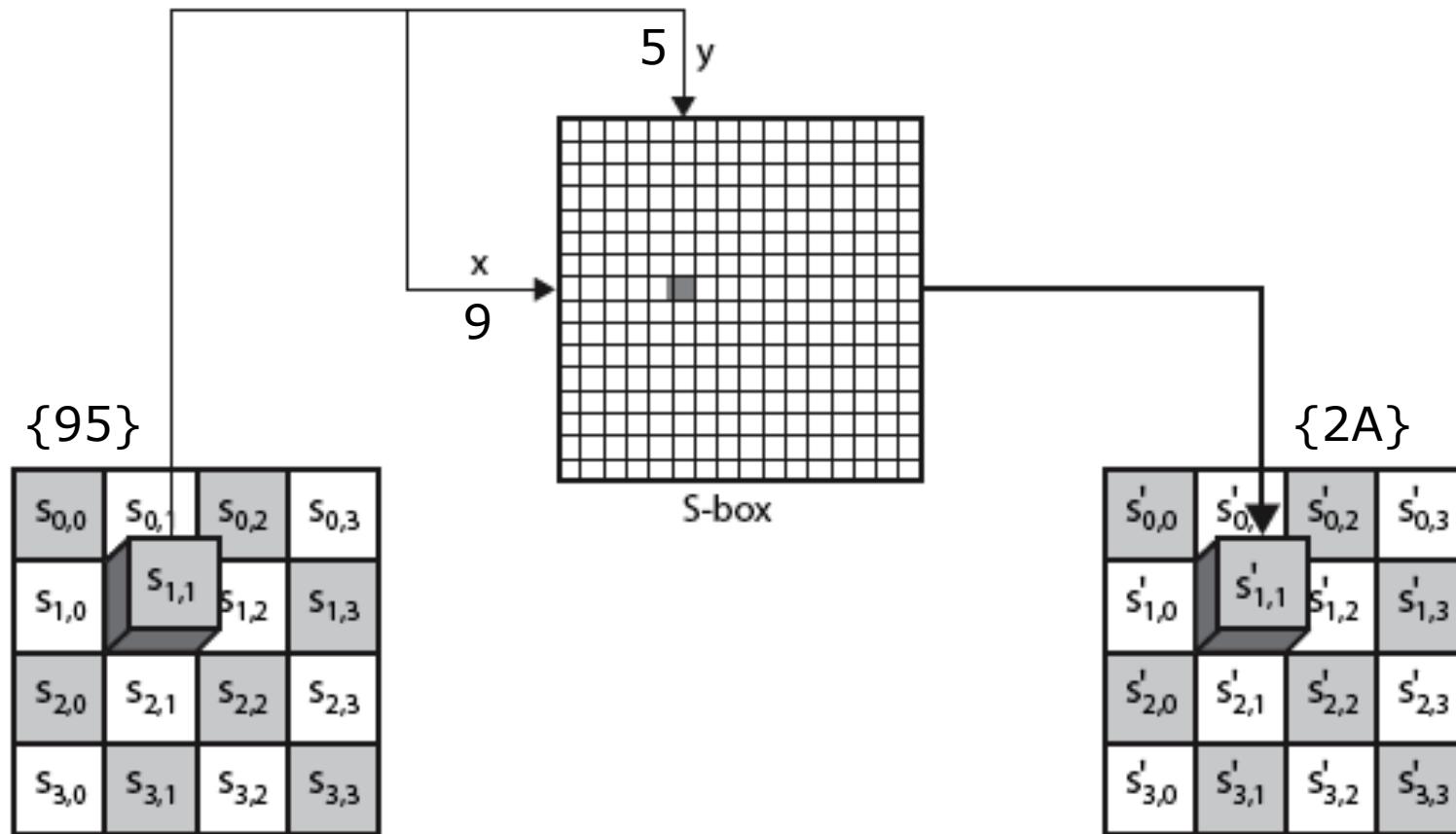
- نوعی تابع غیرخطی محاسبه می‌شود.
- توسط یک جدول 16×16 پیاده‌سازی می‌شود.
- این جدول بر اساس تبدیل مقادیر در میدان متناهی 2^8 ساخته می‌شود و در مقابل حملات شناخته شده مقاوم است.



جایگزینی بایتها (S-box) در AES

- ورودی تابع سطر و ستون درایه جدول را معین کرده و مقدار ذخیره شده در این درایه خروجی تابع است.
- با داشتن یک عنصر از ماتریس حالت
 - سطر جدول = ۴ بیت سمت چپ عنصر
 - ستون جدول = ۴ بیت سمت راست عنصر
- برای رمزگشایی از جدول معکوس استفاده می شود.

جایگزینی بایتها (S-box) در AES





جداول جایگزینی در AES

(a) S-box

	y																
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	4									
	2	B7	FD	93	26	36	3F	F									
	3	04	C7	23	C3	18	96	0									
	4	09	83	2C	1A	1B	6E	5									
	5	53	D1	00	ED	20	FC	B									
	6	D0	EF	AA	FB	43	4D	3									
	7	51	A3	40	8F	92	9D	3									
	8	CD	0C	13	EC	5F	97	4									
	9	60	81	4F	DC	22	2A	9									
	A	E0	32	3A	0A	49	06	2									
	B	E7	C8	37	6D	8D	D5	4									
	C	BA	78	25	2E	1C	A6	E									
	D	70	3E	B5	66	48	03	F									
	E	E1	F8	98	11	69	D9	8									
	F	8C	A1	89	0D	BF	E6	4									

(b) Inverse S-box

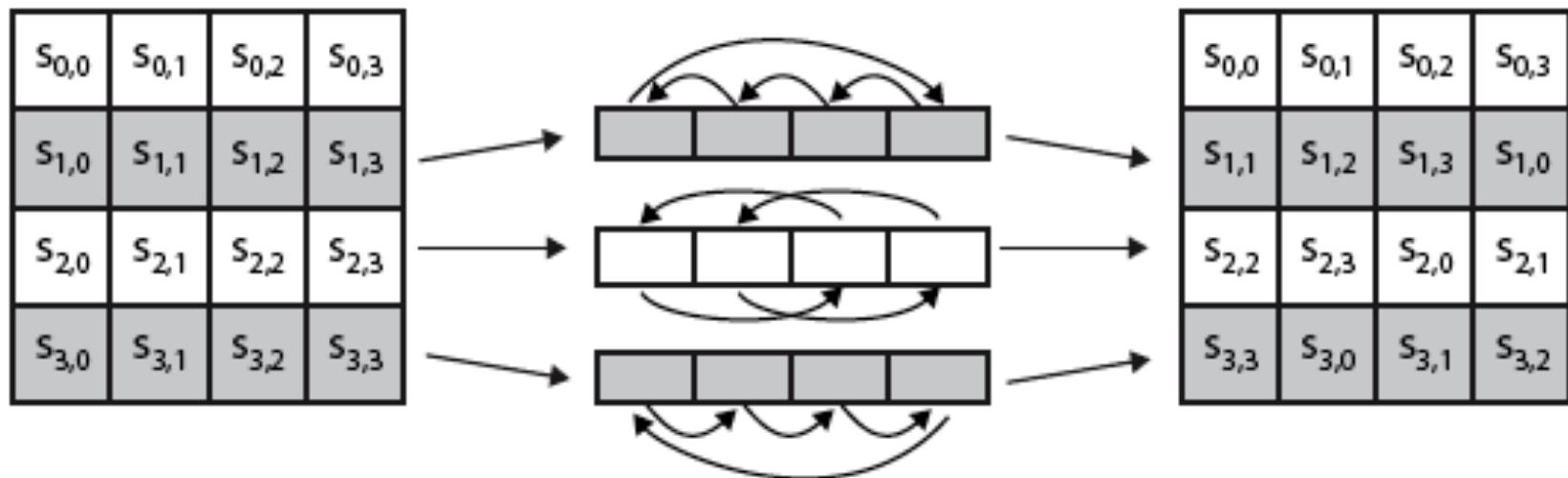
	y																
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
x	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D



شیفت سطّری در AES

- شیفت چرخشی به چپ که در آن
 - سطر اول بدون تغییر
 - سطر دوم یک بایت شیفت چرخشی به چپ
 - سطر سوم دو بایت شیفت چرخشی به چپ
 - سطر چهارم سه بایت شیفت چرخشی به چپ
- در رمزگشایی، شیفت به راست انجام می‌شود.
- از آنجا که داده به صورت ستونی در ماتریس حالت ذخیره شده، لذا این مرحله یک جایگشت بین ستونها انجام می‌دهد.

شیفت سطّری در AES



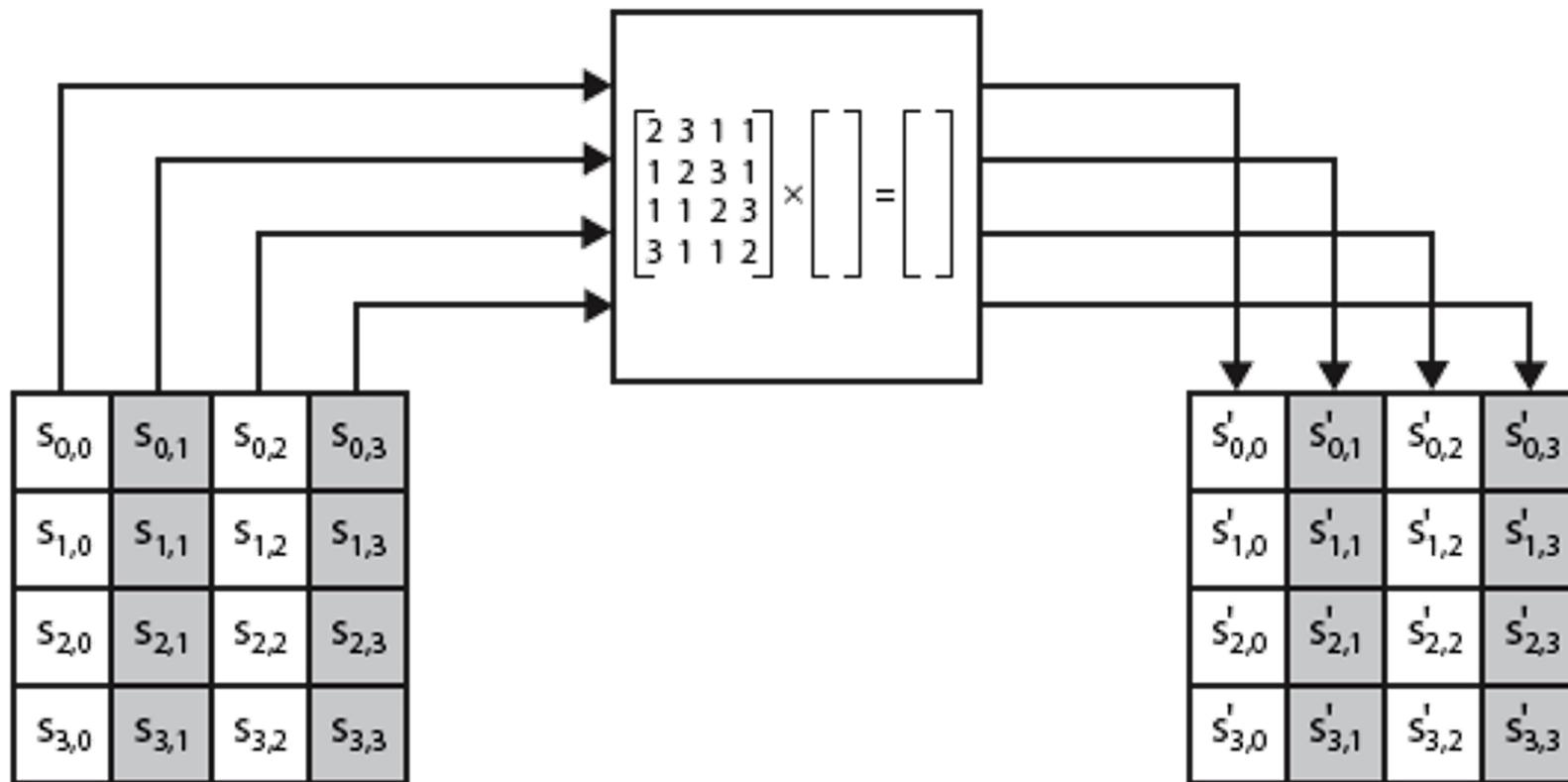


ترکیب ستونها در AES

- هر ستون جداگانه پردازش می‌شود.
- هر بایت با مقداری (وابسته به هر چهار عنصر آن ستون) جایگزین می‌شود.
- با ضرب ماتریسی این کار انجام می‌شود.



ترکیب ستونها در AES





ترکیب ستونها در AES

جمع همان XOR است ولی ضرب باید در میدان متناهی 2^8 انجام شود که آن هم با تعدادی XOR و شیفتدهی قابل انجام است (برای اطلاع از نحوه چگونگی مراجعه شود به فصل ۴ کتاب Stallings).

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

$$s'_{0,j} = (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j}$$

$$s'_{1,j} = s_{0,j} \oplus (2 \cdot s_{1,j}) \oplus (3 \cdot s_{2,j}) \oplus s_{3,j}$$

$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \cdot s_{2,j}) \oplus (3 \cdot s_{3,j})$$

$$s'_{3,j} = (3 \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \cdot s_{3,j})$$



ترکیب ستونها در AES

برای رمزگشایی از ماتریس دیگری در ضرب استفاده می‌شود.

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix} = \begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$



افزودن کلید دور در AES

- ماتریس حالت با کلید دور XOR می‌شود.
- به صورت ستونی انجام می‌شود.
- برای رمزگشایی نیز همین عمل انجام می‌شود.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

 \oplus

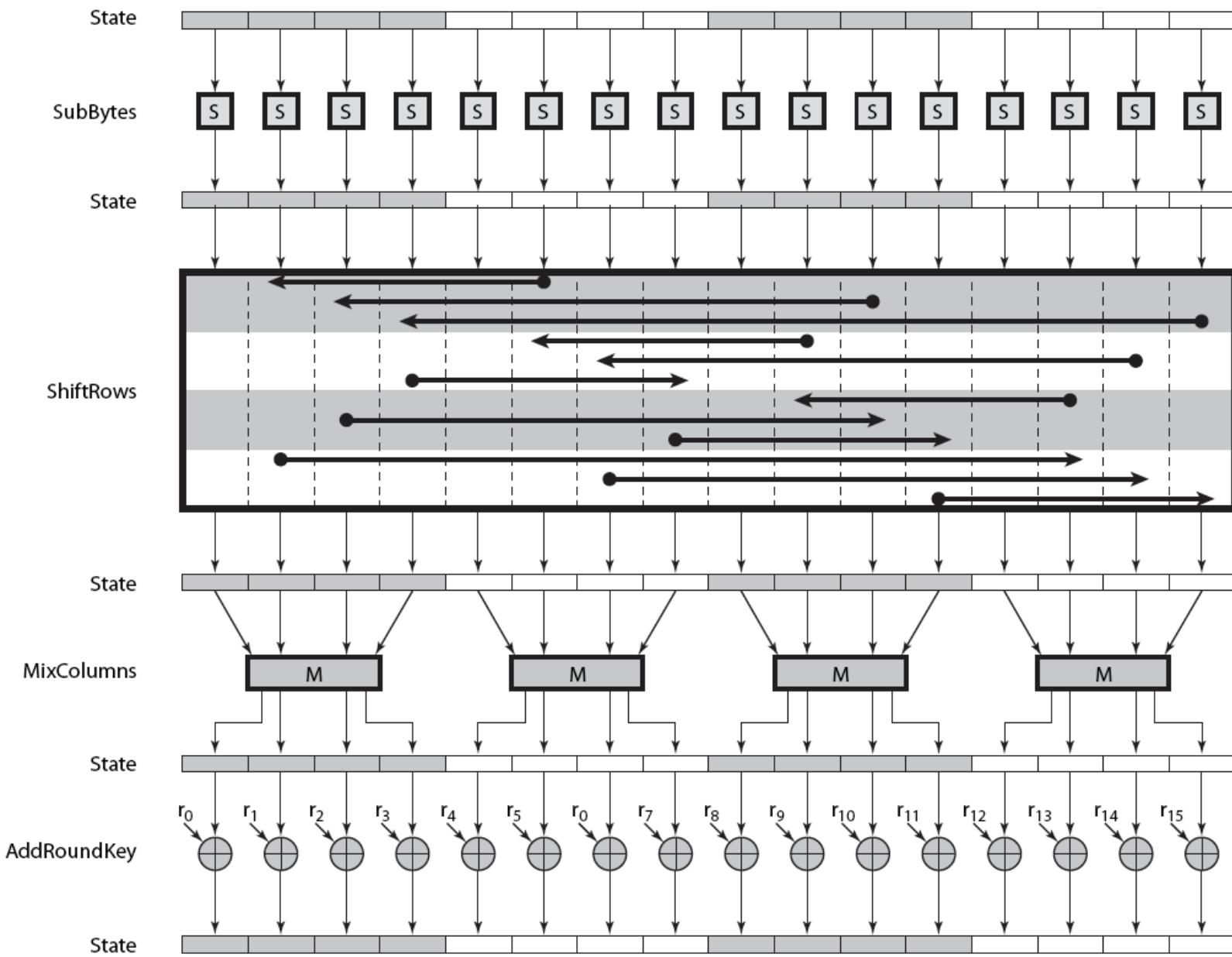
w_i	w_{i+1}	w_{i+2}	w_{i+3}
-------	-----------	-----------	-----------

=

$S'_{0,0}$	$S'_{0,1}$	$S'_{0,2}$	$S'_{0,3}$
$S'_{1,0}$	$S'_{1,1}$	$S'_{1,2}$	$S'_{1,3}$
$S'_{2,0}$	$S'_{2,1}$	$S'_{2,2}$	$S'_{2,3}$
$S'_{3,0}$	$S'_{3,1}$	$S'_{3,2}$	$S'_{3,3}$



پنجم دور الگوریتم AES





بسط کلید در AES

- یک کلید ۱۲۸ بیتی (۱۶ بایتی) دریافت می‌کند و آن را به یک آرایه ۴۴ عنصره (از کلمات ۳۲ بیتی) بسط می‌دهد.
- شروع: کپی کلید در ۴ عنصر (کلمه) اول آرایه
- تکرار: تولید هر عنصر (کلمه $w[i]$) بر اساس $w[1-i]$ و $w[i-4]$
- عناصر موجود در درایه های مضرب ۴ با تابع پیچیده g محاسبه می‌شوند.



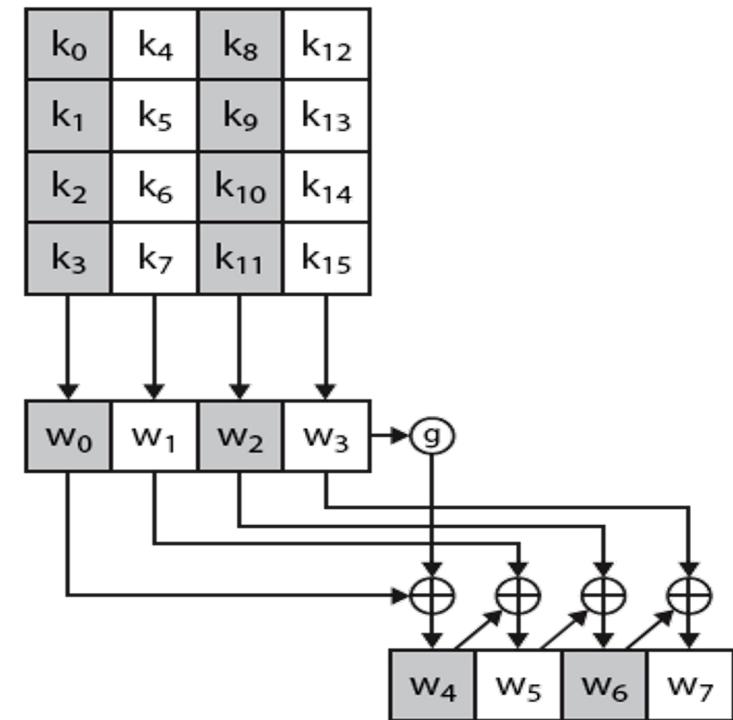
بسط کلید در AES

- If $i=4k$:

$$w[i] = \text{SubWord}(\text{RotWord}(w[i-1])) \oplus Rcon[i/4] \oplus w[i-4]$$

- Otherwise:

$$w[i] = w[i-1] \oplus w[i-4]$$





بسط کلید در AES

□ تابع g شامل زیرتوابع زیر است:

1. شیفت چرخشی به چپ به اندازه یک بایت (RotWord)
2. جایگزینی هر بایت بر اساس جدول S-box (SubWord) در رمزگذاری
3. ترکیب XOR مقدار حاصل از انجام آعمال ۱ و ۲ با مقدار ثابت $Rcon[i/4]$

$$Rcon[i/4] = (RC[i/4], 0, 0, 0)$$

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36



امنیت AES

- تا کنون حمله ای بر روی آن کشف نشده و در مقابل همه حملات معمول آمن طراحی شده است.
- از لحاظ مقایسه با DES:
- فرض کنید ماشینی وجود دارد که کلید DES را از طریق آزمون جامع در یک ثانیه بازیابی می‌کند، یعنی در هر ثانیه 2^{56} کلید را امتحان می‌کند. این ماشین کلید AES را در $10^{12} \times 149$ سال بازیابی می‌نماید.



مجموعه دستورالعمل AES

- اینتل در سال ۲۰۰۸ مجموعه دستورالعمل‌های AES را به CPU‌های خود افزود ← افزایش چشمگیر سرعت CPU
- مجموعه دستورالعمل‌های مشابهی برای سایر معماری‌های ARM وجود دارد.

توصیف	دستورالعمل
اجرای یک دور عادی از رمزگذاری AES	AESENC
اجرای دور آخر از رمزگذاری AES	AESENCLAST
اجرای یک دور عادی از رمزگشایی AES	AESDEC
اجرای دور آخر از رمزگشایی AES	AESDECLAST
کمک در تولید کلید دور AES	AESKEYGENASSIST
کمک در عملیات Inverse Mix Columns	AESIMC
ضرب بدون رقم نقلی (عملیات در میدانهای متناهی)	PCLMULQDQ



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای رمزنگاری



دیگر رمزاهاي متقارن معروف

نام الگوريتم	طول کلید (بيت)	طول بلوک (بيت)	تعداد دور	ويژگی‌ها
IDEA	۱۲۸	۶۴	۸	- عدم گزارش هر گونه حمله
Blowfish	متغير ۳۲ تا ۴۴۸	۶۴	۱۶	- زيرکليدها و S-Box‌ها - وابسته به کلید
RC5	متغير	متغير	متغير	- نياز به حافظه کم - تعداد دورها وابسته به داده
CAST-128	متغير ۴۰ تا ۱۲۸	۶۴	۱۶ یا ۱۲	- استفاده از دو زيرکليد در هر دور - متغير بودن تابع F



مقایسه سرعت الگوریتمها

نام الگوریتم	تعداد سیکل ساعت برای هر دور	تعداد دور	تعداد سیکل ساعت به ازای رمز یک بایت
Blowfish	۹	۱۶	۱۸
RC5	۱۲	۱۶	۲۳
DES	۱۸	۱۶	۴۵
IDEA	۵۰	۸	۵۰
3DES	۱۸	۴۸	۱۰۸



فهرست مطالب

- تعاریف و مفاهیم رمز
- رمز کلاسیک
- رمز متقارن مدرن
- استاندارد رمز متقارن DES
- استاندارد رمز متقارن AES
- رمزهای متقارن معروف
- مدهای کاری رمز متقارن



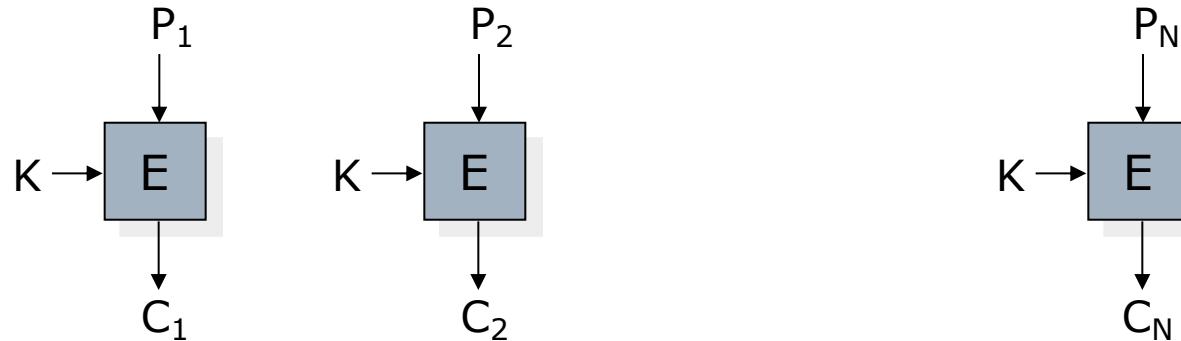
مدھای کاری رمزهای بلوکی

- رمزهای قطعه ای به طور مستقل امنیت زیادی را به ارمغان نمی آورند.
بلکه باید در مدهای کاری مناسب مورد استفاده قرار گیرند.
- مدهای کاری می توانند از رمزهای بلوکی ... CAST-128، DES، AES استفاده کنند.
- برخی مدهای کاری پراهمیت عبارتند از :
 - **ECB:** Electronic Code Book
 - **CBC:** Cipher Block Chaining
 - **CTR:** Counter Mode
 - **CFB:** Cipher Feed Back
 - **OFB:** Output Feed Back

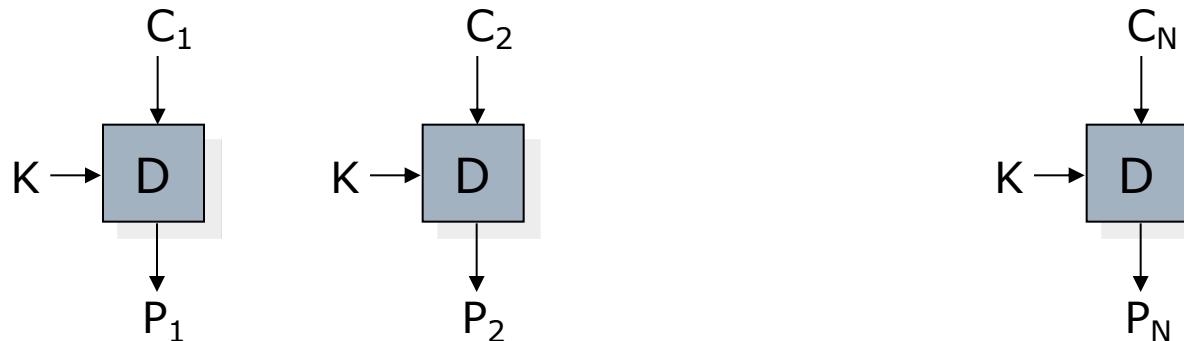


مد کاری ECB (Electronic Code Book)

□ رمزگذاری:



□ رمزگشایی:



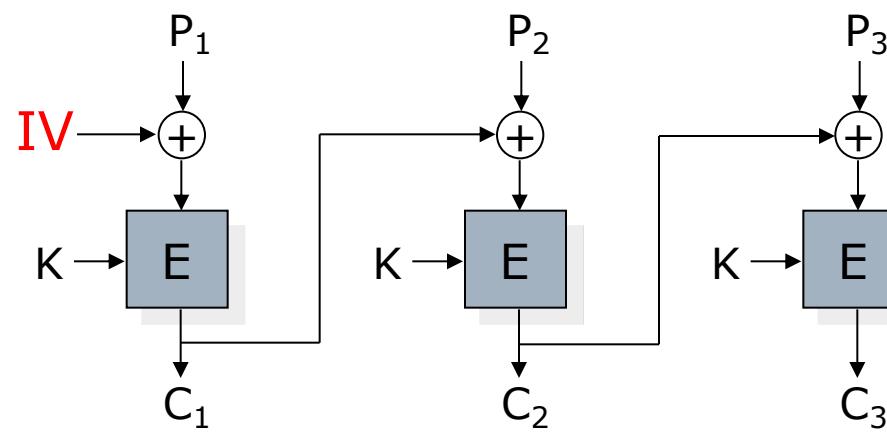


بررسی مد کاری ECB

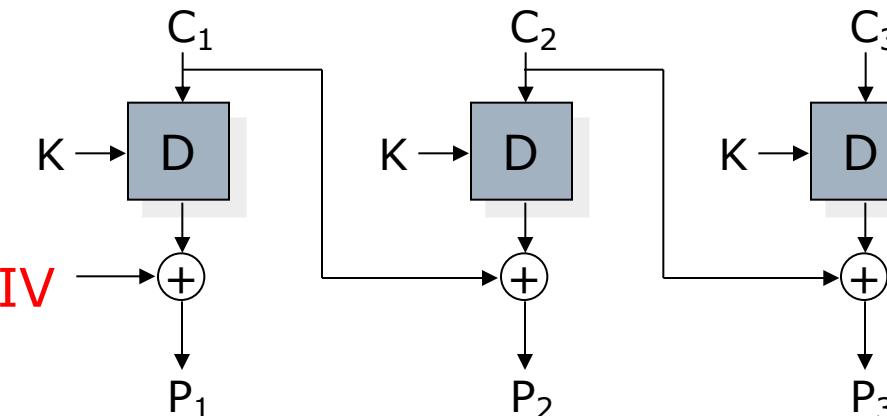
- اشکال اساسی: هر متن آشکار به ازاء کلید ثابت همیشه به یک متن رمز شده نگاشته می‌شود.
- مهاجم می‌تواند دریابد که پیام‌های یکسان ارسال شده‌اند.
- این مد امن محسوب نمی‌شود حتی اگر از یک رمز قطعه‌ای قوی استفاده کنیم.
- ECB مثالی از مواردی است که علی‌رغم بهره‌برداری از عناصر مرغوب، کیفیت نهایی دلخواه نیست.



مد کاری CBC (Cipher Block Chaining)



□ رمزگذاری:



□ رمزگشایی:



مد کاری CBC

- این مد از یک مقدار دهی اولیه تصادفی (IV) بهره می‌گیرد.
- مقدار IV در هر بار رمزگذاری به صورت تصادفی تغییر می‌کند.
- IV همراه با متن رمز شده ارسال می‌شود.
- در صورت ارسال IV بصورت متن آشکار، تحلیلگر ممکن است بتواند با تغییر IV به مقدار جعلی مورد نظر خود، منجر به تغییر خاصی در پیغام واگشاپی شده در سمت گیرنده شود (با توجه به XOR مقدار IV با مقدار رمزگشاپی شده).
- IV نیز باید بصورت رمز شده ارسال شود. برای اینکار می‌توان از مد کاری ECB استفاده کرد.
- هر متن آشکار به ازاء کلید ثابت هر بار به یک متن رمز شده متفاوت نگاشته می‌شود (زیرا مقدار IV تغییر می‌نماید).



بررسی مددکاری CBC

□ ملزومات امنیتی:

- IV باید کاملاً غیر قابل پیش‌بینی باشد.

□ رمزگذاری:

- عملیات رمزگذاری قابل موازی‌سازی نیست.
- مقدار IV و متن آشکار باید در دسترس باشند.

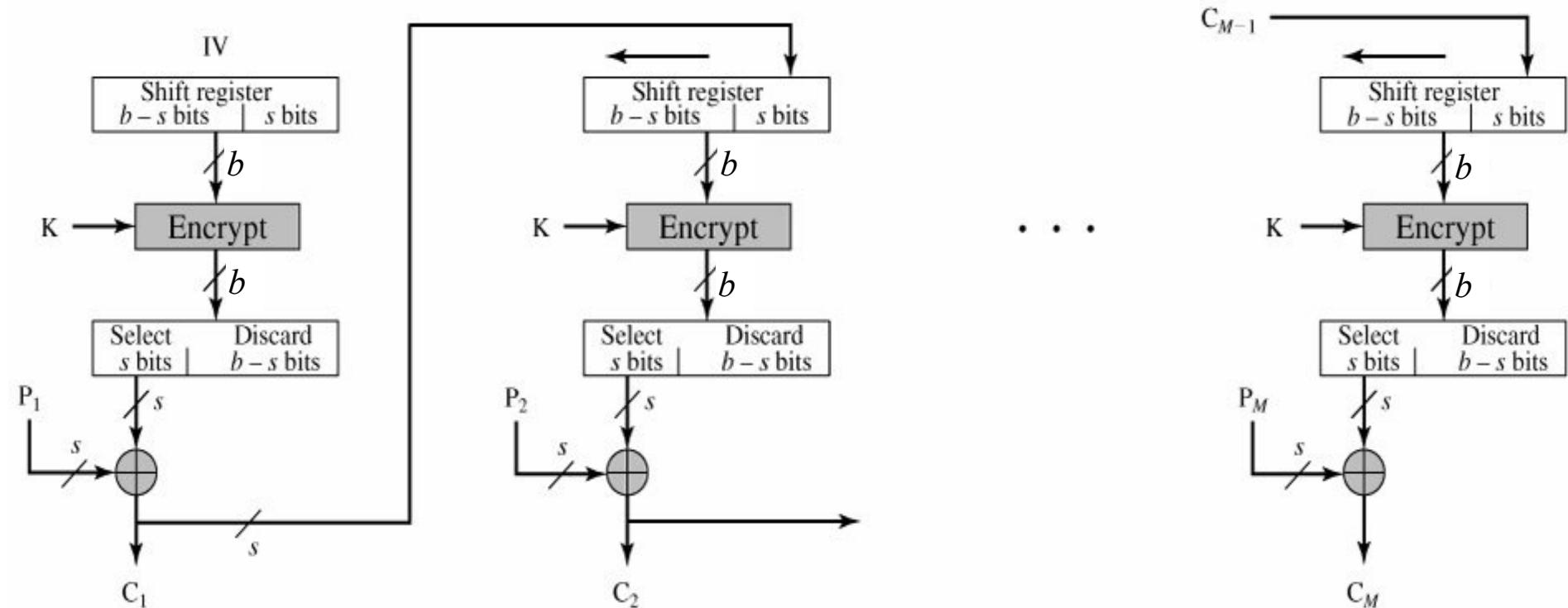
□ رمزگشایی:

- عملیات رمزگشایی قابل موازی‌سازی است.
- مقدار IV و متن رمزشده باید در دسترس باشند.



مد کاری CFB (Cipher Feed Back)

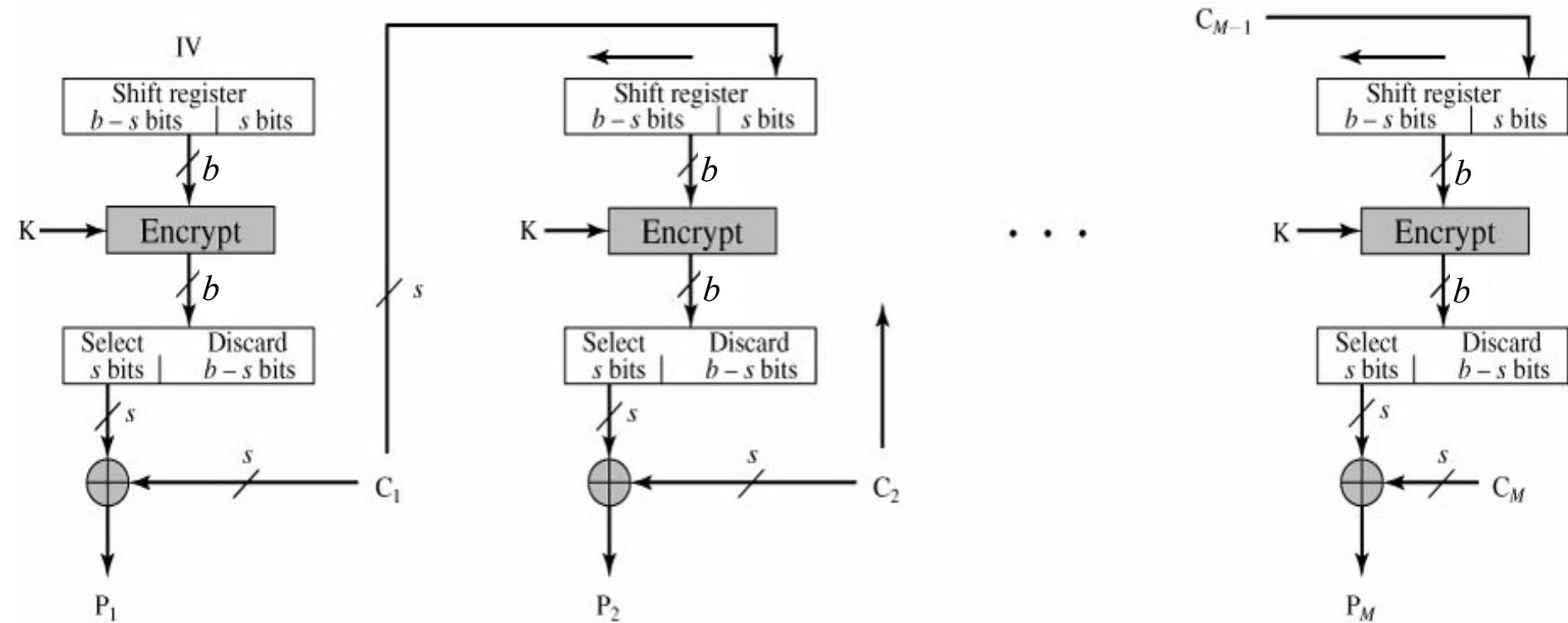
□ رمزگذاری





مد کاری CFB

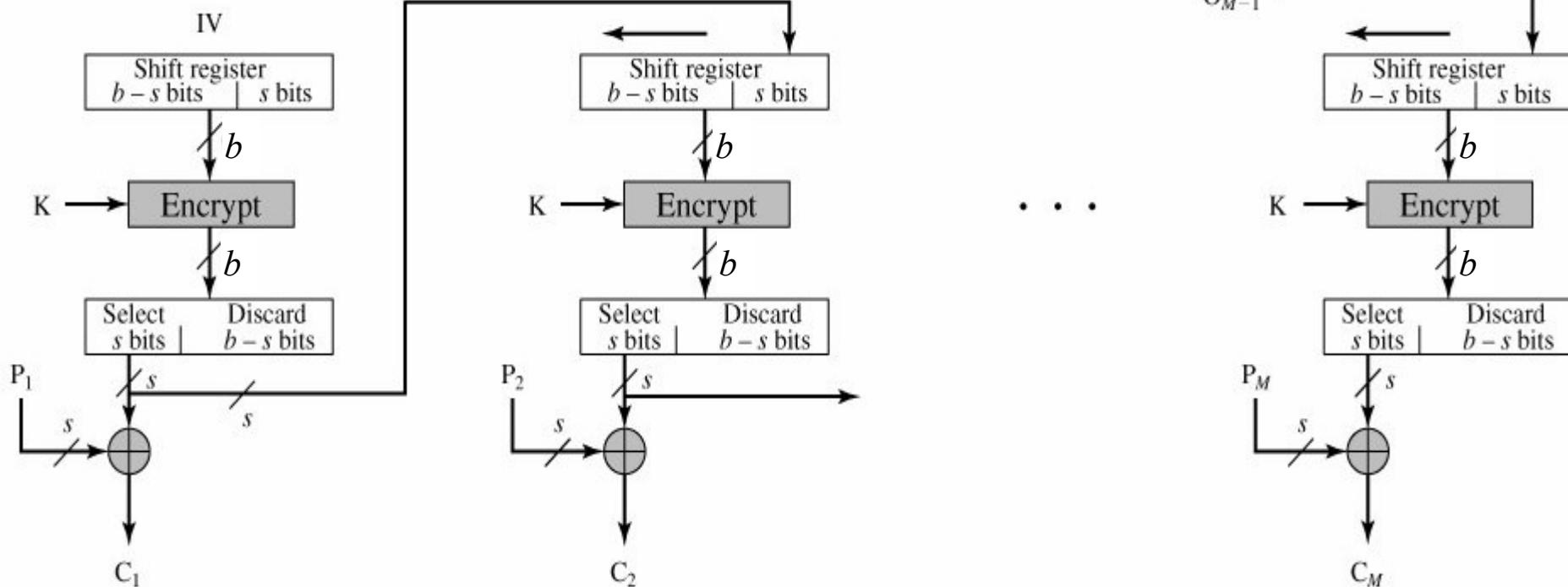
□ رمزگشایی





مد کاری OFB (Output Feed Back)

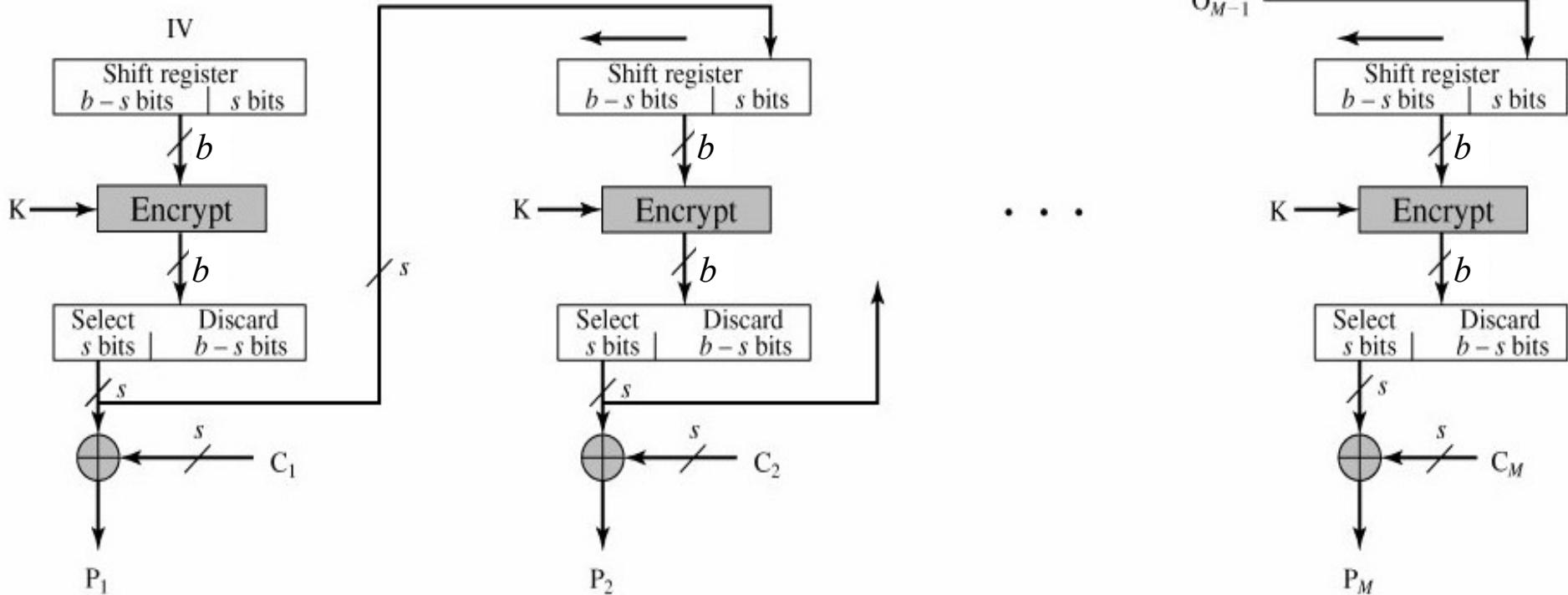
□ رمزگذاری





مد کاری OFB

□ رمزگشایی





مقایسه OFB و CFB

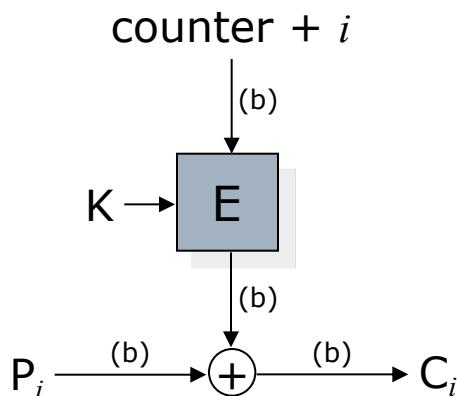
- موارد استفاده OFB و CFB
 - رمز جریانی
 - کاربردهای بی درنگ
-
- عیب CFB: انتشار خطای انتقال
 - این عیب را برطرف می‌کند.



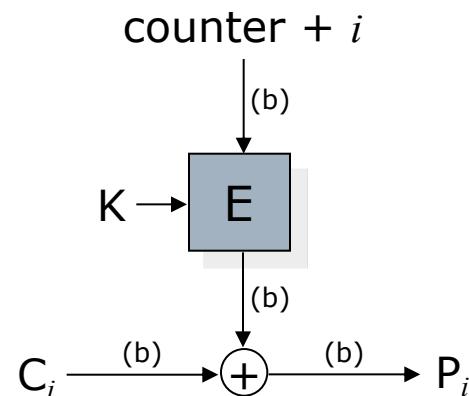
مد کاری CTR (Counter Mode)

- شمارنده به طول قطعه (b بیت) انتخاب شده و می‌تواند با مقدار اولیه صفر یا بصورت تصادفی انتخاب شود.
- برای هر قطعه به شمارنده یک واحد اضافه می‌شود (در پیمانه 2^b)
- می‌توان برای ارسال جریانی داده نیز استفاده کرد (کافی است هر دفعه S بیت از P_i را با خروجی رمز شمارنده، XOR کنیم)

□ رمزگذاری ↓



□ رمزگشایی ↓





بررسی مد کاری CTR

□ ملزومات امنیتی:

- مقادیر شمارنده، در بازه طول عمر کلید، باید مجزا باشند.

□ رمزگذاری:

- عملیات رمزگذاری قابل موازی سازی است.
- برای عملیات رمزگذاری نیازی به متن آشکار نیست.



بررسی مد کاری CTR

□ رمزگشایی:

- عملیات رمزگشایی قابل موازی سازی است.
- برای عملیات رمزگشایی نیازی به متن رمز شده نیست.

□ پیادهسازی:

- به شکل کارایی می‌تواند پیادهسازی سخت‌افزاری و نرم‌افزاری شود.
- از پردازش موازی می‌توان در آن استفاده کرد.



مقایسه کاربرد انواع مدهای کاری

کاربرد	مد کاری
ارسال مقادیر کوچک مانند کلید	ECB (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-گرا و جریانی هر گونه داده مناسب برای ارسال با سرعت بالا	CTR (Counter)



پایان

پست الکترونیکی

amini@sharif.edu

kharrazi@sharif.edu

ياددا الامن والامان



پیوست

جزئیات الگوریتم رمزگاری DES



استاندارد رمزگذاری داده DES

قطعه ۶۴ بیتی متن آشکار



دور ۱

دور ۲

دور ۱۵

دور ۱۶

زیر کلید دور

زیر کلید دور

زیر کلید دور

زیر کلید دور

تولید زیر کلیدهای ۴۸
بیتی از کلید اصلی ۵۶
بیتی برای هر دور

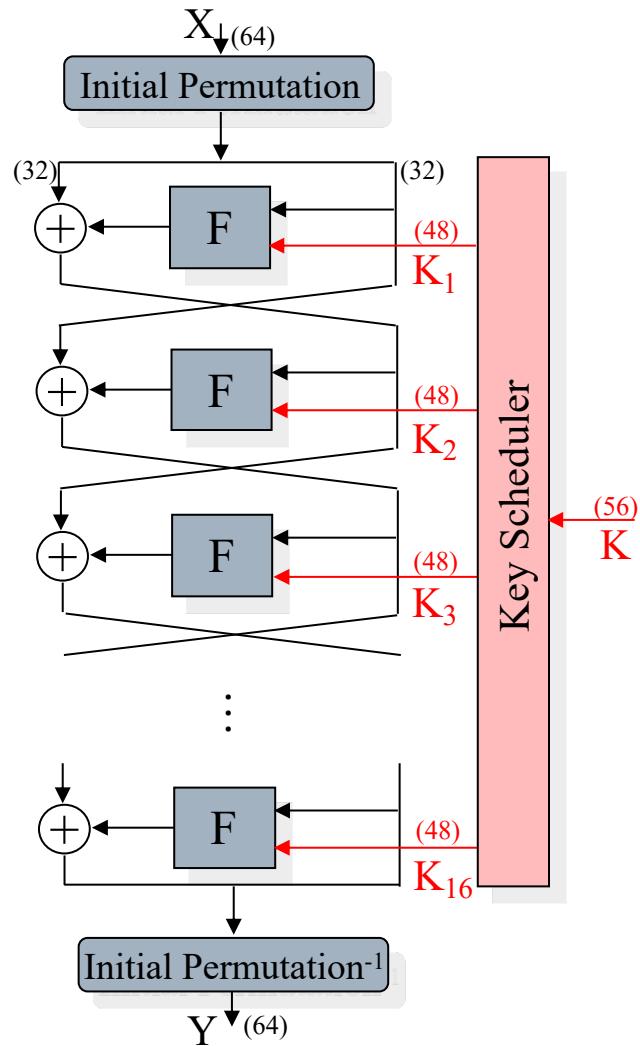


کلید ۵۶ بیتی

قطعه ۶۴ بیتی متن رمزنگاری شده



ساختار فیستل رمز DES





جداول جایگشت اولیه

Initial Permutation (IP)							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Final Permutation (IP⁻¹)

35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

□ تاثیری در رمز ندارند.

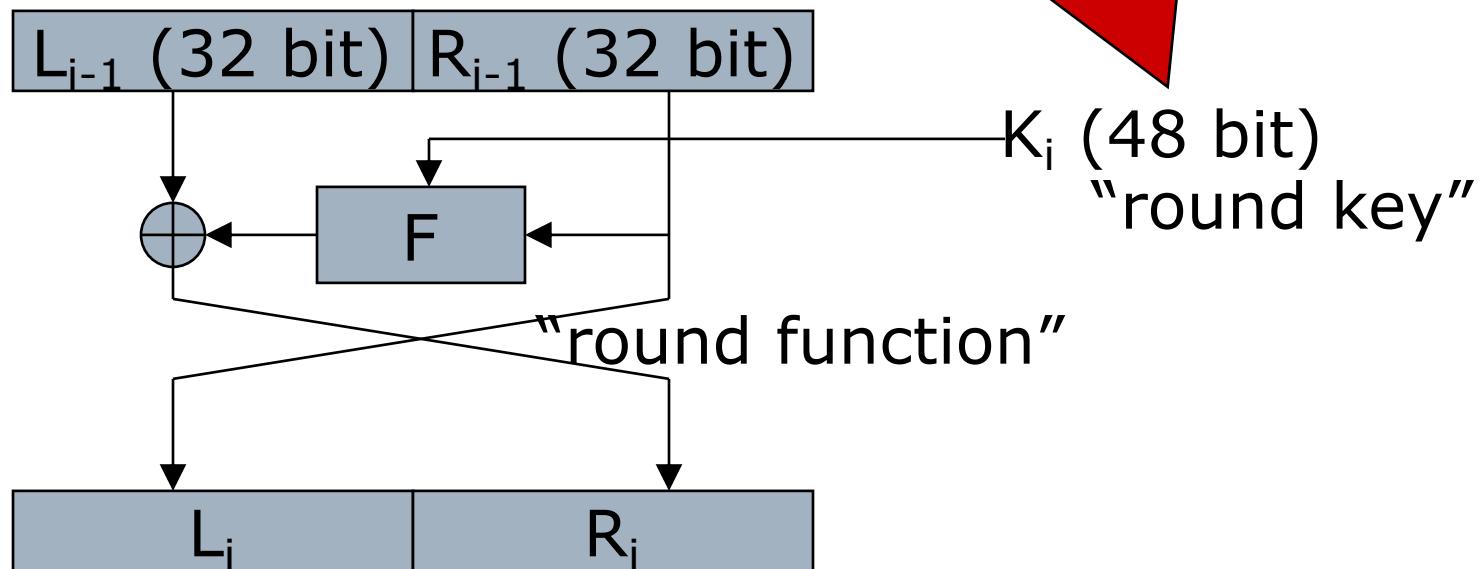
□ صرفاً جهت تسهیل در بارگذاری بلوکها

در سخت‌افزارهای دهه ۷۰



یک دور از DES

توسط زمانبند کلید
تولید میشود.



$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

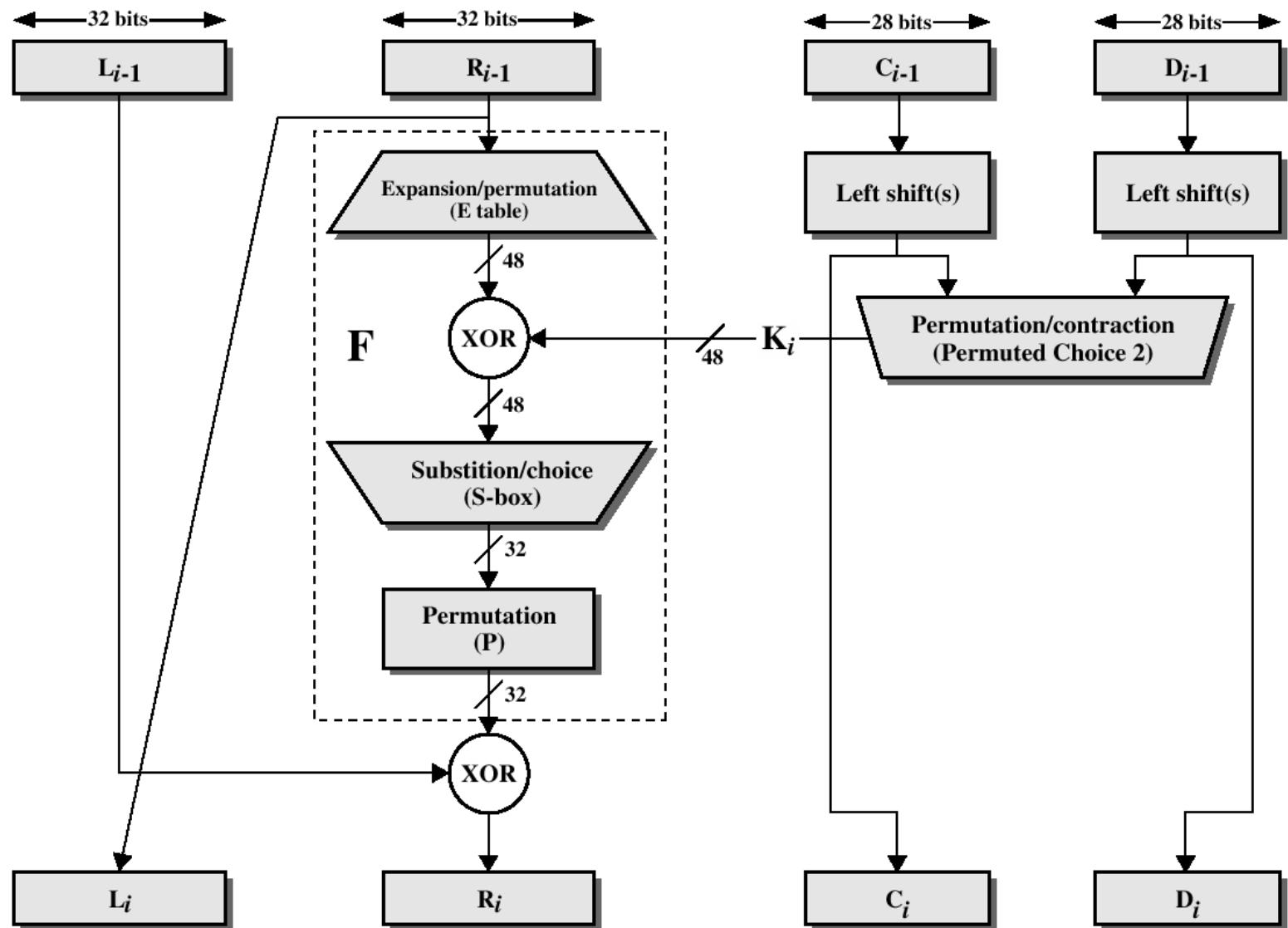
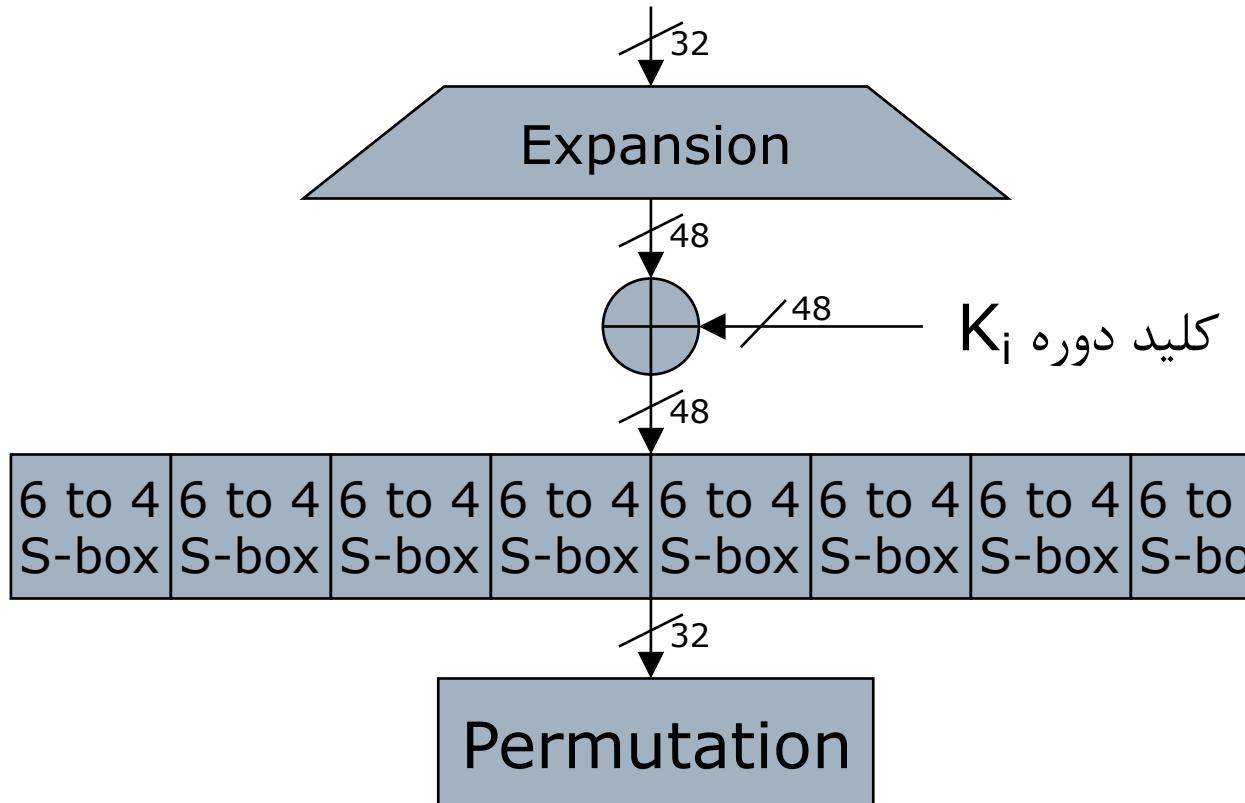


Figure 2.4 Single Round of DES Algorithm



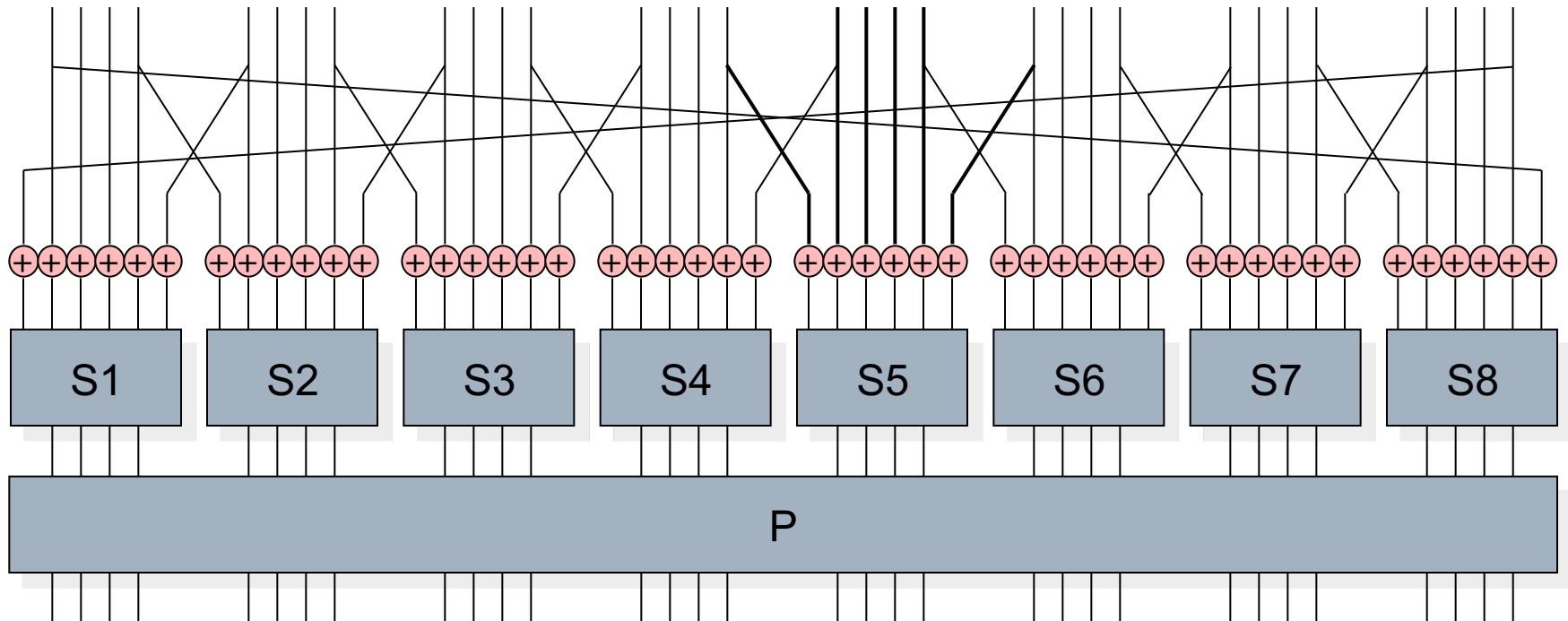
تابع دور DES





تابع دور DES

$K_i \rightarrow$





بررسی S-Box در DES

- تنها بخش غیرخطی از الگوریتم DES هستند.
- غیرقابل برگشت هستند.
- اصول طراحی آنها سری هستند.
- استفاده از S-Box ۸ که هریک ۶ بیت ورودی را به ۴ بیت خروجی تبدیل می‌کنند.
- بیتهای ۱ و ۶ : انتخاب یکی از ۴ سطر ماتریس
- بیتهای ۲ تا ۵ : انتخاب یکی از ۱۶ ستون ماتریس
- برگرداندن عدد موجود در آن خانه از ماتریس به عنوان خروجی
- در مجموع ۴۸ بیت ورودی از هشت S-Box مختلف عبور می‌کنند و ۳۲ بیت برمی‌گردانند.



یک از S-Box DES

		شماره ستون															
شماره ↓ سطر	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	



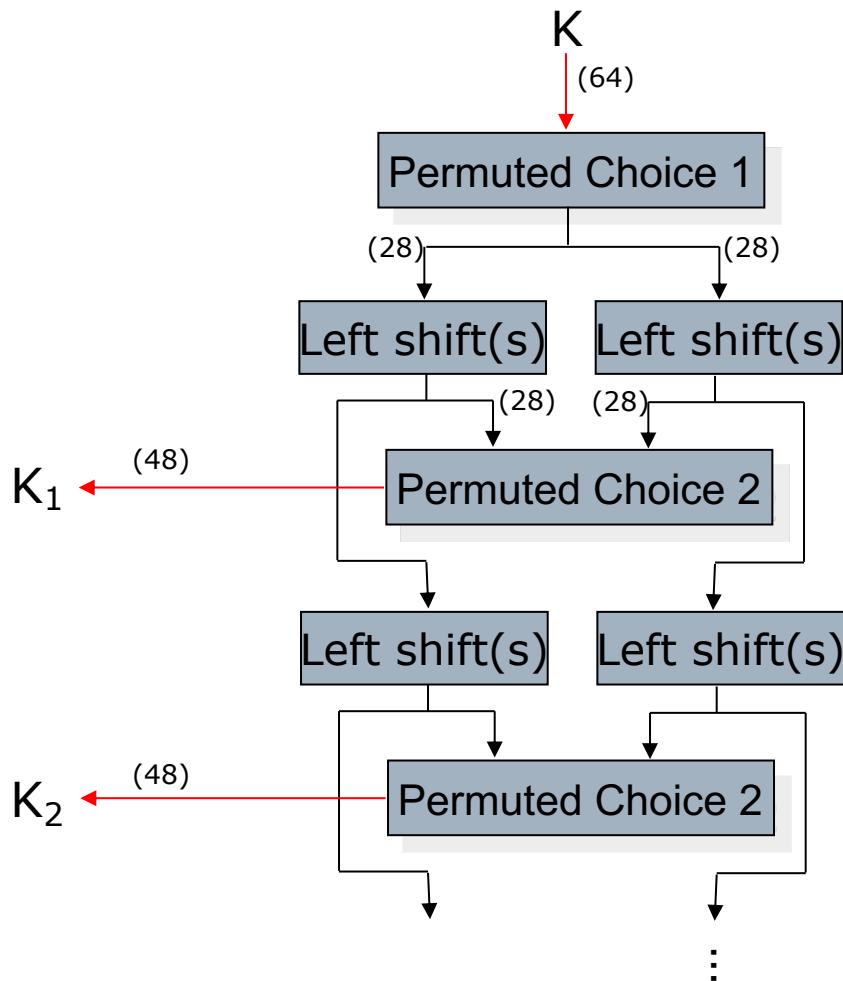
جدول جایگشت

جدول جایگشت مورد استفاده در هر دور DES □

1	16	7	20	21	29	12	28	17
9	1	15	23	26	5	18	31	10
17	2	8	24	14	32	27	3	9
25	19	13	30	6	22	11	4	25



زمانبندی کلید



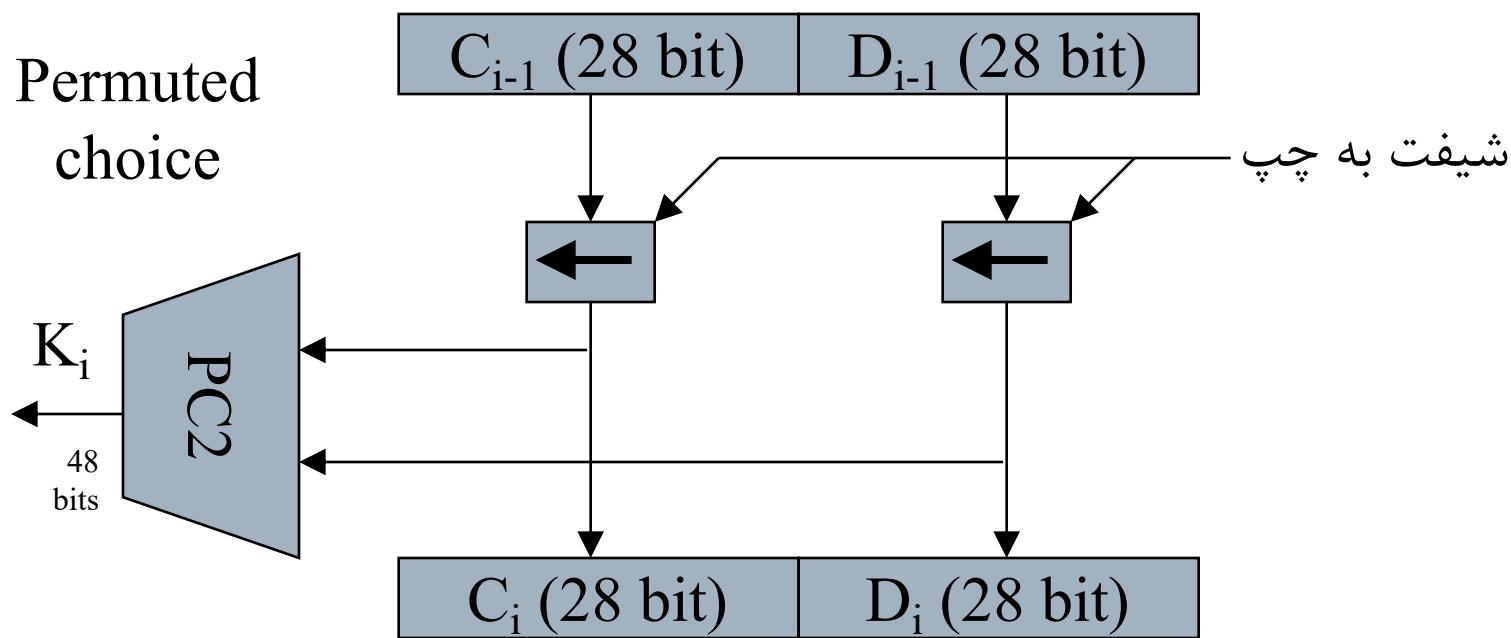
□ هر بیت کلید حدوداً در ۱۴ دور از ۱۶ دور استفاده می‌شود.

□ تابع تعابیر شده برای زمانبندی کلید، یک مقدار ۶۴ بیتی را به عنوان کلید می‌پذیرد ولیکن فقط ۵۶ بیت آن را استفاده می‌کند و بقیه به عنوان parity می‌تواند مورد استفاده قرار گیرد.



زمانبندی کلید

- ✓ کلید اصلی ۵۶ بیت
- ✓ کلید هر دور ۴۸ بیت





عناصر زمانبند کلید

شیفت چرخشی به چپ بر اساس جدول زیر

شماره دور	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
تعداد بیت شیفت	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

جداول جایگشت

Permuted Choice One (PC-1)						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Permuted Choice Two (PC-2)								
14	17	11	24	1	5	3	28	
15	6	21	10	23	19	12	4	
26	8	16	7	27	20	13	2	
41	52	31	37	47	55	30	40	
51	45	33	48	44	49	39	56	
34	53	46	42	50	36	29	32	



میزان توانمندی DES

□ اندازه کلید

- ۵۶ بیت دارای کل فضای حالت $2^{56} = 7.2 * 10^{16}$
- حمله آزمون جامع هرچند مشکل، ولی امکان پذیر است.
- آخرین گزارش ثبت شده در سال ۱۹۹۹ نشان از کشف کلید تنها در عرض ۲۳ ساعت داده اند!

□ حمله زمانی

- پیاده سازی الگوریتم رمز را مورد هدف قرار می دهند.
- الگوریتم برای ورودی های مختلف مدت زمان متفاوتی صرف رمزگذاری می کند.
- بیشتر در کارتهای هوشمند مشکل زا می شوند.
- DES در مقابل حمله زمانی مقاوم است.



زمان لازم برای شکست رمز DES (10^6 decryptions/ μ s)

