

دانشگاه آزاد اسلامی واحد تبریز



نام درس: سیستم مدیریت امنیت اطلاعات

بخش: رمزنگاری

نام استاد: دکتر مسعود کارگر

فهرست مطالب

رمزنگاری

☐ روش‌های مختلف رمزنگاری کلاسیک / مدرن

☐ روش رمزنگاری متقارن

☐ روش رمزنگاری نامتقارن



روش‌های مختلف مقابله با حمله از طریق رمزنگاری

► رمزنگاری در ایجاد سرویس‌های امنیتی زیر کاربرد دارد:

✓ محرمانگی

- اطمینان از اینکه تنها کاربران مورد نظر قادر به درک پیام‌ها می‌باشند.
- رمزگذاری

✓ هویت شناسی

- اطمینان از این که کاربر همانی است که ادعا می‌کند.
- امضا

✓ عدم انکار

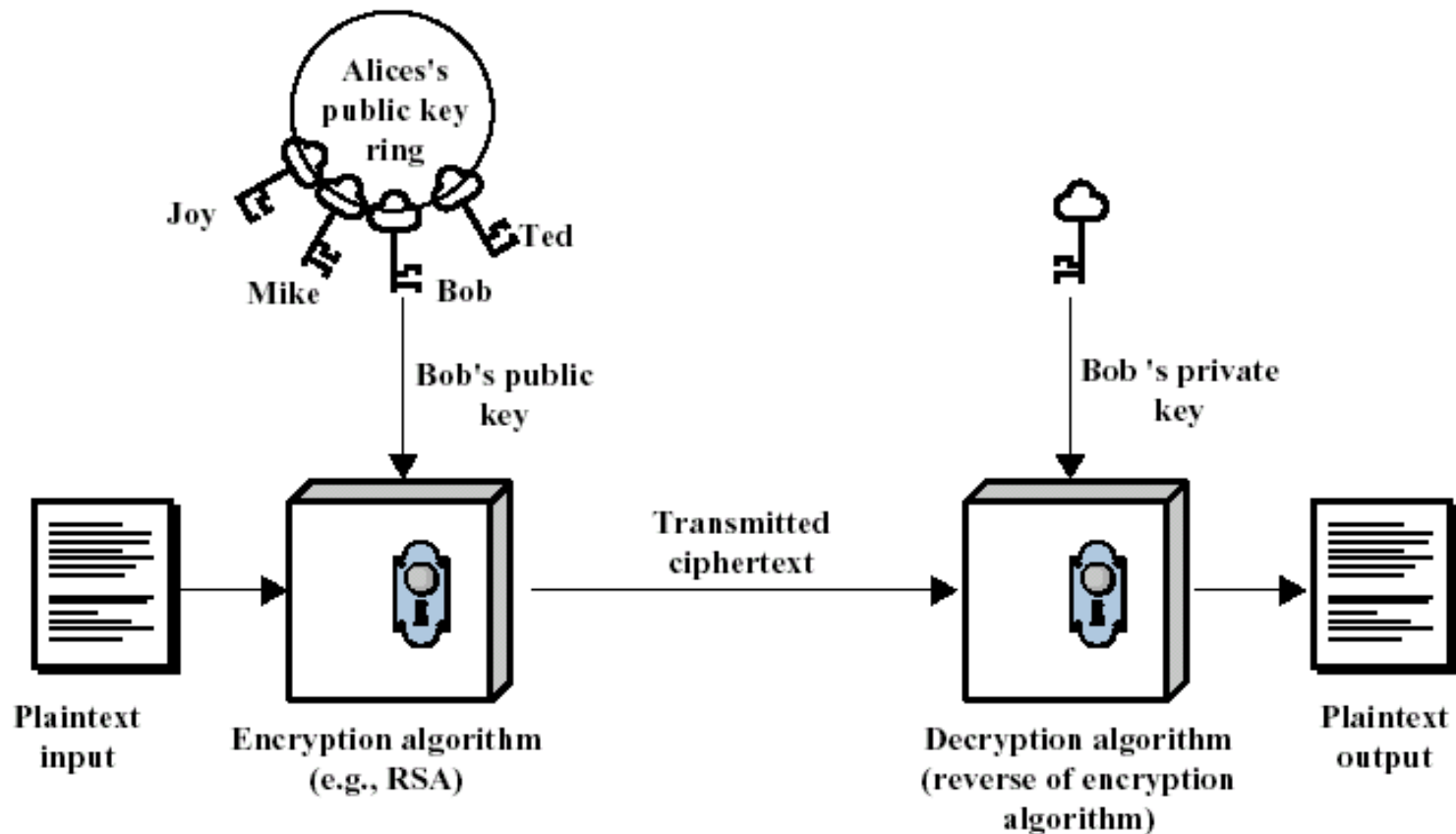
- عدم امکان انکار دریافت یا ارسال توسط گیرنده و فرستنده.
- امضاء

✓ جامعیت

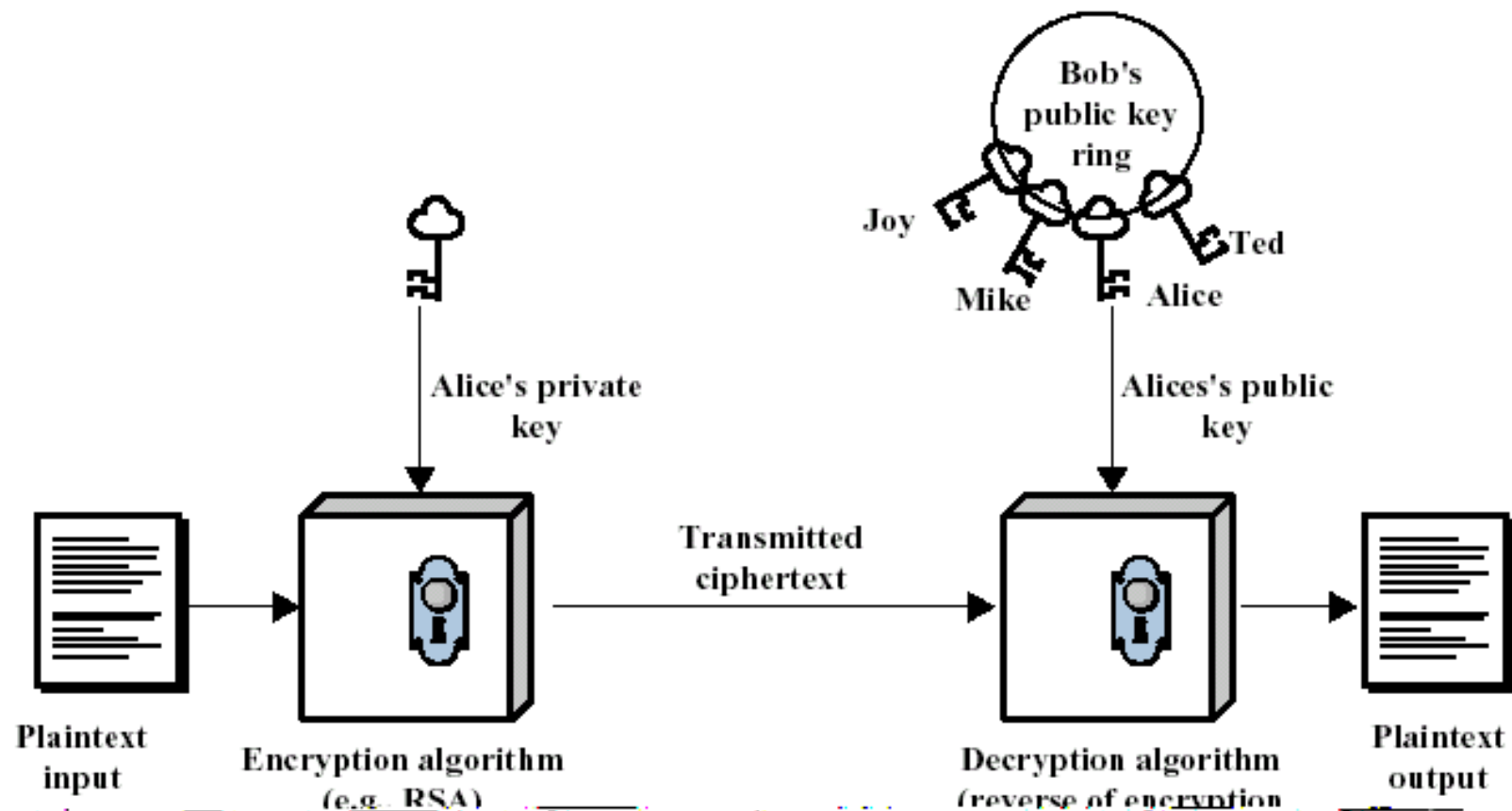
- اطمینان از اینکه آنچه رسیده همان است که فرستاده شده.
- امضاء



سرویس امنیتی رمزنگاری-محرمانگی



سرویس امنیت رمزنگاری-هویت شناسی



روش رمزنگاری سزار

- تک حرفی
- چند حرفی
- ✓ تعریف

- رمزنگاری $C = (P + K) \bmod 26$

- رمزگشایی $P = (C - K) \bmod 26$

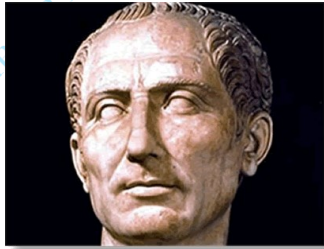
- **P** علامت اختصاری متن ساده (Plain Text)

- **C** علامت اختصاری رمزمتن (Cipher Text)

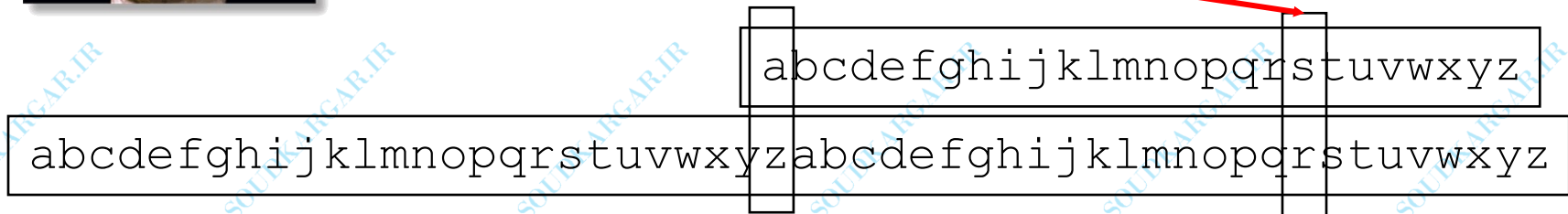
- **K** علامت اختصاری کلید

- **ورودی** : مجموعه ۲۶ حرفی الفبای انگلیسی

مثال (روش سزار) - تک الفبایی



send another catapult



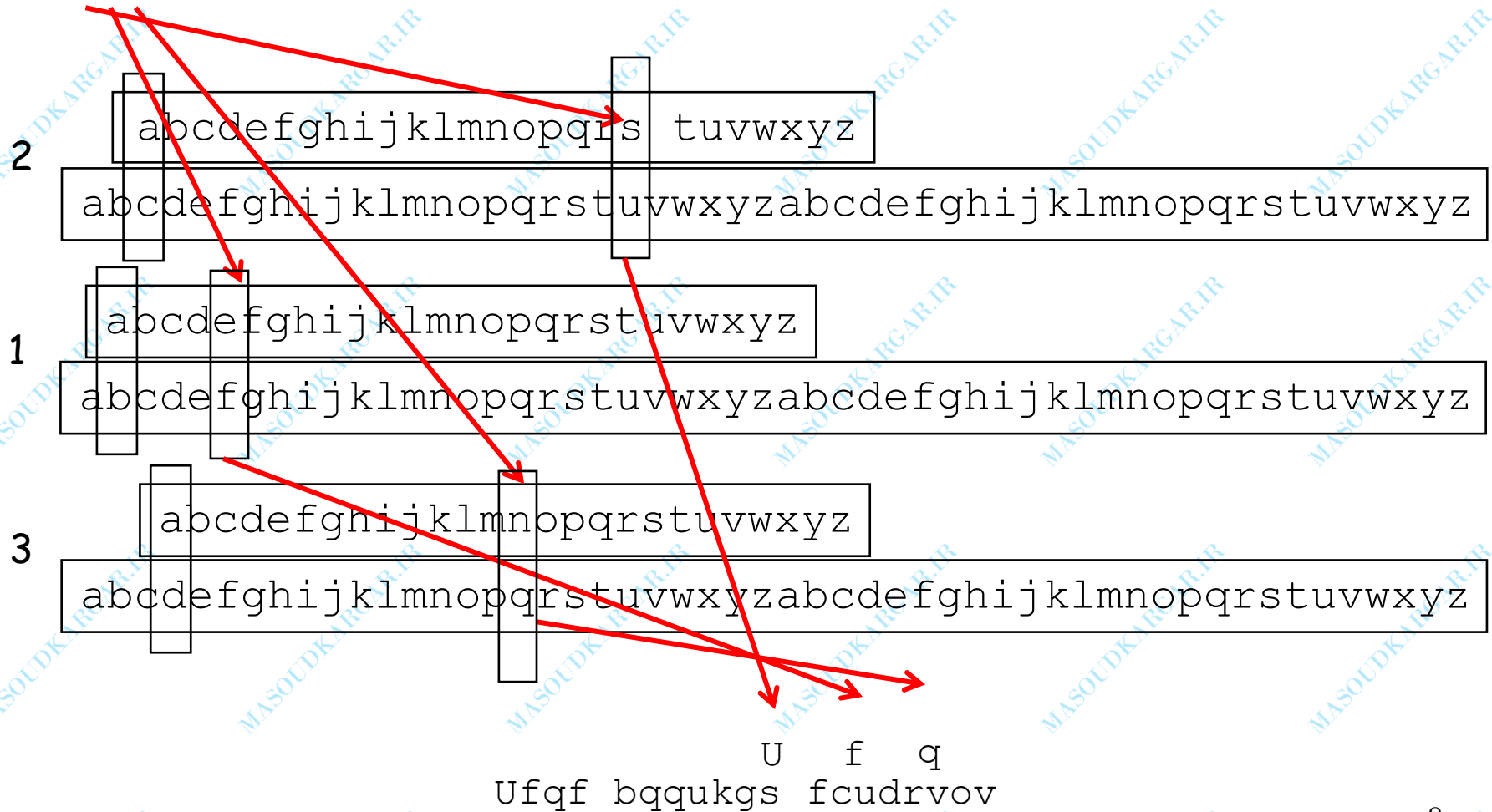
$$K = y$$

$$C = P + K \pmod{26}$$

rdmc zmnsqds bzsotks

مثال (جانشینی ۲۱۳) - چند الفبایی

send another catapult



مثال-جدول ویجنر

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

• استفاده از کلمه در ترکیب با متن

• و انجام محاسبات در پیمانه ۲۶

M = SEND ANOTHER CATAPULT

K = hail ceaserhailcease

C = zevo crolvyciectudx

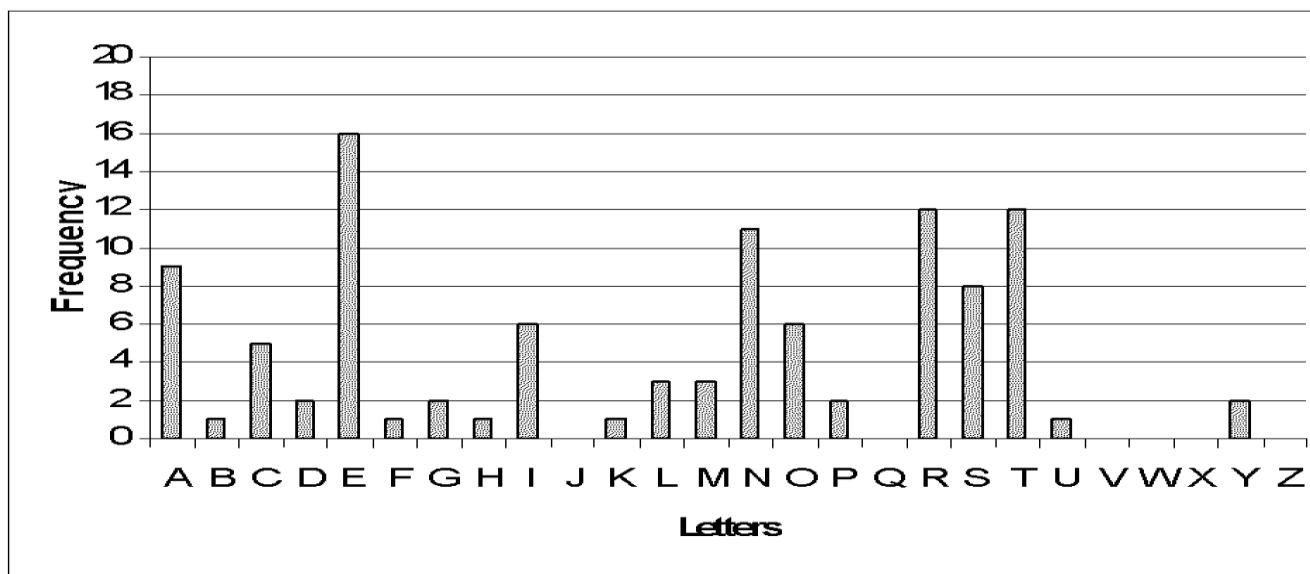
C = zevo crolvyciectudx

K = hail ceaserhailcease

M = SEND ANOTHER CATAPULT

مثال (تحلیل)

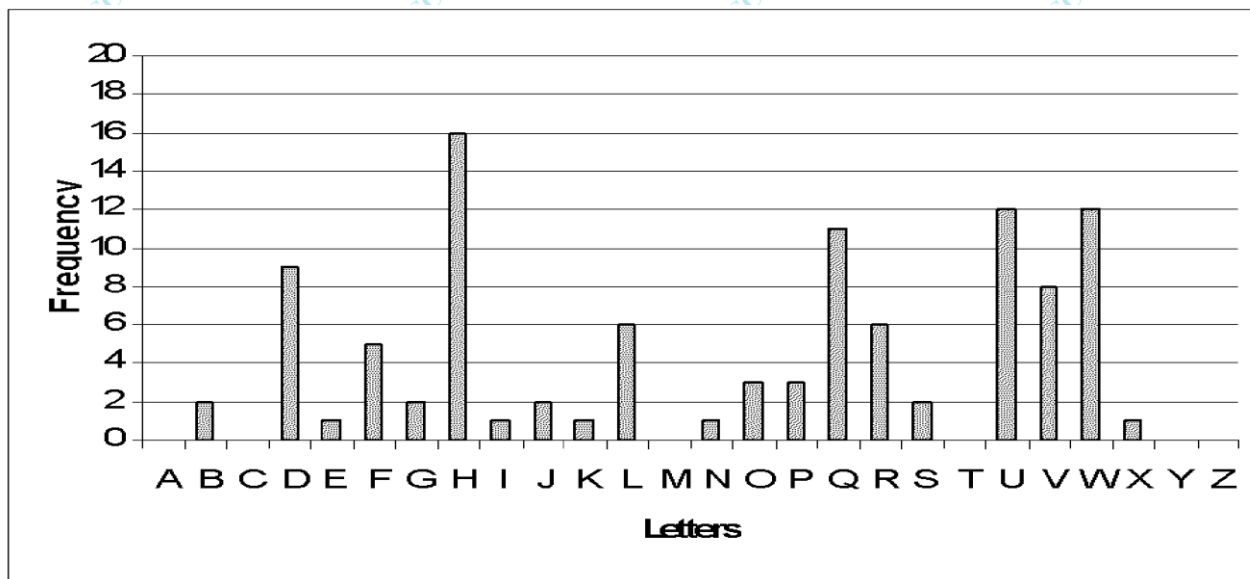
Aerial reconnaissance reports enemy reinforcements estimated at battalion strength entering your sector PD Clarke



فراوانی حروف متن اصلی

مثال (تحلیل سیستم رمز جانشینی سزار)

DHULDOUHFRRQQLVVDQFHUHSRUWVHQHPBUH . . .



فراوانی حروف متن رمز شده (تک الفبایی)

روش رمزنگاری جایگشتی

✓ رمزنگاری

- مبتنی بر جابجایی جای کاراکترها در رشته متن واضح و ارسال به گیرنده.

✓ رمزگشایی

- عمل جایگشت معکوس انجام و تولید متن واضح از روی متن رمز شده.

✓ کلید

- الگوی جایگشت.

✓ هدف

- diffusion (درهم ریختگی) بیشتر است.

مثال (رمزنگاری جایگشتی)

M E G A B U C K

7 4 5 1 2 8 3 6

p l e a s e t r

a n s f e r o n

e m i l l i o n

d o l l a r s t

o m y s w i s s

b a n k a c c o

u n t s i x t w

o t w o a b c d

Plaintext

pleasetransferonemilliondollarsto
myswissbankaccountsixtwo

Ciphertext

AFLLSKSOSELAWAIATOOSSCTCLNMOMANT
ESILYNTWRNNTSOWDPAEDOBUEOERIRICXB

روش رمزنگاری Hill

✓ ادغام بیش از سه حرف برای استحکام بیشتر در مقابل حملات مبتنی بر شاخص های آماری متن.

✓ هر حرف انگلیسی به ترتیب با عددی صحیح بین ۰ تا ۲۵ ($A=0; B=1; C=2; \dots$) جایگزین می شود.

✓ متن در قالب گروه های n حرفی به n حرف جدید نگاشته می شوند. الگوی تبدیل با روابط خطی زیر توصیف می شود:

$$C = (K.P) \bmod 26$$

• C و P دو ماتریس $n \times 1$

• K ماتریس $n \times n$

مثال (رمزنگاری Hill)

Plain Text

→ "ACT" →

$$\begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix}$$

$$\text{Key} = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

$(K \cdot P) \bmod 26$

$C =$



POH

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 19 \end{pmatrix} = \begin{pmatrix} 67 \\ 222 \\ 319 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 14 \\ 7 \end{pmatrix} \pmod{26}$$

روش‌های مدرن رمزنگاری

✓ رمزنگاری متقارن

• کلید یکسان برای رمزگذاری و رمزگشایی استفاده می شود.

- DES (Data Encryption Standard)
- AES(Advanced Encryption standard)
- Blowfis

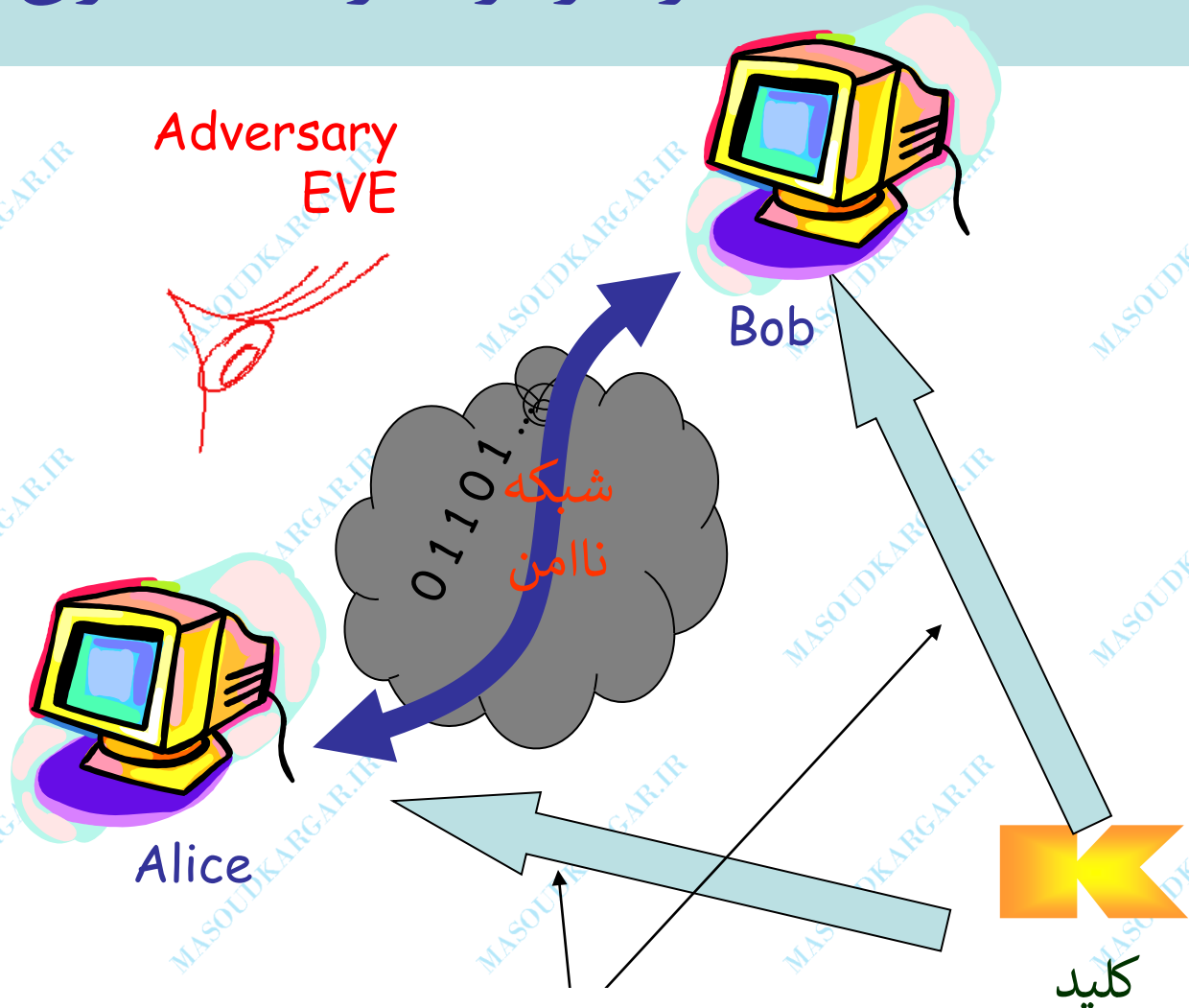
✓ رمزنگاری نامتقارن

• هر کاربر یک کلید عمومی و یک کلید اختصاصی دارد.

• رمزگذاری با کلید عمومی و رمزگشایی توسط کلید اختصاصی انجام می شود.

- RSA(Rivest , Shamir , Adlemen)
- Diffie-Hellman
- ElGamal

عملکرد رمزنگاری متقارن



به طور امن منتقل میشود

کلید
متقارن

ابزار رمزنگاری

✓ رمزهای متقارن را می توان با ابزارهای متفاوتی تولید کرد.

- ابزارهای مهم :

- رمزهای قطعه ای (قالبی)

- پردازش پیغام ها بصورت قطعه به قطعه

- سائز متعارف قطعات ۶۴، ۱۲۸ یا ۲۵۶ بیت

- رمزهای دنباله ای

- پردازش پیغام ها بصورت پیوسته

رمزهای قطعه ای

متن واضح (تقسیم شده به قطعات)



قطعات خروجی

اصول رمزهای قطعه ایی

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

قطعه ۶۴ بیتی متن اصلی

رمزنگاری DES

جایگشت اولیه

دور ۱

دور ۲

دور ۱۵

دور ۱۶

جایگشت معکوس

قطعه ۶۴ بیتی متن رمز شده

زیر کلید دور

تولید زیر کلیدها
از کلید اصلی ۵۶
بیتی برای هر دور

✓ DES از روشهای جانشینی و جایگشتی

استفاده میکند.

✓ ورودی رشته ۶۴ بیتی است.

✓ جابجا کردن محل بیت‌های رشته ۶۴ بیتی

(جایگشت اولیه).

✓ مجموعاً ۱۶ کلید مختلف وجود دارد.

✓ رشته ۶۴ بیتی جدید از وسط به دو قسمت

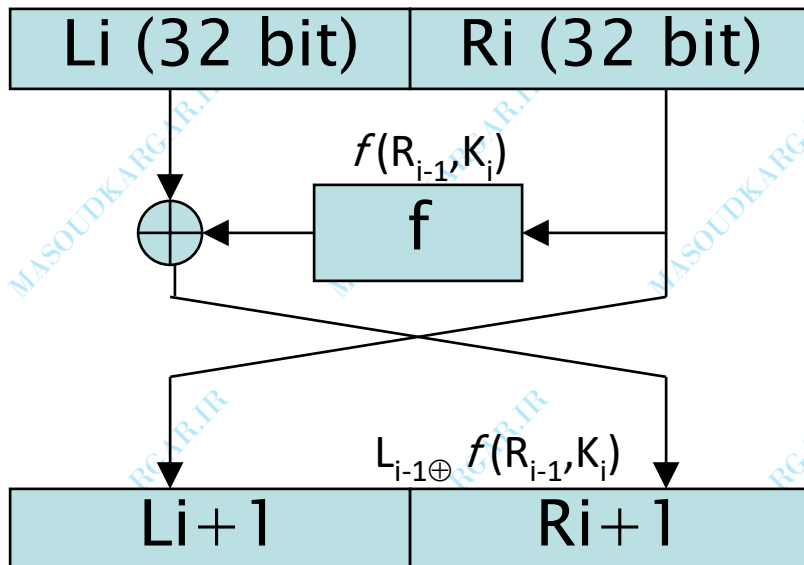
۳۲ بیتی چپ و راست تقسیم می‌شود.

✓ عکس عمل جایگشتی که در ابتدا انجام شده

بود صورت می‌گیرد تا بیت‌ها سر جای‌شان برگردند.

✓ ارسال متن رمز شده.

رمزنگاری DES



✓ ۳۲ بیت سمت چپ را L_i و ۳۲ بیت سمت راست را R_i می‌نامیم .

✓ شکل روبرو یک مرحله از ۱۶ مرحله عملیات را نشان می‌دهد.

در هر مرحله ۳۲ بیت سمت راست مستقیماً به سمت چپ منتقل شده و ۳۲ بیت سمت چپ طبق رابطه زیر به یک رشته بیت جدید تبدیل و به سمت راست منتقل خواهد شد.

$$L_{i-1} \oplus f(R_{i-1}, K_i)$$

✓ پس از مرحله آخر جای R_i و L_i عوض خواهد شد.

رمزنگاری نامتقارن

- کلید های رمزگذاری و رمزگشایی متفاوت اما مرتبط هستند.

- برای رمزنگاری کلید عمومی گامهای زیر را برمیداریم:

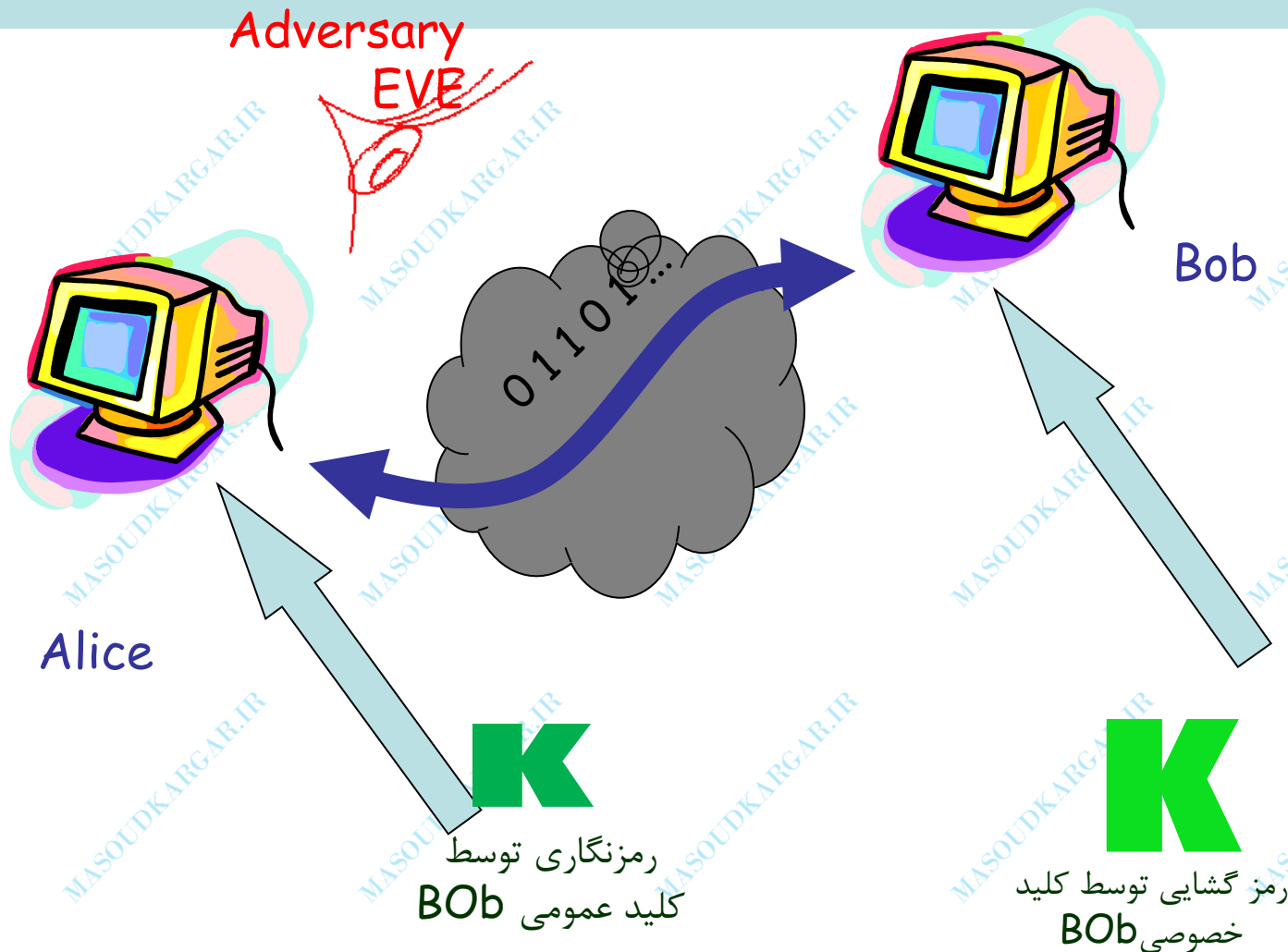
- ✓ هر کاربر یک زوج کلید رمزگذاری و رمزگشایی تولید میکند.

- ✓ کاربران کلید رمزگذاری خود را به صورت عمومی اعلان میکنند درحالی که کلید رمزگشایی مخفی میباشد.

- ✓ همگان قادر به ارسال پیام رمز شده برای هر کاربر دلخواه با استفاده از کلید رمزگذاری (عمومی) او میباشند.

- ✓ هر کاربر میتواند با کمک کلید رمزگشایی (خصوصی) پیامهایی که با کلید رمزگذاری (عمومی) او رمز شده رمزگشایی کند.

عملکرد رمزنگاری نامتقارن



الگوریتم Diffie - Hellman

توافق بر روی مقادیر q و α

Alice

Bob

عدد تصادفی X_A را انتخاب میکند

عدد تصادفی X_B را انتخاب میکند

$$Y_A = \alpha^{X_A} \bmod q$$

$$Y_B = \alpha^{X_B} \bmod q$$

$$K_{AB} = (Y_B)^{X_A} \bmod q$$

$$K_{AB} = (X_A)^{Y_B} \bmod q$$

$$\alpha^{(X_A \times X_B)} \bmod q$$

کلید مشترک برابر است با

الگوریتم Diffie - Hellman

• مثال

– توافق روی $q=353$ و $\alpha=3$

– تولید کلیدهای مخفی

• انتخاب $x_A=97$ توسط A و $x_B=233$ توسط B

– محاسبه کلید عمومی

$$y_A = 3^{97} \bmod 353 = 40 \quad \bullet$$

$$y_B = 3^{233} \bmod 353 = 248 \quad \bullet$$

– محاسبه کلید جلسه مورد توافق

$$K_{AB} = y_B^{x_A} \bmod 353 = 248^{97} = 160 \quad \bullet$$

$$K_{AB} = y_A^{x_B} \bmod 353 = 40^{233} = 160 \quad \bullet$$

رمزنگاری RSA

✓ متن ای که باید رمز شود ، به بلوکهای K کاراکتری تبدیل می شود.

✓ هر بلوک طبق قاعده دلخواه به یک عدد صحیح تبدیل می شود. (P_i)

• با جفت عدد صحیح (e, n) برای تمام بلوکها اعداد جدیدی طبق رابطه زیر بدست می آید:

$$C_i = (P_i)^e \bmod n$$

رمزنگاری

• کلید (e, n) که با آن متن رمز می شود "کلید عمومی" (Public key) گویند.

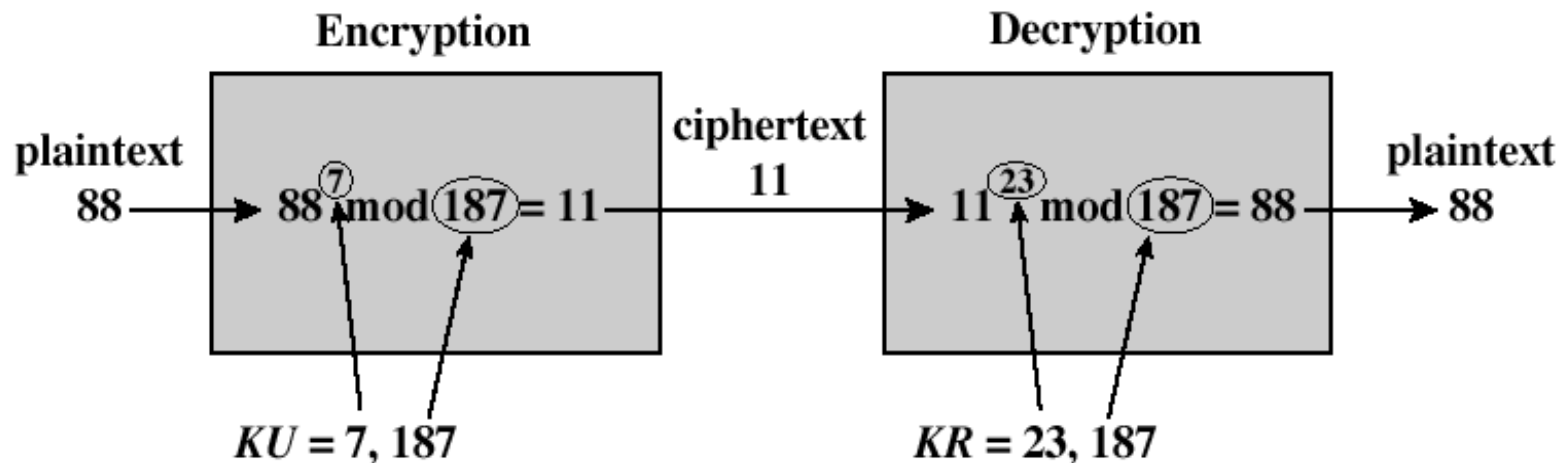
✓ کدهای C_i ، بجای متن اصلی ارسال می شود.

$$P_i = (C_i^d) \bmod n$$

رمزگشایی

• کلید (d, n) که با آن متن از رمز خارج می شود "کلید خصوصی" (Private key) گویند.

مثال (رمزنگاری RSA)



► روش انتخاب و معیارهای e , d , n

✓ انتخاب دو عدد اول دلخواه p , q .

✓ محاسبه عدد n , Z را طبق دو رابطه روبرو:

$$p = 17, q = 11$$

$$n = p * q = 187$$

$$Z = p-1 * q-1 = 160$$

$$\text{pick } e = 7$$

✓ انتخاب عدد e بگونه ای که نسبت به Z اول باشد.

✓ انتخاب عدد d بر اساس e بگونه ای انتخاب کنید تا رابطه زیر برقرار باشد:

$$d.e = 1 \bmod Z \rightarrow d = 23$$

برنامه پایتون برای محاسبه مقدار **d**

```
for i in range(10000):  
    d=((i*7))%160  
    if d==1:  
        print(i)
```