

# مقدمه ای بر رمزنگاری

# اصطلاحات

- Plaintext یا Cleartext: متن رمز نشده
- Ciphertext: متن رمز شده
- Encryption یا Encipher: عملیات رمز کردن متن رمز نشده
- Decryption یا Decipher: عملیات رمزگشایی متن رمز شده
- Cryptography: علم رمزنگاری
- Cryptanalysis: علم شکستن رمز
- Cryptology: مطالعه Cryptography و Cryptanalysis
- Cryptosystem: الگوریتم هایی که عملیات Encryption و Decryption را انجام می دهند

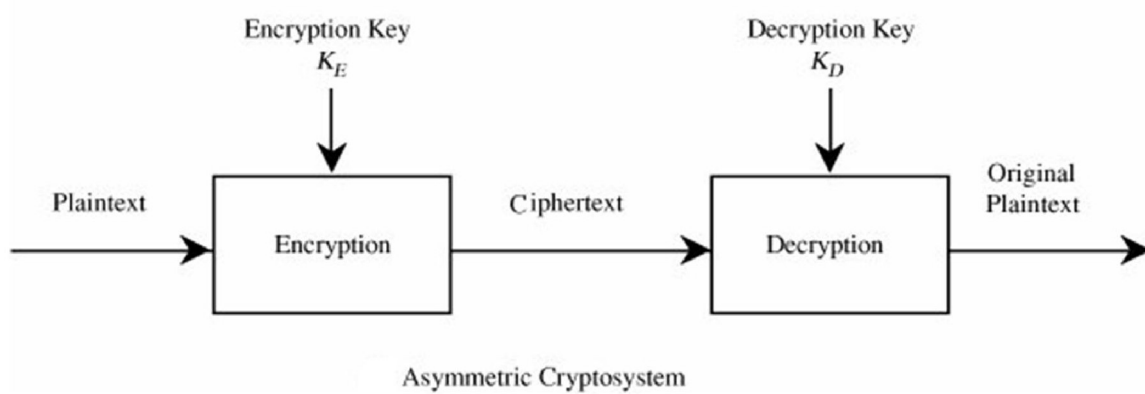
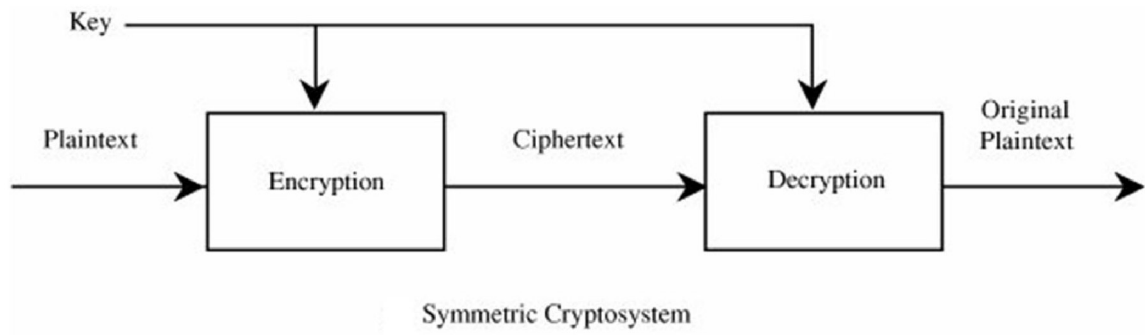
# Decryption , Encryption



# انواع Cryptosystem

- متقارن (Symmetric)
  - کلیدهای Encryption و Decryption یکسان هستند.
  - $C = E(K, P)$  –
  - $P = D(K, C)$  –
  - Secret Key –
- نامتقارن (Asymmetric)
  - کلیدهای Encryption و Decryption متفاوت هستند.
  - $C = E(K_E, P)$  –
  - $P = D(K_D, C)$  –
  - Public Key –

# انواع Cryptosystem



# Cryptanalysis

- شکستن پیام
- شکستن کلید
- شکستن الگوریتم

# تکنیک های Encryption

- جایگزینی (Substitution)

- استفاده از یک جدول برای جایگزینی کاراکترهای Plaintext
- مزیت: سادگی
- ضعف: به سادگی قابل شکستن است.

- جایگشتی (Permutation یا Transposition)

- کاراکترهای Plaintext را جابجا می کنیم
- مزیت: سادگی
- ضعف: قابل شکستن است.

# جایگزینی (Substitution)



# Caesar Cipher

$$c_i = E(p_i) = (p_i + 3) \bmod 26 \quad \bullet$$

<b>Plaintext</b>	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
<b>Ciphertext</b>	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

# One-Time Pads

- استفاده از تعداد زیادی کلید غیر تکراری برای رمز کردن
- نمونه روش ها

Long Random Number Sequences –

Vernam Cipher –

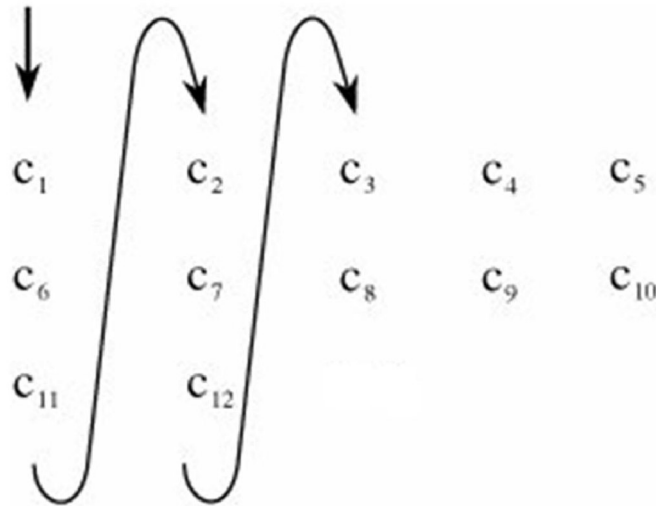
Book Cipher –

Plaintext	V	E	R	N	A	M	C	I	P	H	E	R
Numeric Equivalent	21	4	17	13	0	12	2	8	15	7	4	17
+ Random Number	76	48	16	82	44	3	58	11	60	5	48	88
= Sum	97	52	33	95	44	15	60	19	75	12	52	105
= mod 26	19	0	7	17	18	15	8	19	23	12	0	1
Ciphertext	t	a	h	r	s	p	i	t	x	m	a	b

# جایگشتی (Permutation یا Transposition)

# Columnar Transposition

- Plaintext:  $c_1 c_2 c_3 c_4 c_5 c_6 c_7 c_8 c_9 c_{10} c_{11} c_{12}$
- Ciphertext:  $c_1 c_6 c_{11} c_2 c_7 c_{12} c_3 c_8 c_4 c_9 c_5 c_{10}$

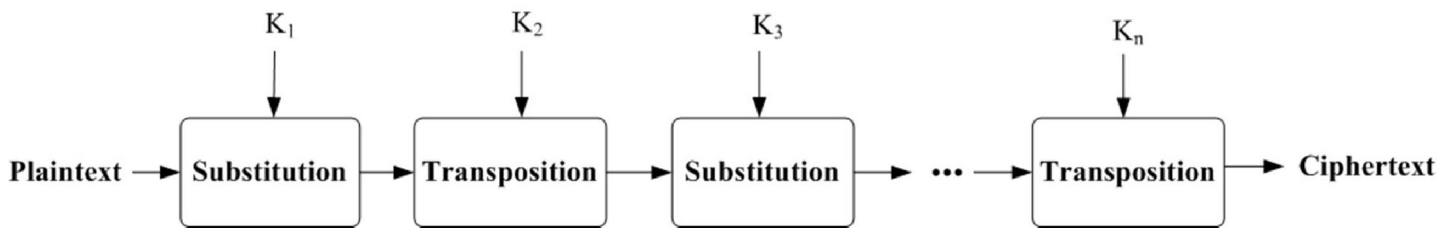


ترکیب جایگزینی و جایگشتی

# Product Cipher

- خروجی الگوریتم (جایگزینی یا جایگشتی) به عنوان ورودی الگوریتم (جایگزینی یا جایگشتی)

$$C = E_n(E_{n-1}(\dots(E_1(P, K_1)), K_{n-1}), K_n) \quad \bullet$$



# انواع رمزنگاری

## • Stream Cipher fast

– هر یک از کاراکترهای Plaintext را به یک کاراکتر Ciphertext تبدیل می کند

## • Block Cipher more secure

– کاراکترهای Plaintext را به بلاک های مختلف تقسیم می کند  
و هر بلاک را به یک بلاک Ciphertext تبدیل می کند

# Stream Cipher

- الگوریتم های متقارن

- RC4

- مزایا

- سرعت بالا

- میزان انتشار خطای پایین

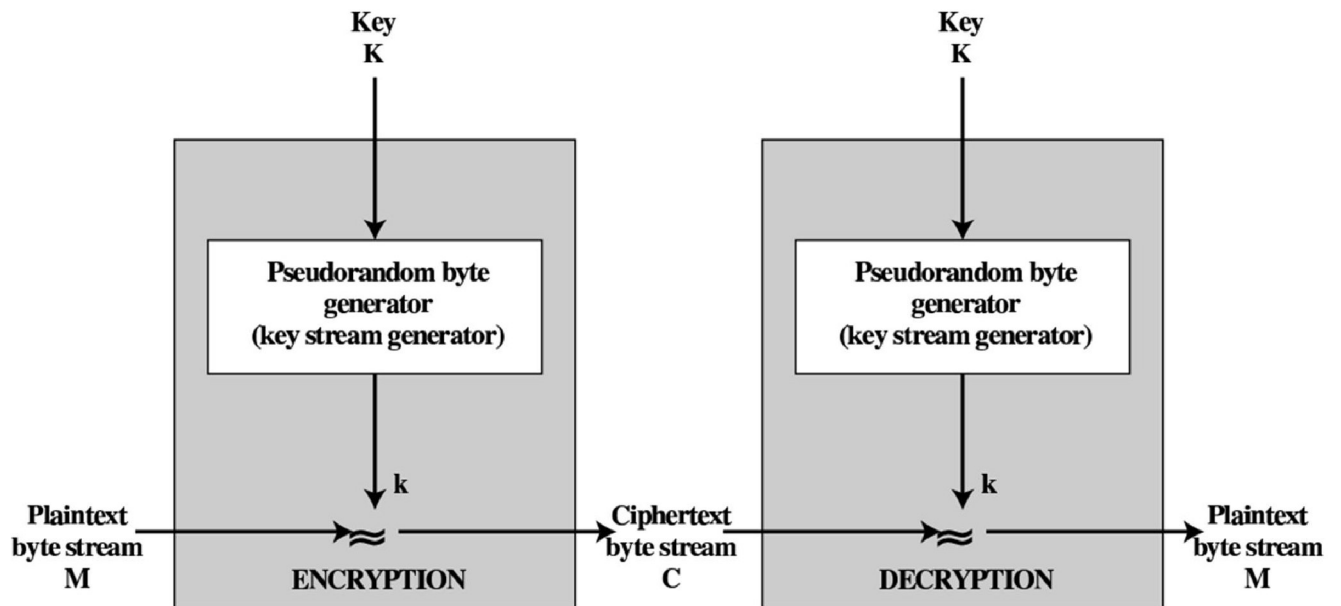
- معایب

- Low Diffusion

- آسیب پذیر در مقابل تغییرات ایجاد شده در پیام



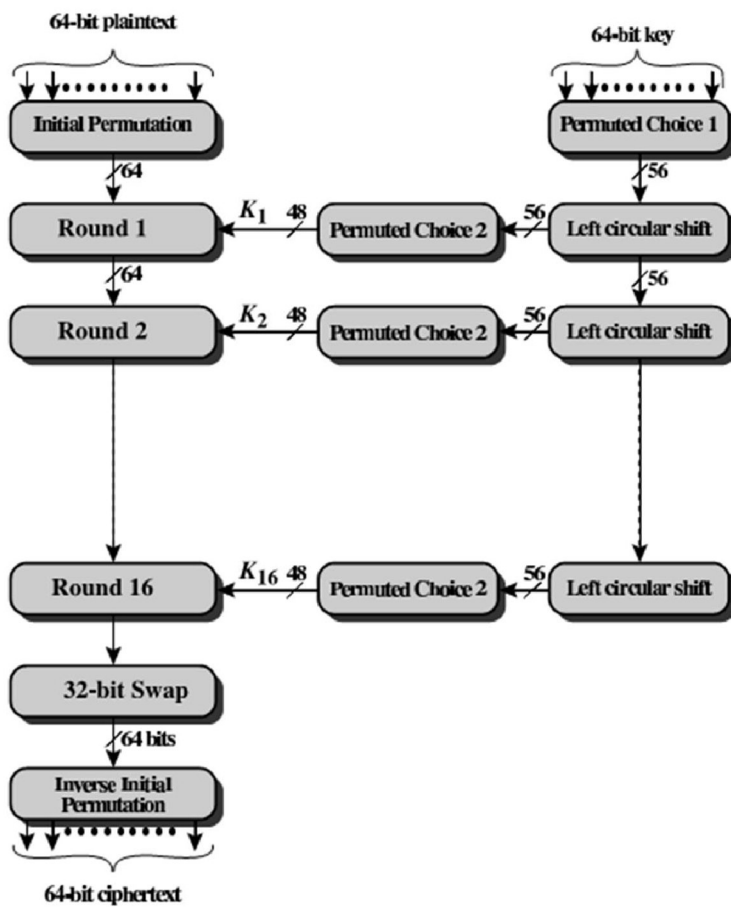
# Stream Cipher



# Block Cipher

- الگوریتم های متقارن
  - Data Encryption Standard (DES)
    - Double DES (2DES)
    - Triple DES (3DES)
  - Advanced Encryption Standard (AES) ✓
- مزایا
  - High Diffusion
  - مقاوم در مقابل تغییرات ایجاد شده در پیام
- معایب
  - سرعت پایین
  - میزان انتشار خطای بالا

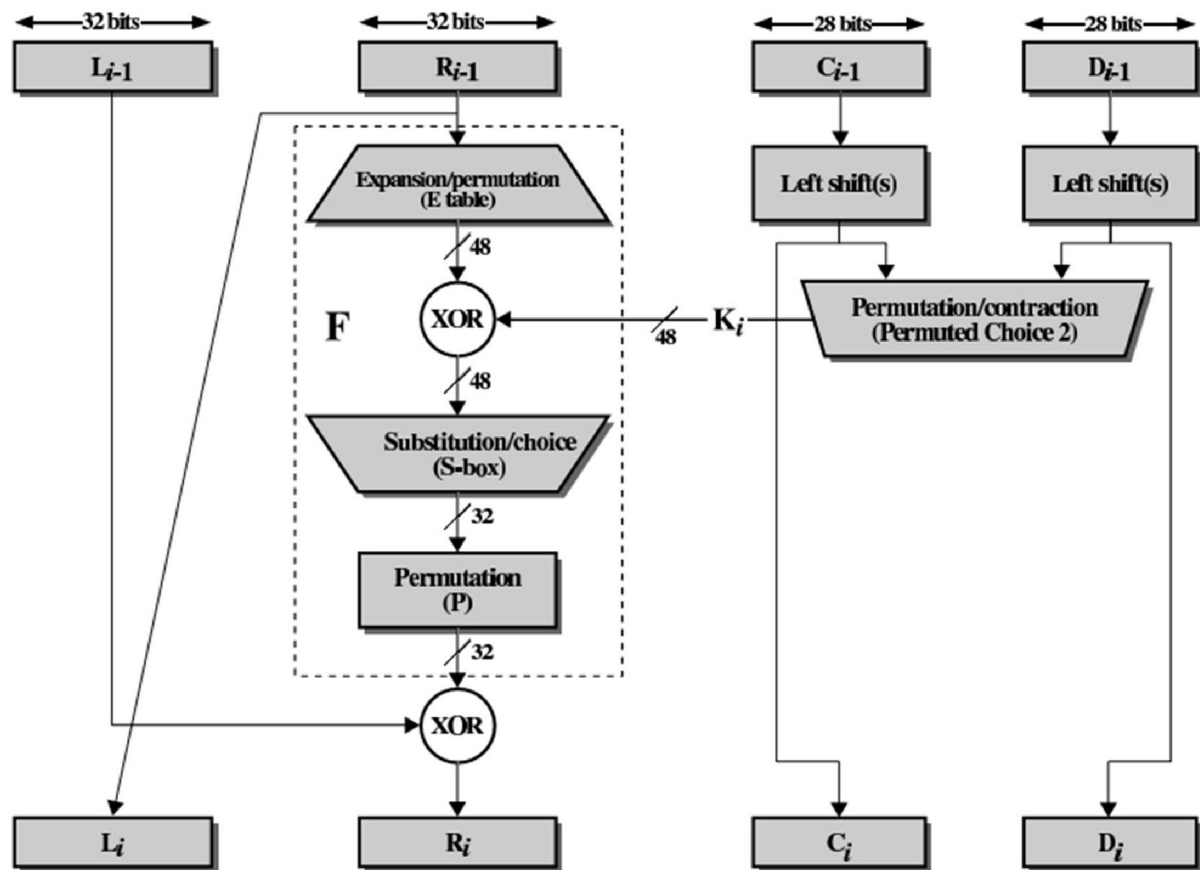
# Data Encryption Standard (DES)



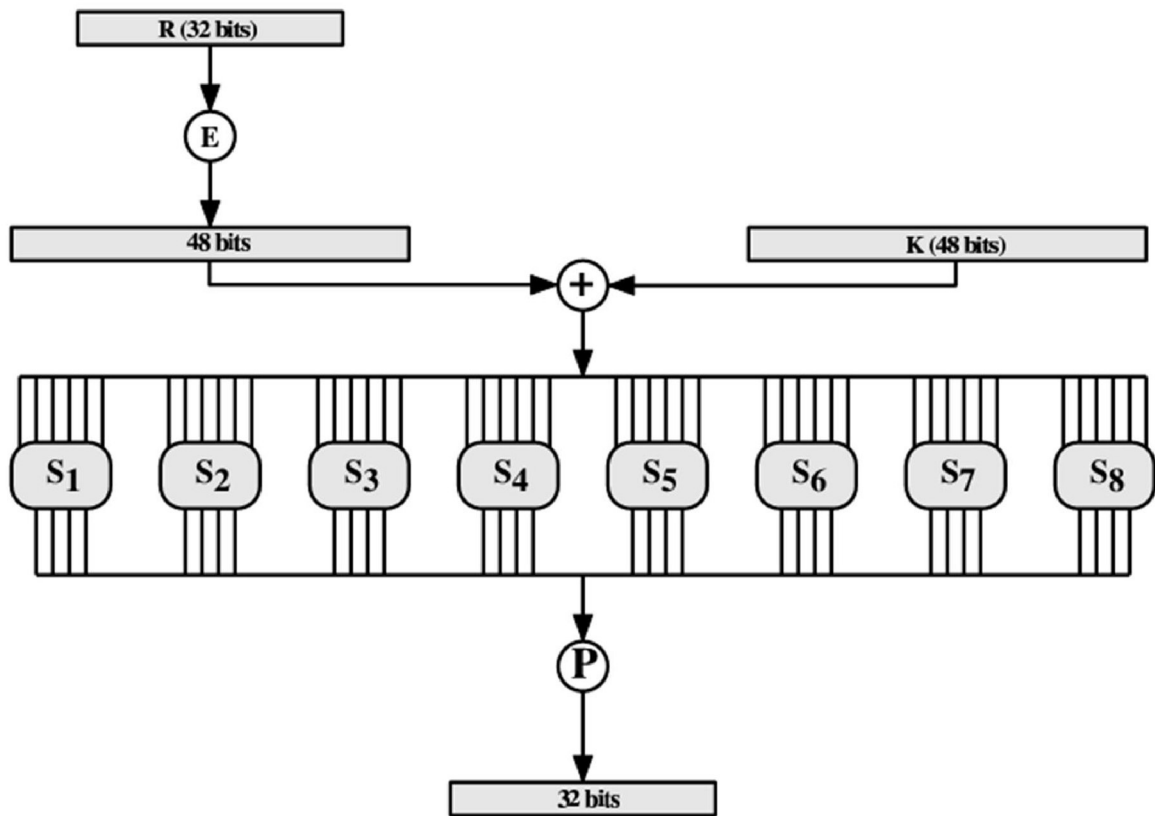
- الگوریتم متقارن
- طول کلید: ۵۶ بیتی
- طول بلاک: ۶۴ بیت

Key is 56 bit. 8 bits are used for parity.

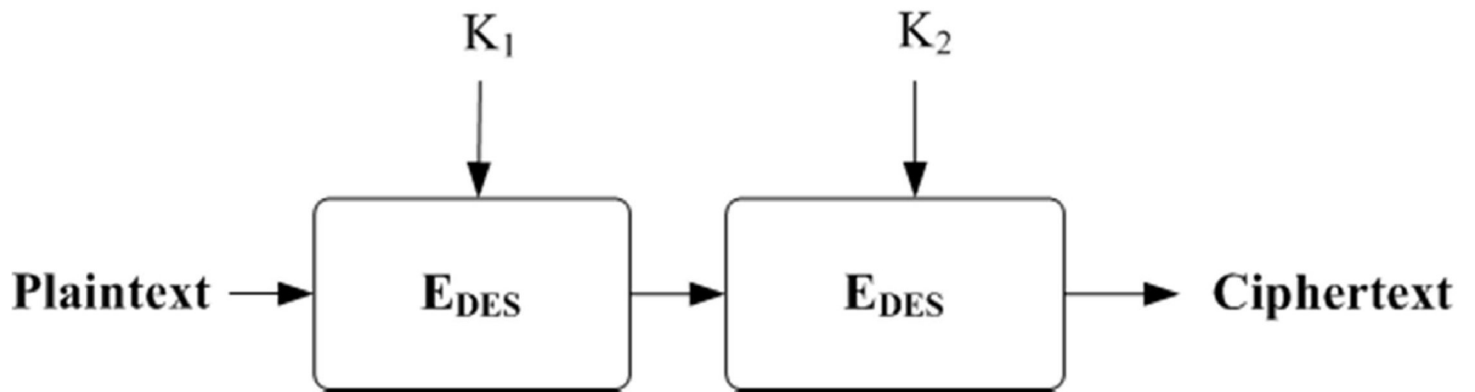
# نحوه اجرای Round i ام



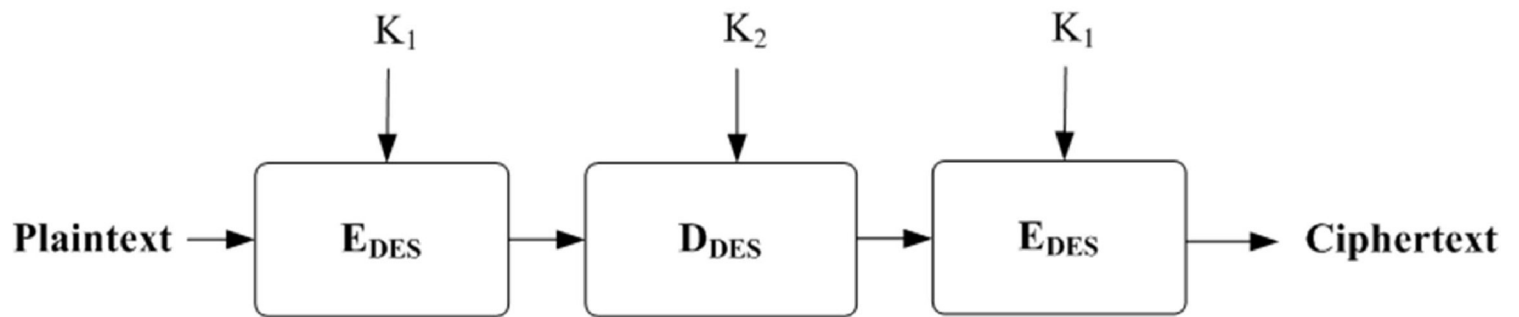
محاسبه  $F(R_{i-1}, K_i)$



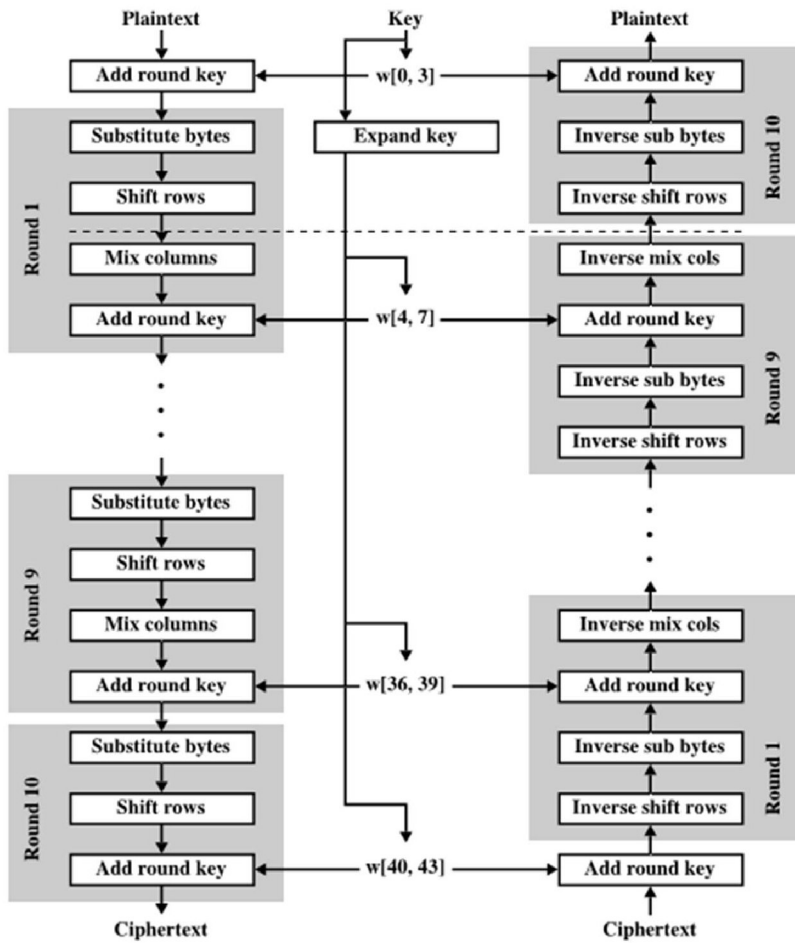
# Double DES (2DES)



# Triple DES (3DES)



# Advanced Encryption Standard (AES)



- الگوریتم متقارن
- طول کلید:
  - ۱۲۸ بیت
  - ۱۹۲ بیت
  - ۲۵۶ بیت
- طول بلاک: ۱۲۸ بیت




# Public-Key Cryptography

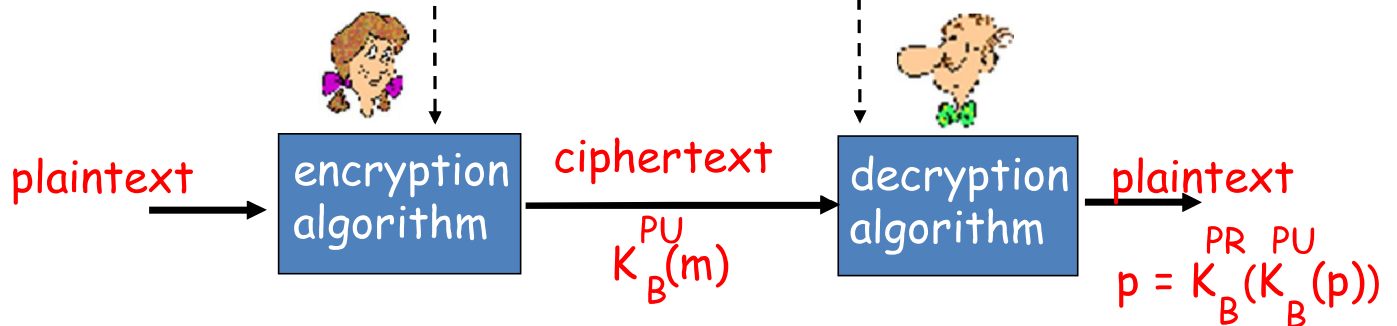
- دو کلید مختلف برای Encryption و Decryption
  - کلید عمومی (Public Key)
  - کلید خصوصی (Private Key)
- $P = D(K_{PR}, E(K_{PU}, P)) = D(K_{PU}, E(K_{PR}, P))$
- الگوریتم نمونه
  - Rivest-Shamir-Adelman (RSA)

# Public-Key Cryptography

Still man in the middle is possible. Attacker advertises his public key

  $K_B^{PU}$  Bob's public key

  $K_B^{PR}$  Bob's private key



# Rivest-Shamir-Adelman (RSA)

- دو عدد اول و بزرگ ۱۰۲۴ بیتی  $p$  و  $q$  را انتخاب می کنیم
- دو عدد  $n$  و  $z$  را حساب می کنیم:
  - $n = pq$
  - $z = (p-1)(q-1)$
- عدد  $e$  را انتخاب می کنیم به طوری که:
  - $e < n$
  - $e$  و  $z$  نسبت به هم اول هستند
- عدد  $d$  را انتخاب می کنیم به طوری که:
  - $ed \bmod z = 1$
- دو کلید عمومی و خصوصی را محاسبه می کنیم
  - کلید عمومی:  $(n, e)$
  - کلید خصوصی:  $(n, d)$

# تبادل کلید (Key Exchange)

- اشتراک کلید بین فرستند و گیرنده برای تبادل اطلاعات
- کلید نشست (Session Key)
- روش

Public-Key Key Exchange –

# Public-Key Key Exchange

$$A: MSG = E(PU_B, E(K_{session}, PR_A))$$

$$B: K_{session} = D(PU_A, D(MSG, PR_B))$$

# Diffie-Hellman Key Exchange

*Two public big prime number  $(a, p)$ ,  $a < p$*

$$PR_A < p, PR_B < p$$

$$PU_A = a^{PR_A} \bmod p$$

$$PU_B = a^{PR_B} \bmod p$$

$$K_{session} = (PU_A)^{PR_B} \bmod p = (PU_B)^{PR_A} \bmod p$$

# صحت پیام (Message Integrity)

- تابع Hash
- Message Authentication Code (MAC)
- امضای دیجیتال (Digital Signature)
- گواهینامه (Certificate)

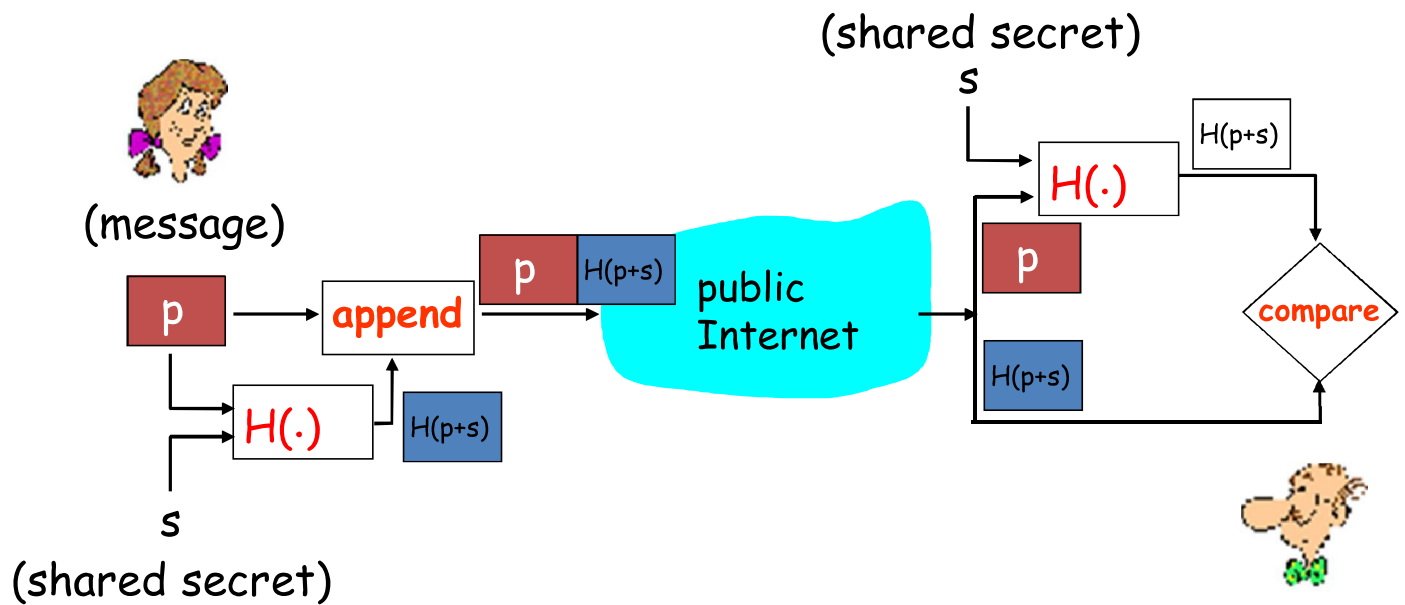
To reach Confidentiality: EncryptionTo r

## صحت پیام

- Bob پیامی از Alice دریافت می کند
  - Bob باید مطمئن باشد که پیام واقعاً از طرف Alice است
  - پیام Alice در بین راه تغییر نکرده باشد
- تابع Hash
  - پیام ورودی با هر طولی را به یک پیام با طول ثابت تبدیل می کند
  - احتمال اینکه دو پیام مختلف دارای Hash های یکسان باشند، خیلی پایین است.
  - تابع Hash یک طرفه (One-way Function) است و از روی پیام خروجی نمی توان به پیام اصلی رسید



# Message Authentication Code (MAC)



# الگوریتم های موجود MAC

- Message Digest (MD5)

- پیام خروجی ۱۲۸ بیتی

- Secure Hash Algorithm (SHA-1)

- پیام خروجی ۱۶۰ بیتی

# امضای دیجیتال (Digital Signature)

- تأیید هویت فرستنده
- بررسی صحت پیام
- MAC امضا شده

Bob's message, p

Dear Alice  
Oh, how I have missed  
you. I think of you all the  
time! ... (blah blah blah)  
Bob

  $K_B^{PR}$  Bob's private  
key

public key  
encryption  
algorithm

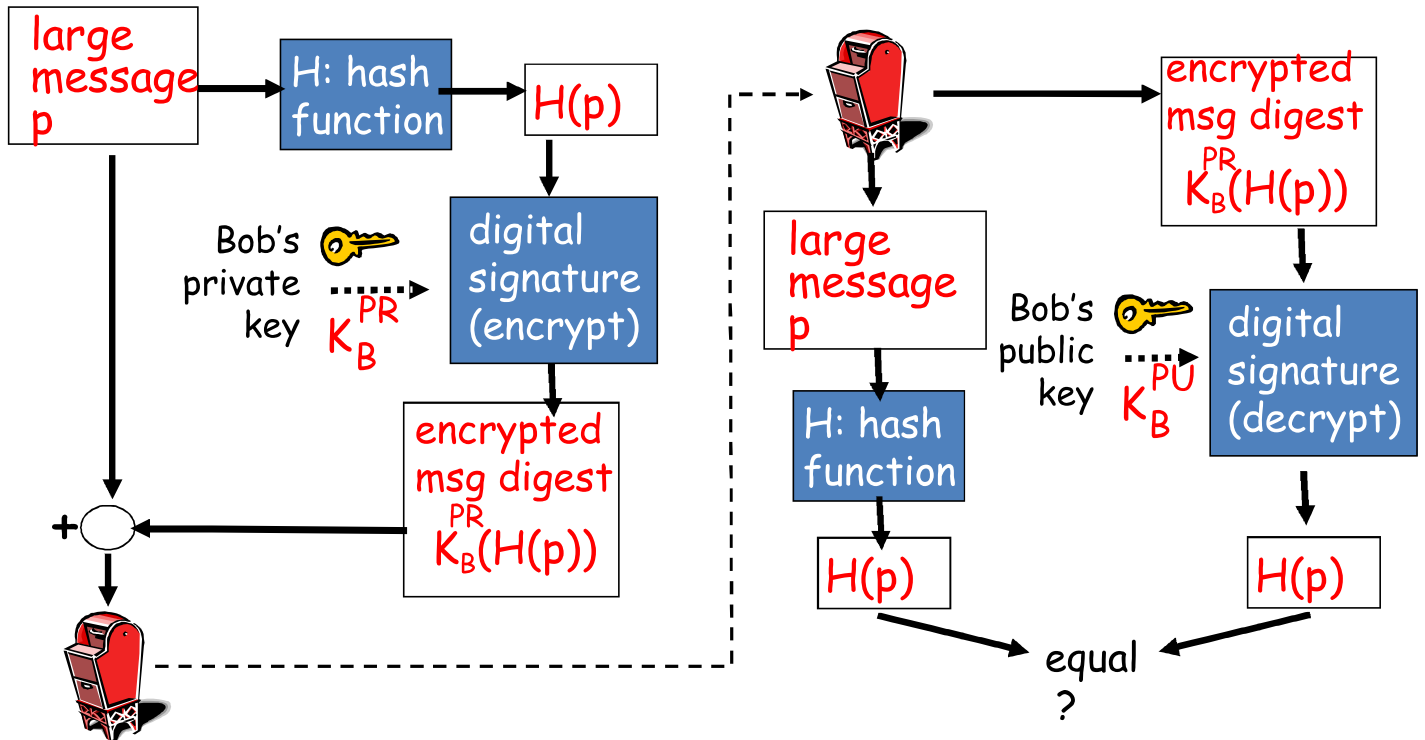
$K_B^{PR}(p)$

Bob's message, p,  
signed (encrypted)  
with his private key

# نحوه کار امضای دیجیتال

Bob پیام امضا شده را می فرستد

Alice صحت و هویت پیام را بررسی می کند

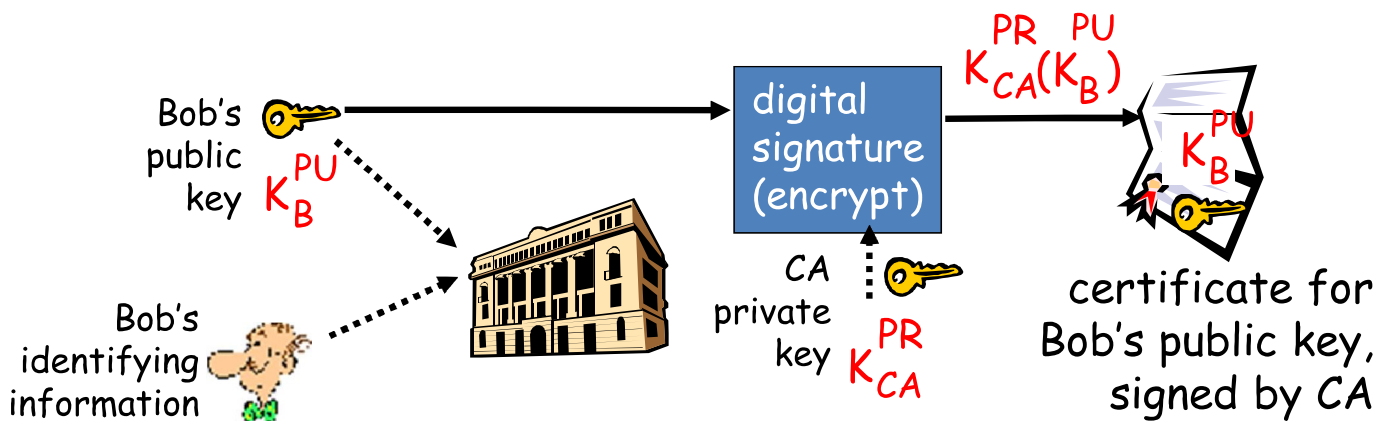


# گواهینامه (Certificate)

- اشتراک گذاری کلید عمومی به طور امن
- حمله (Man-In-The-Middle (MITM
- استفاده از امضای دیجیتال
- Certificate Authority (CA)
- مرکز صدور گواهینامه

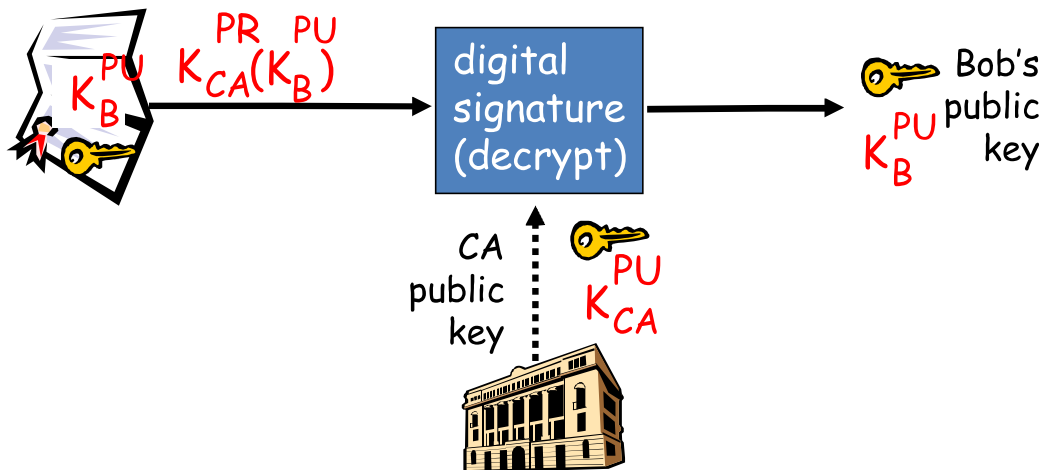
# صدور گواهینامه

- Bob کلید عمومی خود را به CA می دهد
- CA، با استفاده از کلید خصوصی خود، کلید عمومی Bob را امضا می کند (گواهینامه)

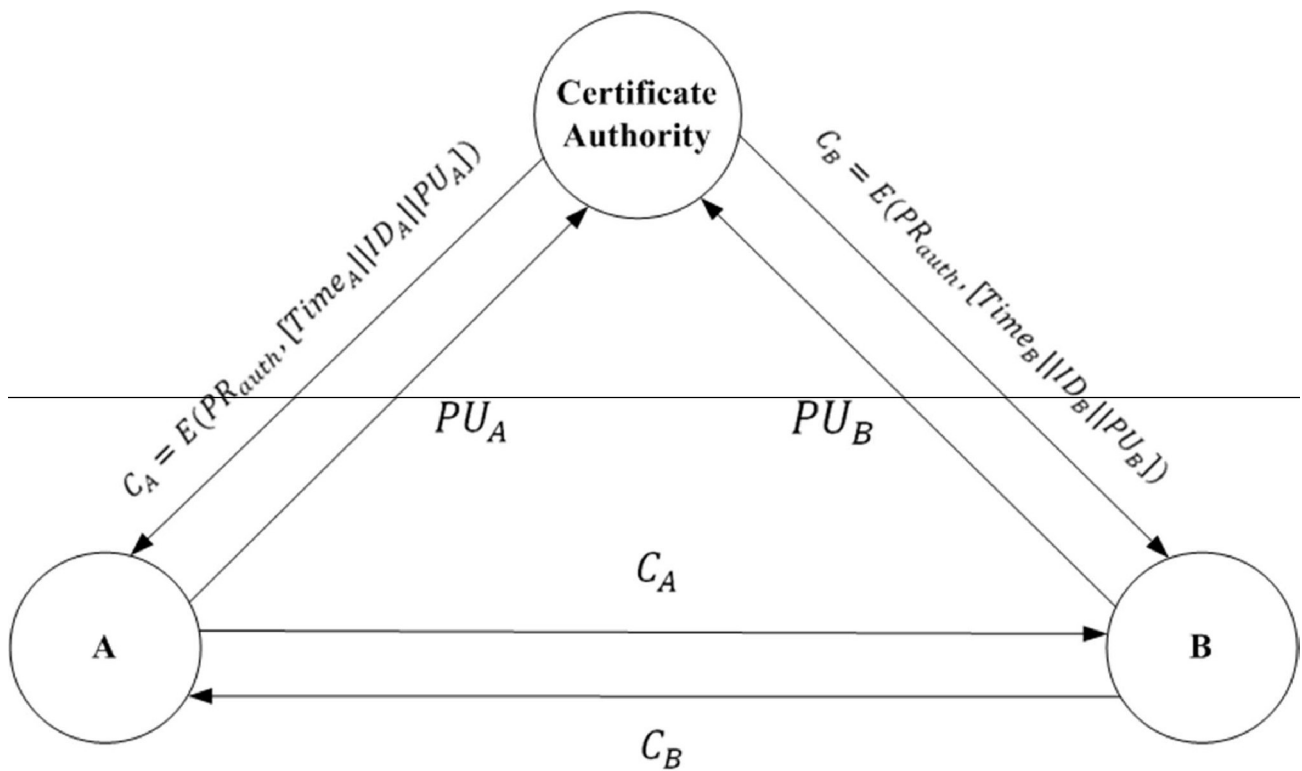


# دریافت کلید عمومی

- Alice می خواهد کلید عمومی Bob را بدست آورد
  - گواهینامه Bob را دریافت می کند.
  - از کلید عمومی CA استفاده می کند و کلید عمومی Bob را بدست می آورد.



# Certificate Authority



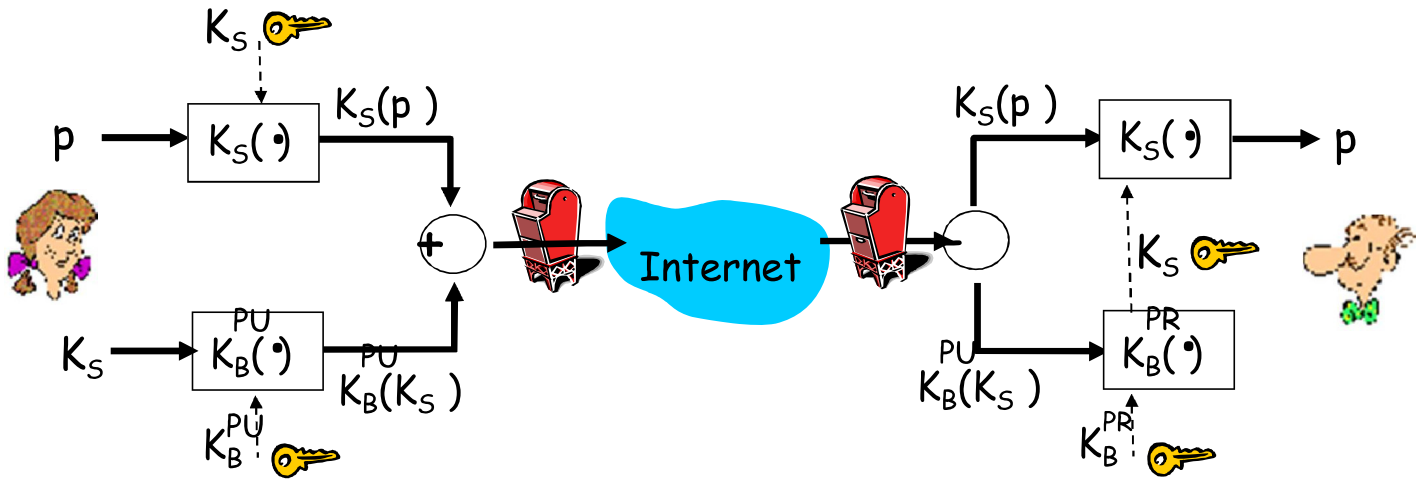
black list of CA: revealed private keys related to certs.



# Secure Email

• Alice می خواهد به Bob ایمیل بفرستد

– محرمانه باشد

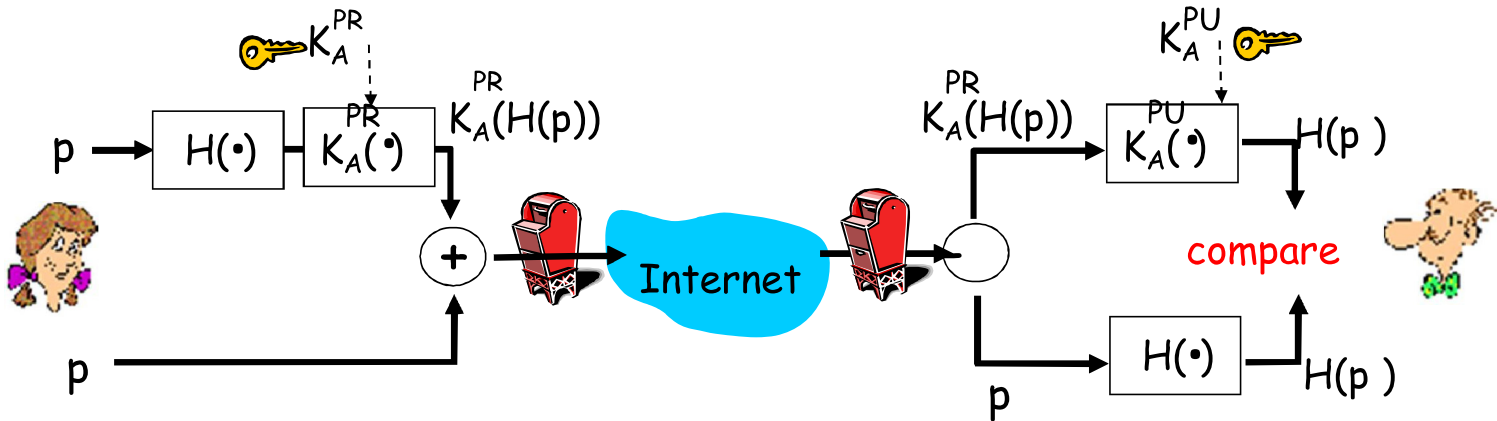


# Secure Email

• Alice می خواهد به Bob یک ایمیل بفرستد

– هویت فرستنده قابل تایید باشد

– صحت پیام ایمیل قابل تایید باشد



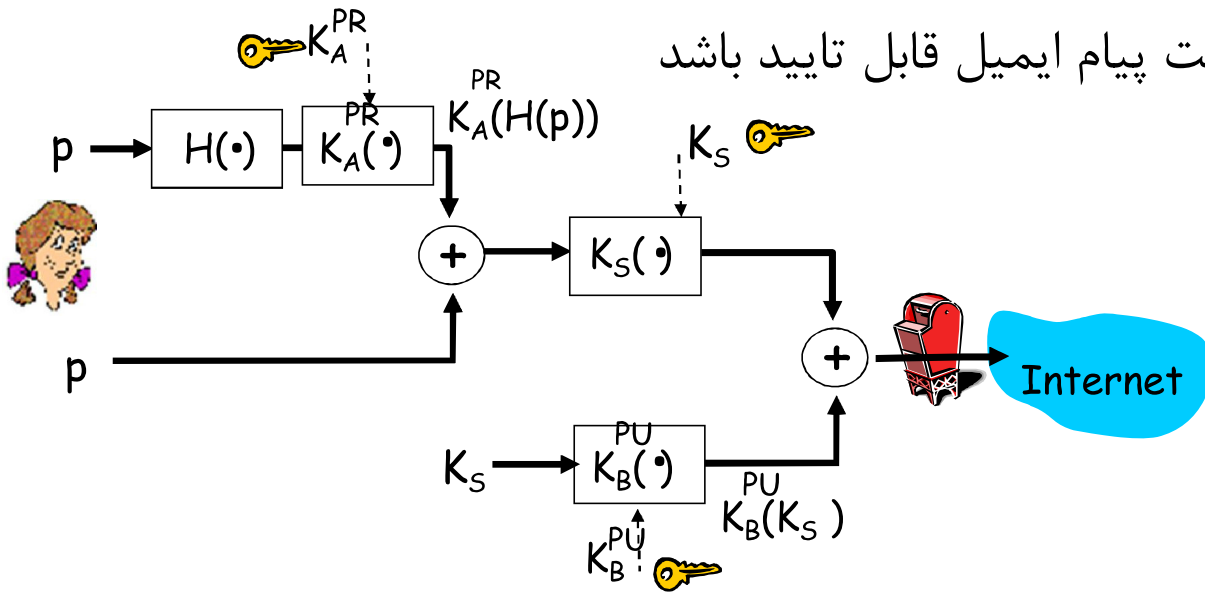
# Secure Email

• Alice می خواهد به Bob یک ایمیل بفرستد

– محرمانه باشد

– هویت فرستنده قابل تایید باشد

– صحت پیام ایمیل قابل تایید باشد



# Pretty Good Privacy (PGP)

- استاندارد برای ارسال ایمیل های امن
- استفاده از:
  - رمزنگاری متقارن
  - رمزنگاری کلید عمومی
  - تابع Hash
  - امضای دیجیتال
- فراهم کردن:
  - محرمانگی
  - تایید هویت فرستند
  - صحت پیام

# خلاصه

Block Cipher یا Stream Cipher	Asymmetric یا Symmetric	الگوریتم
Block Cipher	Symmetric	DES
Block Cipher	Symmetric	2DES
Block Cipher	Symmetric	3DES
Block Cipher	Symmetric	AES
Stream Cipher	Symmetric	RC4
Block Cipher	Asymmetric	RSA

# خلاصه

Public Key (Asymmetric)	Secret Key (Symmetric)	خصوصیت
۲	۱	تعداد کلید
کلید خصوصی باید به صورت امن نگهداری شود کلید عمومی می تواند در معرض عموم قرار گیرد	باید به صورت امن نگهداری شود	نگهداری کلید
تعویض کلید و تأیید هویت	رمز کردن و صحت	استفاده
کلید عمومی می تواند برای توزیع دیگر کلیدها استفاده شود	مشکل دارد	تبادل کلید
خیلی پایین	بالا	سرعت