

# یادالامن والامان



## رمزگاری متقارن

توسط: حمید رضا شهریاری

دانشگاه صنعتی امیرکبیر

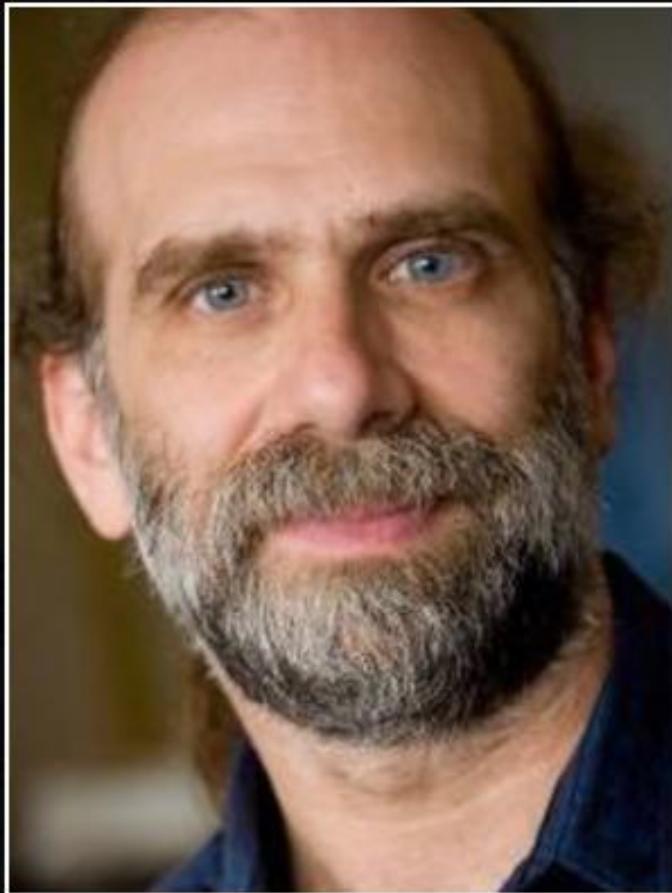
دانشکده مهندسی کامپیووتر

<http://www.aut.ac.ir/shahriari>

# فهرست مطالب

---

- تعاریف
- رمزهای کلاسیک
- الگوریتم‌های رمزهای متقارن و رمزهای قطعه‌ای
- استانداردهای رمزگذاری آمریکا
- الگوریتم‌های دیگر رمزنگاری
- استفاده از رمزهای قطعه‌ای
- مدهای کاری رمزهای قطعه‌ای
- واژه نامه

A portrait photograph of Bruce Schneier, a middle-aged man with a full, grey beard and mustache, and receding hairline. He is looking directly at the camera with a slight smile. He is wearing a dark blue collared shirt.

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

— *Bruce Schneier* —

AZ QUOTES

# فهرست مطالب

- 
- تعاریف
  - رمزهای کلاسیک
  - الگوریتم‌های رمزهای متقارن و رمزهای قطعه‌ای
  - استانداردهای رمزگذاری آمریکا
  - الگوریتم‌های دیگر رمزنگاری
  - استفاده از رمزهای قطعه‌ای
  - مدھای کاری رمزهای قطعه‌ای
  - واژه نامه
-

# تعاريف

---

- plaintext - **the original message**
  - ciphertext - **the coded message**
  - cipher - **algorithm for transforming plaintext to ciphertext**
  - key - **info used in cipher known only to sender/receiver**
  - encipher (encrypt) - **converting plaintext to ciphertext**
  - decipher (decrypt) - **recovering ciphertext from plaintext**
  - cryptography - **study of encryption principles/methods**
  - cryptanalysis (codebreaking) - **the study of principles/methods of deciphering ciphertext without knowing key**
  - cryptology - **the field of both cryptography and cryptanalysis**
-

# رمزنگاری متقارن (Symmetric)

---

- یا معمولی/کلید خصوصی/ تک کلیدی
- فرستنده و گیرنده از یک کلید مشترک استفاده می کنند
- تمام رمزنگاریهای کلاسیک از نوع متقارن هستند
- تنها نوع رمزنگاری تا قبل از دهه 70

# مدل رمزگاری متقاض

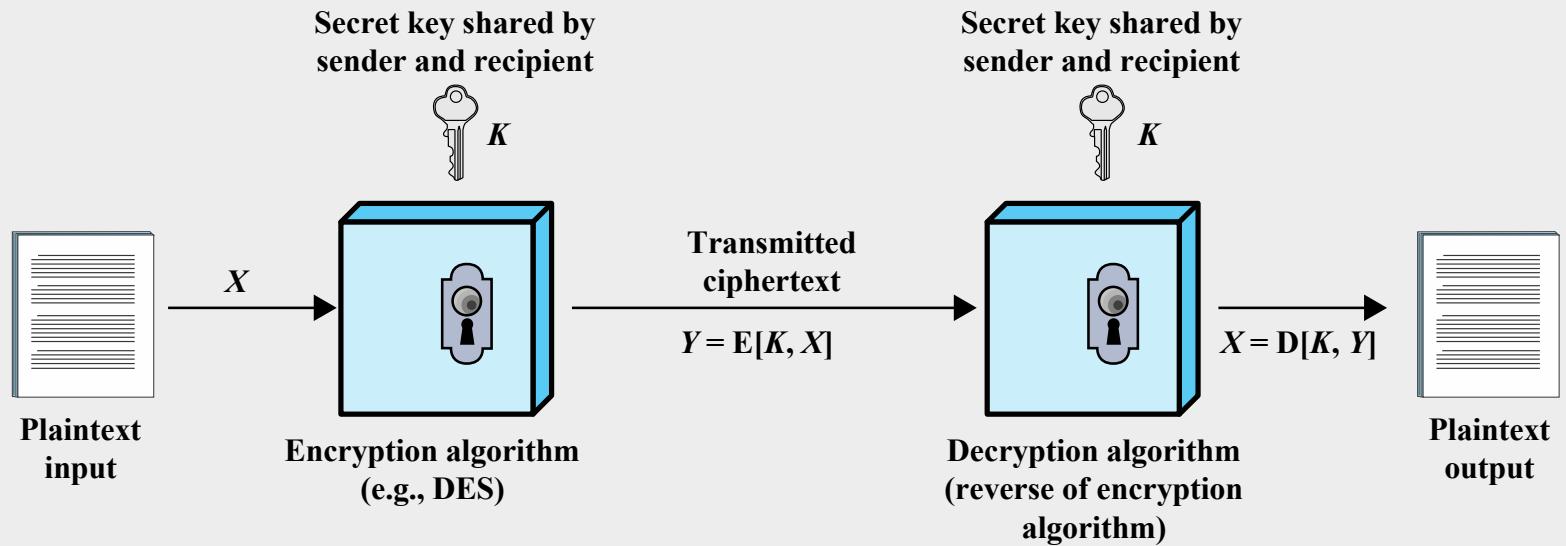


Figure 2.1 Simplified Model of Symmetric Encryption

# نیازمندیها

---

دو نیازمندی برای استفاده امن از رمزنگاری متقاضیان:

■ یک الگوریتم رمزنگاری قوی

■ یک کلید سری که تنها فرستنده و گیرنده از آن آگاه هستند

$$Y = E_K(X)$$

$$X = D_K(Y)$$

فرض بر آن است که الگوریتم برای همه مشخص است.

بنابراین نیاز به یک کanal امن برای توزیع کلید است.

# رمز نگاری

---

□ می تواند توسط ابعاد زیر مشخص شود:

■ نوع عملهای مورد استفاده برای رمز کردن

□ جایگزینی/تبدیل/ضرب

■ تعداد کلیدهای مورد استفاده

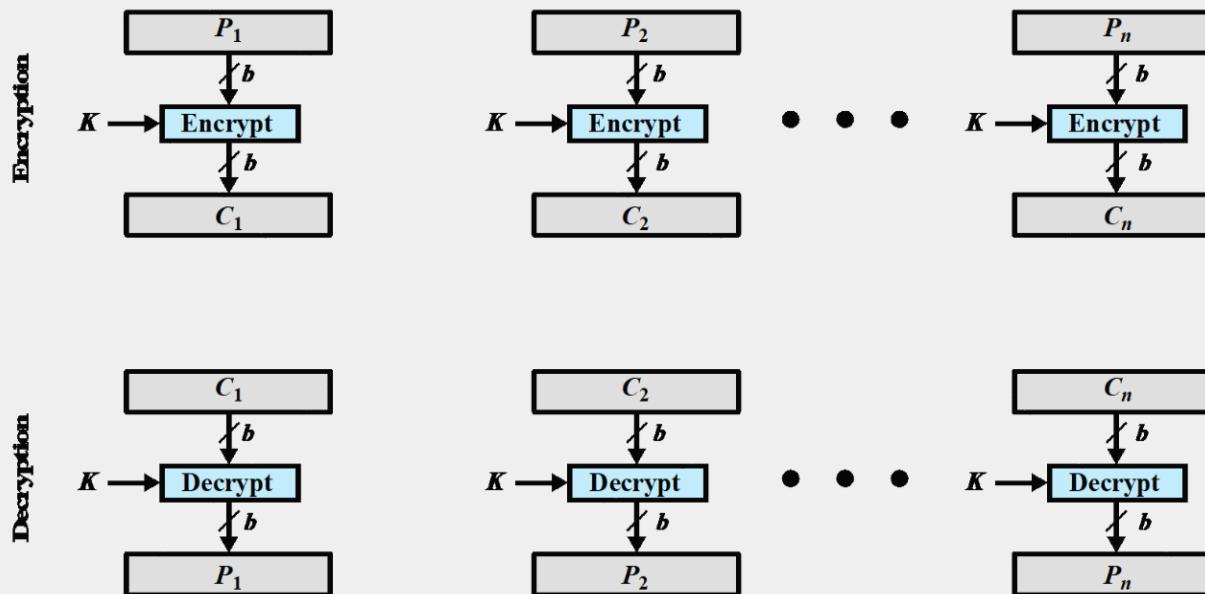
□ یک کلید یا خصوصی/دو کلید یا عمومی

■ روش پردازش متن واضح

□ بلوکی یا قطعه‌ای (Block cipher)

□ جریانی یا نهری یا دنباله‌ای (Stream cipher)

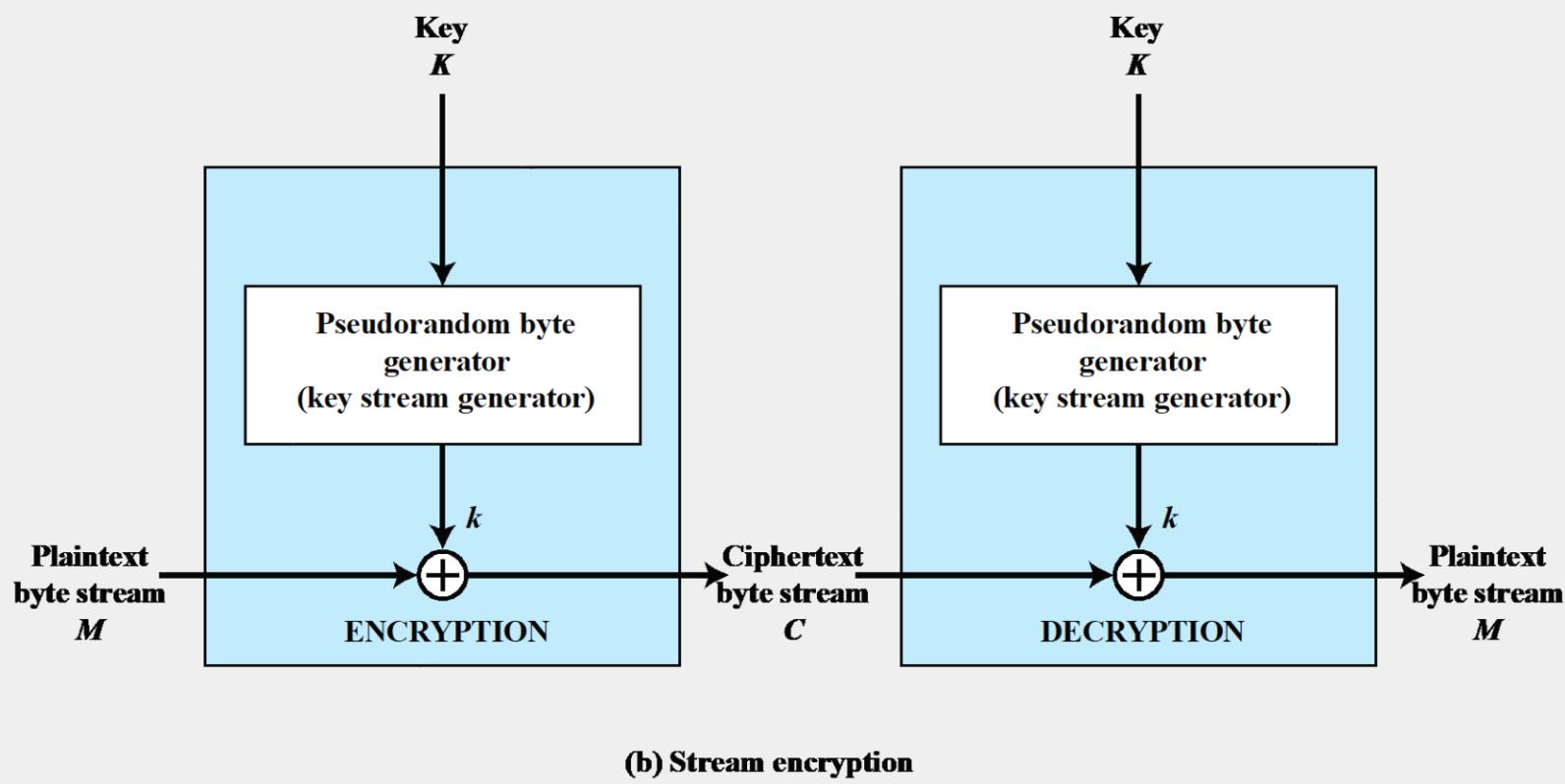
# رمزنگاری بلوکی



(a) Block cipher encryption (electronic codebook mode)

# رمزگاری جریانی

برای اینجا می‌خواهیم روشی را برای ایجاد کلید رمزنگاری دریابیم که می‌تواند هر دو کاربر را در میان خود را می‌گذارد.





# Block & Stream Ciphers

## Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

## Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

# انواع حملات تحلیل رمز نگاری

---

- ciphertext only
  - **only know algorithm / ciphertext**
- known plaintext
  - **know one or more plaintext & ciphertext pairs**
- chosen plaintext
  - **select plaintext and obtain ciphertext to attack cipher**
- chosen ciphertext
  - **select ciphertext and obtain plaintext to attack cipher**
- chosen text
  - **select either plaintext or ciphertext to en/decrypt to attack cipher**

# أنواع حملات

- أنواع حملات وارده بر اساس امکانات تحلیلگر
- Cipher text Only : تحلیلگر تنها متن رمز شده را دارد.
  - Known Plaintext : تحلیلگر چند نمونه از متن اصلی و متن رمز شده متناظر با آن را دارد.
  - Chosen Plaintext : تحلیلگر می تواند الگوریتم رمز را بر روی مقدار زیادی از متن واضح اعمال نماید و متن رمز شده را ببیند.
- \* در کلیه حالت فوق فرض شده است که الگوریتم رمنگاری بر تحلیلگر روشن است

# انواع حملات تحلیل

Type of Attack	Known to Cryptanalyst
Ciphertext only	<ul style="list-style-type: none"><li>•Encryption algorithm</li><li>•Ciphertext to be decoded</li></ul>
Known plaintext	<ul style="list-style-type: none"><li>•Encryption algorithm</li><li>•Ciphertext to be decoded</li><li>•One or more plaintext-ciphertext pairs formed with the secret key</li></ul>
Chosen plaintext	<ul style="list-style-type: none"><li>•Encryption algorithm</li><li>•Ciphertext to be decoded</li><li>•Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li></ul>
Chosen ciphertext	<ul style="list-style-type: none"><li>•Encryption algorithm</li><li>•Ciphertext to be decoded</li><li>•Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul>
Chosen text	<ul style="list-style-type: none"><li>•Encryption algorithm</li><li>•Ciphertext to be decoded</li><li>•Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key</li><li>•Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key</li></ul>

# جستجوی تمام حالات (Brute Force Search)

- ابتدایی ترین حمله
- فرض بر این است که متن واضح قابل شناسایی است.

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/ $\mu$ s	Time required at $10^6$ encryptions/ $\mu$ 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	$5.4 \times 10^{18}$ years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu\text{s} = 5.9 \times 10^{36}$ years	$5.9 \times 10^{30}$ years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu\text{s} = 6.4 \times 10^{12}$ years	$6.4 \times 10^6$ years

# دیگر تعاریف

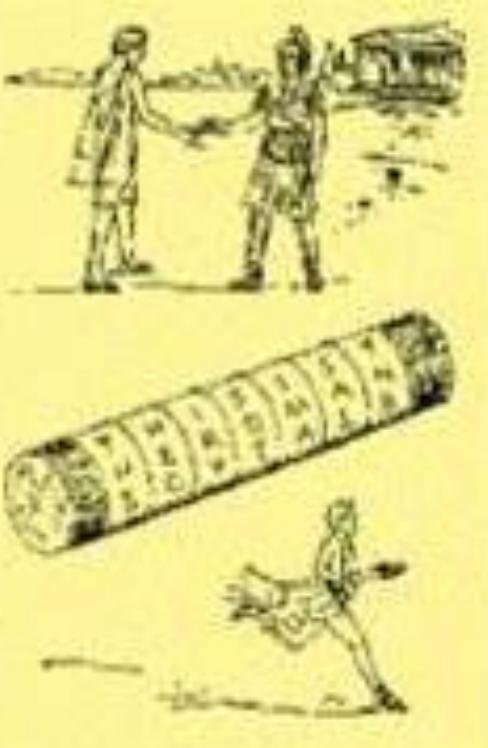
---

- **امنیت مطلق**
  - مستقل از قدرت محاسباتی در دسترس، متن رمز شده اطلاع کافی برای تعیین قطعی متن واضح ارائه نکند (و بنابراین الگوریتم رمز مستقل از مدت زمانی که دشمن در اختیار دارد قابل شکستن نباشد)
- **امنیت محاسباتی (یک یا هر دو شرط زیر)**
  - هزینه شکستن رمز بیش از ارزش اطلاعات رمز شده باشد
  - زمان مورد نیاز برای شکستن رمز از طول عمر مفید اطلاعات بیشتر باشد.

# فهرست مطالب

---

- تعاریف
  - رمزهای کلاسیک
  - الگوریتم‌های رمزهای متقارن و رمزهای قطعه‌ای
  - استانداردهای رمزگذاری آمریکا
  - الگوریتم‌های دیگر رمزنگاری
  - استفاده از رمزهای قطعه‌ای
  - مدهای کاری رمزهای قطعه‌ای
  - واژه نامه
  - پیوست ۱: DES
-



## رمزهای کلاسیک

□ حدود پانصد سال پیش از میلاد مسیح برای انتقال اطلاعات نظامی از وسیله‌ای استفاده می‌کردند به نام **سکیتال**

□ این وسیله یک تکه چوب ساده بود که با پیچیدن کاغذ پاپیروس به دور آن، پمام رمز آشکار می‌شد. در این روش، هم فرستنده و هم گیرنده رمز باید دارای اسکلتیلی با قطر یکسان باشند.



Creative Commons

# رمزهای کلاسیک

---

- قبل از به فرآگیر شدن سیستم‌های کامپیوتری و به خصوص از زمان جنگ جهانی دوم مورد استفاده قرار می‌گرفتند.
- قبل از به وجود آمدن سیستم‌های کامپیوتری امروزی به صورت دستی انجام می‌شدند.
- مبتنی بر دو روش اصلی جایگشتی و جایگزینی است

# باقیایی کبوتر نامه بر جنگ جهانی دوم حاوی نامه رمز شده



PIGEON SERVICE			
TO	X05		
FROM	1		
Originator's No.	Date.	In reply to No.	
ASAHIN	HYPICO	PIFISU	YASDC
KYOKO	DTHRP	COFTH	MAAPK
PASUZ	WTYHP	CHAWW	HTRAH
NLXKE	HEHIC	ONHIS	HLLW
HAOTTA	BBQRH	DJWH	TRZEH
LIXFH	RAGHT	TRZCQ	FNWYQ
ALDTS	AQIRU	AOKHN	17 1522/6

NURP 40 TW 194  
NURP 37 OR 76

GCHQ

# رمزهای کلاسیک

## جايكشتنی

- جانشینی
- جانشینی یک حرف با حرف دیگر
- تک الفبایی
- چند الفبایی
- حملات شناخته شده با استفاده از:
- توزیع فرکانس‌ها
- تعداد رخدادها
- حروف مشابه و احتمال کلمات
- تحلیل pattern (الگوها)

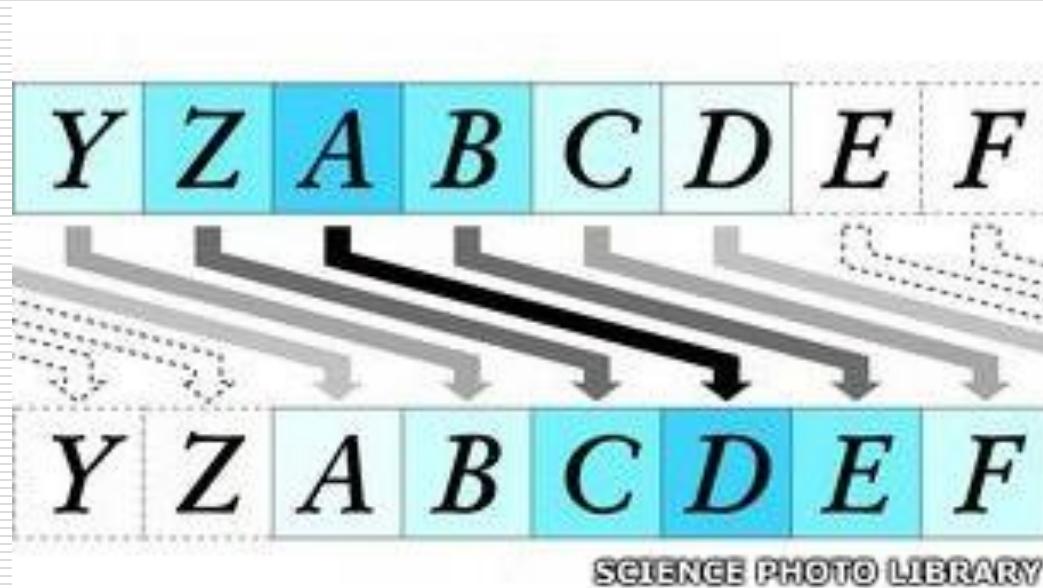
جابجایی بین حروف متن اصلی

هدف در هم ریختگی بیشتر است

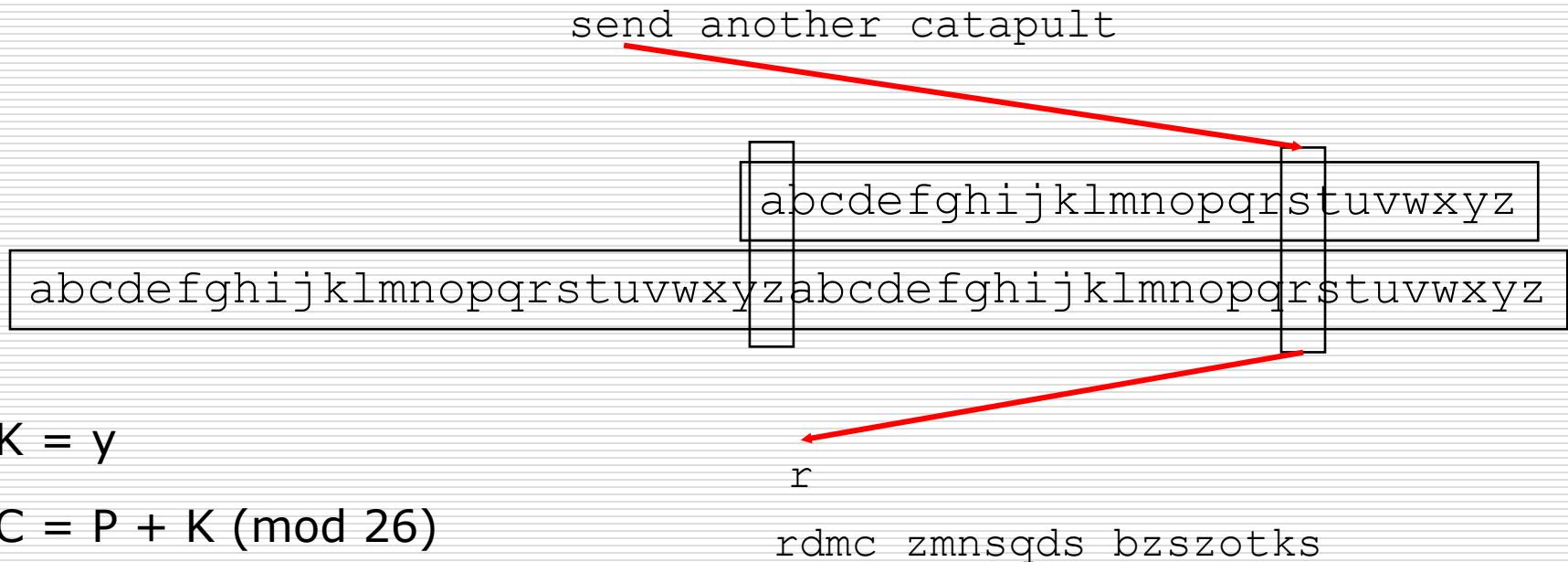
شکست رمز سخت‌تر اما اگر یک

pattern (الگو) آشکار شود، همه  
متن شکسته شده است.

# رمز سزار



# جانشینی (سزار) - رمز تک الفبایی



- تنها از یک فرمول جایگزینی مشابه فرمول فوق استفاده می‌شود
- به خاطر سپاری آنها آسان است
- مشاهده pattern‌ها به آسانی امکان پذیر است

رمز تک الفبایی

# جانشینی چندالفایی

---

## رمز چندالفایی

- استفاده از فرمول‌های جانشینی مختلف به صورت متوالی
- منجر به کاهش الگوها می‌شود
- همچنان می‌توان از توزیع حروف برای شکستن رمز استفاده کرد

# جانشینی ۲۱۳

send another catapult

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

Ufqf bqqukgs fcudrvov

# جدول Vigenerه

- نوعی رمز جانشینی چند الفبایی محسوب می‌شود
- از یک ماتریس ۲۶ در ۲۶ و یک کلید برای رمزگذاری متن استفاده می‌شود
- حروف متوالی کلید، سطر ماتریس و حروف متوالی متن، ستون ماتریس را مشخص می‌کنند.
- کلید معمولاً یک کلمه چندحرفی است که تکرار می‌شود.

M = SEND ANOTHER CATAPULT

K = hail ceaserhailcease

C = z e v o c r o l l v y c i e c t u d x

# Enigma Machine

---

ماشین متحرکی برای رمزنگاری و رمزگشایی **Enigma** □  
استفاده از تعدادی روتور ماشین (الکتریکی-مکانیکی) ■



German military



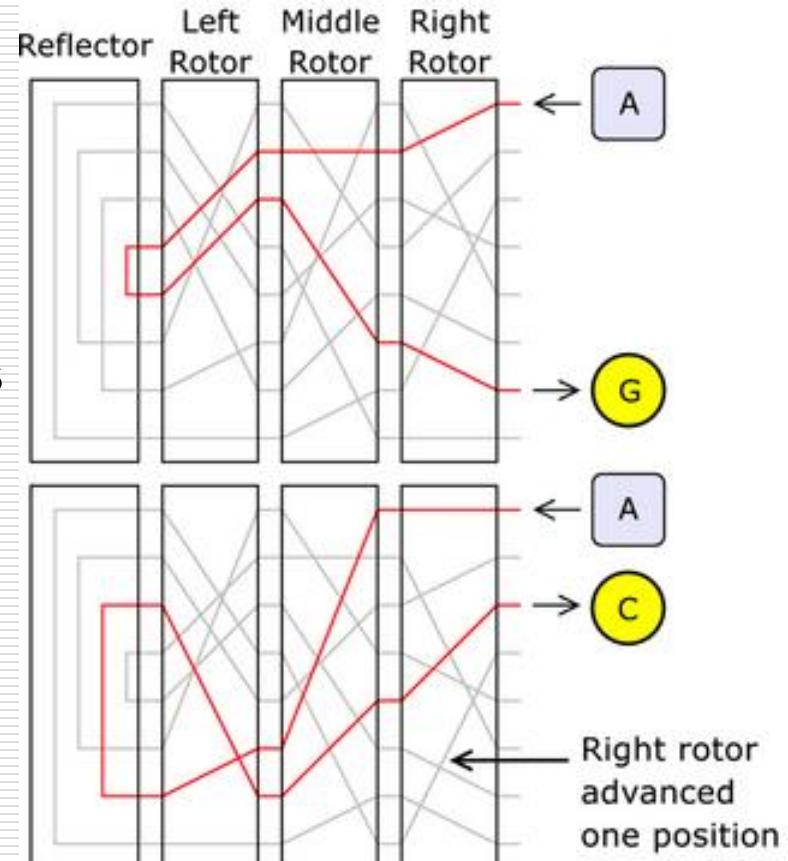
Japan commercial

# Rotor Machines

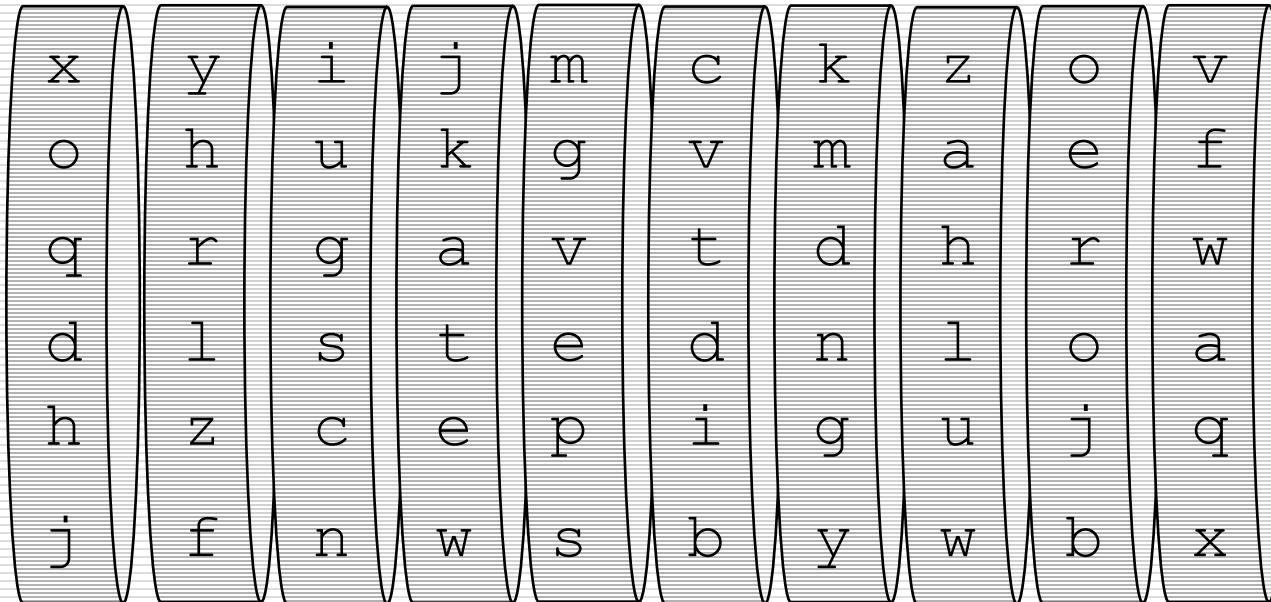
- ماشین روتر یک پیاده سازی الکترونیکی-مکانیکی از رمز چندالفایی محسوب می شود
- در این روش، داده ها از داخل تعدادی سیلندر که در مقابل هم قرار گرفته اند، عبور می کنند.
- به ازای هر حرف از ورودی، سیلندر اول به اندازه یک حرف می چرخد با یک دور گردش کامل هر روتر ، روتر بعدی به اندازه یک حرف جابجا می شود
- دوره تناوب ماشین روتر با افزایش تعداد روتراها افزایش می یابد( $26^n$ )
- آلمان ها اعتقاد داشتند که ماشین روتر طراحی شده توسط آنها، **Enigma**، غیرقابل شکست است، ولی متفقین توانستند رمز آن را کشف کند و بسیاری از اطلاعات سری آنها را فاش کند.

# Enigma Machine

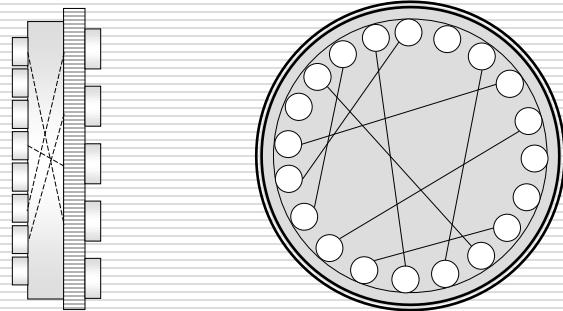
**Enigma encryption for two consecutive letters — current is passed into set of rotors, around the reflector, and back out through the rotors again. Letter A encrypts differently with consecutive key presses, first to G, and then to C. This is because the right hand rotor has stepped, sending the signal on a completely different route.**



# Rotor Machines



Enigma - German Machine  
had 3 rotors



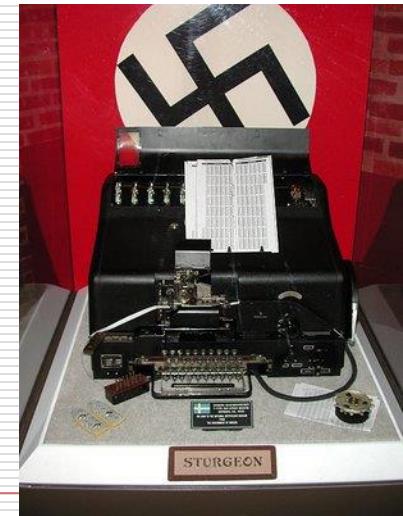
# Enigma

---



# ابزارهای رمزگاری در جنگ جهانی دوم

- A few here
  - Sigaba (*United States*)
  - Typex (*Britain*)
  - Lorenz cipher (*Germany*)
  - Geheimfernenschreiber (*Germany*)
- For more, see
  - <http://w1tp.com/enigma/>



# رمز جایگشتی

---

- جایجایی حروف در متن اصلی بدون تغییر حروف الفبا
- با هدف ایجاد پراکندگی

امکان استفاده ترکیبی از آن با رمز جانشینی

- ایده اساسی مورداستفاده در رمزنگاری متقارن می‌باشد

## مثال (جایگشتی ستونی)

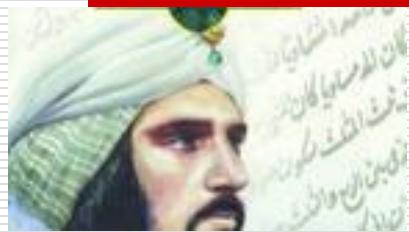
S	E	N	D	*
A	N	O	T	H
E	R	*	C	A
T	A	P	U	L
T	*	*	*	*

- ایده : متن را به صورت سطری بنویسیم و به صورت ستونی بخوانیم

- کلید: تعداد ستونها (در اینجا ۵)
- کلید: می‌توان ترتیب نوشتن ستون‌ها را نیز تغییر داد.

= SAETTENRA\*NO\*P\*DTCU\*\*HAL\*

# تحلیل رمز



نامه‌ای در عربی نوشته، از این‌جهت ممکن است این کتاب را تفسیر اعرابی می‌نامند. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد.

براندۀ دانشگاهی پاریس نوشته شده و میراث اسلامی است.

الخوارزمی از این‌جهت ممکن است این کتاب را تفسیر اعرابی می‌نامند. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد. این کتاب در عربی نوشته شده و محتواهایی از ادب عربی، فلسفه، علم و مذهب دارد.

در قرن سوم هجری، "ابویوسف الکندی"، یکی از دانشمندان جهان اسلام، نخستین کتاب درباره رمز را تالیف کرد.

الکندی که بیش از دویست جلد کتاب در علوم مختلف نوشته است، متولد کوفه بود و بیشتر به قصد رمزگشایی از قرآن کتابی نوشت به نام "رساله در کشف معما".

او در این کتاب، رمزگشایی براساس میزان تکرار نشانه‌ها (بسامد یا فرکانس) را ابداع کرد. برای مثال پرکاربردترین حروف در عربی الف و لام هستند، اما بسامد حرف ج یکدهم آنهاست. بنابراین می‌توان از میزان تکرار نشانه‌ها، حروف را مشخص کرد.

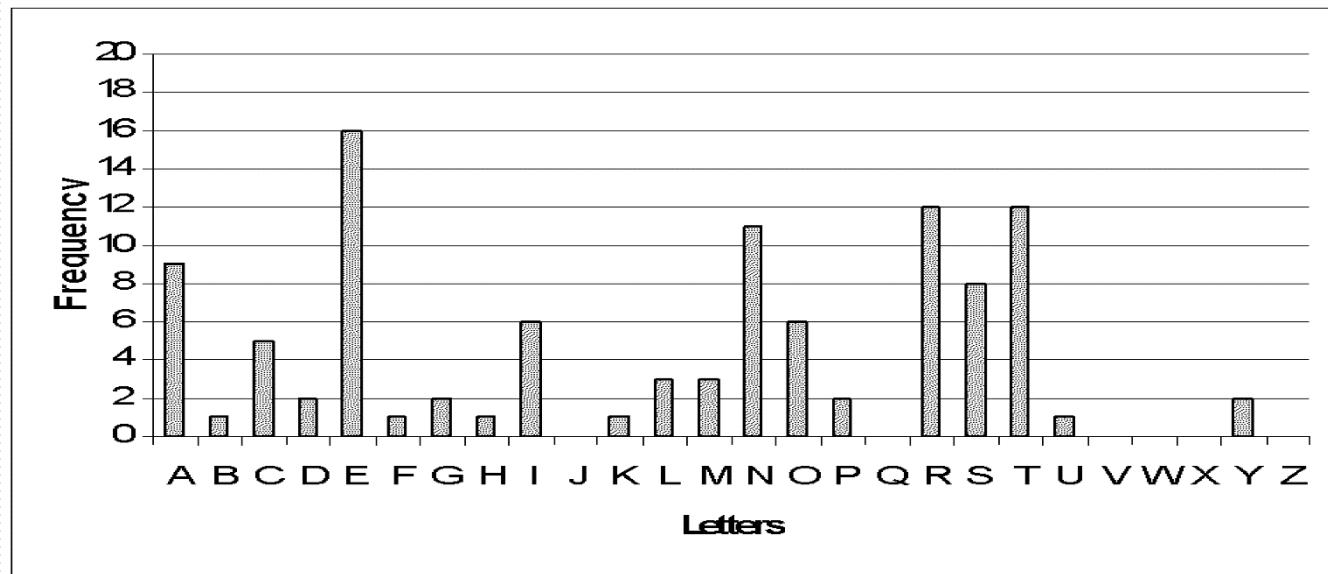
# ایده‌های تحلیل رمز کلاسیک

- فراوانی حروف (etanos...)
- فراوانی ترکیبات حروف (th, nt)
- حروف (تشخیص) ابتدا و انتهای کلمه (th\_\_\_\_, \_\_\_\_nt, \_\_\_\_gh)
- نظم موجود در الفبای زبان
- متند Kasiski : این روش بر مبنای یافتن الگوهای تکراری (عموماً سه حرفی) در متن رمز شده و پیدا کردن طول کلید مورداً استفاده استوار است.
- ایده : فاصله بین دو تکرار از الگوهای تکراری، باید حتماً بر طول کلید مورد استفاده بخشیزدیر باشد.

Brute Force      حملات

# تحليل رمز كلاسيك (مثال)

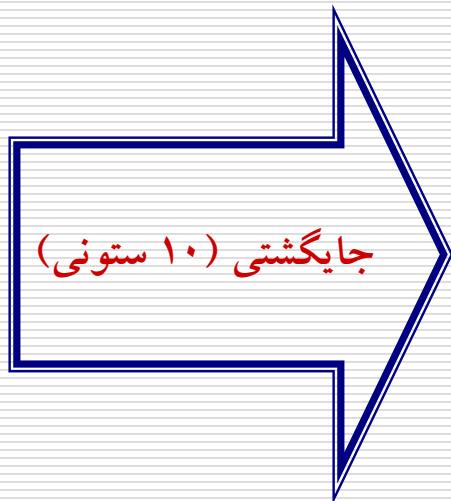
Aerial reconnaissance reports enemy reinforcements estimated at battalion strength entering your sector PD Clarke



فراوانی حروف متن اصلی

# تحليل رمز كلاسيك(مثال)

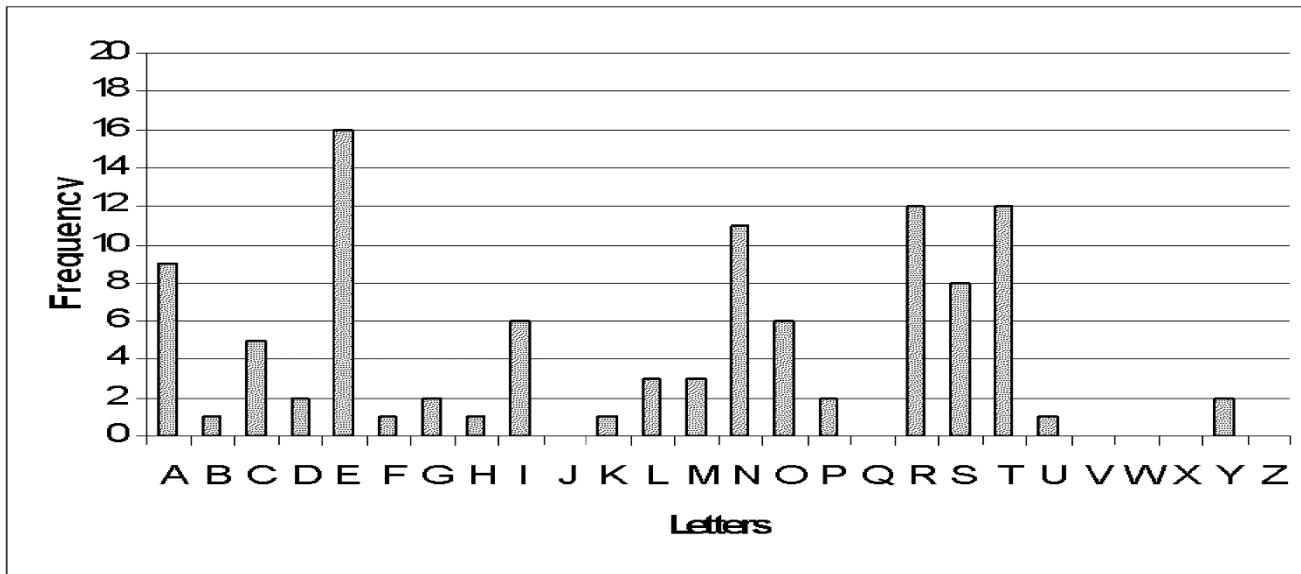
aerialreco  
nnaisance  
reportsene  
myreinforc  
ementsesti  
matedatbat  
talionstre  
ngthenteri  
ngyoursect  
orPDClarke



ANRMEMTNNO  
ENEYMAAGGR  
RAPRETLTYP  
IIOENEIHOD  
ASRITDOEUC  
LSTNSANNRL  
RASFETSTSS  
ENEOSBTEER  
CCNRTARRCK  
OEECITEITE

# تحليل رمز كلاسيك(مثال)

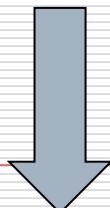
**ANRMEMTNNOENEYMAAGGRRAPRETLTYPPIOENE  
IHODASRITDOEUCLSTNSANNRLRASFETSTSSEN  
EOSBTEERCCNRTARRCKOEECITEITE**



فراوانی حروف متن رمز شده

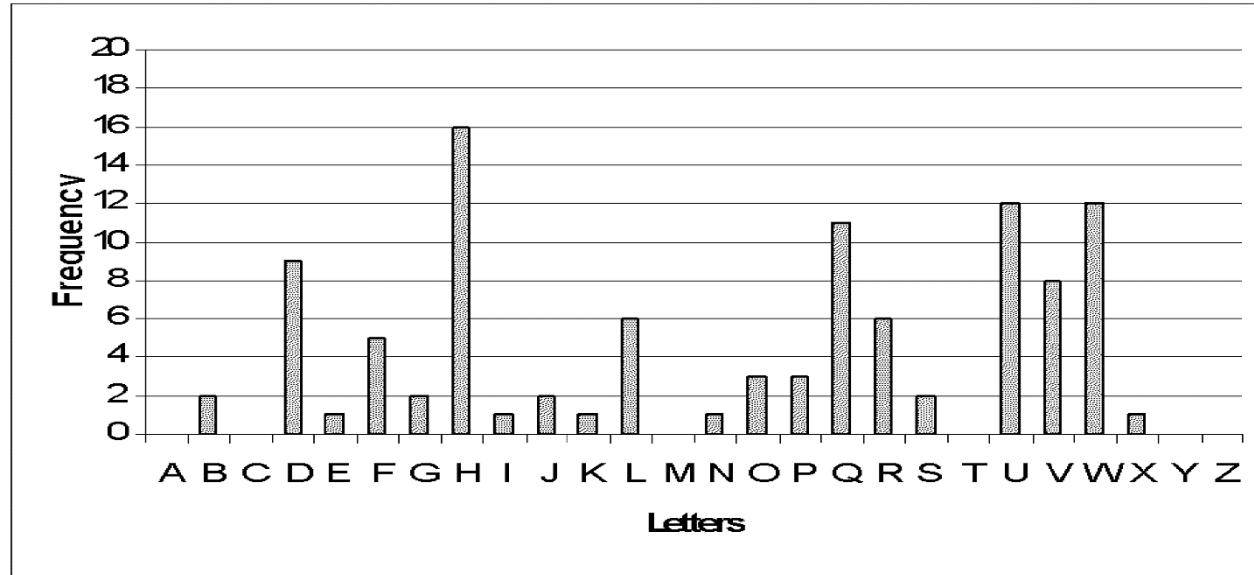
# تحلیل رمز کلاسیک

- از مقایسه نمودارهای قبلی می‌توان فهمید در **رمزنگاری جایگشتی** :
  - فراوانی حروف در متن رمزشده تفاوتی با فراوانی متن اصلی ندارد.
  - تحلیلگر نمی‌تواند از نمودارهای فراوانی استفاده کند.
- ولی در جایگزینی تک الفبایی این امکان وجود دارد(مطابق شکل اسلاید بعدی)
  - با مقایسه این نمودار با نمودار استاندارد فراوانی حروف، می‌توان تناظر احتمالی حروف را پیدا کرد.



# تحليل رمز كلاسيك (مثال)

DHULDOUHF RQQLVVDQFH UHSRUWVHQHPBUH . . .



فراوانی حروف متن رمز شده (تك الفبايي)

# فهرست مطالب

- تعاریف
- رمزهای کلاسیک
- الگوریتم‌های رمزهای متقارن و رمزهای قطعه‌ای
- استانداردهای رمزگذاری آمریکا
- الگوریتم‌های دیگر رمزنگاری
- استفاده از رمزهای قطعه‌ای
- مدهای کاری رمزهای قطعه‌ای
- واژه نامه
- پیوست ۱ : DES

# رمزگذاری کلاسیک-رمزگذاری مدرن

---

- روش‌های رمزگذاری مدرن، علاوه بر بر اعمال جابجایی و جایگشت از توابع ساده مانند **XOR** استفاده می‌شود.
- مجموعه اعمال فوق طی مراحل متوالی روی متن اولیه اعمال می‌شوند.
- تکنیک بکارگرفته شده در **Rotor Machine** ها الهام بخش روش‌های رمزگذاری مدرن بوده است

# تابع رمزنگاری کامل (One-Time Pad)

- ایده : برای رمزکردن یک داده به طول  $n$  کلیدی به طول  $n$  هزینه کنیم.
- در این صورت به ازای هر  $M$  و  $C$  داریم:
$$P(M|C) = P(M)$$
- یعنی داشتن هر تعداد متن نمونه رمزشده کمکی به تحلیلگر نمی کند.
- امنیت این روش به تصادفی بودن کلید بستگی دارد.

# تابع رمزنگاری کامل (One-Time Pad)

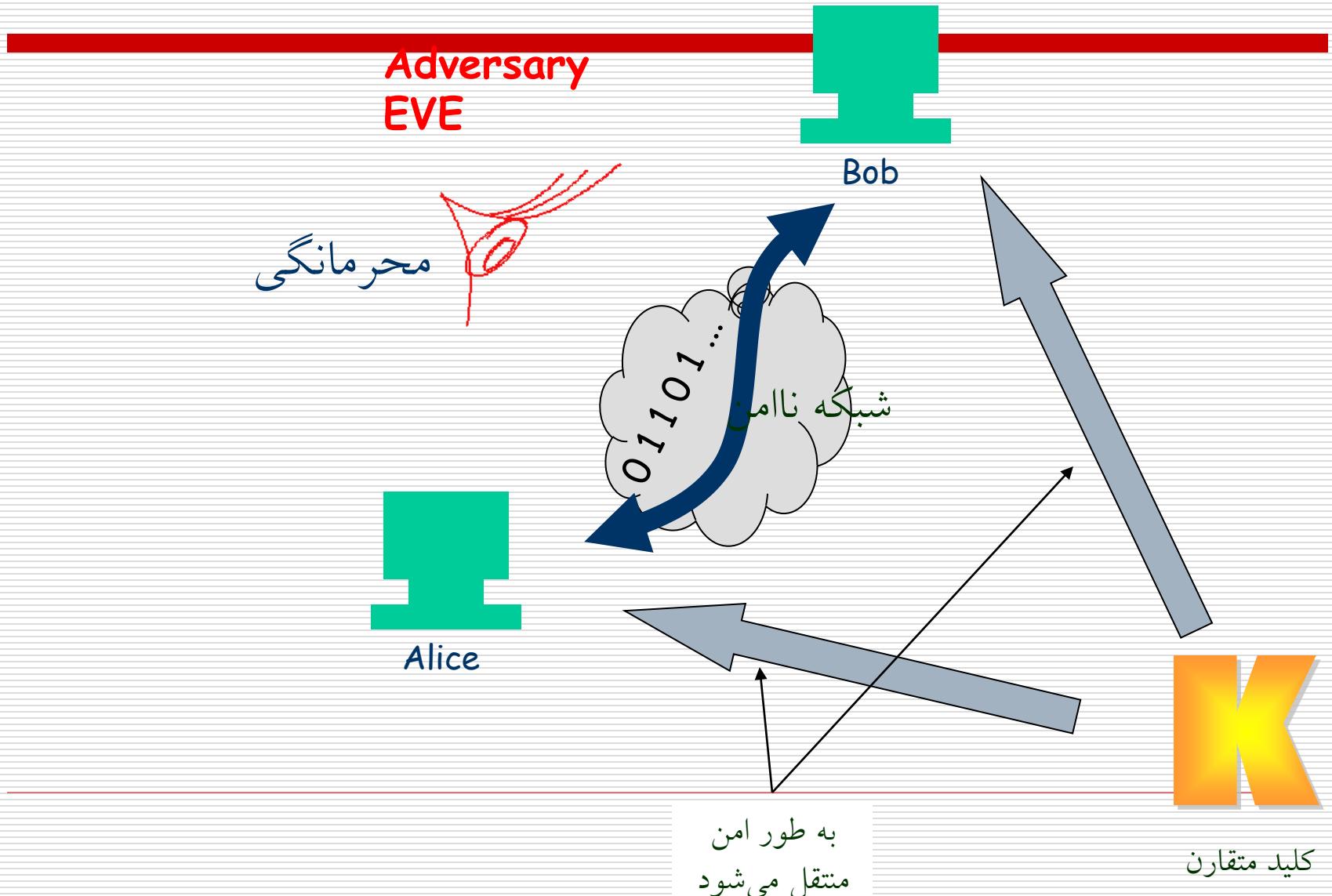
- در عمل استفاده از چنین روشی مقدور نیست
- تولید کلید تصادفی به حجم بالا از نظر عملی دشوار است.
- توزیع امن کلید : اگر بتوانیم کانال امنی برای توزیع کلیدی با این حجم پیدا کنیم، آیا بهتر نیست از همین کانال برای انتقال داده اصلی استفاده کنیم؟!
- در عمل از روش‌هایی استفاده می‌کنیم که شکستن رمز را برای تحلیلگر با توجه به تکنولوژیهای موجود و در زمان محدود غیرممکن سازد.

# رمزنگاری متقارن

برای تبادل این  
اطلاعات مخفی  
نیاز به کانال امن  
داریم.

- دو طرف به دنبال برقراری ارتباط محرمانه هستند.
- ارتباط بر روی محیط ناامن انجام می‌پذیرد.
- طرفین پیامهای خود را رمز می‌کنند.
- در رمزنگاری متقارن، الگوریتم‌های رمزنگاری آنها تابع اطلاعات مخفی است که فقط طرفین از آنها مطلع می‌باشند.

کلید مخفی



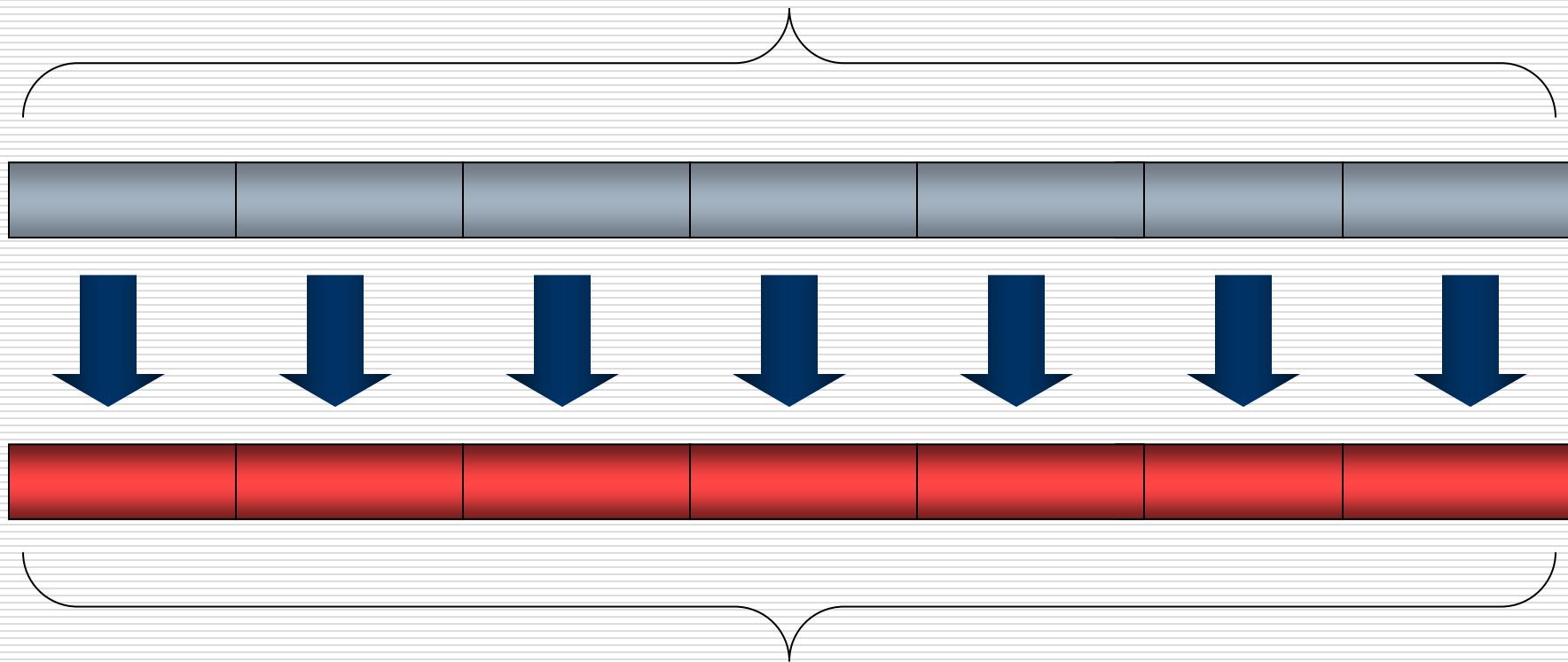
# الگوریتم‌های رمزهای متقارن

---

- رمزهای متقارن را می‌توان با دو روش عمدۀ تولید کرد
  - رمزهای قطعه‌ای
    - پردازش پیغام‌ها به صورت قطعه به قطعه
    - سایز متعارف مود استفاده برای قطعات ۶۴، ۱۲۸ یا ۲۵۶ بیتی است
  - رمزهای دنباله‌ای
    - پردازش پیغام‌ها به صورت پیوسته

# رمزهای قطعه‌ای

متن واضح ( تقسیم شده به قطعات )



قطعات خروجی

# اصل رمزهای قطعه‌ای

---

- 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 ساده‌ای همچون جایگزینی و جایگشت استوار است.
-

# استانداردهای رمزهای قطعه‌ای آمریکا

---

□ رمزهای قطعه‌ای استاندارد

■ استاندارد رمزگذاری داده DES

■ استاندارد رمزگذاری پیشرفته AES

□ تحت نظارت

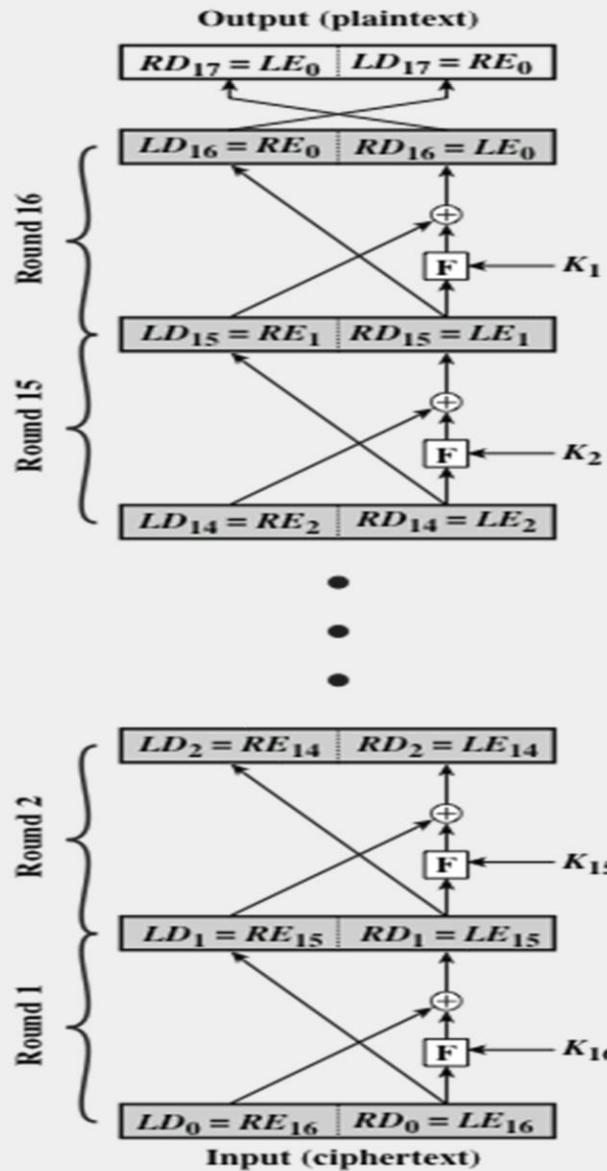
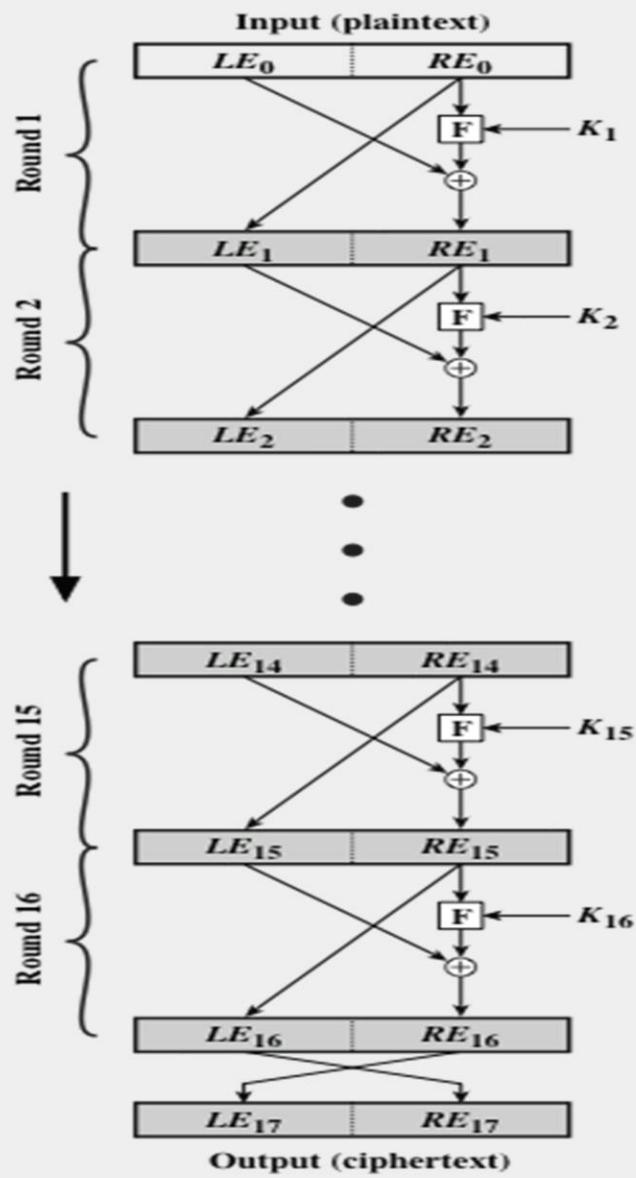
**National Institute of Science and Technology (NIST)**

---

# ساختار رمزهای فیستل

---

□ معمولاً الگوریتم‌های رمزنگاری از ساختاری تبعیت می‌کنند  
که توسط فیستل در سال 1973 در **IBM** پیشنهاد شد.



**Figure 2.2 Feistel Encryption and Decryption (16 rounds)**

# عوامل موثر در طراحی رمژهای فیستل

---

- رمژهای فیستل به عوامل و پارامترهای زیر بستگی دارند:
  - طول قطعه (بلوک)
  - طول کلید
  - تعداد دورها
  - الگوریتم تولید زیرکلیدها
- هر چه پیچیده تر باشد، تحلیل هم سخت تر می شود.
- سرعت رمزنگاری/رمزگشایی
- تابع دور (**Round function**)
- سادگی تحلیل

# Feistel Cipher Design Elements

- Larger block sizes mean greater security but reduced encryption/decryption speed

## Block size

## Key size

- Larger key size means greater security but may decrease encryption/decryption speed

- The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security

## Number of rounds

- Greater complexity generally means greater resistance to cryptanalysis

## Round function

## Fast software encryption/decription

- In many cases, encryption is embedded in applications or utility functions in such a way as to preclude a hardware implementation; accordingly, the seed of execution of the algorithm becomes a concern

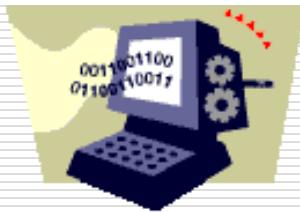
- If the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a higher level of assurance as to its strength

## Subkey generation algorithm

- Greater complexity in this algorithm should lead to greater difficulty of cryptanalysis

## Ease of analysis

# استاندارد رمزگذاری داده DES



مرور

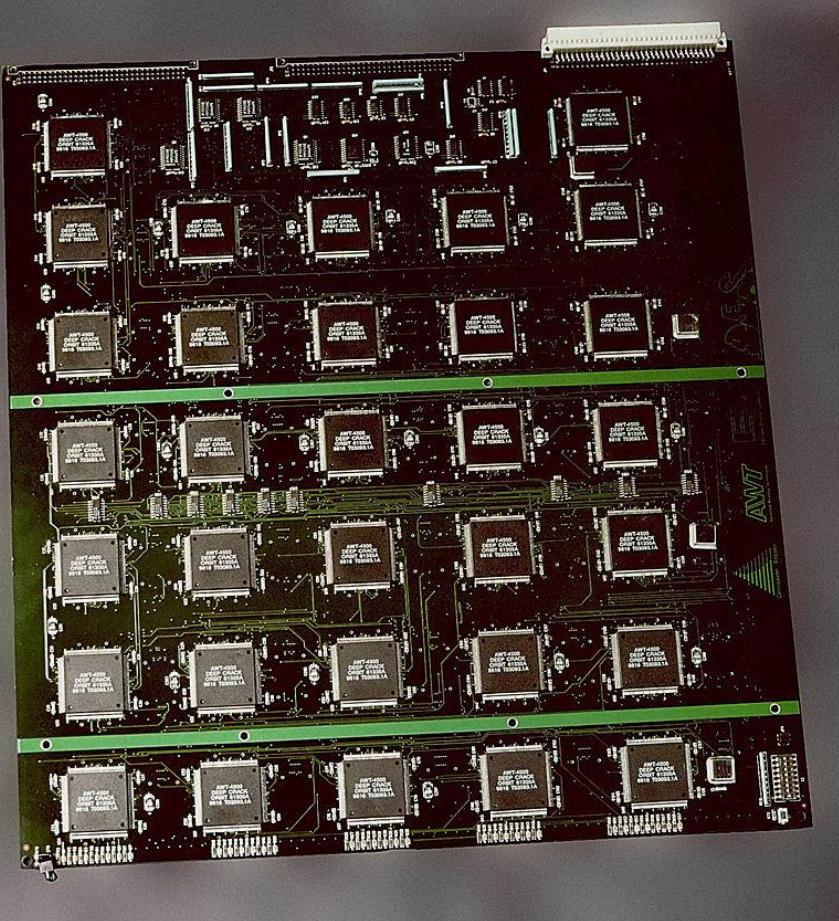
- در سال ۱۹۷۴ توسط **IBM** تولید شد
- پس از انجام تغییراتی توسط **NSA**, در سال ۱۹۷۶ **NIST** آن را پذیرفت.
- اساس الگوریتم ترکیبی از عملیات جایگزینی و جایگشت می‌باشد.
- مشخصات:
  - طول کلید ۵۶ بیت
  - طول قطعه‌های ورودی و خروجی : ۶۴ بیت
  - تعداد دورها: ۱۶ دور
- الگوریتم‌های رمزگذاری و رمزگشایی عمومی هستند، ولی مبانی ریاضی و اصول طراحی آنها فاش نشد.
- در گذشته بسیار پر استفاده بود.
- نام دیگر آن **DEA** است. (الگوریتم به نام **DEA** و استاندارد مربوط به نام **DES**)

# DES امن نیست!

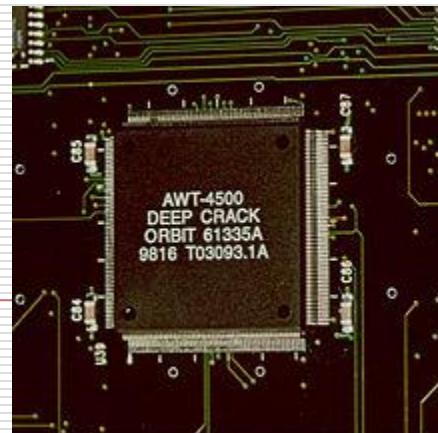
---

- 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.
- منظور از آزمون جامع فضای کلید همان جستجوی کامل کلید با استفاده از روش **Brute Force** می‌باشد.
- به الگوریتم‌های امن تر با طول کلید بالاتر نیاز داریم.
- علاوه بر این DES طراحی شفاف و روشن ندارد.

# DES Cracker

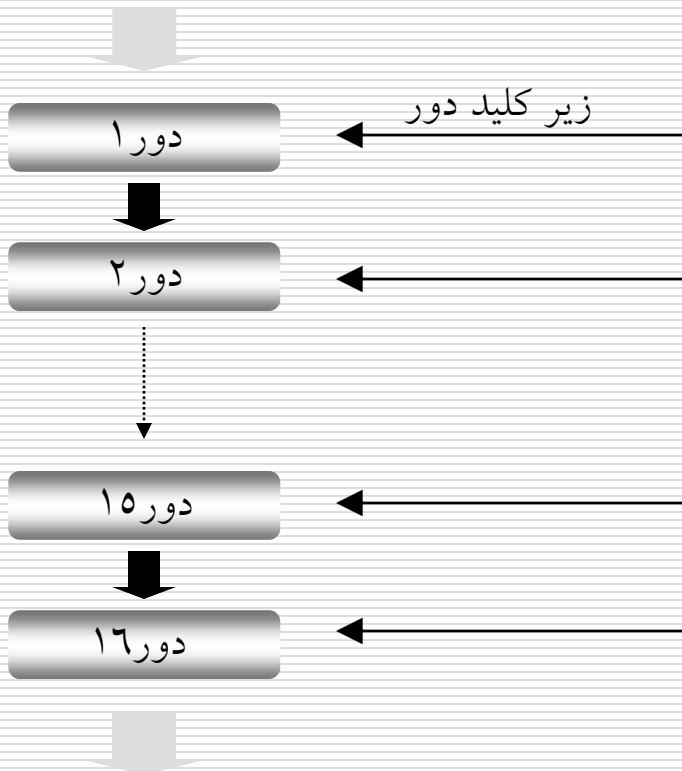


- در سال 1998 موسسه (EFF) مدار خاص حمله فضای جامع به DES را ساخت.
- دارای 1856 چیپ خاص منظوره
- قیمت کمتر از \$250,000
- در کمتر از 56 ساعت DES شکسته شد.



# استاندارد رمزگذاری داده DES

قطعه ۶۴ بیتی متن واضح

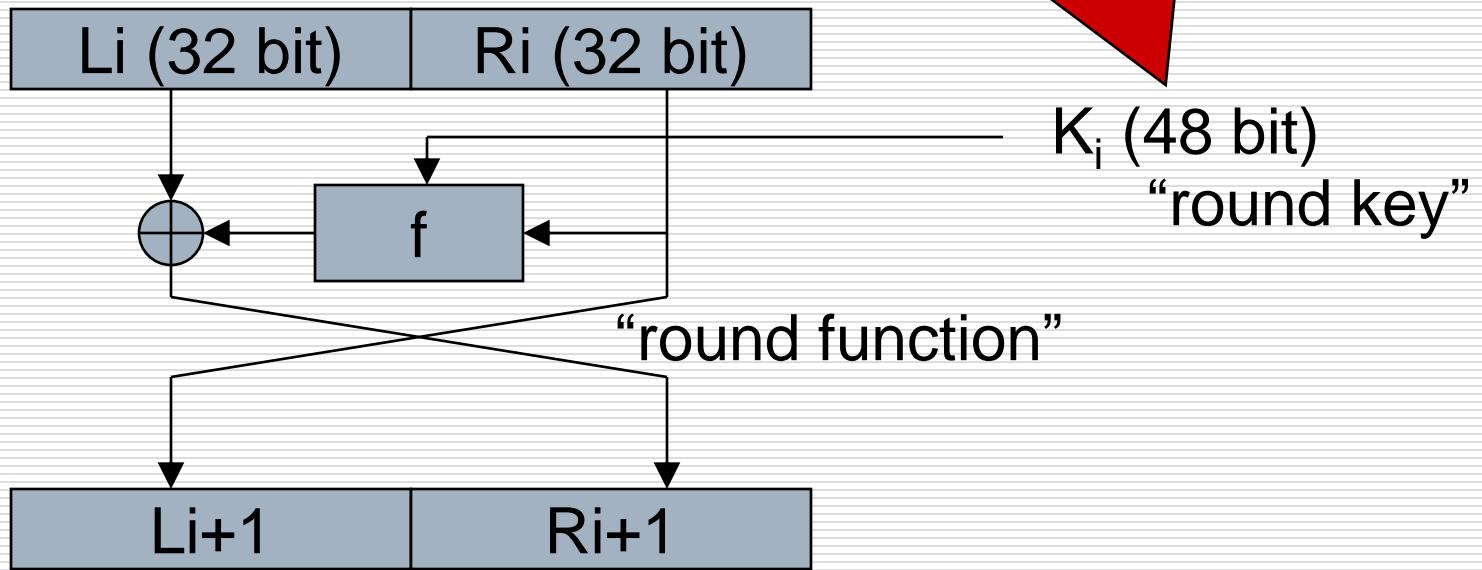


تولید زیر کلیدهای ۴۸  
بیتی از کلید اصلی ۵۶  
بیتی برای هر دور

کلید ۵۶ بیتی

# یک دور از DES

توسط زمانبندی کلید  
تولید می‌شود.



# یک دور از DES

اعمال انجام شده در هر دور: □

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

جزئیات بیشتر الگوریتم DES در پیوست 1 ■

# DES میزان توانمندی

اندازه کلید □

۵۶ بیت دارای کل فضای حالت  $2^{56} = 7.2 * 10^{16}$  ■

حمله آزمون جامع هرچند مشکل، ولی امکانپذیر است ■

آخرین گزارش ثبت شده در سال ۱۹۹۹ نشان از کشف کلید تنها در عرض ۲۲ ساعت داده‌اند! □

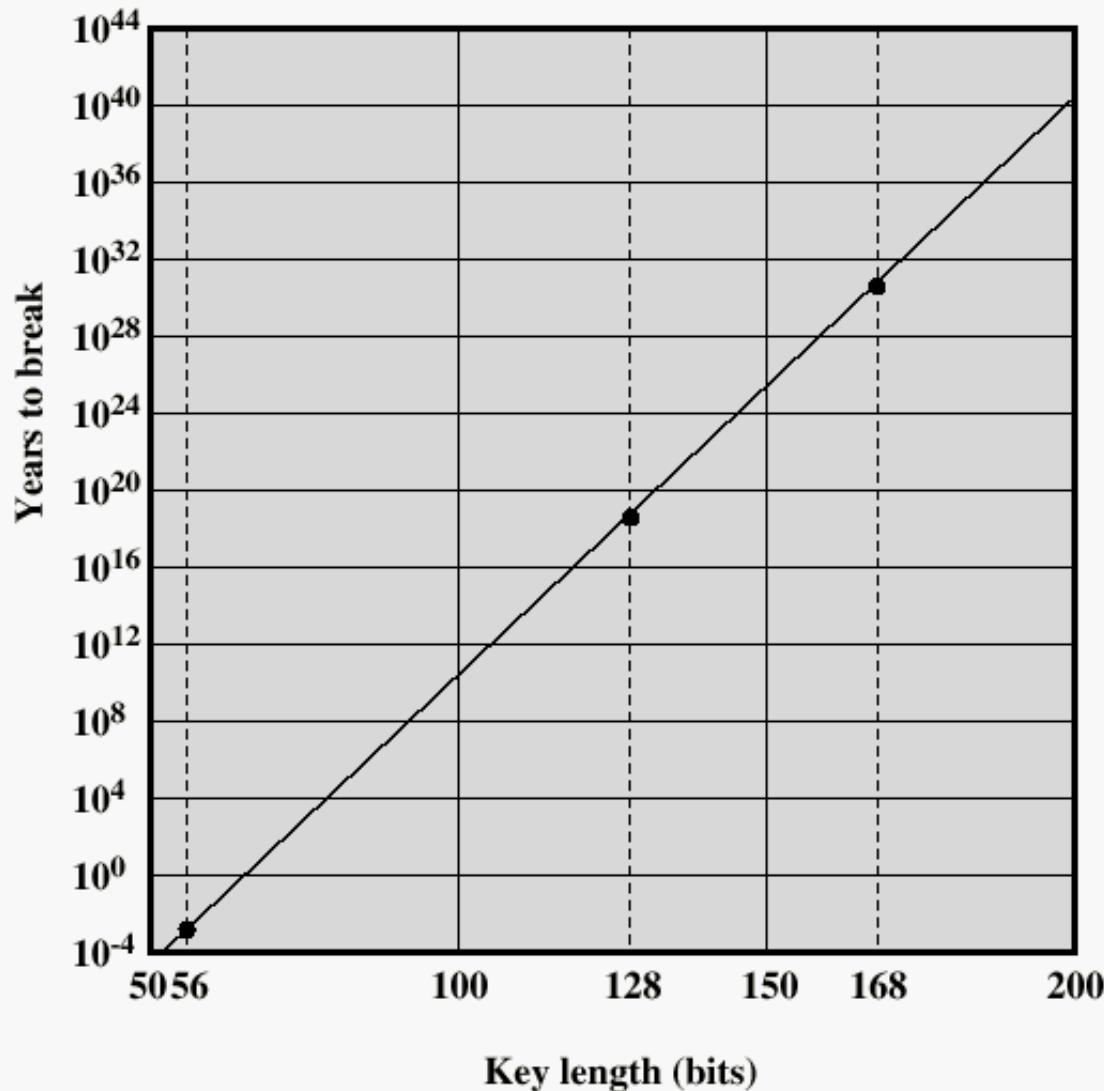
حمله زمانی □

پیاده سازی DES را مورد هدف قرار می‌دهند ■

الگوریتم برای ورودی‌های مختلف در زمانهای متفاوت پاسخ می‌دهد ■

بیشتر در کارتهای هوشمند مشکل زا می‌شوند ■

# Time to break a code ( $10^6$ decryptions/ $\mu\text{s}$ )



# حمله تحلیلی به DES

- عموما حملات آماری هستند
- از ساختار داخلی **DES** استفاده می کنند
- تشخیص همه یا بعضی از بیت های کلید میانی
- جستجوی کامل روی بقیه بیت ها
- شامل
  - تحلیل تفاضلی
  - تحلیل خطی

# فهرست مطالب

- تعاریف
- رمزهای کلاسیک
- الگوریتم‌های رمزهای متقارن و رمزهای قطعه‌ای
- استانداردهای رمزگذاری آمریکا
- الگوریتم‌های دیگر رمزنگاری
- استفاده از رمزهای قطعه‌ای
- مدهای کاری رمزهای قطعه‌ای
- واژه نامه
- پیوست ۱ : DES



# TDEA یا 3DES

مسئله:

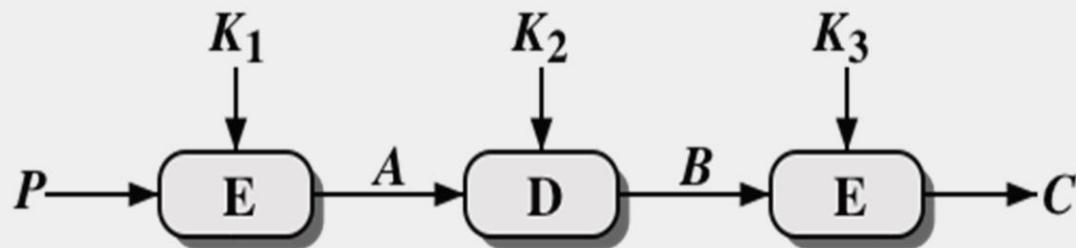
آسیب پذیری **DES** در مقابل حمله آزمون جامع

راه حل:

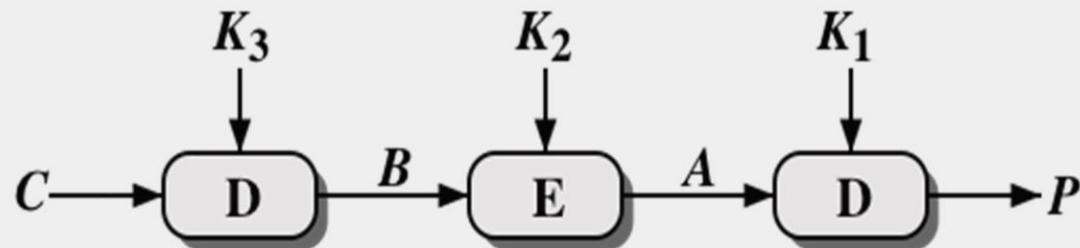
استفاده از الگوریتم های رمزنگاری دیگر

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

# TDEA ⋮ 3DES



(a) Encryption



$$C = E_{K_3}[D_{K_2}[E_{K_1}[P]]]$$

# 3DES

## استفاده از الگوریتم **3DES** □

- از دو مرحله رمزنگاری و یک مرحله رمزگشایی با سه کلید مجزا استفاده می‌شود
- فضای کلید به ۱۶۸ بیت گسترش می‌یابد
- در صورت استفاده از یک کلید یکسان، **DES** با **3DES** مطابقت می‌کند
- نسبت به الگوریتم‌های دیگر مانند **RC5** و **Blowfish** سرعت کمتری دارد
- تا کنون حمله‌ای علیه آن گزارش نشده است
- مشکل اصلی **3DES** و به طور کلی **DES** سختی پیاده سازی نرم‌افزاری و عدم کارآیی آن است.

# AES استاندارد رمزگذاری پیشرفته

---

□ **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. (خوشبختانه!)

□ در سال ۲۰۰۰ رایندال (**Rijndael**) به عنوان برنده اعلام شد

■ استاندارد جدید تحت عنوان استاندار رمزگذاری پیشرفته **AES** مورد قبول واقع شد.

---

# AES فینالیست های مسابقه

---

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

منتخب!



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

*A Performance Comparison of the Five AES Finalists*  
*B. Schneier and D. Whiting*

# مشخصات استاندارد رمزگذاری پیشرفته AES

---

**FIPS PUB 197**  استاندارد

طول کلید ۱۲۸، ۱۹۲ و ۲۵۶ بیت

طول قطعه‌های ورودی و خروجی : ۱۲۸ بیت

تعداد دورها به طول کلید و نیز طول قطعه بستگی دارد.  
 برای ۱۲۸ بیت: ۹ دور

---

# نحوه کار AES-128

---

- الگوریتم زمان بندی کلید نقش تهیه کلید برای هر دور بر اساس کلید اصلی را بر عهده دارد.
  - متن واضح ۱۲۸ بیتی به شکل یک ماتریس حالت  $4 \times 4$  در می آید.
  - هر درایه یک بایت از متن واضح را نشان می دهد
  - این ماتریس در انتهای مولد متن رمز است.
-

# نحوه کار AES-128

- در هر دور ۴ عمل بر روی ماتریس حالت اعمال می‌شود.
- جایگزینی بایتها : جایگزینی درایه های ماتریس حالت با استفاده از یک **S-box**
- جابجایی سط्रی
- ترکیب ستونها: ترکیب خطی ستونها با استفاده از ضرب ماتریسی
- اضافه نمودن کلید دور: جمع مبنای دو ماتریس حالت با کلید دور

# s-box

- نوعی تابع غیر خطی محسوب می‌شود
- توسط یک جدول پیاده سازی می‌شود.
- در آن مصالحه‌ای بین کارایی و امنیت برقرار است:
  - جدول بزرگ: الگوریتم قویتر
  - جدول کوچک: پیاده سازی ساده‌تر
- ورودی تابع سطر و ستون درایه جدول را معین کرده و مقدار ذخیره شده در این درایه خروجی تابع است.

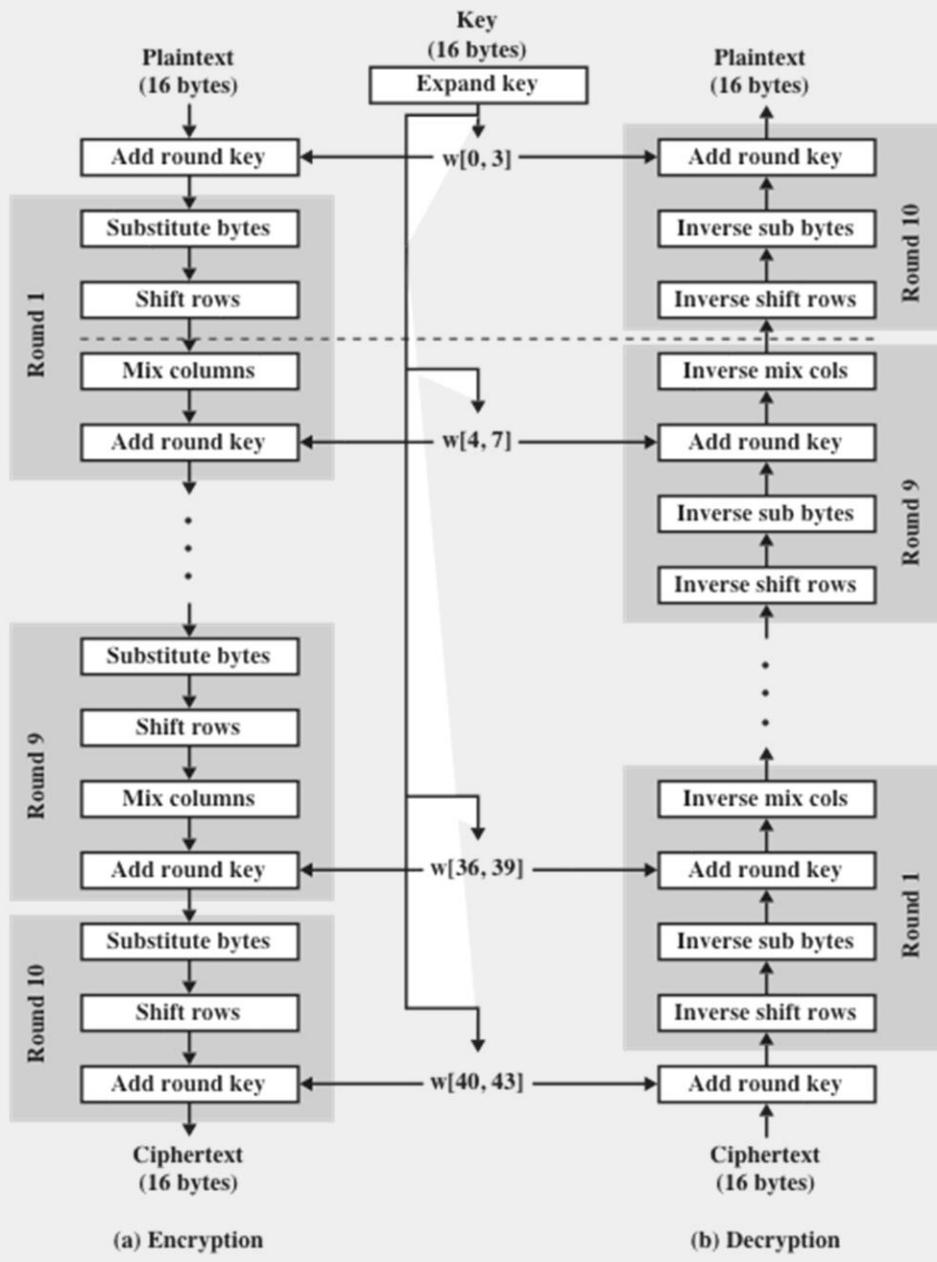


Figure 2.4 AES Encryption and Decryption

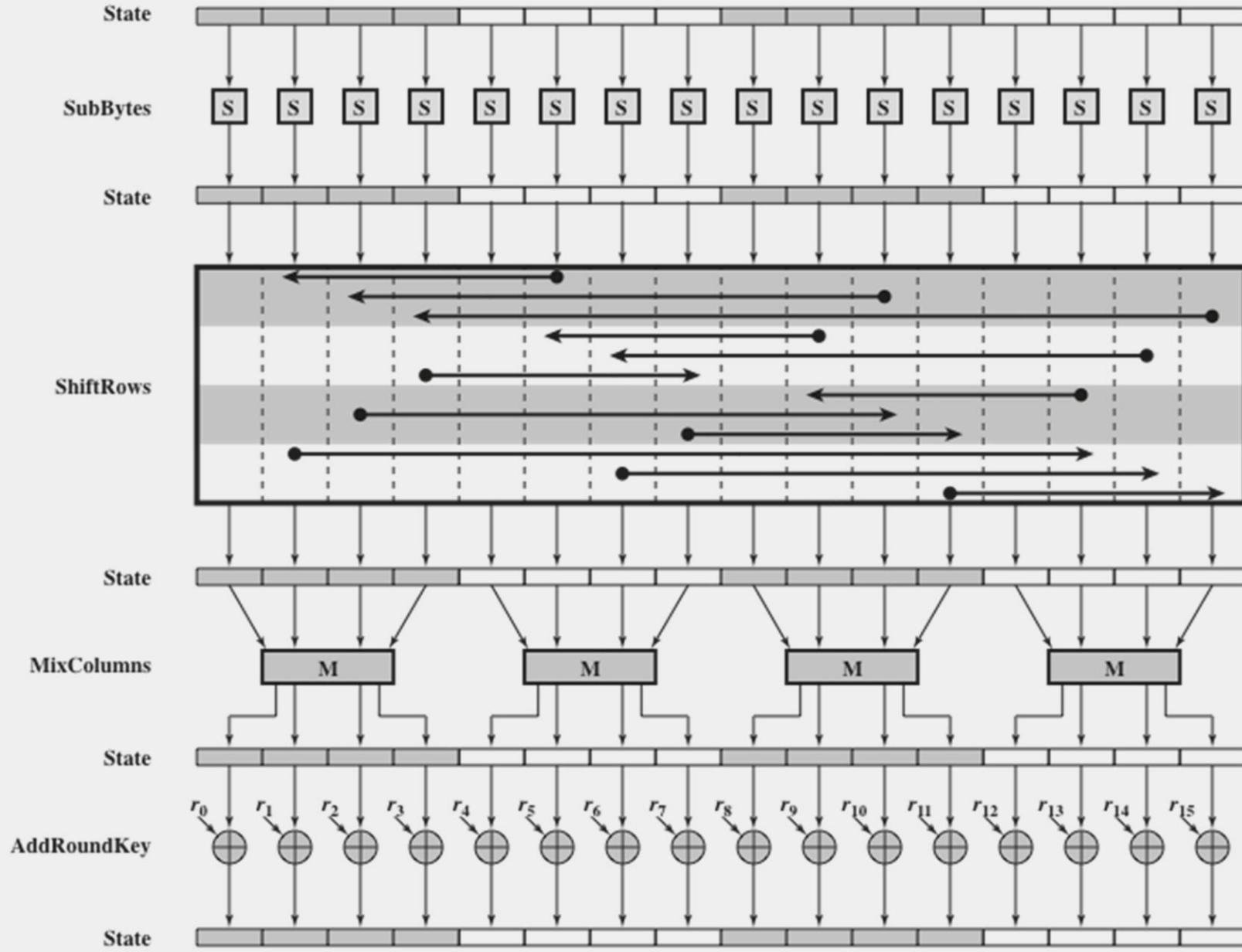


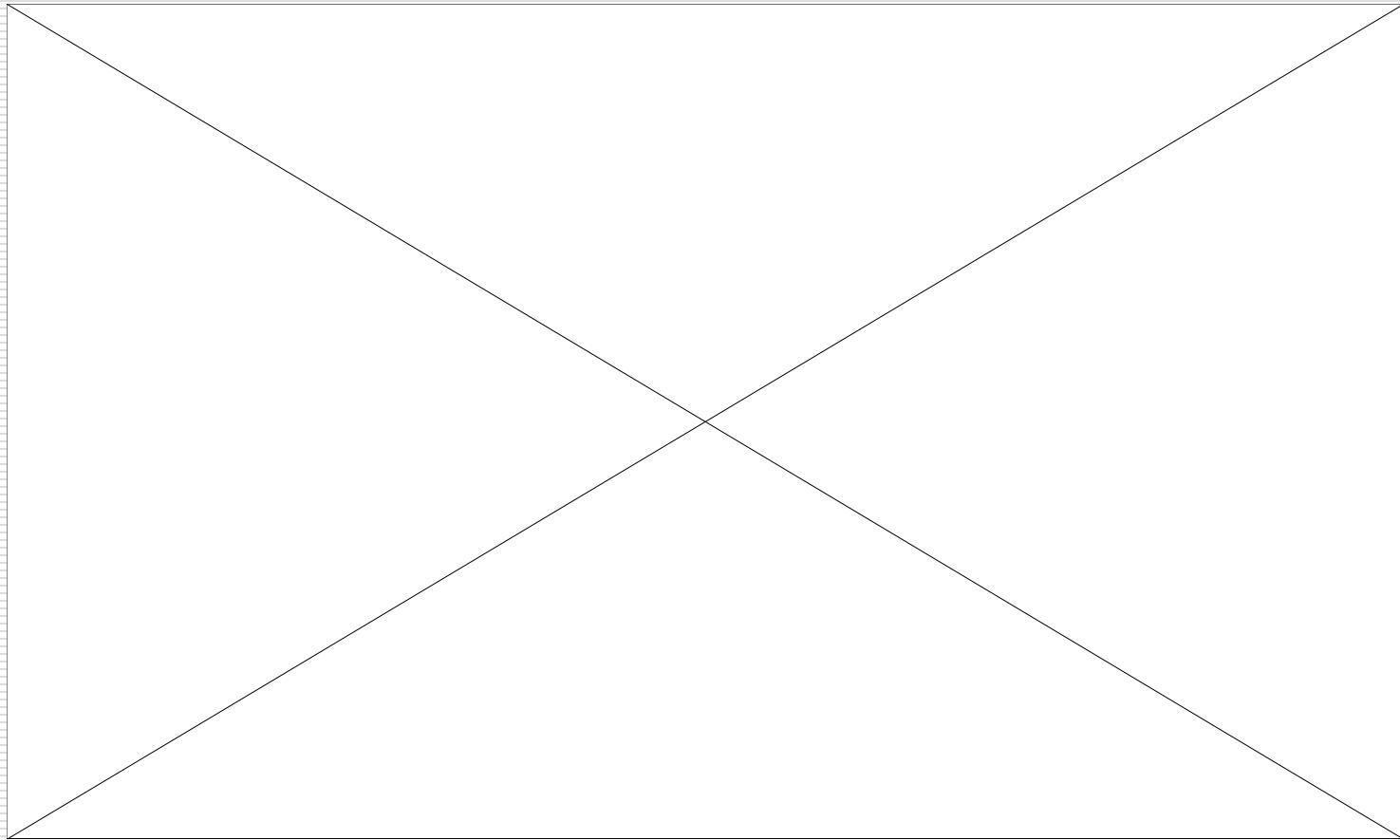
Figure 2.5 AES Encryption Round

# Rijndael

---

- مراحل انجام الگوریتم **Rijndael** را در قالب یک فلش بررسی می‌کنیم.
  
- از آدرس زیر قابل دریافت می‌باشد:  
<http://www.esat.kuleuven.ac.be/~rijmen/rijndael/>
  
- فایل **Flash** باید در شاخه اسلاید قرار داشته باشد.

# Rijndael



# AES امنیت

---

- کماکان در حال بررسی
- 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  $2^{55}$  کلید را امتحان می‌کند. این ماشین کلید AES را در  $149 \times 10^{12}$  سال بازیابی می‌نماید.

# مقایسه سه الگوریتم رمزگاری متقاض

	DES	Triple DES	AES
<b>Plaintext block size (bits)</b>	64	64	128
<b>Ciphertext block size (bits)</b>	64	64	128
<b>Key size (bits)</b>	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard

AES = Advanced Encryption Standard

# متوسط زمان جستجوی کامل فضای کلید

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at $10^9$ decryptions/s	Time Required at $10^{13}$ decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55} \text{ ns} = 1.125 \text{ years}$	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127} \text{ ns} = 5.3 \times 10^{21}$ years	$5.3 \times 10^{17} \text{ years}$
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167} \text{ ns} = 5.8 \times 10^{33}$ years	$5.8 \times 10^{29} \text{ years}$
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191} \text{ ns} = 9.8 \times 10^{40}$ years	$9.8 \times 10^{36} \text{ years}$
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255} \text{ ns} = 1.8 \times 10^{60}$ years	$1.8 \times 10^{56} \text{ years}$

---

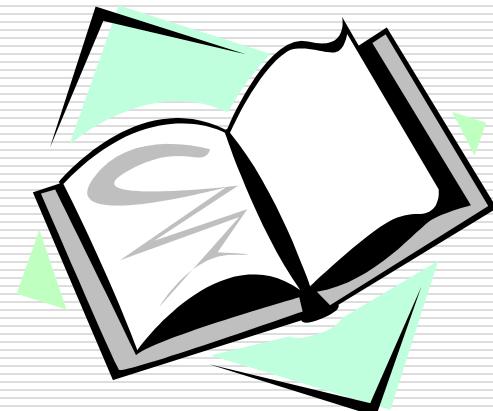
# AES مطالعه مراجع

---

برای اطلاعات بیشتر به آدرس‌های زیر رجوع کنید.

<http://www.nist.gov/aes>

<http://www.esat.kuleuven.ac.be/~rijmen/rijndael>



# مقایسه سرعت الگوریتم‌ها



Algorithm/Mode	Clocks/Byte	Setup time (mSec)
DES/CTR	54.7	15320
Twofish/CTR	29.4	14121
AES/CTR (128-bit key)	12.6	1277
RC6/CTR	17.3	5128

Source: <https://www.cryptopp.com/benchmarks.html>

# فهرست مطالب

- تعاریف
- رمزهای کلاسیک
- الگوریتم‌های رمزهای متقارن و رمزهای قطعه‌ای
- استانداردهای رمزگذاری آمریکا
- الگوریتم‌های دیگر رمزنگاری
- استفاده از رمزهای قطعه‌ای
- مدهای کاری رمزهای قطعه‌ای
- واژه نامه
- پیوست ۱ : DES
- پیوست ۲ : 3DES, IDEA, Blowfish, RC5, CAST-128

## استفاده از رمزهای قطعه‌ای

---

- رمزهای قطعه‌ای به طور مستقل امنیت زیادی را به ارمغان نمی‌آورند. بلکه باید در مدهای کاری مناسب مورد استفاده قرار گیرند
  
- رمزهای قطعه‌ای به عنوان اجزای سازنده الگوریتم‌های رمز نگاری استفاده می‌شوند.

## استفاده از رمزهای قطعه‌ای - ۲

- فرض کنیم یک رمز قطعه‌ای امن داریم. چگونه از آن برای رسیدن به اهداف خود بھر جوییم؟
- مساله اساسی: در برخی موارد علی‌رغم بھر برداری از عناصر مرغوب، کیفیت نهایی دلخواه نیست.
- مثال:
  - ساختمان ضعیف با وجود استفاده از مصالح قوی
  - پوشک نامرغوب با وجود استفاده از پارچه‌های مرغوب
  - غذای نا مناسب با وجود استفاده از مواد اولیه با کیفیت
- در ادامه خواهیم دید مدهای کاری که متن‌های مشابه را به متن‌های رمزشده یکسان تبدیل می‌کنند، امن نیستند. صرف نظر از رمز قطعه‌ای مورد استفاده!

# وضعيت ايده آل

- ساختار الگوريتم رمز نگاري متقارن(مد کاري) به گونه اي باشد که قابلیت های عناصر سازنده خود (رمزهای قطعه ای) را به ارت بيرد.
- يعني با اطمینان از رمزهای قطعه ای، بتوانيم از الگوريتم رمز نگاري نيز مطمئن شويم.



# فهرست مطالب

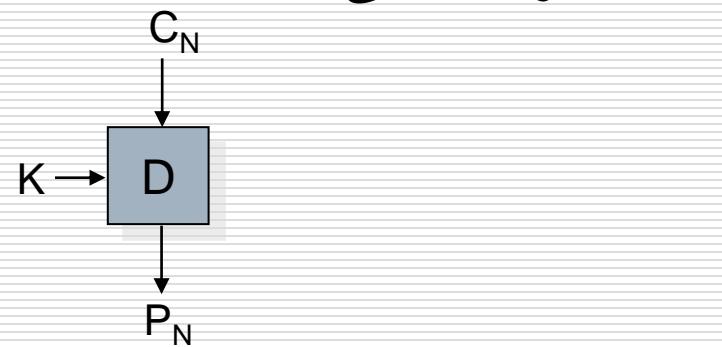
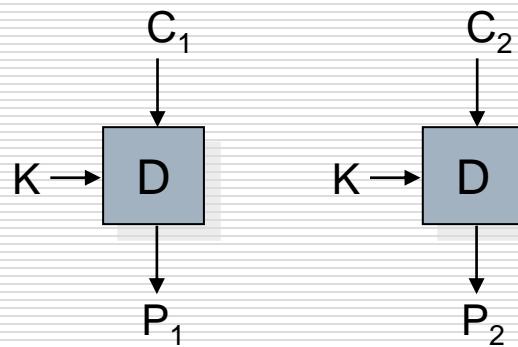
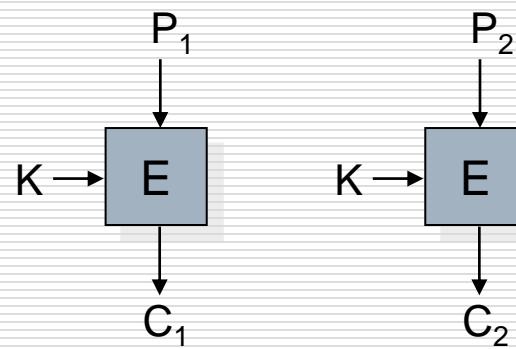
---

- الگوریتم‌های رمزهای متقارن و رمزهای قطعه‌ای
  - استانداردهای رمزگذاری آمریکا
  - الگوریتم‌های دیگر رمزنگاری
  - استفاده از رمزهای قطعه‌ای
  - مدھای کاری رمزهای قطعه‌ای
  - لغت نامه
- پیوست ۱: DES**   
**پیوست ۲: IDEA, Blowfish, RC5, CAST-128**

# مدھای کاری رمزهای قطعه ای

- امروزه مدھای کاری با توجه به امنیت قابل اثبات طراحی می شوند.
- مدھای کاری می توانند از رمزهای قطعه ای **CAST-128, DES, AES, ...** استفاده کنند
- برخی مدھای کاری پراهمیت عبارتند از :
  - **ECB: Electronic Code Book**
  - **CBC: Cipher Block Chaining**
  - **CTR: Counter Mode**
  - **CFB: Cipher Feed Back**
  - **OFB: Output Feed Back**

# ECB مد کاری



# بررسی مد کاری ECB

---

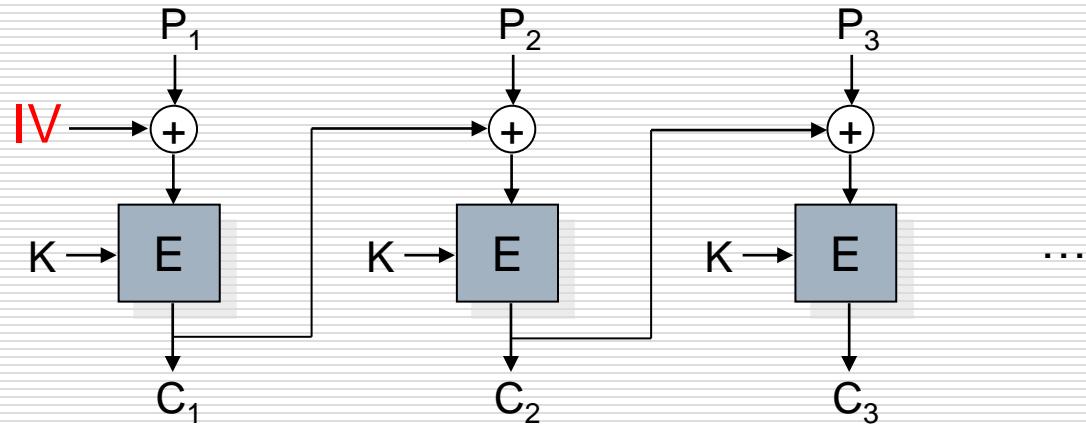
- اشکال اساسی: هر متن واضح به ازای کلید ثابت همیشه به یک متن رمز شده نگاشته می‌شود.
- دشمن می‌تواند دریابد که پیامهای یکسان ارسال شده‌اند.

این مد امن نیست حتی اگر از یک رمز قطعه‌ای قوی استفاده کنیم.

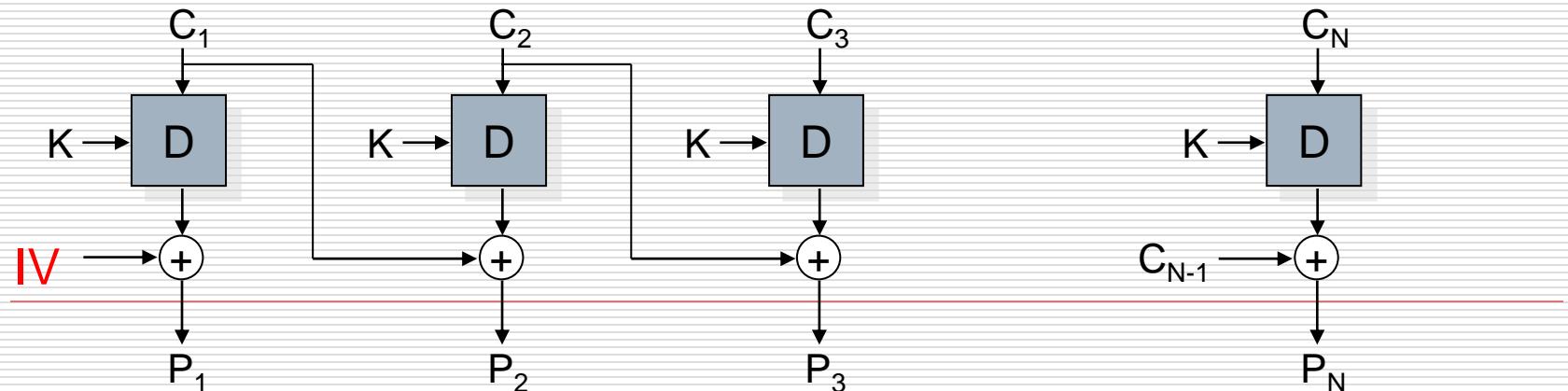
- ECB مثالی از مواردی است که با وجود بهره‌برداری از عناصر مرغوب، کیفیت نهايی دلخواه نیست.

# CBC مد کاری

رمز نگاری:



رمز گشایی:



# CBC مد کاری

- این مد از یک مقدار دهی اولیه تصادفی، **IV**، بهره میگیرد.
- مقدار **IV** در هر بار رمز نگاری به صورت تصادفی تغییر میکند.
- **IV** همراه با متن رمز شده ارسال میشود.
- **ECB IV** نیز باید به صورت رمز شده ارسال شود. برای اینکار میتوان از مد کاری استفاده کرد.
- در صورت ارسال **IV** به صورت متن واضح، تحلیلگر ممکن است بتواند با فرستادن **IV** جعلی منجر به تغییر پیغام واگشاپی شده در سمت گیرنده شود.
- هر متن واضح به ازای کلید ثابت هر بار به یک متن رمز شده متفاوت نگاشته میشود (زیرا مقدار **IV** تغییر مینماید).

# بررسی مد کاری CBC Cipher Block Chaining



ملزومات امنیتی:

- **IV** باید کاملاً غیر قابل پیش بینی 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 وادر به افزایش طول پیام بشویم.

طول پیام باید مضربی از طول قطعه باشد.

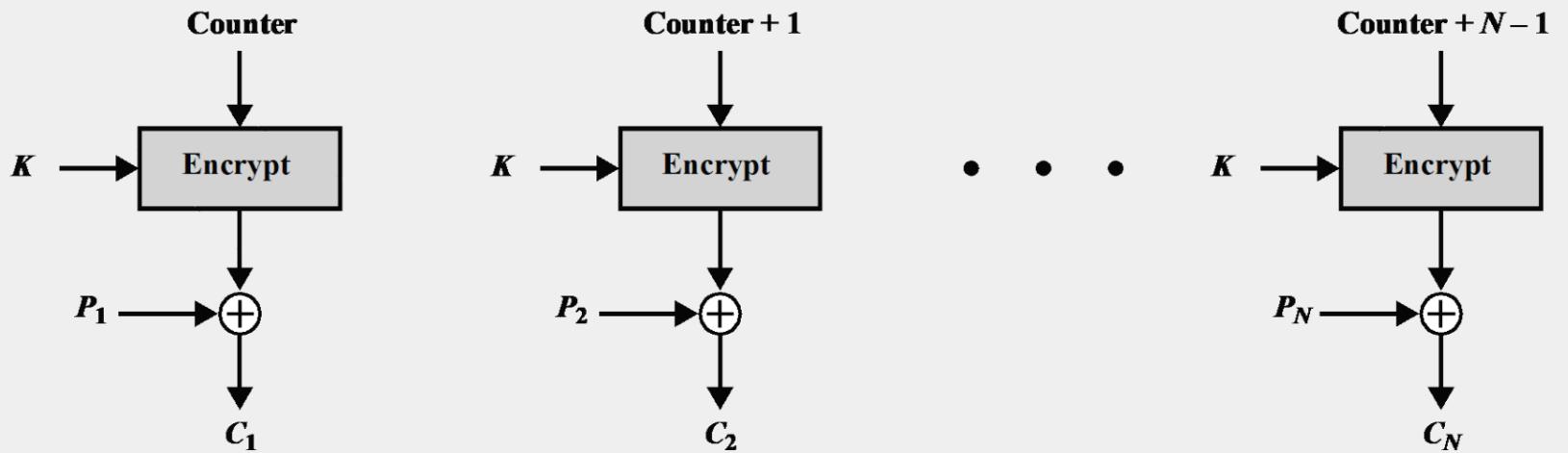
پیاده سازی:

- رمزگشایی و رمزنگاری، هر دو باید پیاده سازی شوند.

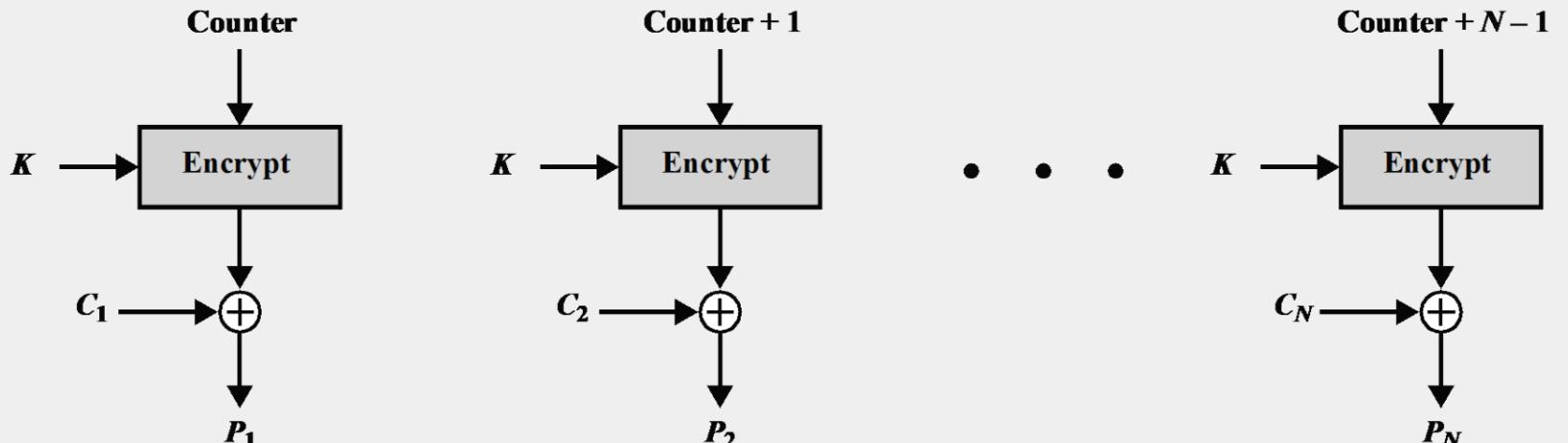
# مد کاری CTR Counter-mode Encryption

- رمز نگاری ↓
- رمزگشایی ↓
- شمارنده به طول بلاکهای مورنظر انتخاب شده و می‌تواند با مقدار اولیه صفر یا به صورت تصادفی انتخاب شود





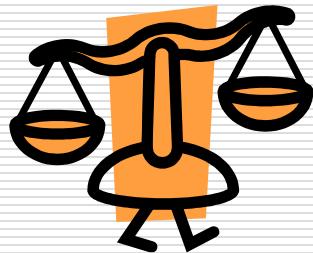
(a) Encryption



(b) Decryption

**Figure 20.8 Counter (CTR) Mode**

# بررسی مذکاری CTR



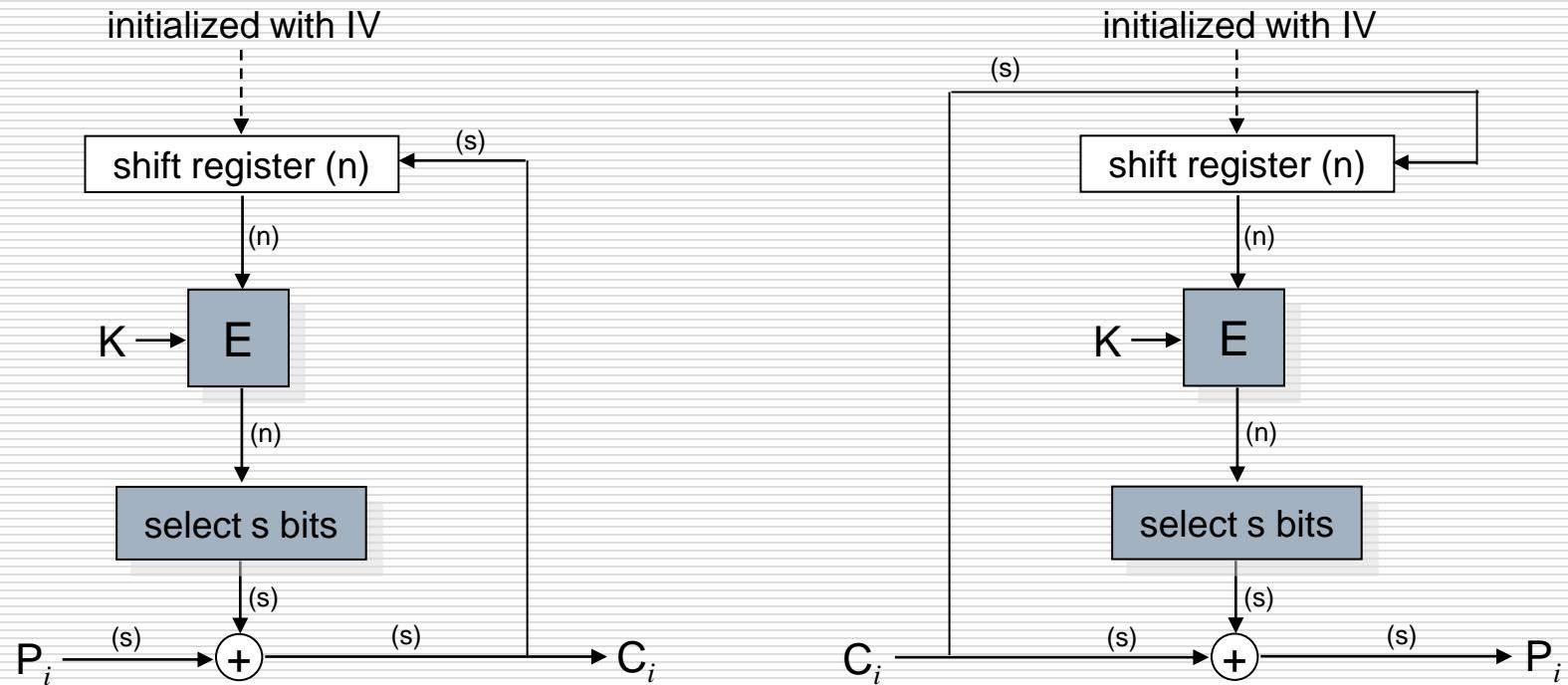
برای استفاده از رمز قطعه‌ای صرفاً مقدار شمارنده موردنیاز است.  
می‌توان ابتدا مقدار  $E_K(counter + i)$  را محاسبه نمود و سپس با رسیدن  $C_i$  متن نهایی را بازیابی کرد.

- ملزومات امنیتی:
  - مقادیر شمارنده، در بازه طول عمر کلید، باید مجزا باشند.
- رمزگاری:
  - عملیات رمزگاری قابل موازی سازی است.
  - برای عملیات رمزگاری نیازی به متن واضح نیست.
  - مقادیر شمارنده برای عملیات رمزگاری مورد نیاز است.
- رمزگشایی:
  - عملیات رمزگشایی قابل موازی سازی است.
  - برای عملیات رمزگشایی نیازی به متن رمز شده نیست.
  - مقادیر شمارنده برای عملیات رمزگاری مورد نیاز است.
- طول پیام:
  - هیچ گاه نیازی به افزایش طول پیام نداریم.
  - متن رمز شده می‌تواند هم طول با پیام کوتاه شود.
- پیاده‌سازی:
  - تنها رمز نگاری باید پیاده‌سازی شود.

# CFB مد کاری

↓ رمز نگاری

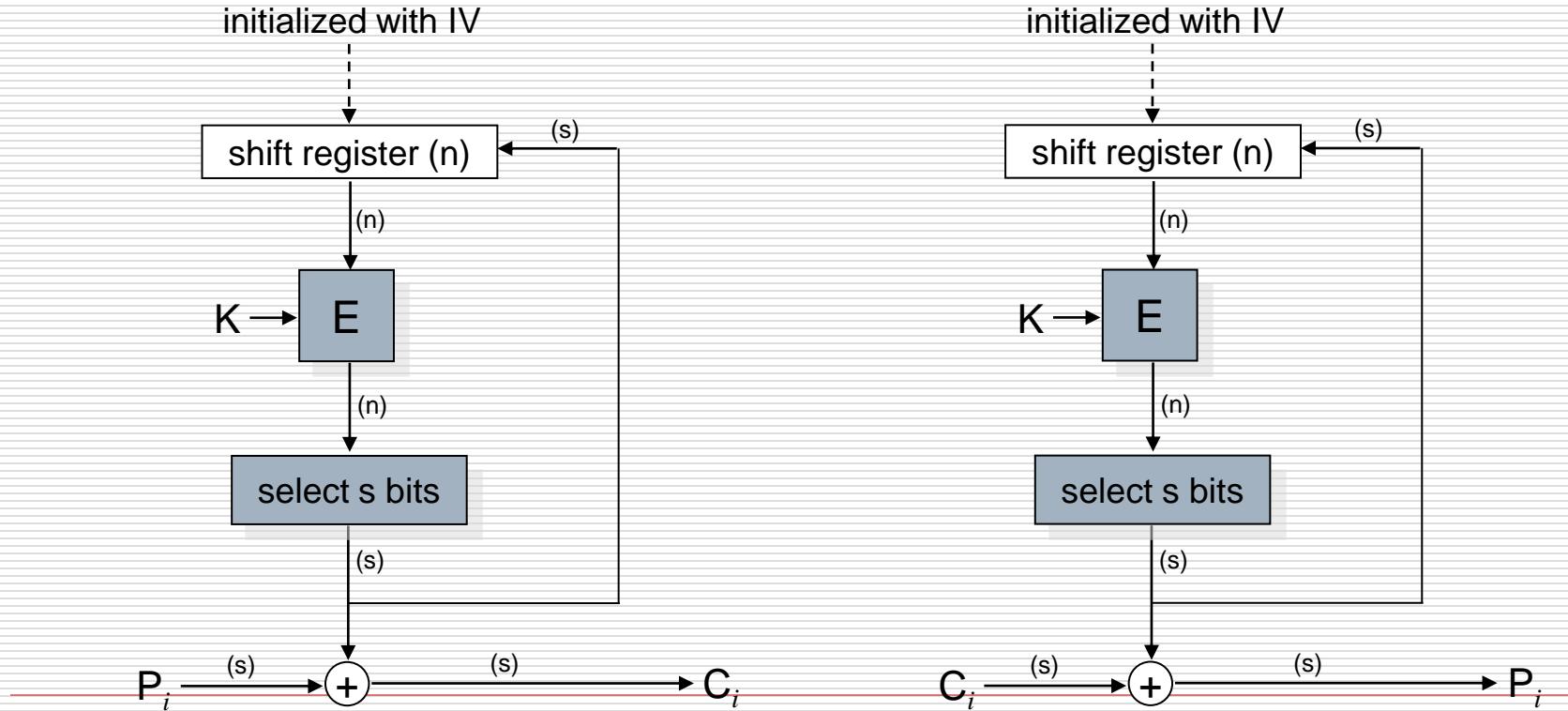
↓ رمزگشایی



# OFB مد کاری

↓ رمز نگاری

↓ رمزگشایی



# مقایسه OFB و CFB

---

## موارد استفاده OFB و CFB

- رمز جریانی □
  - کاربردهای بی درنگ □
  - عیب :CFB □
  - انتشار خطای انتقال □
  - OFB این عیب را برطرف می کند. □
-

# واژه نامه

<b>Meet-in-the-Middle attack</b>	حمله ملاقات در میانه
<b>Round</b>	دور
<b>Symmetric Encryption Scheme</b>	رمزنگاری متقارن
<b>Stream Cipher</b>	رمز جریانی / دنباله ای
<b>Block Cipher</b>	رمز قطعه ای
<b>Symmetric Cipher</b>	رمز متقارن
<b>Key Schedule</b>	زمان بندی کلید
<b>plaintext</b>	متن واضح
<b>Confidentiality</b>	محرومگی
<b>parallelization</b>	موازی سازی
<b>MAC: Message authentication code</b>	کد احراز اصالت پیام

<b>Authentication</b>	احراز هویت
<b>Brute Force</b>	آزمون جامع
<b>AES</b>	استاندارد رمزگذاری پیشرفته
<b>DES</b>	استاندارد رمزگذاری داده
<b>Padding</b>	افزایش طول پیام
<b>Provable Security</b>	امنیت قابل اثبات
<b>Differential cryptanalysis</b>	تحلیل تفاضلی
<b>linear cryptanalysis</b>	تحلیل خطی
<b>Substitution</b>	جایگزینی
<b>Permutation</b>	جایگشت
<b>Side channel attack</b>	حمله کانال جانبی
<b>Timing Attack</b>	حمله زمانی

پیوست 1

# جزئیات الگوریتم DES

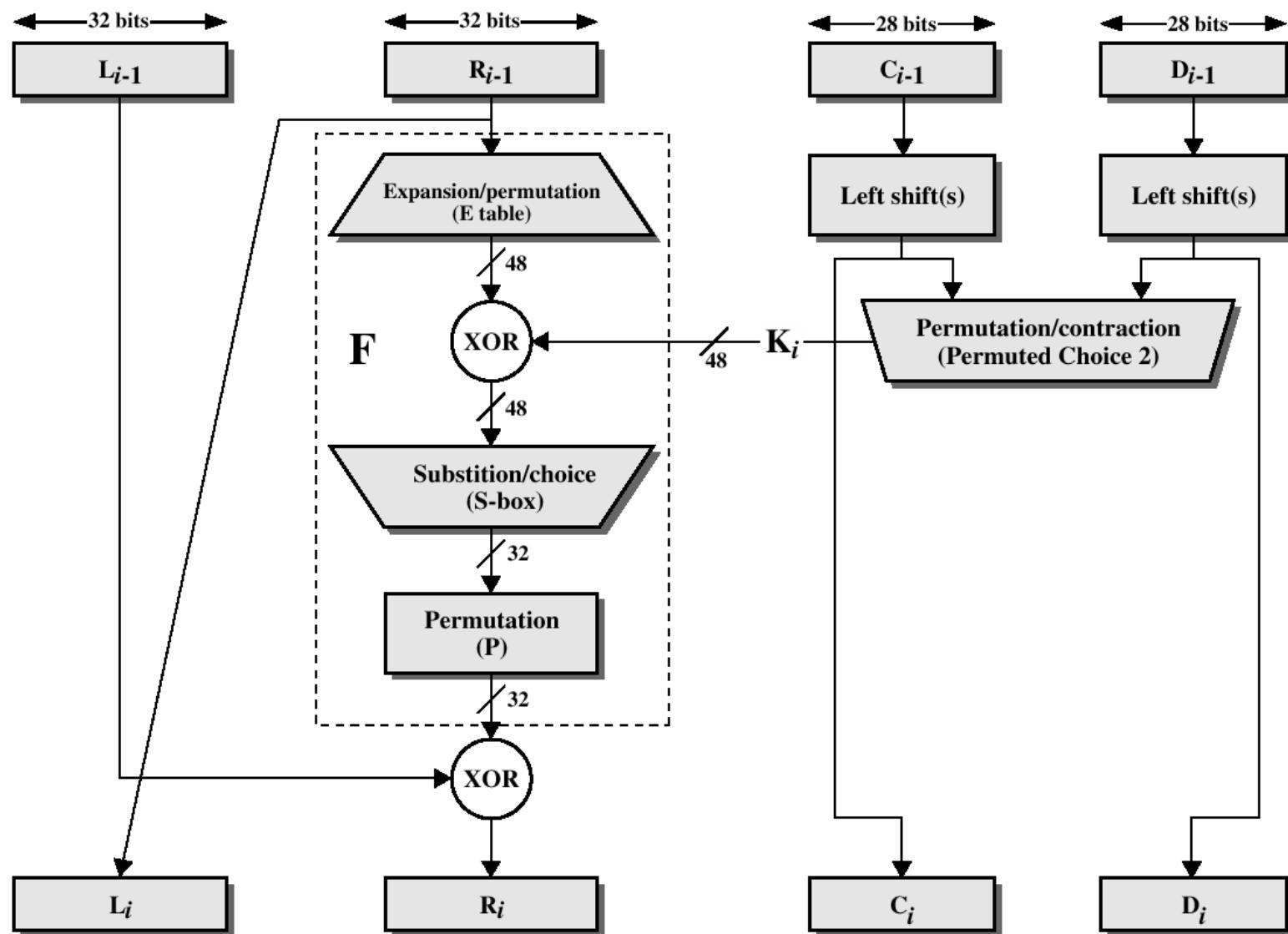
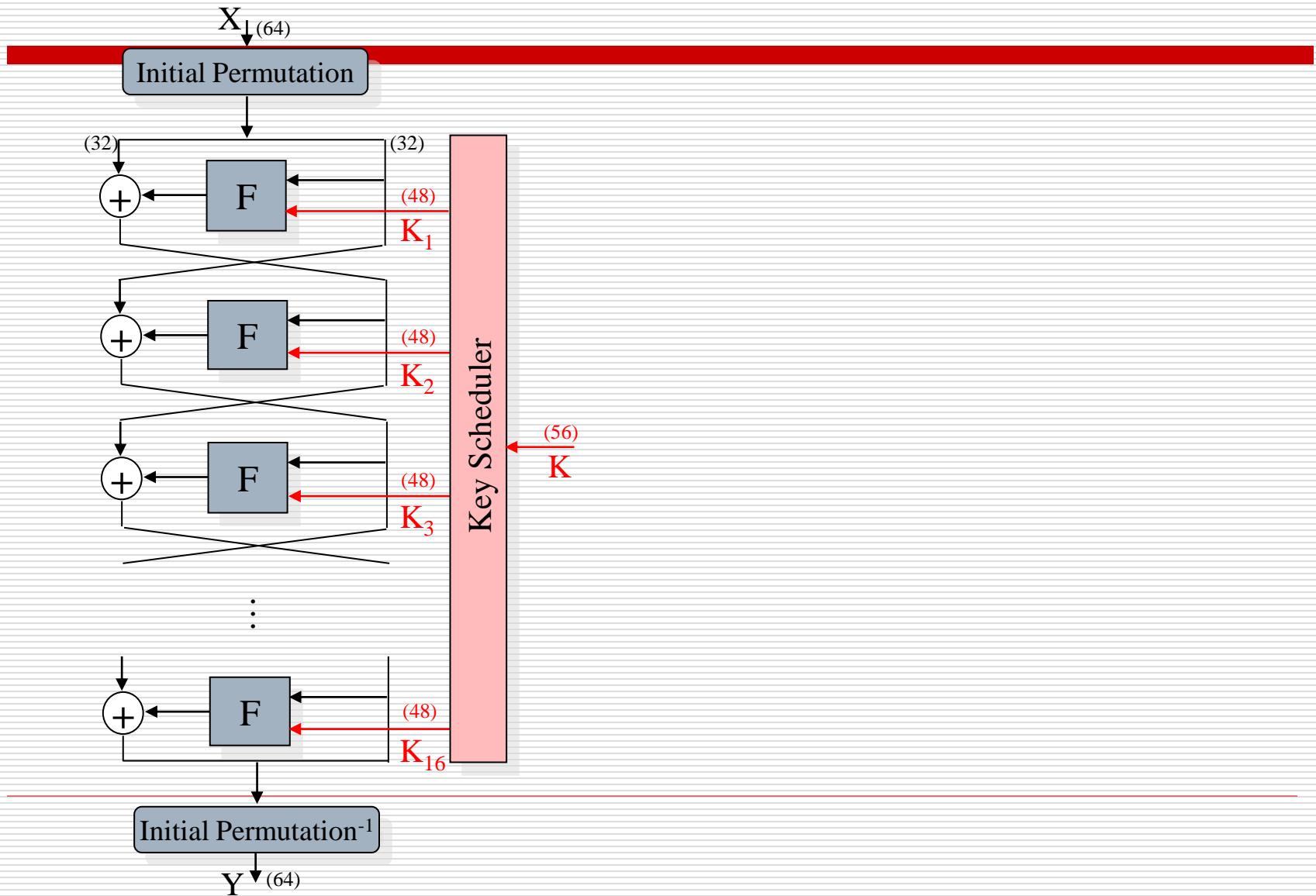
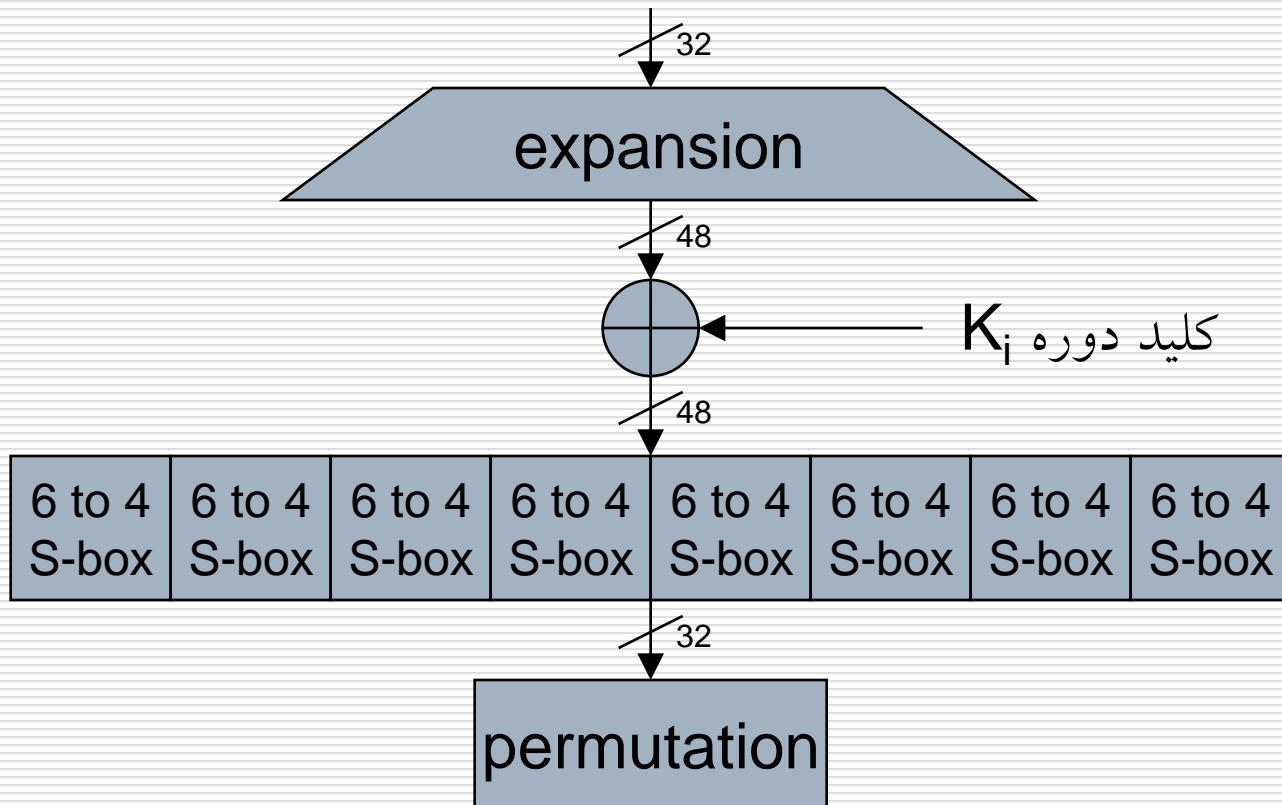


Figure 2.4 Single Round of DES Algorithm

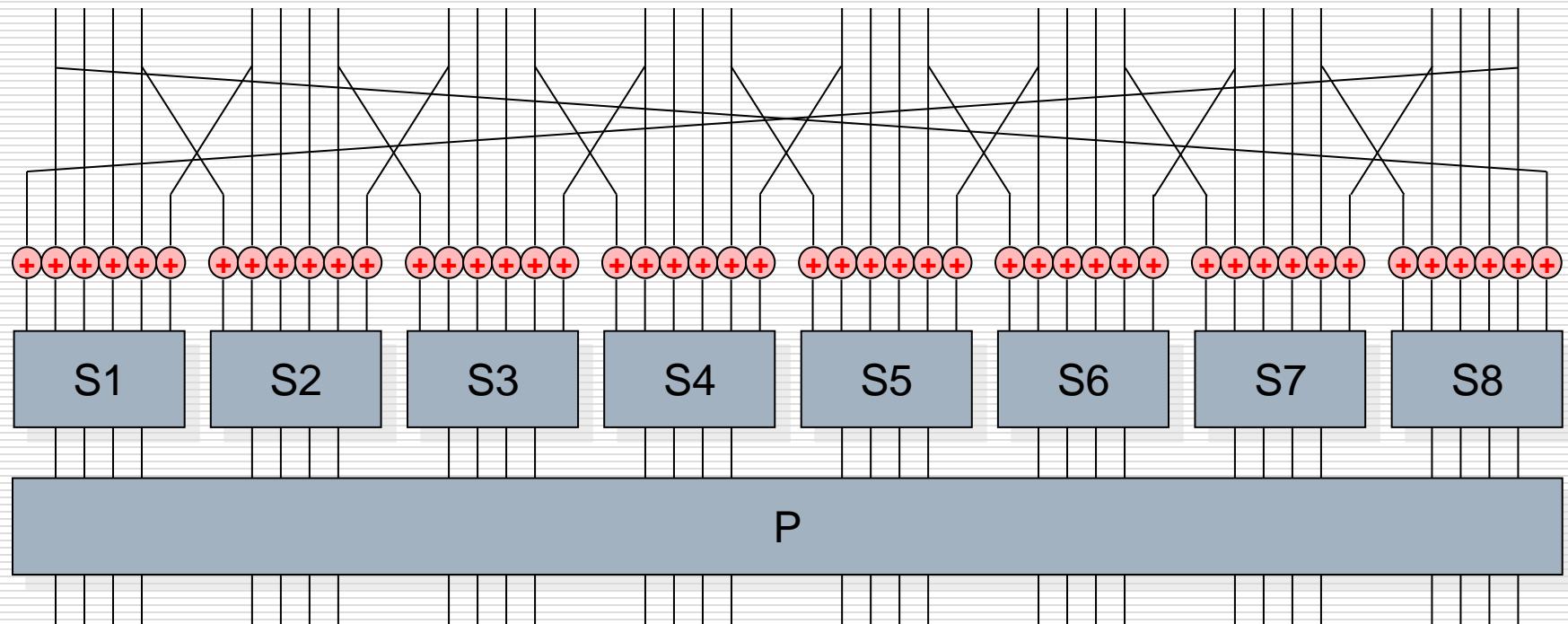
# ساختار Feistel رمز DES



# تابع دور DES



# تابع دور DES



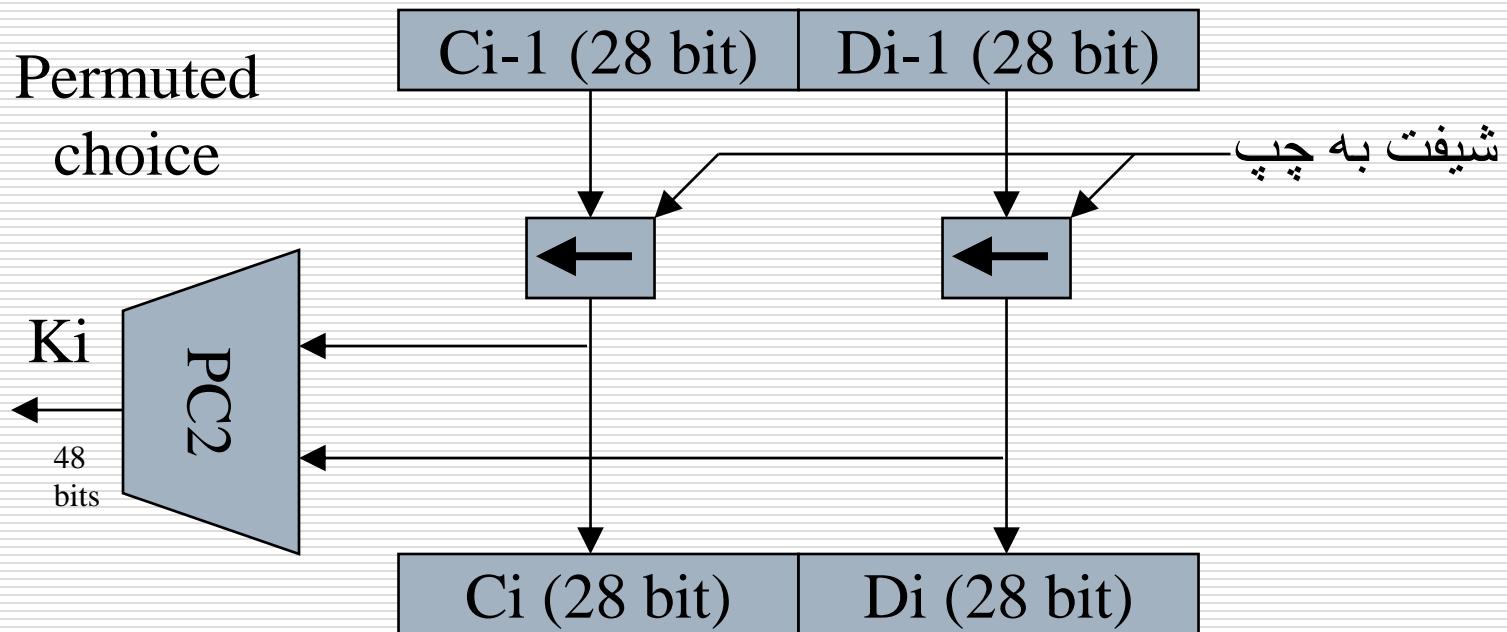
# بررسی S-box در DES

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

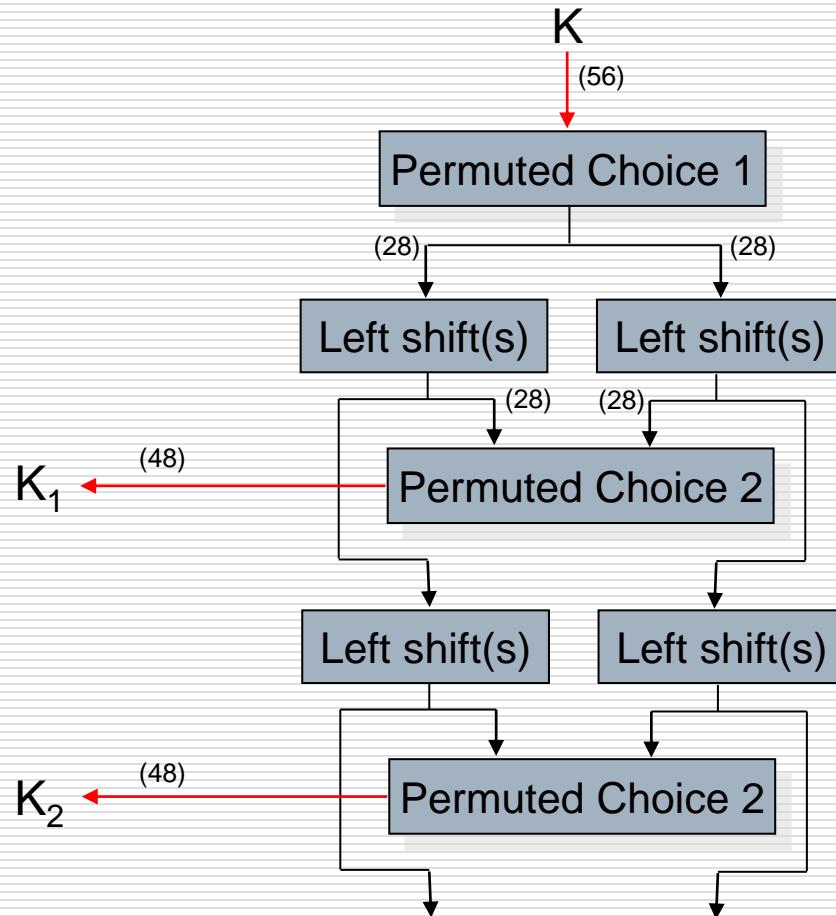
# یک DES S-Box از

		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	

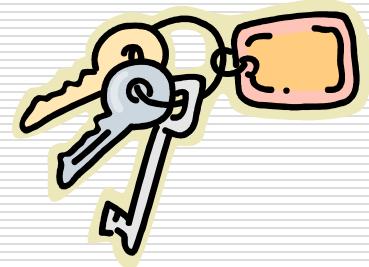
# Key-schedule



# زمانبندی کلید



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



# تحليل تفاضلی و خطی DES

## تحليل تفاضلی

- ارائه شده توسط **Murphy** و دیگران در سال ۱۹۹۰
- مبتنی بر اینکه تغییرات ورودی چگونه به تغییرات در خروجی منتقل می‌شوند
- نیاز به  $2^{47}$  زوج **plaintext/ciphertext** انتخابی دارد

## تحليل خطی

- ارائه شده توسط **Matsui** در سال ۱۹۹۱
- مبتنی بر یافتن یک تقریب خطی از تبدیلات انجام شده توسط **DES**
- نیاز به  $2^{47}$  زوج **plaintext/ciphertext** انتخابی دارد

این روشها در واقع آماری محسوب می‌شوند.

این روشها هنوز به طور عملی امکان پذیر نیستند.

جستجوی کامل ساده‌تر به نظر می‌رسد!

---

## پیوست 2 - برخی الگوریتم های دیگر رمزنگاری: IDEA, BLOWFISH, RC5, CAST-128

# الگوریتم IDEA

- ابداع شده توسط Lai و Messay در سال ۱۹۹۰
- سرعت بیشتر نسبت به DES (در پیاده سازی نرم افزاری)
- ویژگیها 
  - طول کلید : ۱۲۸ بیت
  - طول بلاک : ۶۴ بیت
  - تعداد دورها : ۸ دور
  - انجام عملیات روی عملوندهای ۱۶ بیتی

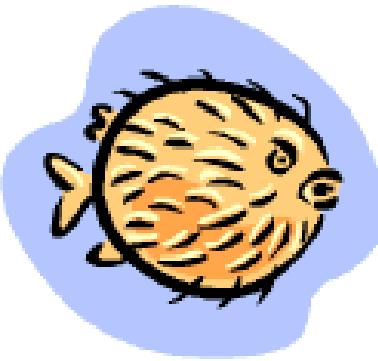


# تحلیل IDEA

- تا کنون هیچ حمله عملی علیه **IDEA** شناخته نشده است
- به نظر می‌رسد تا مدت‌ها نسبت به حملات امن باشد
- طول کلید ۱۲۸ بیتی حمله آزمون جامع را غیرممکن می‌کند (حداقل با تکنولوژیهای موجود)
- در **PGP** استفاده می‌شود.

# الگوریتم Blowfish

- طراحی شده توسط Schneier در سال ۹۴/۱۹۹۳
- وجود پیاده سازی های پرسرعت روی پردازنده های ۳۲ بیتی
- فشردگی: نیاز به کمتر از  $5^k$  حافظه
- پیاده سازی آسان
- تحلیل الگوریتم آسان
- طول کلید متغیر: درجه امنیت قابل تغییر است.



# Blowfish ویژگیهای

---

- طول بلاک : ۶۴ بیت
- تعداد دورها : ۱۶ دور
- طول کلید متغیر : ۳۲ تا ۴۴۸ بیت
- تولید زیرکلید و **S-Box** های وابسته به کلید
- ۱۸ زیرکلید ۳۲ بیتی که در آرایه **P** ذخیره می‌شوند
- ۴ **S-Box** با اندازه **8\*32** که در آرایه **S** ذخیره می‌شوند
- باز تولید کند زیرکلید ها : تولید زیرکلیدها به ۵۲۱ مرحله رمزنگاری احتیاج دارد

# الگوریتم RC5

- انطباق با نرم افزارها و سخت افزارهای مختلف
- سرعت اجرای زیاد : عملیات روی کلمه ها انجام می شوند
- انطباق با پردازنده های با تعداد بیت‌های متفاوت
- طول بلاک متغیر
- طول کلید متغیر
- تعداد دورهای متغیر
- نیاز به حافظه کم
- طراحی و تحلیل الگوریتم ساده
- تعداد دورهای وابسته به داده : تحلیل رمز را مشکل می کند

# الگوریتم CAST-128

- ابداع شده توسط **Tavares** و **Adams** در سال ۱۹۹۷
- طول کلید متغیر: از ۴۰ تا ۱۲۸ بیت (افزایش ۸ بیتی)
- تعداد دور: ۱۶ دور
- مشابه ساختار کلاسیک **Feistel** می‌باشد با دو تفاوت زیر:
  - در هر دور از دو زیرکلید استفاده می‌کند
  - تابع **F** به دور بستگی دارد
- در حال استفاده در **PGP** (امن سازی سرویس ایمیل)