به نام خدا

دانشکده مهندسی برق،
دانشگاه صنعتی شریف

مبانی رمزنگاری و امنیت شبکه

سیستم‌های رمزنگاری کلید همگانی

Public Key Cryptography

مهتاب میرمحسنی

نیم‌سال دوم (بهار) ۹۸-۹۹

مقدمه

- رمزنگاری متقارن
  - جانشینی و جابجایی
  - انتقال امن کلید: تعداد کلید مورد نیاز برای ارتباط n کاربر $\binom{n}{2}=\frac{n(n-1)}{2}$
- رمزنگاری کلید همگانی
  - انقلاب در تاریخ رمزنگاری
  - بر اساس توابع ریاضی
  - نامتقارن بر پایه دوکلید
- سیستم نامتقارن یا دو کلیدی (Asymmetric=Two Key)
  - رابطه مشکل (یک طرفه) میان تبدیلات (کلیدهای) رمزگذاری و رمزگشایی
  - یکی از کلیدها می‌تواند آشکار (همگانی) باشد ← رمزنگاری کلید همگانی
  - به دنبال حل مساله توزیع کلید و امضا در رمز متقارن، پیدا شد

رمزنگاری کلید همگانی

- برخی برداشت‌های نادرست از این سیستم‌ها وجود دارد

1. رمزنگاری کلید همگانی (نامتقارن) امن‌تر از رمزنگاری متقارن است!
   - امنیت وابسته به طول کلید و امکان پردازش (قدرت محاسباتی) دشمن می‌باشد
2. با معرفی رمزنگاری کلید همگانی، رمزهای متقارن کاربردی ندارند!
   - سربار محاسبات پیچیده در رمزنگاری کلید همگانی
   - توزیع کلید و امضا
3. مساله توزیع کلید در رمزنگاری کلید همگانی بدیهی است!
   - باید مطمئن شویم که کلید همگانی متعلق به شخص مدعی است
   - نیاز به مرجع سوم و پروتکل مربوطه دارد

مفاهیم

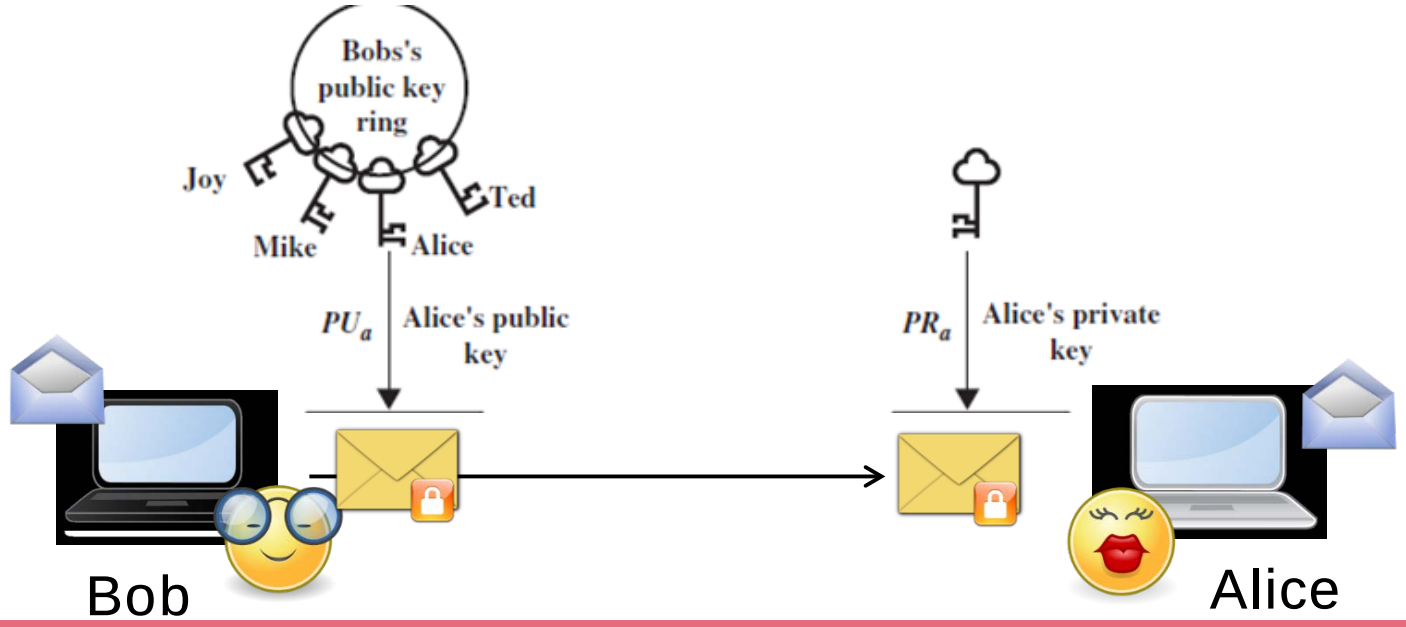
- کلیدهای نامتقارن: دو کلید برای رمزگذاری و رمزگشایی (یا امضا و تایید آن)
  - کلید همگانی (PU)
  - کلید خصوصی (PR)
  - بدست آوردن کلید خصوصی از روی کلید همگانی (از نظر محاسباتی) غیر ممکن است
- گواهی‌نامه کلید همگانی (Public Key Certificate)
  - گواهی‌نامه‌ای از طرف مرجع معتبر جهت اختصاص کلید به کاربرها (امضا شده توسط کلید خصوصی مرجع معتبر)
- زیرساخت کلید همگانی (Public Key Infrastructure (**PKI**))
  - زیرساختی برای صدور، نگهداری و ابطال (revoke) گواهی‌نامه و زوج کلیدها
  - مجموعه‌ای از سیاست‌ها، پردازش‌ها، سرورها، نرم‌افزارها و ...

سیستم‌های رمزنگاری کلید همگانی
Public Key Cryptosystems

- معرفی در سال ۱۹۷۶ توسط دیفی و هلمن (Diffie & Hellman)
  - حل مساله توزیع کلید و امضا
- معرفی مستقلاً توسط مرکل (Merkle)
- هر کاربر دارای دو کلید است: مثلاً کاربر A
  - یک کلید همگانی (public): همه می‌دانند (PU_a)
  - یک کلید خصوصی (private) مخفی: تنها نزد خود کاربر (PR_a)
  - توابع یک‌طرفه:
    - محاسبه PR از روی PU از نظر محاسباتی غیرممکن
    - محاسبه PU از روی PR ساده
- کلید سیستم‌های متقارن: کلید مخفی (secret)
- برخی الگوریتم‌ها مانند RSA: یکی از کلیدها برای رمزگذاری و دیگری برای رمزگشایی

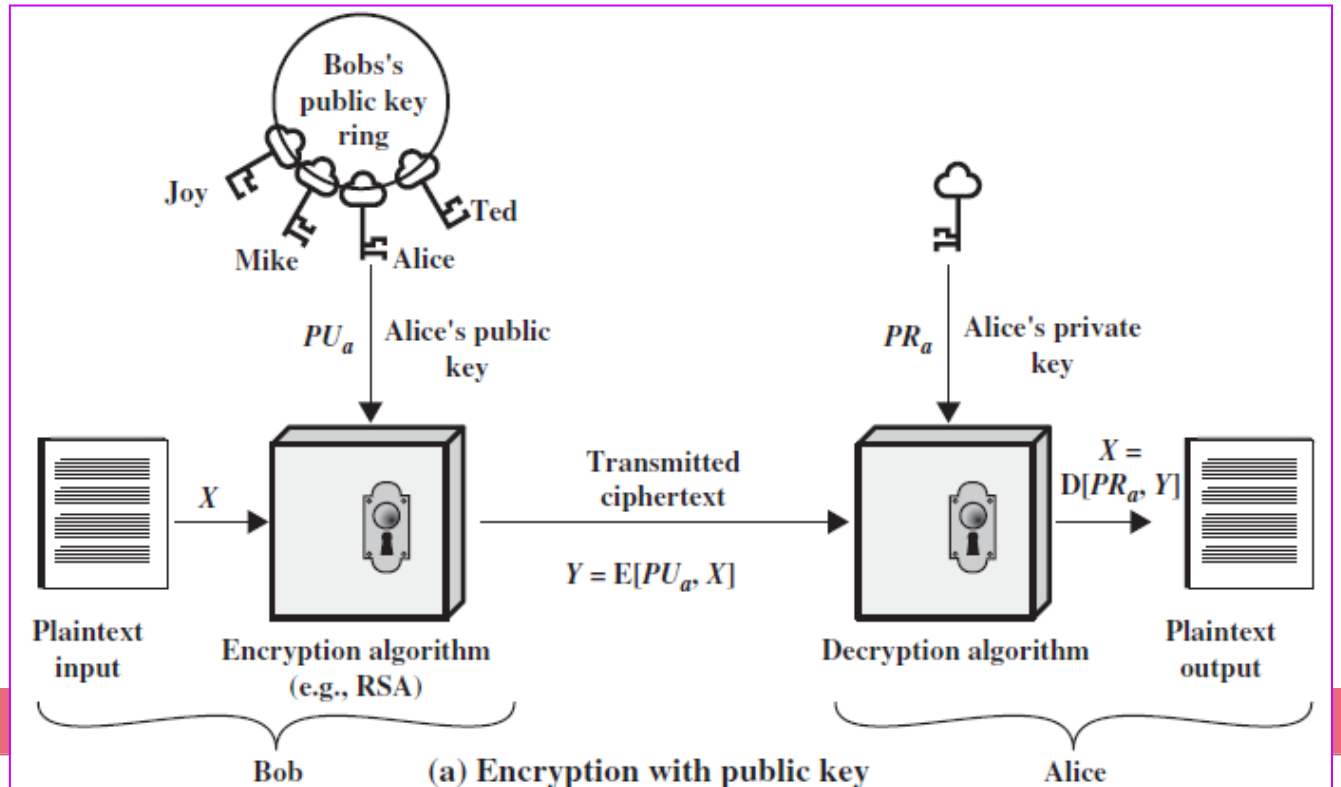
رمزگذاری با کلید همگانی

- هر کاربر دو کلید تولید می‌کند
  - یکی را در اختیار دیگران قرار می‌دهد (در یک فایل قابل دسترس): کلید همگانی
  - کلید دیگر: کلید خصوصی
- باب برای ارسال پیام **محرمانه** به آلیس، آن را با کلید همگانی آلیس رمز و ارسال می‌کند
- آلیس، پیام دریافتی را با کلید خصوصی خود (تنها در اختیار آلیس) می‌گشاید



رمزگذاری با کلید همگانی

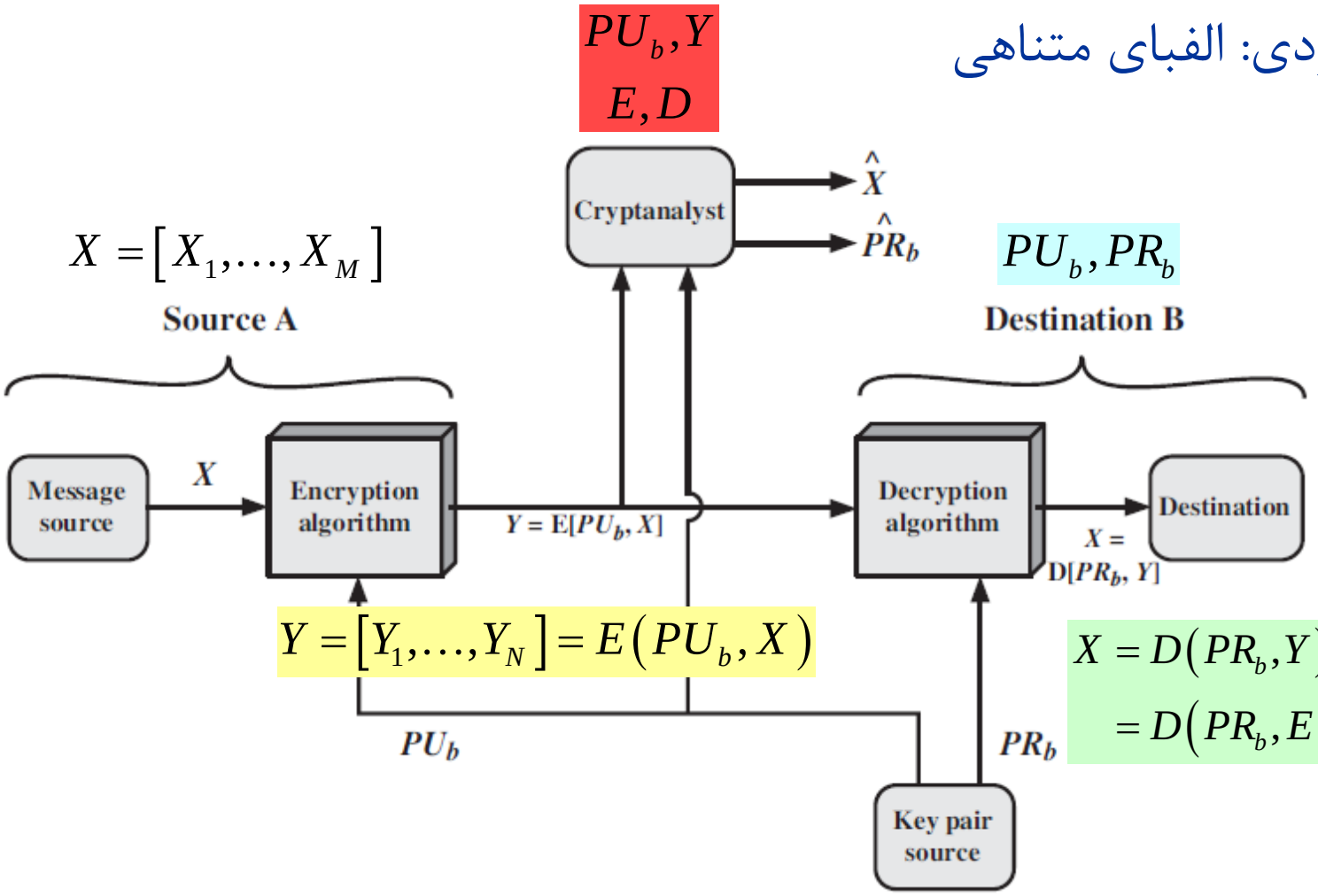
- همه کلیدهای همگانی را دارند
- کلیدهای خصوصی توزیع نمی‌شوند
- امنیت: تا زمانی‌که کلید خصوصی مخفی بماند
- با تغییر کلید خصوصی توسط کاربر، کلید همگانی متناظر جدید، انتشار می‌یابد



(a) Encryption with public key

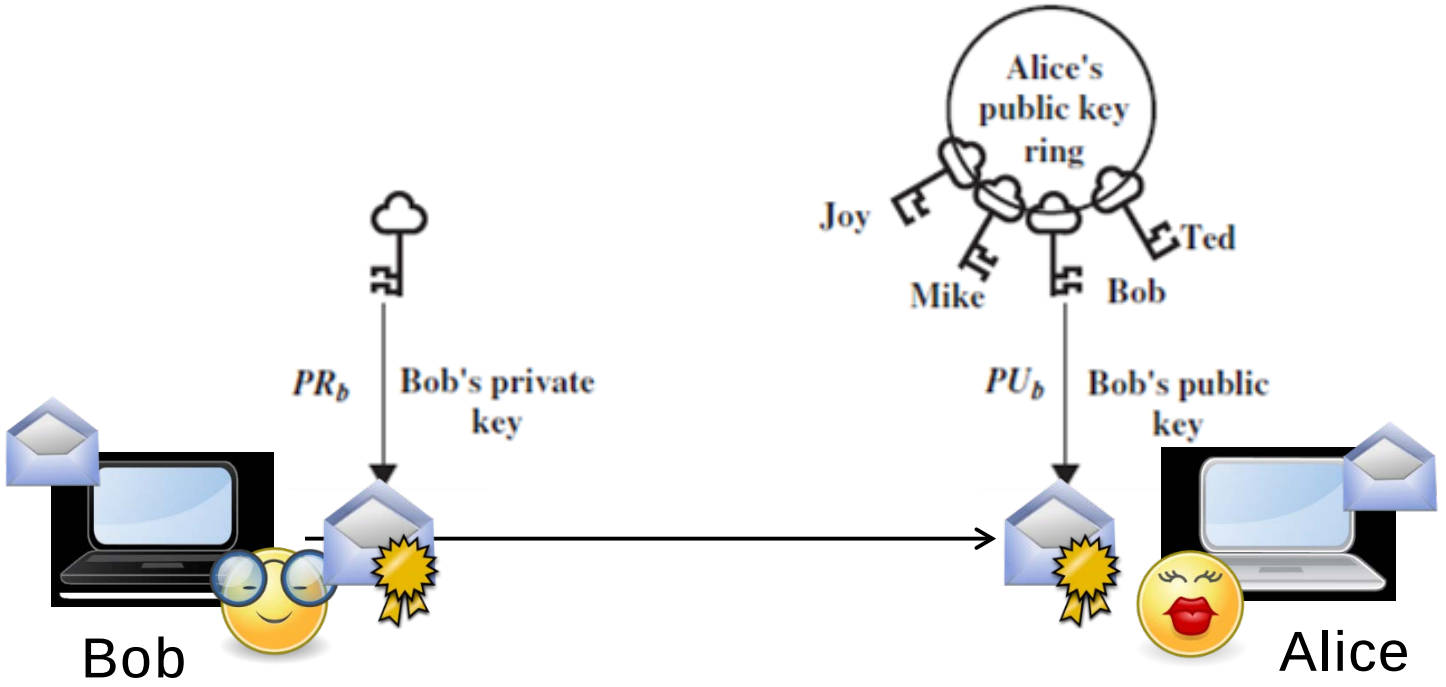
محرمانگی با استفاده از رمزنگاری کلید همگانی

- رمزگذاری با کلید همگانی گیرنده
- ورودی: الفبای متناهی

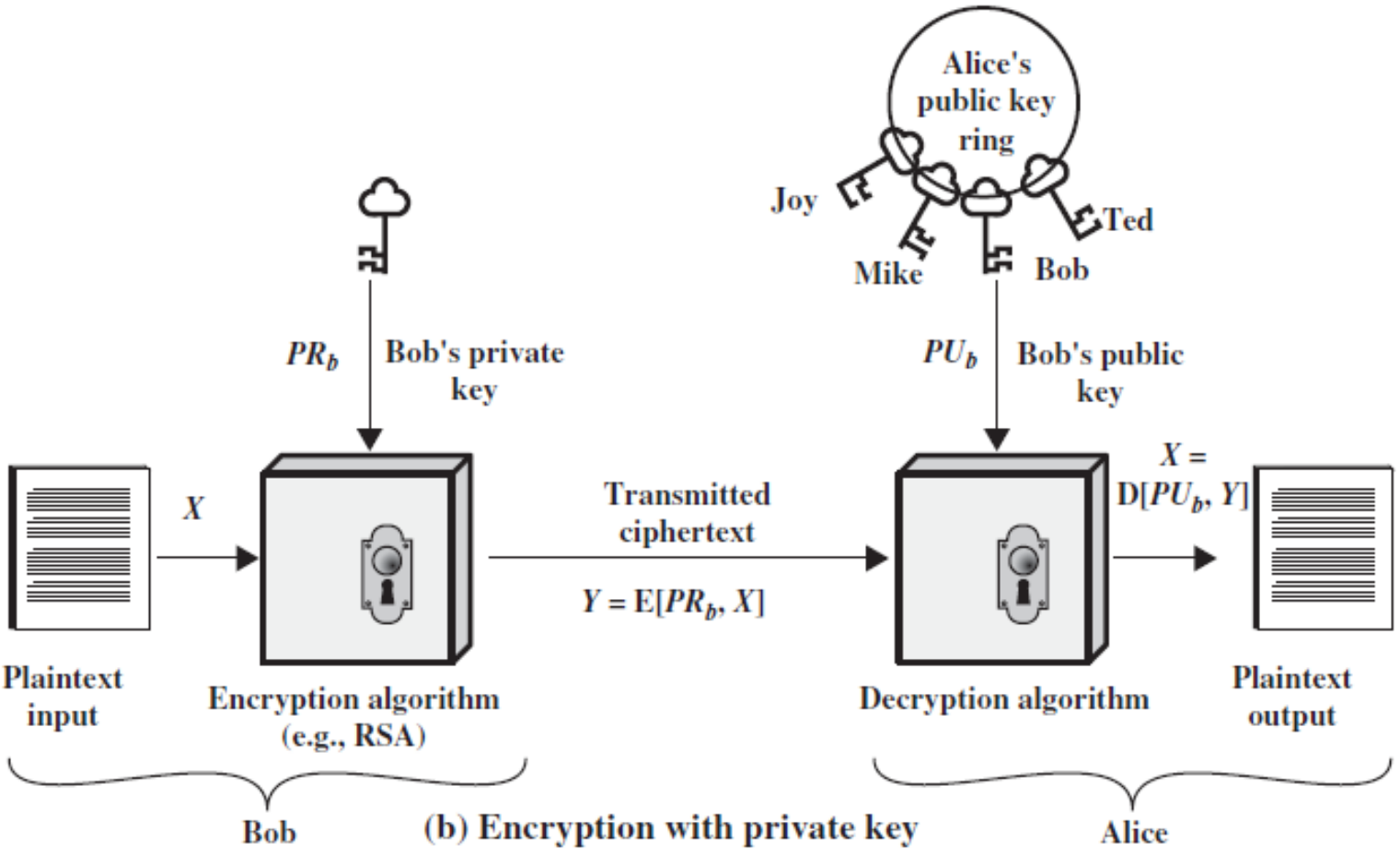


رمزگذاری با کلید خصوصی

- باب پیام ارسالی را توسط کلید خصوصی خود رمز و ارسال می‌کند
- آلیس با استفاده از کلید همگانی باب آن را رمزگشایی می‌کند
- احراز اصالت منبع و پیام (یکپارچگی داده)، امضای دیجیتال



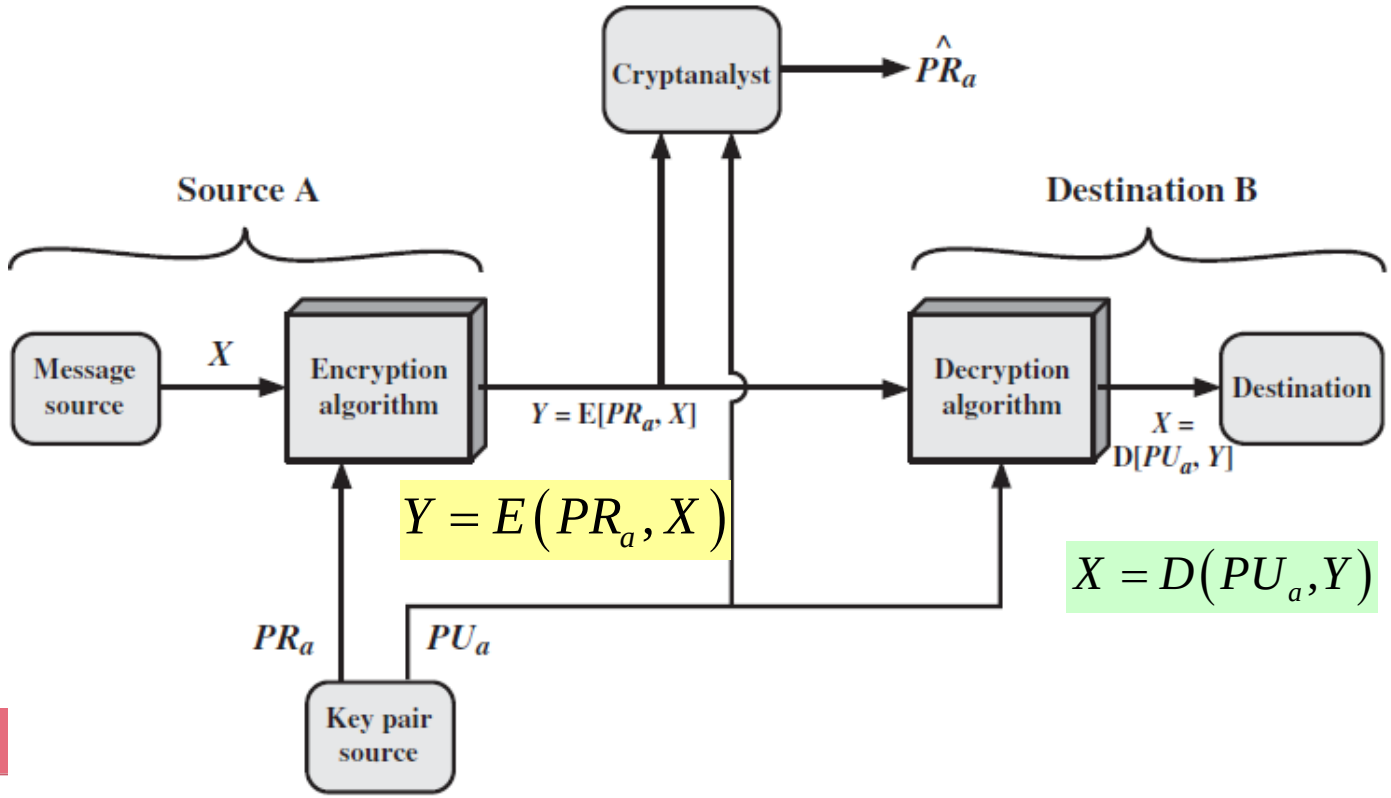
رمزگذاری با کلید خصوصی



(b) Encryption with private key

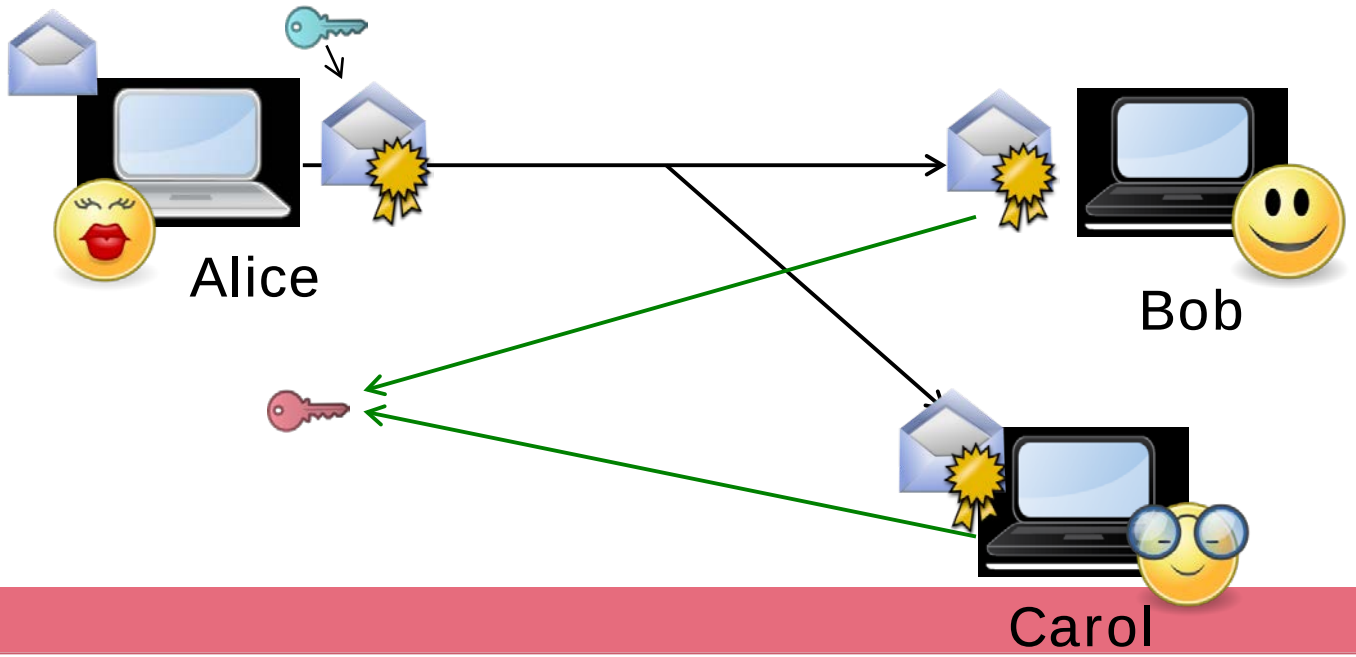
احراز اصالت با استفاده از رمزنگاری کلید همگانی امضای دیجیتال

- عدم ایجاد محرمانگی: کلید همگانی A را همه می‌دانند
- کلید خصوصی A تنها در اختیار خودش است
  - تنها A می‌تواند این پیام را بفرستد ← امضای دیجیتال (احراز اصالت منبع- انکارناپذیری)
  - بدون دسترسی به این کلید خصوصی، امکان تغییر پیام وجود ندارد (احراز اصالت پیام- یکپارچگی داده)



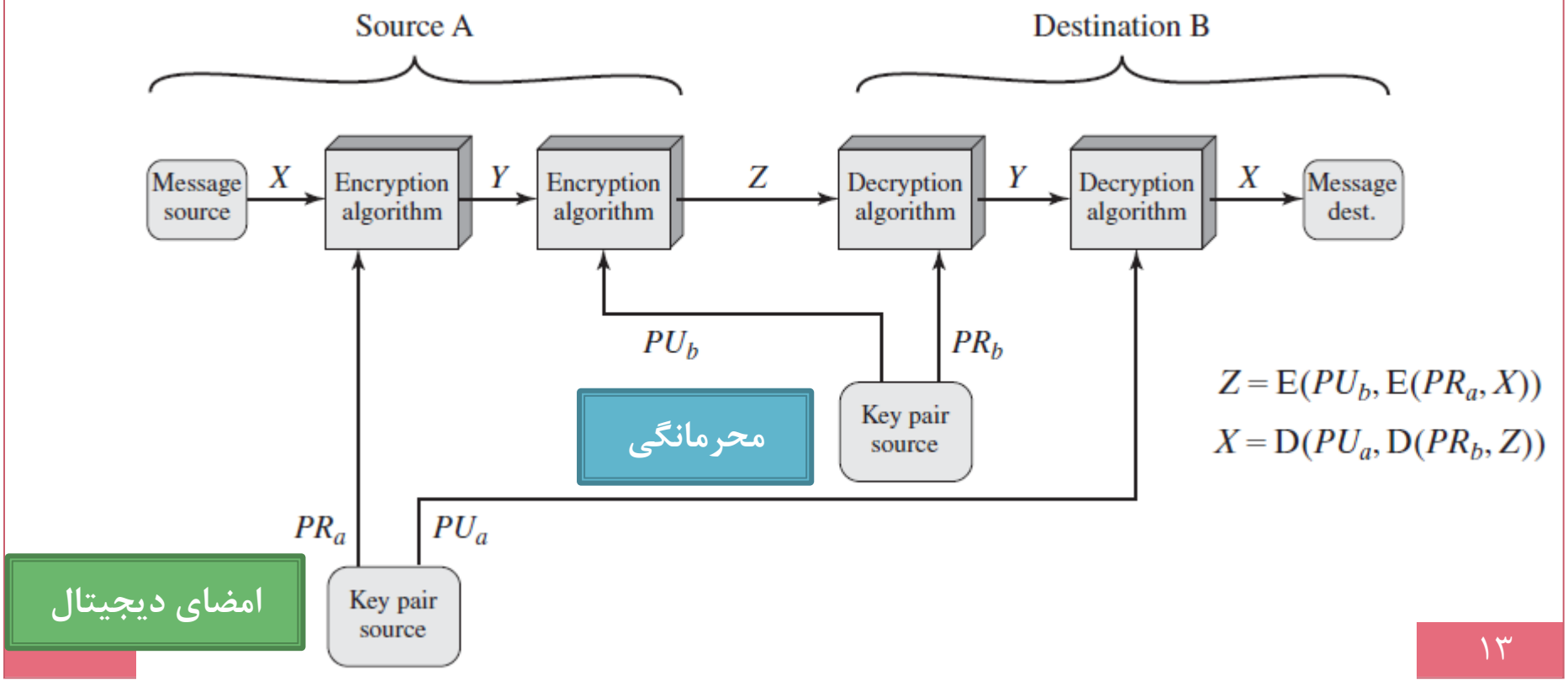
احراز اصالت با استفاده از رمزنگاری کلید همگانی
امضای دیجیتال

- نیاز به حافظه زیاد
  - هر متن اصلی و متن رمزشده متناظر باید ذخیره شوند (جهت بررسی در صورت اختلاف)
- قسمتی (یا تابعی) از پیام رمز شود (authenticator)
  - بدون تغییر آن، نتوان متن اصلی را تغییر داد
  - اگر با کلید خصوصی فرستنده رمز شود، امضایی است که منبع، محتوای داده و ترتیب آن را تایید می‌کند



محرمانگی و احراز اصالت توام در سیستم‌های کلید همگانی

- دو بار استفاده از رمز کلید همگانی
- ایراد: چهار بار اعمال الگوریتم پیچیده (محاسباتی) کلید همگانی



کاربردهای سیستم‌های رمزنگاری کلید همگانی

- **رمزنگاری (محرمانگی)**
  - فرستنده پیام را با استفاده از کلید همگانی گیرنده رمز می‌کند
- **امضای دیجیتال**
  - فرستنده پیام (یا authenticator) را با کلید خصوصی خود امضا می‌کند
- **مبادله کلید (Key exchange)**
  - دو طرف جهت توافق بر کلید نشست (کلید مخفی رمز متقارن) مشارکت می‌کنند
  - روش‌های متفاوتی بر پایه کلید خصوصی یک طرف یا هر دو طرف وجود دارد

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No

الزامات سیستم‌های رمزنگاری کلید همگانی

در کار اولیه دیفی و هلمن، الگوریتم مناسب دو سیستم قبلی پیشنهاد نشده بود ولی الزامات چنین الگوریتمی مطرح شده بود

1. تولید زوج کلید (همگانی و خصوصی) برای هر کاربر از نظر محاسباتی ساده باشد

2. تولید متن رمز شده برای کاربر A، با دانستن پیام و کلید همگانی گیرنده (PU_b)، از نظر محاسباتی ساده باشد

$$C = \mathrm{E}(PU_b, M)$$

3. رمزگشایی متن رمز شده برای کاربر B، با دانستن کلید خصوصی خود (PR_b)، از نظر محاسباتی ساده باشد

$$M = \mathrm{D}(PR_b, C) = \mathrm{D}[PR_b, \mathrm{E}(PU_b, M)]$$

الزامات سیستم‌های رمزنگاری کلید همگانی

4. بدست آوردن کلید خصوصی (PR_b) برای مهاجم با دانستن کلید همگانی (PU_b)، از نظر محاسباتی غیر ممکن باشد

5. بدست آوردن پیام (M) برای مهاجم با دانستن کلید همگانی (PU_b) و متن رمزشده (C)، از نظر محاسباتی غیر ممکن باشد

6. ترتیب دو کلید مهم نباشد (شرط لازم نیست)

$$M = \mathrm{D}[PU_b, \mathrm{E}(PR_b, M)] = \mathrm{D}[PR_b, \mathrm{E}(PU_b, M)]$$

تابع یک‌طرفه دریچه‌دار
trap-door one-way function

- تابع یک‌طرفه: تابع یک-به-یکی که محاسبه آن از نظر محاسباتی ساده ولی محاسبه معکوس (یکتا) آن از نظر محاسباتی غیر ممکن باشد
  - ساده: قابل محاسبه در زمان چندجمله‌ای
  - کلاس P از نظر پیچیدگی

$Y = \mathrm{f}(X)$ easy

$X = \mathrm{f}^{-1}(Y)$ infeasible

- تابع یک‌طرفه دریچه‌دار: تابع یک‌طرفه‌ای که محاسبه معکوس آن با داشتن اطلاعات اضافه (دریچه) ساده باشد

$Y = \mathrm{f}_k(X)$ easy, if k and X are known

$X = \mathrm{f}_k^{-1}(Y)$ easy, if k and Y are known

$X = \mathrm{f}_k^{-1}(Y)$ infeasible, if Y is known but k is not known

- طراحی الگوریتم کلید همگانی، متناظر با یافتن تابع یک‌طرفه دریچه‌دار مناسب است

حملات سیستم‌های رمزنگاری کلید همگانی

- حمله جستجوی فراگیر
  - راه حل: افزایش طول کلید
  - افزایش نمایی پیچیدگی رمزگذاری و رمزگشایی با طول کلید (بر اساس محاسبه تابع معکوس)
  - طول کلید مناسب برای مقابله با این حمله ← سرعت الگوریتم بسیار کم برای کاربردهای کلی
  - کاربرد سیستم‌های رمزنگاری کلید همگانی محدود به **توزیع کلید** و **امضای دیجیتال** شده است
- محاسبه کلید خصوصی از کلید همگانی
  - از نظر ریاضی اثبات نشده که غیرممکن است
  - تمامی الگوریتم‌ها (حتی RSA پرکاربرد) مورد شک است ← دید متفاوت

حملات سیستم‌های رمزنگاری کلید همگانی

- حمله پیام احتمالی (probable-message attack)
  - مخصوص رمزنگاری کلید همگانی
  - اگر طول پیام کوتاه باشد (مثلا کلید ۵۶ بیتی DES)، مهاجم با استفاده از کلید همگانی گیرنده (که در اختیار دارد) می‌تواند تمامی پیام‌های ممکن را رمز کرده و با مقایسه آن ها با متن رمز شده، پیام را بیابد
  - مستقل از طول کلید رمز الگوریتم کلید همگانی، حمله تبدیل به جستجوی فراگیر یک کلید ۵۶ بیتی می‌شود
  - مقابله: افزودن بیت‌های تصادفی به پیام‌های ساده

الگوریتم رمز RSA

- توسط Rivest-Shamir-Adleman در سال ۱۹۷۷ در MIT طراحی شد و در ۱۹۷۸ به چاپ رسید
- معروف‌ترین و پرکاربردترین الگوریتم رمزنگاری کلید همگانی
- رمز قالبی است که (هر قالب) متن اصلی و متن رمز شده اعداد صحیح بین 0 و n-1 هستند
- طول قالب معمولا برابر با ۱۰۲۴ است $n \leq 2^{1024}$
- بر اساس توان رسانی (نمای) پیمانه‌ای
- امنیت بر اساس تجزیه یک عدد به عوامل اول آن (کلاس np)

الگوریتم رمز RSA

$$C = M^{e} \bmod n$$

$$C^{d} \bmod n = \left(M^{e}\right)^{d} \bmod n = M^{ed} \bmod n \overset{?}{=} M$$

- قالب پیام M
- قالب متن رمز شده C

- n: پیمانه محاسبات= حاصلضرب دو عدد اول بزرگ $n = pq$
- کلید خصوصی: (p,q,d)
- کلید همگانی: (n,e)
- قضیه: اگر $ed \equiv 1 \bmod \phi(n)$ و $(M,n)=1$ باشند، آنگاه: $C^{d} \bmod n = M$

$$C^{d} \bmod n = M^{ed} \bmod n = M^{1+l\phi(n)} \bmod n = M\left(\underbrace{M^{\phi(n)} \bmod n}_{1}\right)^{l} \bmod n = M$$

$$d = e^{-1} \bmod \phi(n)$$

الگوریتم رمز RSA

$$C = M^{e} \bmod n$$
$$M = C^{d} \bmod n = \left(M^{e}\right)^{d} \bmod n = M^{ed} \bmod n$$

- قالب پیام M
- قالب متن رمز شده C

- n: پیمانه محاسبات= حاصلضرب دو عدد اول بزرگ $n = pq$
- کلید خصوصی: (p,q,d) کلید همگانی: (n,e)
- شکستن: بدست آوردن d $d = e^{-1} \bmod \phi(n)$
- محاسبه $\phi(n)$
  - کلاس np
  - اگر p و q معلوم: کلاس p $\phi(n) = (p-1)(q-1)$

محرمانگی با استفاده از الگوریتم رمز RSA

کاربر A بخواهد پیام **محرمانه** M را برای کاربر B ارسال کند:

- کلید خصوصی: $PR = (n, d) = (p, q, d)$
- کلید همگانی: $PU = (n, e)$
- کاربر A: $C = M^{e_B} \bmod n_B$
- کاربر B: $C^{d_B} \bmod n_B = M^{e_B d_B} \bmod n_B = M$

احراز اصالت با استفاده از الگوریتم رمز RSA

- کاربر A بخواهد پیام **معتبر** M را برای کاربر B ارسال کند:
- کلید خصوصی: $PR = (n, d) = (p, q, d)$
- کلید همگانی: $PU = (n, e)$
- کاربر A:

$$C = M^{d_A} \bmod n_A$$

- کاربر B:

$$C^{e_A} \bmod n_A = M^{e_A d_A} \bmod n_A = M$$

الزامات RSA

1. مقادیر e, d, n پیدا شوند که: $M^{ed} \bmod n = M$

$(M, n) = 1$

$ed \equiv 1 \bmod \phi(n)$

$\gcd(e, \phi(n)) = 1 \quad , \quad \gcd(d, \phi(n)) = 1$

2. محاسبه $M^e \bmod n$ و $C^d \bmod n$ ساده باشد (از نظر محاسباتی)

3. بدست آوردن d از روی e غیر ممکن باشد (از نظر محاسباتی)

p, q, two prime numbers	(private, chosen)
$n = pq$	(public, calculated)
e, with $\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$	(public, chosen)
$d \equiv e^{-1} \pmod{\phi(n)}$	(private, calculated)

الگوریتم رمز RSA

Key Generation Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by Bob with Alice's Public Key

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by Alice with Alice's Public Key

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

مثال RSA

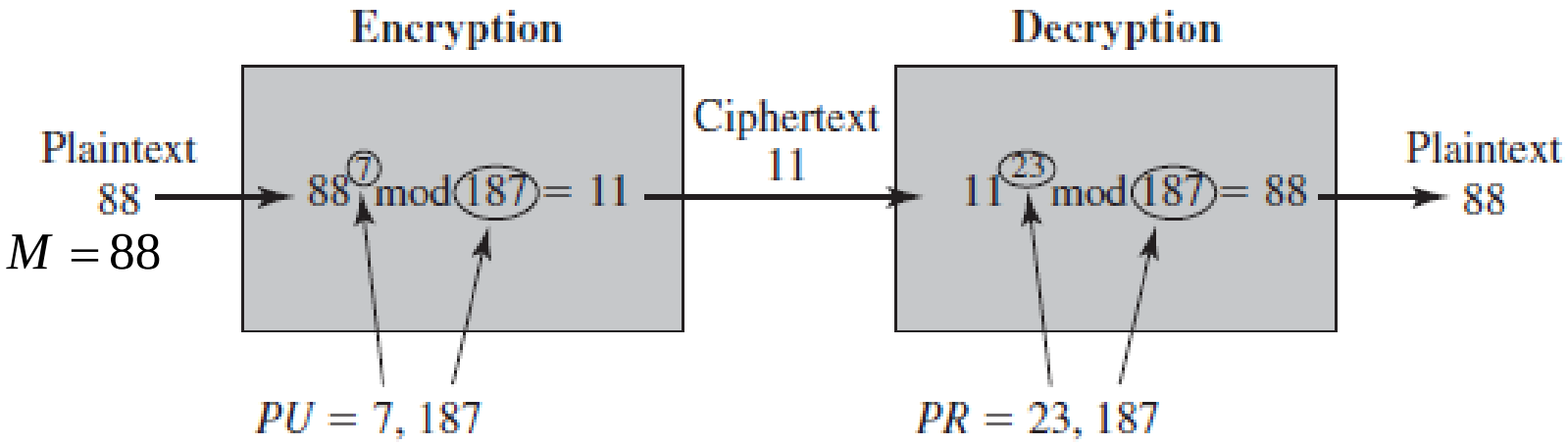
$p = 17, q = 11$

$n = pq = 187$

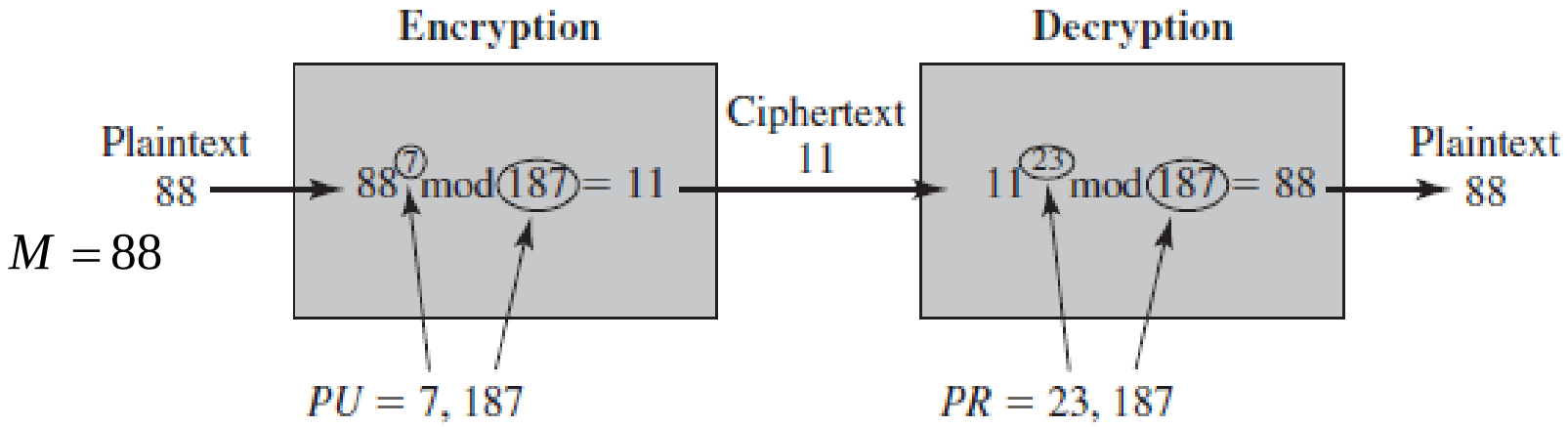
$\phi(n) = (p-1)(q-1) = 160$

$\gcd(e, \phi(n)) = 1 \rightarrow e = 7$

$d = e^{-1} \bmod \phi(n) = 7^{-1} \bmod 160 = 23$



مثال RSA



$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 7744 \bmod 187 = 77$

$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$

$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$

$11^1 \bmod 187 = 11$

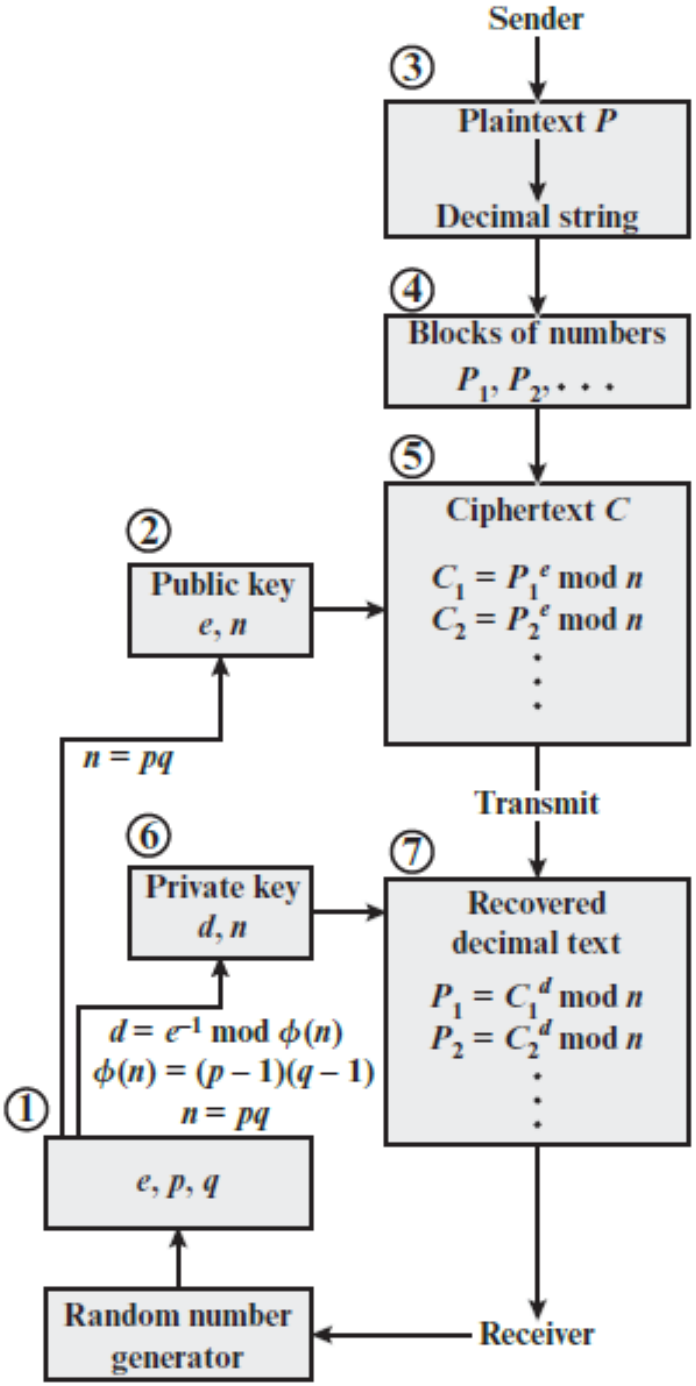
$11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$

$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$

$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$

قالبی RSA


Sender
③
Plaintext P
Decimal string
④
Blocks of numbers
$P_1, P_2, \ldots$
⑤
Ciphertext C
$C_1 = P_1^e \bmod n$
$C_2 = P_2^e \bmod n$
②
Public key
e, n
$n = pq$
Transmit
⑥
Private key
d, n
⑦
Recovered decimal text
$P_1 = C_1^d \bmod n$
$P_2 = C_2^d \bmod n$
$d = e^{-1} \bmod \phi(n)$
$\phi(n) = (p-1)(q-1)$
$n = pq$
①
e, p, q
Random number generator
Receiver

محاسبات توان رسانی (نمای) پیمانه‌ای

- تکرار مرحله‌ای

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

$$x^{11} = x \cdot x^2 \cdot x^8$$

- نمایش باینری: $b_k b_{k-1} \ldots b_0$

$$a^b$$

$$b = \sum_{b_i \neq 0} 2^i$$

```
c ← 0; f ← 1
for i ← k downto 0
    do  c ← 2 × c
        f ← (f × f) mod n
    if  bi = 1
        then c ← c + 1
             f ← (f × a) mod n
return f
```

$$a^b = a^{\left(\sum_{b_i \neq 0} 2^i\right)} = \prod_{b_i \neq 0} a^{(2^i)}$$

$$a^b \bmod n = \left[\prod_{b_i \neq 0} a^{(2^i)}\right] \bmod n = \left(\prod_{b_i \neq 0} \left[a^{(2^i)} \bmod n\right]\right) \bmod n$$

محاسبات توان رسانی (نمای) پیمانه‌ای
استفاده از کلید خصوصی

$$M = C^d \bmod n \qquad n = pq$$

$$V_p = C^d \bmod p \quad V_q = C^d \bmod q$$

$$X_p = q \times (q^{-1} \bmod p) \quad X_q = p \times (p^{-1} \bmod q)$$

- قضیه باقی‌مانده چینی (CRT)

$$M = (V_p X_p + V_q X_q) \bmod n$$

- قضیه فرمت

$$V_p = C^d \bmod p = C^{d \bmod (p-1)} \bmod p \qquad V_q = C^d \bmod q = C^{d \bmod (q-1)} \bmod q$$

حملات RSA

- حمله جستجوی فراگیر (به فضای کلید)
- حملات ریاضی
- حمله زمانی
- حمله متن رمز منتخب (Chosen ciphertext attacks)
  - حمله نوع چهارم

حملات RSA

- حمله جستجوی فراگیر (به فضای کلید)
  - کلید (d) طولانی
  - کاهش سرعت الگوریتم
- حملات ریاضی
  - تجزیه n به دو عامل اول ← محاسبه $\phi(n)=(p-1)(q-1)$ ← محاسبه $d=e^{-1} \bmod \phi(n)$
  - محاسبه مستقیم $\phi(n)$
  - محاسبه مستقیم d
- حمله زمانی
- حمله متن رمز منتخب (Chosen ciphertext attacks)
  - حمله نوع چهارم

$$\mathrm{E}(PU, M_1) \times \mathrm{E}(PU, M_2) = \mathrm{E}(PU, [M_1 \times M_2])$$

حملات ریاضی RSA

- تجزیه n به دو عامل اول ← محاسبه $\phi(n)=(p-1)(q-1)$ ← محاسبه $d=e^{-1} \bmod \phi(n)$
- محاسبه مستقیم $\phi(n)$ پیچیدگی: معادل با تجزیه n به دو عامل اول
- محاسبه مستقیم d: پیچیدگی الگوریتم‌های پیشنهادی (تا کنون)، معادل با تجزیه n به دو عامل اول است
- در حال حاضر RSA با طول کلید ۱۰۲۴ تا ۲۰۴۸ بیت: p و q از مرتبه 10^{75} تا 10^{100}

Number of Decimal Digits	Number of Bits	Date Achieved
100	332	April 1991
110	365	April 1992
120	398	June 1993
129	428	April 1994
130	431	April 1996
140	465	February 1999
155	512	August 1999
160	530	April 2003
174	576	December 2003
200	663	May 2005
193	640	November 2005
232	768	December 2009

حمله زمانی RSA

- با مشاهده زمان رمزگشایی یک متن رمز شده، اطلاعاتی در مورد کلید و متن اصلی بدست می‌آید
- مهم: دید متفاوت + حمله نوع اول (فقط با متن رمز)

مقابله:

- ثابت کردن زمان توان رسانی پیمانه‌ای
  - کاهش کارآیی
- تاخیر تصادفی
  - نویز کافی
- کورسازی (Blinding): متن رمزشده پیش از به توان رسیدن در یک عدد تصادفی ضرب شود
  - در پیاده‌سازی‌ها گنجانده شده است (RSA Data Security)
  - ۲٪ الی ۱۰٪ کاهش کارآیی

مبادله کلید دیفی–هلمن
Diffie-Hellman key exchange

- معرفی در سال ۱۹۷۶ توسط دیفی و هلمن
  - تعریف سیستم‌های کلید همگانی
- مبادله کلید (راز) ⟵ توافق بر روی کلید مخفی (الگوریتم رمز متقارن)

- بر اساس سختی محاسبه لگاریتم گسسته
- برای هر عدد صحیح b و ریشه اولی a (برای عدد اول p)، نمای یکتای i وجود دارد، به طوری‌که:

$$b \equiv a^i \pmod{p} \qquad \text{where } 0 \leq i \leq (p-1)$$

  - لگاریتم گسسته b در مبنای a و پیمانه p

$$i = \mathrm{d}\log_{a,p}(b)$$

مبادله کلید دیفی–هلمن

- دو مقدار همگانی: عدد اول q و عدد صحیح α (ریشه اولی p)
- دو کاربر A و B به مبادله کلید می‌پردازند
- کاربر A: عدد تصادفی صحیح $X_A < q$ را انتخاب می‌کند و $Y_A = \alpha^{X_A} \bmod q$
- کاربر B: به طور مستقل عدد تصادفی صحیح $X_B < q$ را انتخاب می‌کند و $Y_B = \alpha^{X_B} \bmod q$
- هر دو کاربر مقادیر X را به طور خصوصی نزد خود نگه‌می‌دارد و مقادیر Y را به طور همگانی به کاربر دیگر ارسال می‌کند
- کلید در کاربر A: $K = (Y_B)^{X_A} \bmod q$
- کلید در کاربر B: $K = (Y_A)^{X_B} \bmod q$
- دو کلید برابرند!

مبادله کلید دیفی–هلمن

- مهاجم به q, α, Y_A, Y_B دسترسی دارد
- مجبور به محاسبه لگاریتم گسسته
  - مثلا برای بدست آوردن کلید خصوصی B

$$X_B = \mathrm{d}\log_{\alpha,p}(Y_B)$$

  - سپس، می‌تواند کلید را به طریقی که کاربر B محاسبه می‌کند، بیابد
- محاسبه لگاریتم گسسته برای اعداد اول بزرگ از نظر محاسباتی غیر ممکن به نظر می‌رسد

$$Y_A = \alpha^{X_A} \bmod q \ , \ Y_B = \alpha^{X_B} \bmod q$$

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

$$K_B = (Y_A)^{X_B} \bmod q$$

$$\begin{aligned} K &= (Y_B)^{X_A} \bmod q \\ &= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \\ &= (\alpha^{X_B})^{X_A} \bmod q \\ &= \alpha^{X_B X_A} \bmod q \\ &= (\alpha^{X_A})^{X_B} \bmod q \\ &= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \\ &= (Y_A)^{X_B} \bmod q \end{aligned}$$

Global Public Elements

q	prime number
α	$\alpha < q$ and α a primitive root of q

User A Key Generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{XA} \bmod q$

User B Key Generation

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{XB} \bmod q$

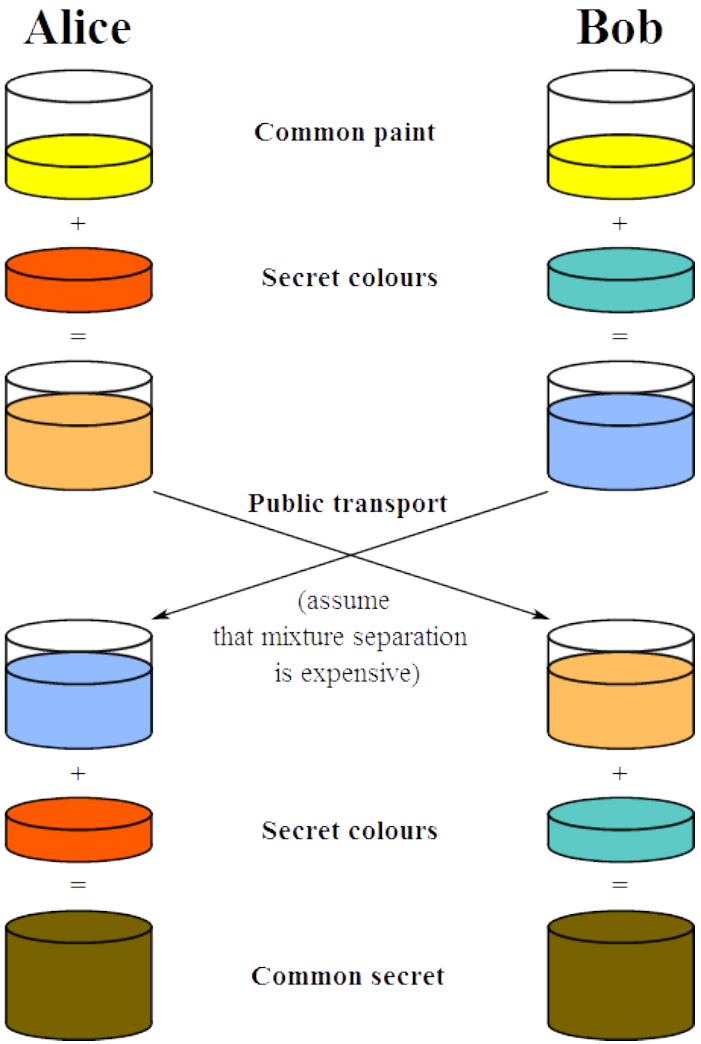
Calculation of Secret Key by User A

$$K = (Y_B)^{XA} \bmod q$$

Calculation of Secret Key by User B

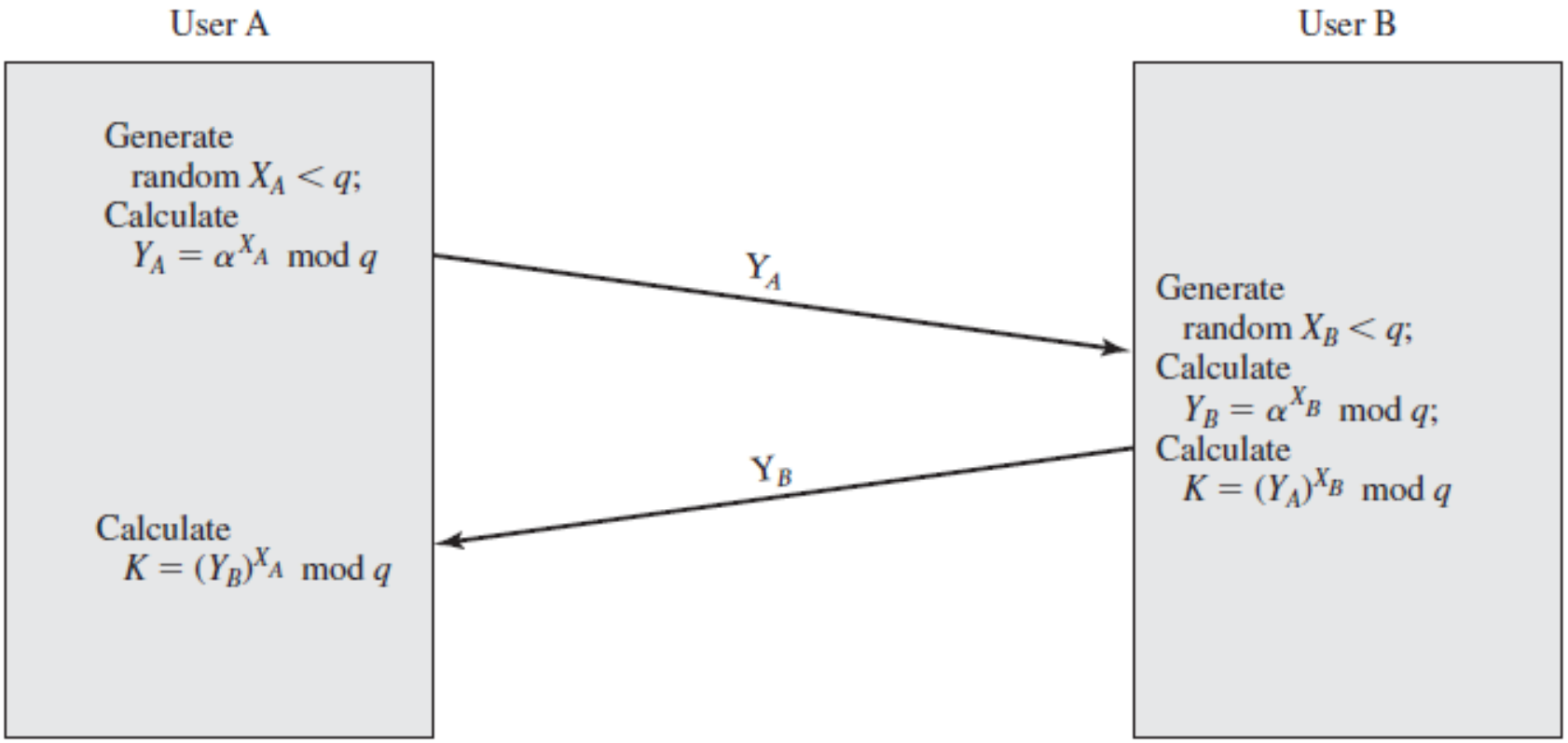
$$K = (Y_A)^{XB} \bmod q$$

مبادله کلید دیفی–هلمن



src: wikipedia

پروتکل‌های مبادله کلید



پروتکل مبادله کلید در شبکه

- گروهی از کاربرها (مثلا کاربرها در یک LAN)
- کلید خصوصی (X_i) را تولید و کلید همگانی (Y_i) را محاسبه می‌کنند
- کلیدهای همگانی همراه با مقادیر همگانی q و α در یک مرجع معتبر ذخیره می‌شوند
- کاربر j می‌تواند به کلید همگانی کاربر i دسترسی یابد و با محاسبه کلید مخفی، پیام خود را به آن ارسال کند
- محرمانگی: تنها کاربر j و کاربر i به کلید مخفی دسترسی دارند
- احراز اصالت: کاربر j می‌داند که تنها کاربر i می‌توانسته با استفاد از این کلید رمز کند
- آسیب‌پذیر در برابر حمله تکرار

حمله فرد در میانه
Man-in-the-Middle Attack

انتخاب تصادفی کلیدهای خصوصی: X_{D1}, X_{D2}

محاسبه کلیدهای همگانی: Y_{D1}, Y_{D2}

Bob

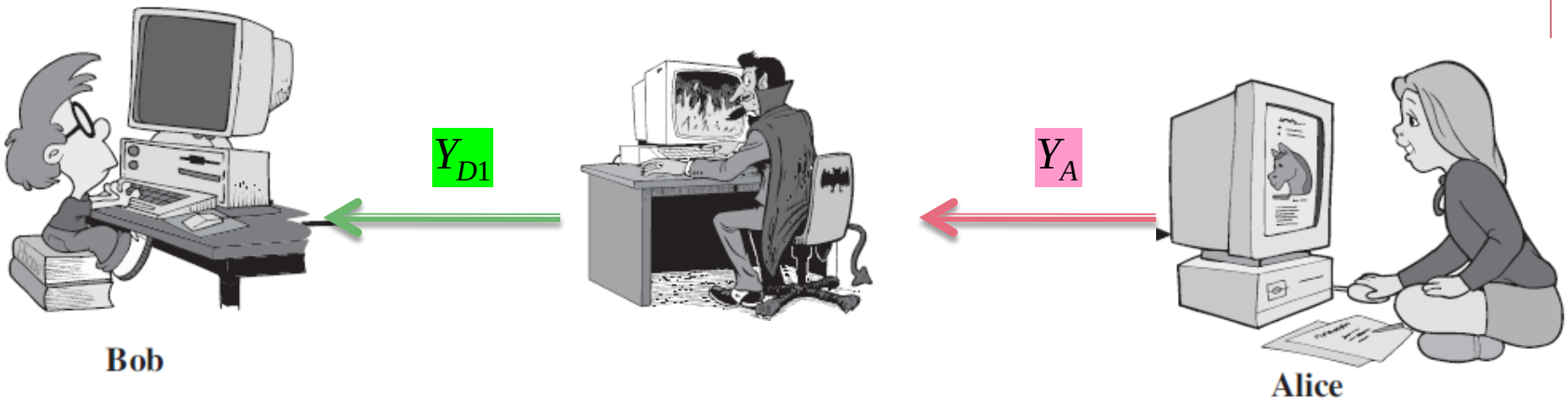
Alice

حمله فرد در میانه
Man-in-the-Middle Attack

انتخاب تصادفی کلیدهای خصوصی: X_{D1}, X_{D2}

محاسبه کلیدهای همگانی: Y_{D1}, Y_{D2}

محاسبه: $K2 = (Y_A)^{X_{D2}} \bmod q$

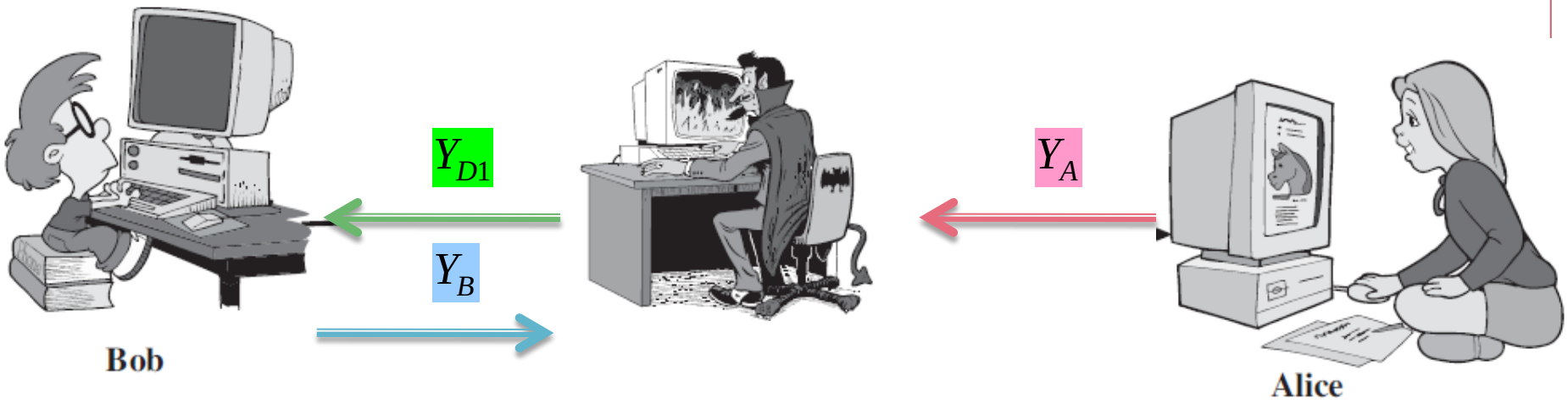


حمله فرد در میانه
Man-in-the-Middle Attack

انتخاب تصادفی کلیدهای خصوصی: X_{D1}, X_{D2}

محاسبه کلیدهای همگانی: Y_{D1}, Y_{D2}

محاسبه: $K2 = (Y_A)^{X_{D2}} \bmod q$



محاسبه: $K1 = (Y_{D1})^{X_B} \bmod q$

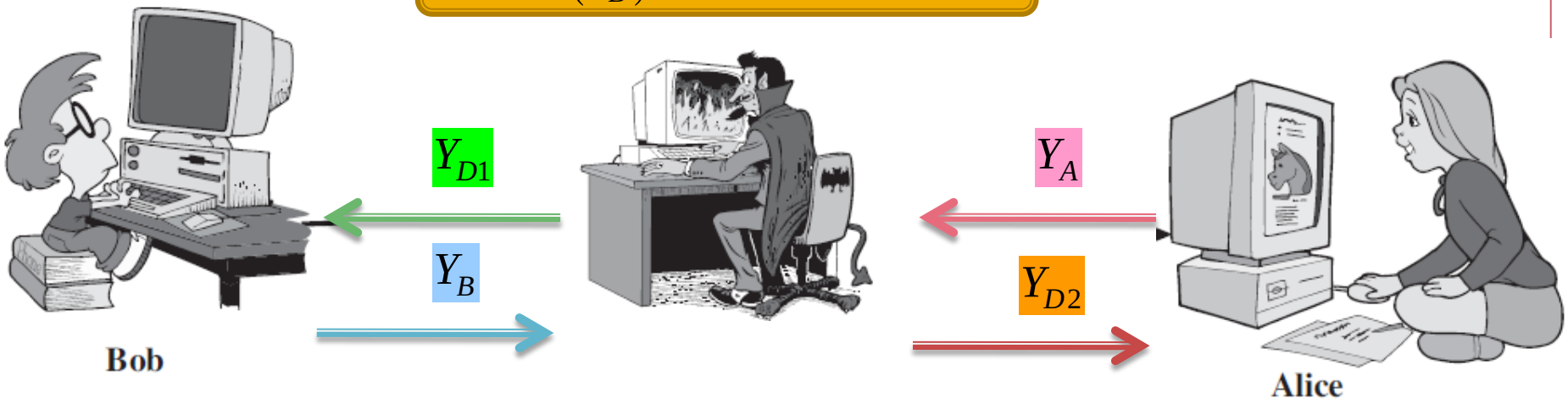
حمله فرد در میانه
Man-in-the-Middle Attack

انتخاب تصادفی کلیدهای خصوصی: X_{D1}, X_{D2}

محاسبه کلیدهای همگانی: Y_{D1}, Y_{D2}

محاسبه: $K2 = (Y_A)^{X_{D2}} \bmod q$

محاسبه: $K1 = (Y_B)^{X_{D1}} \bmod q$



محاسبه: $K1 = (Y_{D1})^{X_B} \bmod q$

حمله فرد در میانه
Man-in-the-Middle Attack

انتخاب تصادفی کلیدهای خصوصی: X_{D1}, X_{D2}

محاسبه کلیدهای همگانی: Y_{D1}, Y_{D2}

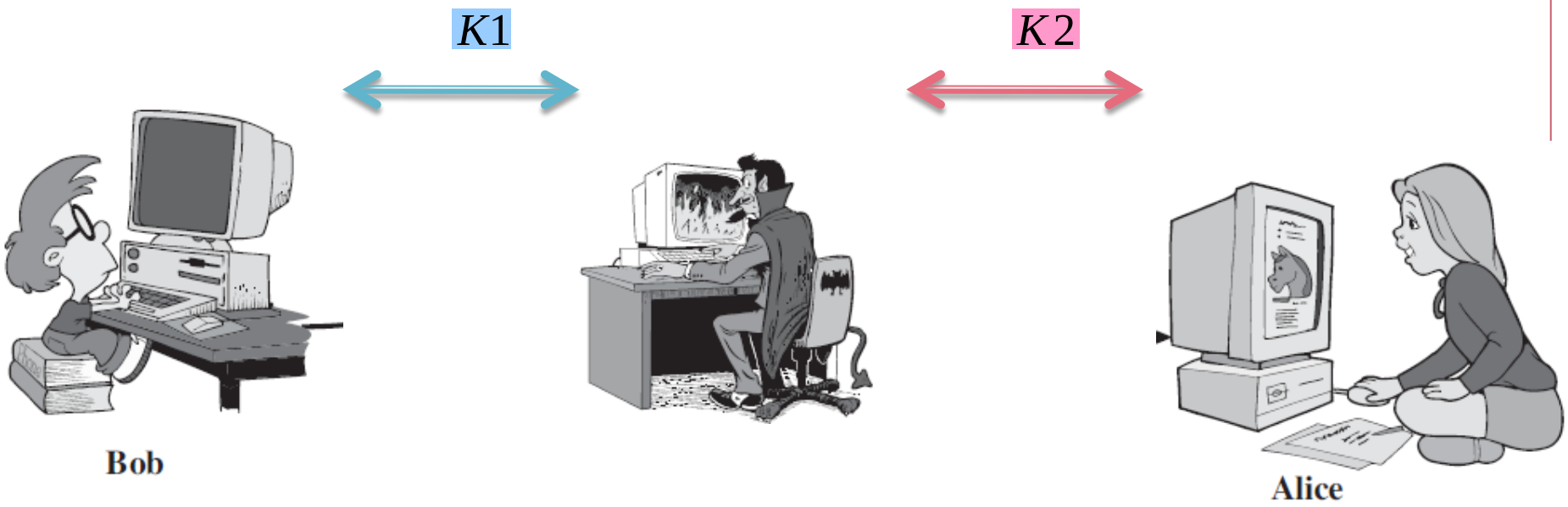
محاسبه: $K2 = (Y_A)^{X_{D2}} \bmod q$

محاسبه: $K1 = (Y_B)^{X_{D1}} \bmod q$

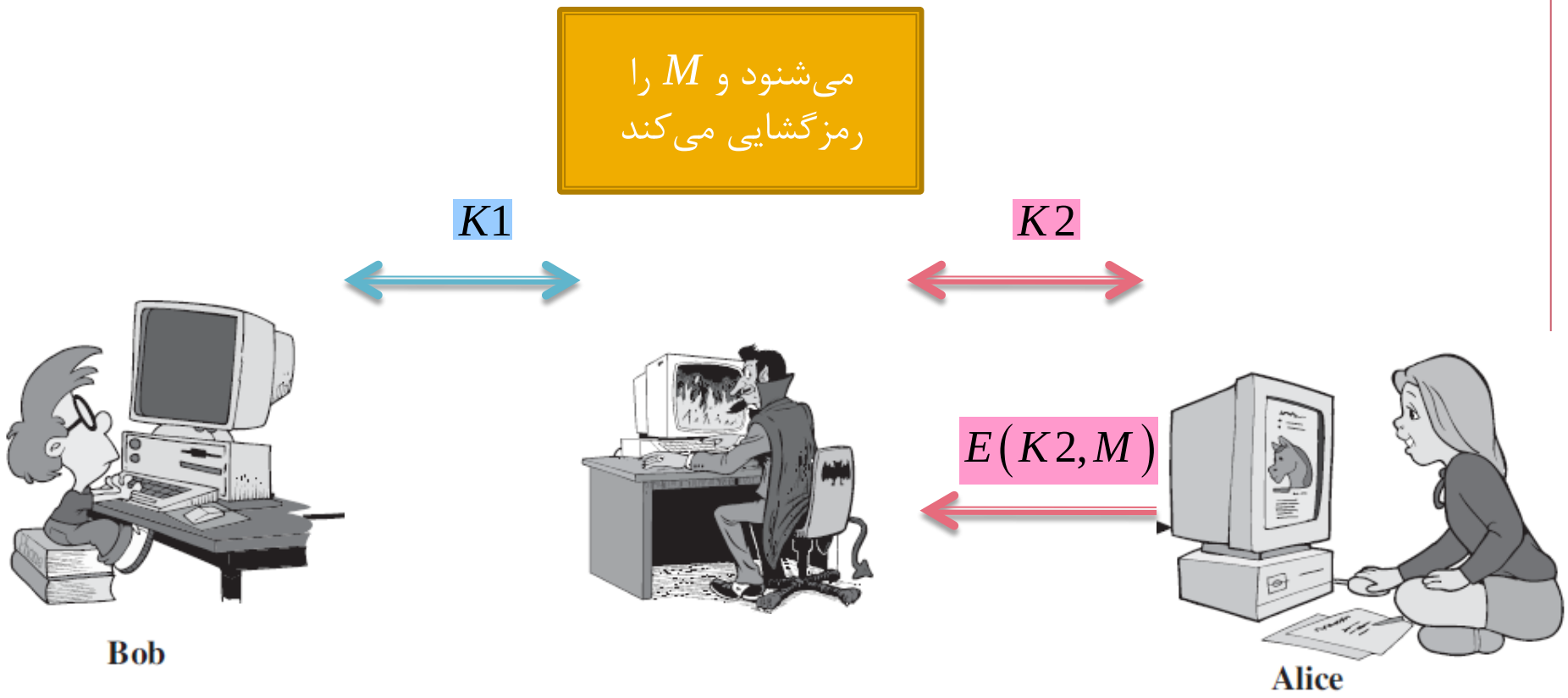
محاسبه: $K1 = (Y_{D1})^{X_B} \bmod q$

محاسبه: $K2 = (Y_{D2})^{X_A} \bmod q$

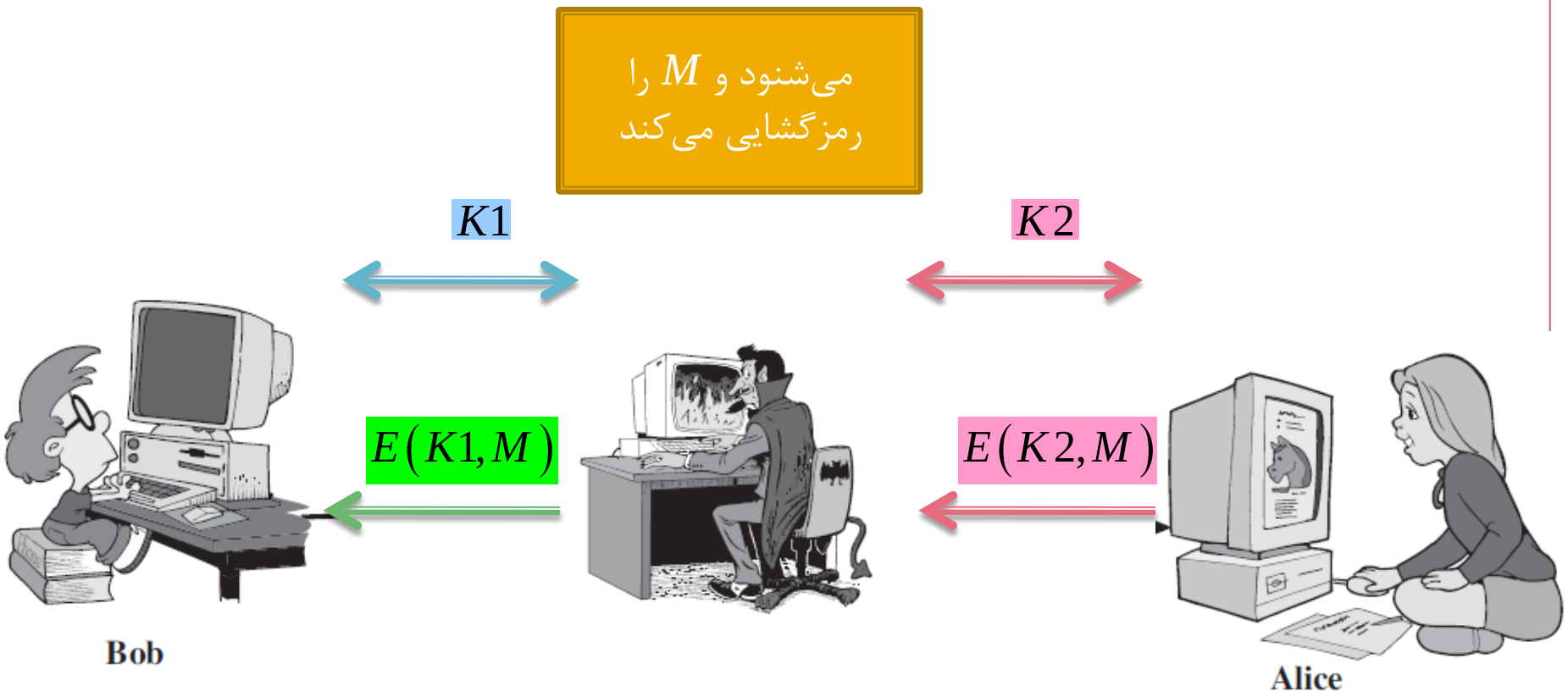
حمله فرد در میانه
Man-in-the-Middle Attack



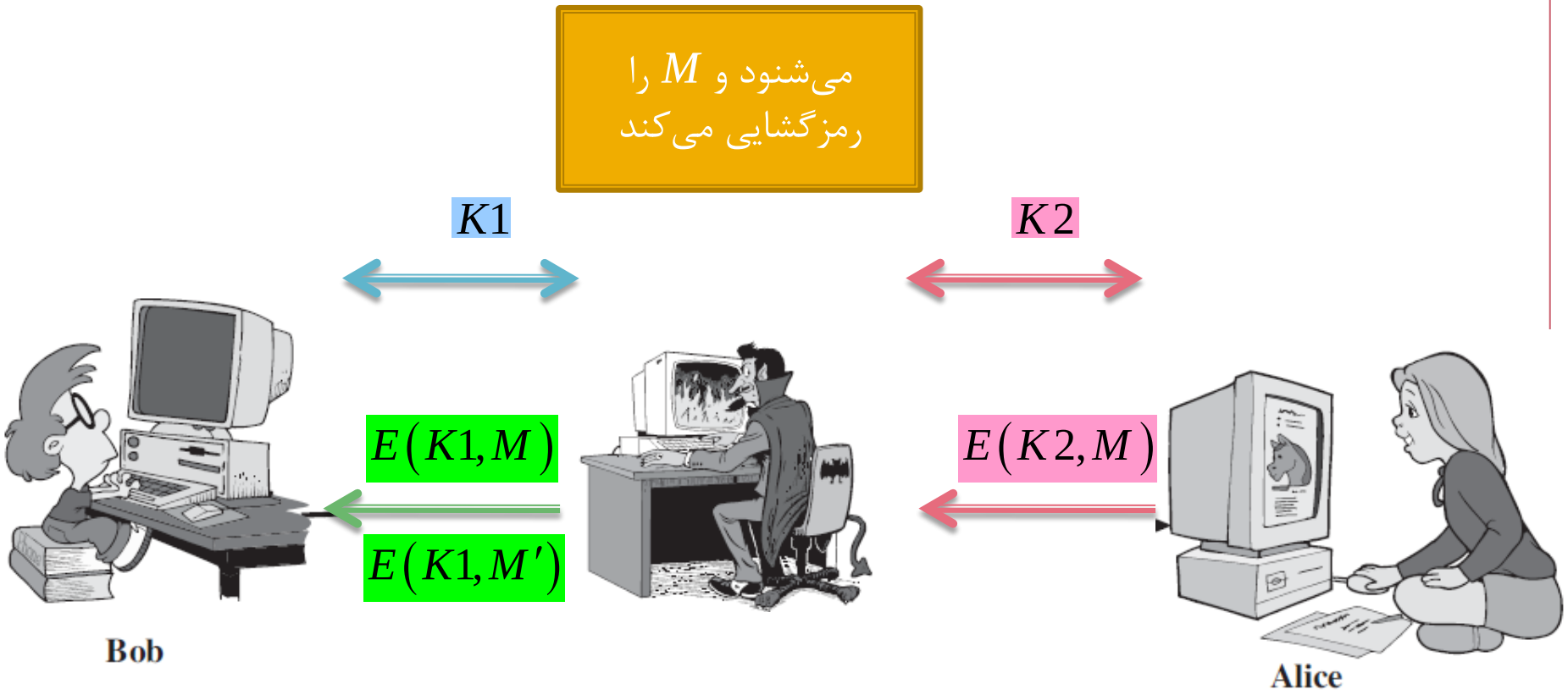
حمله فرد در میانه
Man-in-the-Middle Attack



حمله فرد در میانه
Man-in-the-Middle Attack



حمله فرد در میانه
Man-in-the-Middle Attack



- مقابله: استفاده از امضای دیجیتال یا گواهی‌نامه کلید همگانی

سیستم رمزنگاری Elgamal

- ۱۹۸۴
- بر پایه سختی مساله لگاریتم گسسته

- استاندارد امضای دیجیتال
  - digital signature standard (DSS)

- استاندارد ایمیل S/MIME

Global Public Elements

q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice

Select private X_A	$X_A < q - 1$
Calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public key	$\{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key

Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

Decryption by Alice with Alice's Private Key

Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$

- سیستم رمزنگاری Elgamal
- رمزگذاری با کلید همگانی
  - محرمانگی

صحت سیستم رمزنگاری Elgamal

- بدست آوردن کلید K
  - از $C_1 = \alpha^k \bmod q$

$$\begin{aligned} K &= (Y_A)^k \bmod q \\ &= \left(\alpha^{X_A} \bmod q\right)^k \bmod q \\ &= \alpha^{kX_A} \bmod q \\ &= (C_1)^{X_A} \bmod q \end{aligned}$$

- بدست آوردن پیام (متن اصلی)
  - از $C_2 = KM \bmod q$

$$\begin{aligned} \left(C_2 K^{-1}\right) \bmod q &= KMK^{-1} \bmod q \\ &= M \bmod q \\ &= M \end{aligned}$$

امنیت سیستم رمزنگاری Elgamal

- پیام طولانی: تقسیم به قالب‌ها
  - استفاده از k یکتا برای هر قالب

- بر پایه سختی مساله لگاریتم گسسته
- بدست آوردن کلید خصوصی A $X_A = \mathrm{d}\log_{\alpha,q}(Y_A)$
- بدست آوردن کلید یکبار مصرف K $k = \mathrm{d}\log_{\alpha,q}(C_1)$

Elliptic curve – خم بیضوی

- فضای پیوسته

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

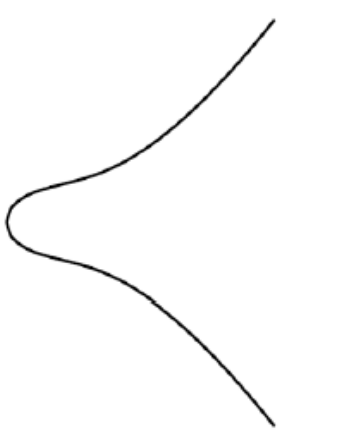
- خم بیضوی با دو پارامتر a و b

$$y^2 = x^3 + ax + b$$

- $E(a,b)$ = همه نقاط خم فوق + نقطه O

- تشکیل گروه آبلی

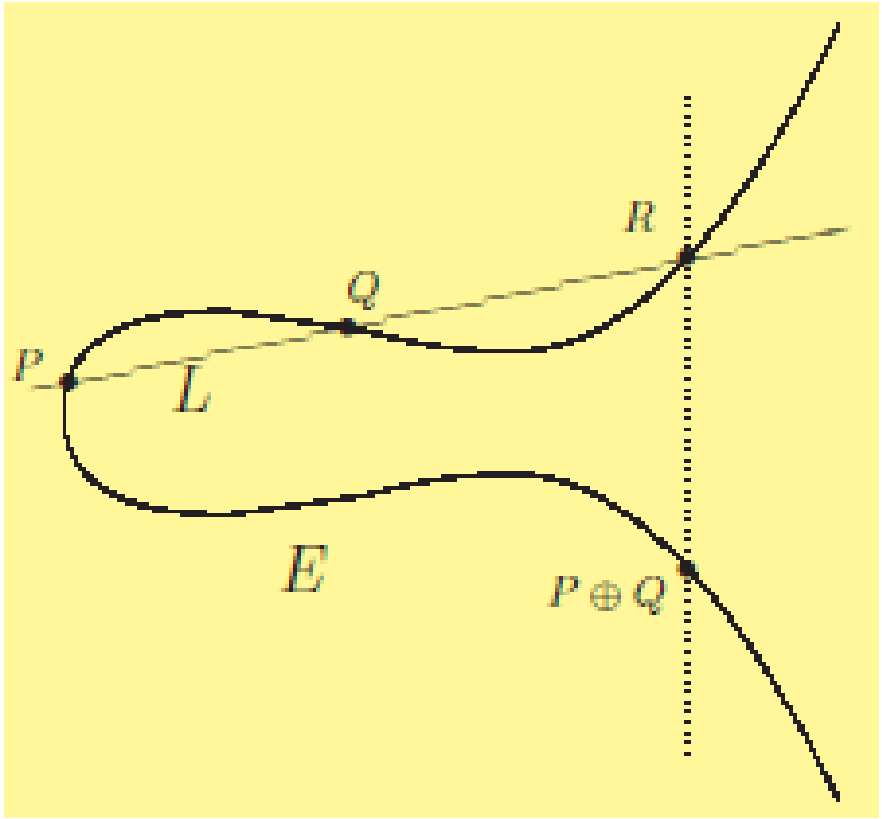
$$4a^3 + 27b^2 \neq 0$$

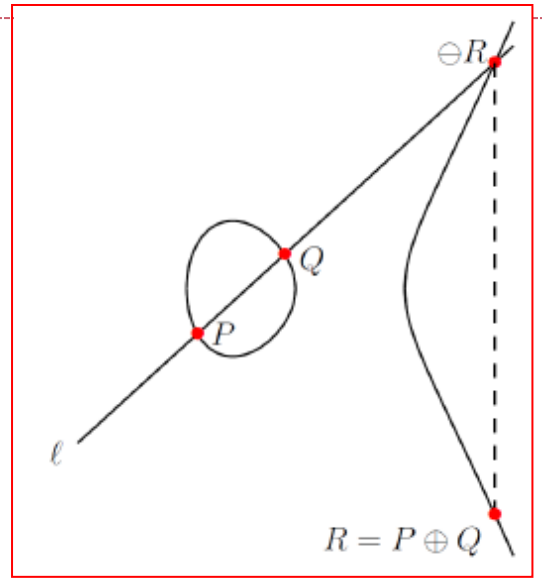


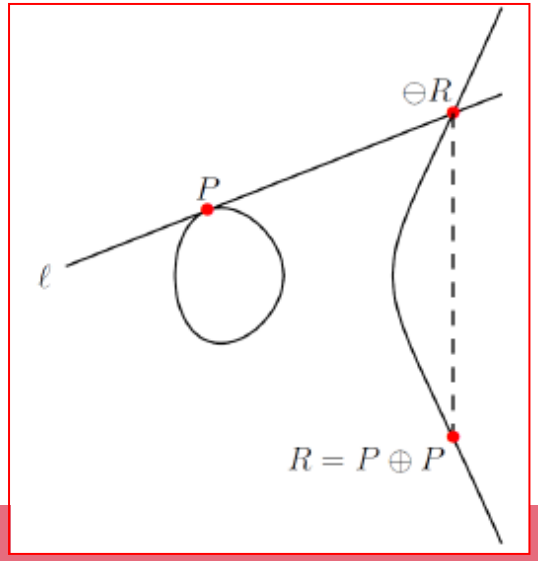
$E/\mathbb{R}: y^2 = x^3 + x + 1$

$E/\mathbb{R}: y^2 = x^3 - x$

اپراتور جمع گروه در خم بیضوی



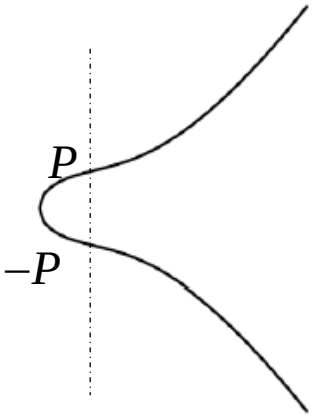


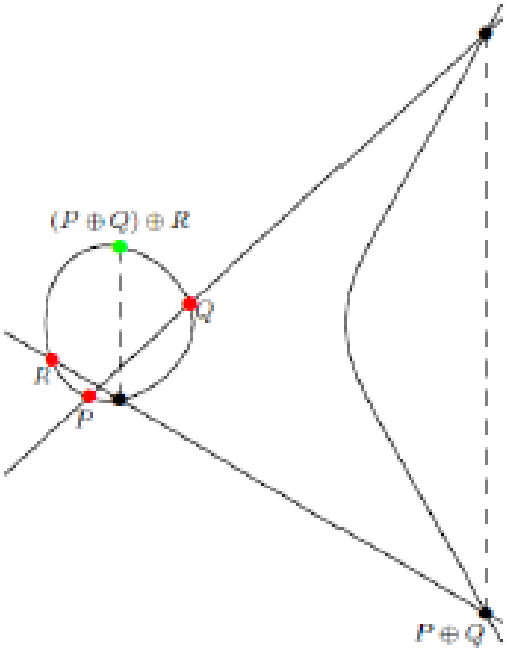


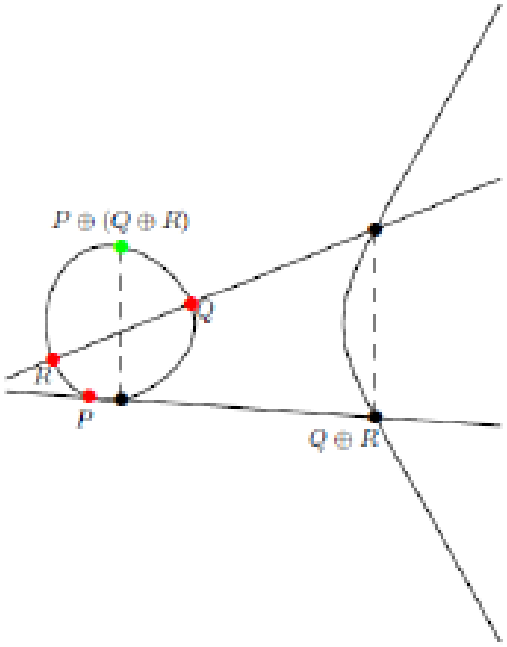
اپراتور جمع گروه در خم بیضوی

$$
\begin{aligned}
P + \mathcal{O} &= \mathcal{O} + P = P && \text{for all } P \in E.\\
P + (-P) &= \mathcal{O} && \text{for all } P \in E.\\
P + (Q + R) &= (P + Q) + R && \text{for all } P, Q, R \in E.\\
P + Q &= Q + P && \text{for all } P, Q \in E.
\end{aligned}
$$

- گروه جابجاپذیر







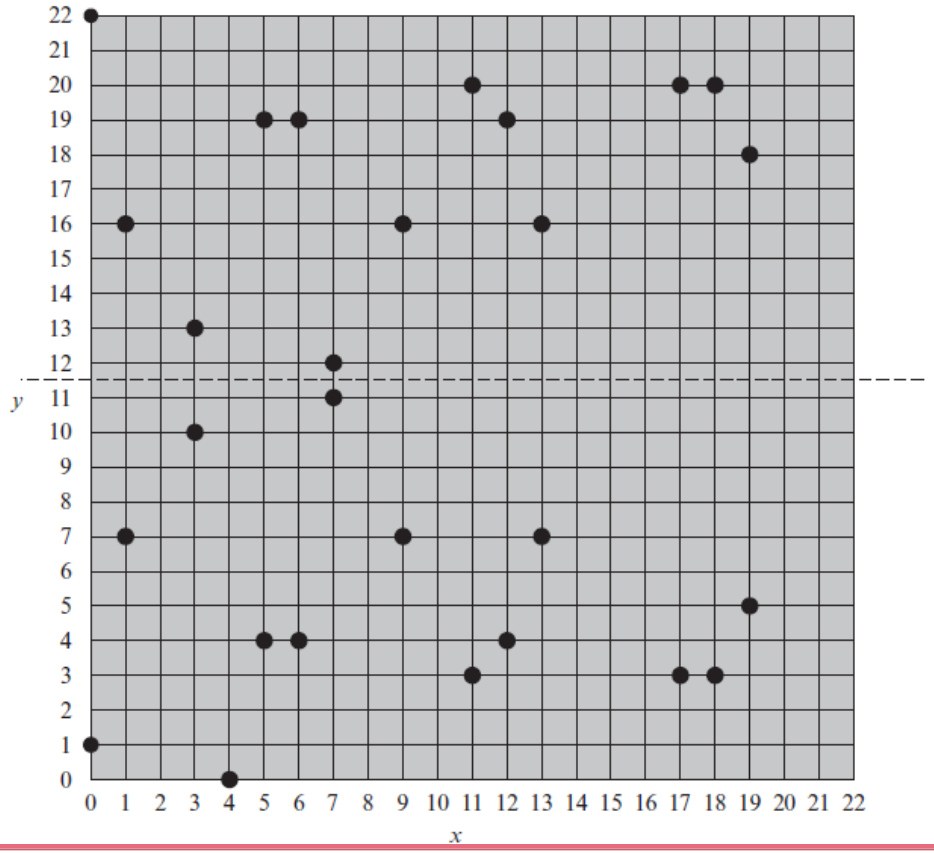
خم بیضوی

- فضای گسسته: $GF(2^m)$ یا Z_p

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

$$a = 1, b = 1, p = 23$$

$$E_{Z_{23}}(1,1)$$



سیستم رمزنگاری مبتنی بر خم بیضوی

- جمع در خم بیضوی مشابه ضرب در DH یا RSA
- ضرب در خم بیضوی مشابه توان رسانی در DH یا RSA

$$a \times k = \underbrace{(a + a + \ldots + a)}_{k \text{ times}}$$

$$a^k \bmod q = \underbrace{(a \times a \times \ldots \times a)}_{k \text{ times}} \bmod q$$

- مساله سخت در در خم بیضوی مشابه مساله لگاریتم گسسته (DLP) در DH یا RSA
  - با داشتن a و $(a \times k)$، k را مخاسبه کن

مبادله کلید مبتنی بر خم بیضوی (مشابه DH)
ECC Diffie–Hellman Key Exchange

Global Public Elements

$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation

Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

User B Key Generation

Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A

$K = n_A \times P_B$

Calculation of Secret Key by User B

$K = n_B \times P_A$

رمزگذاری مبتنی بر خم بیضوی

Global Public Elements	
$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation	
Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

کاربر A برای ارسال پیام محرمانه P_m به کاربر B

- عدد صحیح مثبت k را انتخاب می‌کند
- رمزگذاری $C_m = \{kG, P_m + kP_B\}$
- رمزگشایی $P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$

امنیت سیستم رمزنگاری مبتنی بر خم بیضوی
NIST SP-800-57

- بهترین الگوریتم شناخته شده لگاریتم خم بیضوی: Pollard rho method
- توصیه استانداردها از ۲۰۳۰ برای طول کلید:
  - ۳۰۷۲-۱۴۳۶۰ بیت برای RSA
  - ۲۵۶-۵۱۲ بیت برای ECC
- پیچیدگی محاسباتی RSA و ECC برای طول کلید یکسان تقریبا برابر است

Symmetric Key Algorithms	Diffie–Hellman, Digital Signature Algorithm	RSA (size of n in bits)	ECC (modulus size in bits)
80	$L = 1024$ $N = 160$	1024	160–223
112	$L = 2048$ $N = 224$	2048	224–255
128	$L = 3072$ $N = 256$	3072	256–383
192	$L = 7680$ $N = 384$	7680	384–511
256	$L = 15,360$ $N = 512$	15,360	512+

تولید دنباله شبه تصادفی بر اساس رمز نامتقارن

- پیچیدگی محاسباتی رمز کلید همگانی: مناسب برای PRF
- Micali–Schnorr PRNG بر پایه RSA
  - ANSI standard X9.82 و ISO standard 18031
- مشابه سبک OFB رمز متقارن

$$N = [\log_2 n] + 1$$
$$r + k = N$$