یا ذاالامن والامان

رمزنگاری نامتقارن (کلیدعمومی)

مبانی امنیت اطلاعات و شبکه‌های کامپیوتری

محمدرضا رازیان*

بهار و تابستان 1395

مرکز تخصصی آپا

دانشگاه سمنان

مرکز تخصصی آپا دانشگاه سمنان

http://cert.semnan.ac.ir

آزمایشگاه امنیت داده و شبکه شریف

http://dnsl.ce.sharif.ir

*Homepage: www.mrazian.com

فهرست مطالب

- مبانی رمزنگاری کلید عمومی
- مقایسه با رمزنگاری سنتی و متقارن
- کاربردهای رمزنگاری کلید عمومی
- الگوریتم رمز RSA
- الگوریتم رمز دیفی-هلمن
- الگوریتم رمز ال.جمل

مبانی رمزنگاری کلید عمومی

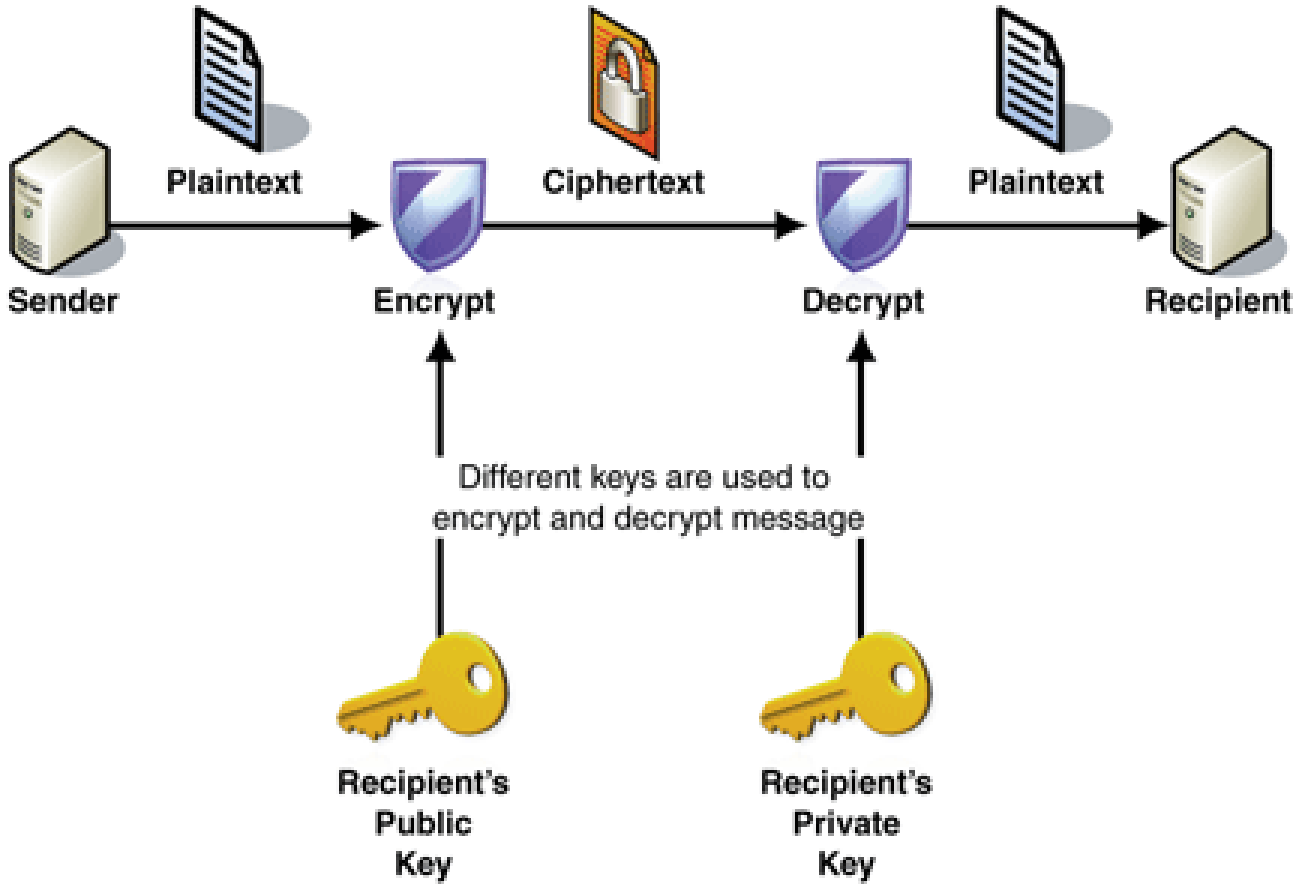
- رمزنگاری کلید عمومی اساساً با انگیزه رسیدن به دو هدف طراحی شد:
  - حل مساله توزیع کلید در روشهای رمزنگاری متقارن
  - امضای دیجیتال

- دیفی و هلمن اولین راه حل را در ۱۹۷۶ ارایه دادند.

رمزنگاری کلید عمومی

- کلیدهای رمزگذاری و رمزگشایی متفاوت اما مرتبط هستند.
- رسیدن به کلید رمزگشایی از کلید رمزگذاری از لحاظ محاسباتی ناممکن است.
- (در حفظ محرمانگی) رمزگذاری امری همگانی است و اساساً نیازی به اشتراک گذاشتن اطلاعات محرمانه ندارد.
- (در حفظ محرمانگی) رمزگشایی از طرف دیگر امری اختصاصی بوده و محرمانگی پیام‌ها محفوظ می‌ماند.

رمزنگاری کلید عمومی



نمادها و قراردادها

- **کلید عمومی:** کلید رمزگذاری (در حفظ محرمانگی)
  - این کلید را برای شخص A با PU_a نشان می‌دهیم.
- **کلید خصوصی:** کلید رمزگشایی (در حفظ محرمانگی)
  - این کلید را برای شخص A با PR_a نشان می‌دهیم.

نیازمندیهای رمزنگاری کلید عمومی

- از نظر محاسباتی برای طرف B، تولید یک زوج کلید (کلید عمومی PU_b و کلید خصوصی PR_b) آسان باشد.
- برای فرستنده، تولید متن رمز آسان باشد:

$$C = E_{PU_b}(M)$$

- برای گیرنده، رمزگشایی متن با استفاده از کلید متناظر آن آسان باشد:

$$M = D_{PR_b}(C) = D_{PR_b}[E_{PU_b}(M)]$$

نیازمندیهای رمزنگاری کلید عمومی

- از نظر محاسباتی، تولید کلید خصوصی (PR_b) با دانستن کلید عمومی (PU_b) غیر ممکن باشد.
- بازیابی پیام M، با دانستن PU_b و C غیرممکن باشد.
- ویژگی تقارنی: از هر یک از کلیدها می‌توان برای رمزکردن استفاده کرد. در این صورت از کلید دیگر برای رمزگشایی استفاده می‌شود.

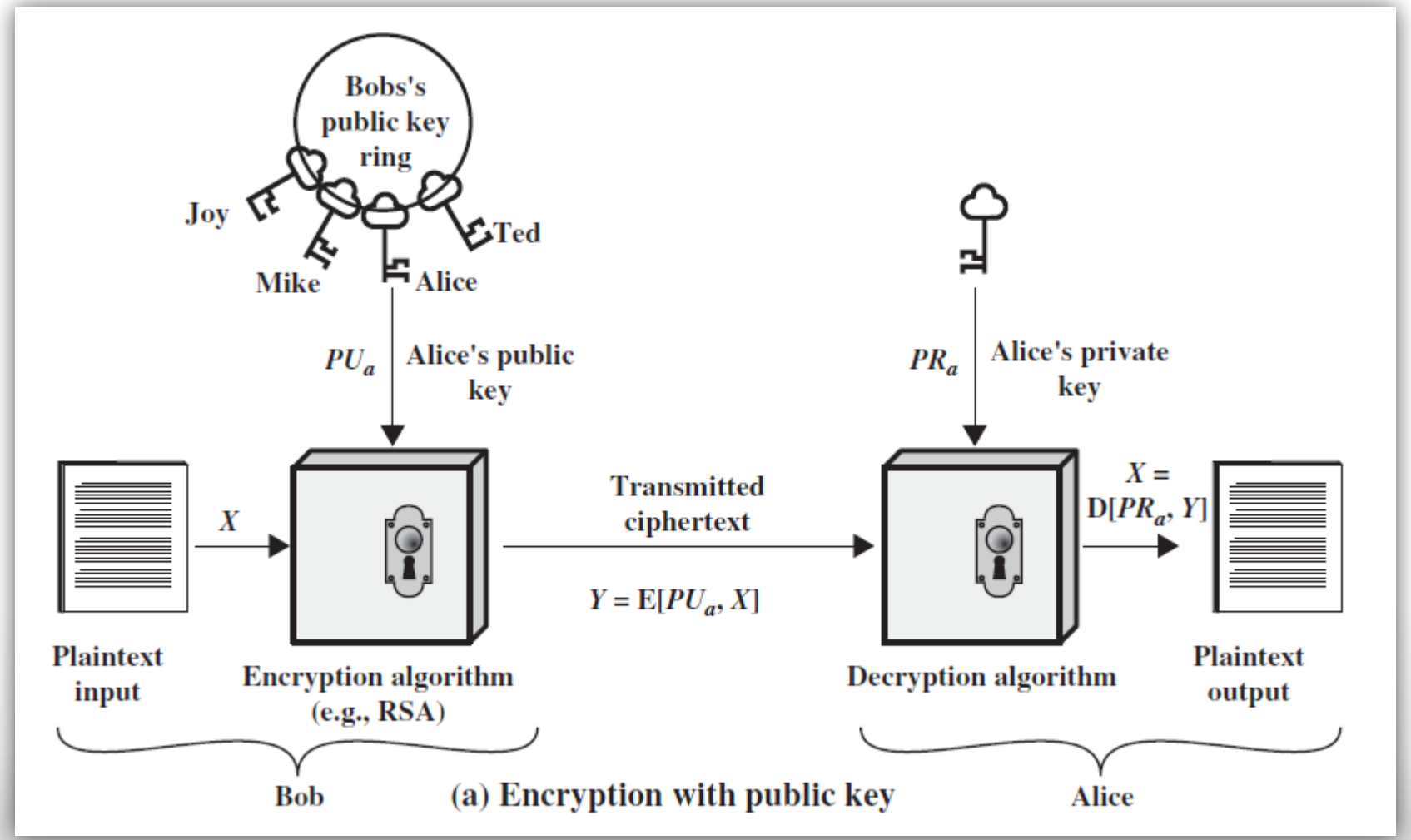
$$M = D_{PR_b}[E_{PU_b}(M)] = D_{PU_b}[E_{PR_b}(M)]$$

رمزگذاری کلید عمومی

- برای رمزنگاری کلید عمومی گام‌های زیر را برمی‌داریم:

1. هر کاربر یک زوج کلید رمزگذاری و رمزگشایی تولید می‌کند.
2. کاربران کلید رمزگذاری خود را به صورت عمومی اعلان می‌کنند درحالی که کلید رمزگشایی مخفی می‌باشد.
3. همگان قادر به ارسال پیام رمز شده برای هر کاربر دلخواه با استفاده از کلید رمزگذاری (عمومی) او هستند.
4. هر کاربر می‌تواند با کمک کلید رمزگشایی (خصوصی) پیام‌هایی که با کلید رمزگذاری (عمومی) او رمز شده رمزگشایی کند.

رمزگذاری با کلید عمومی



رمزگذاری با کلید خصوصی

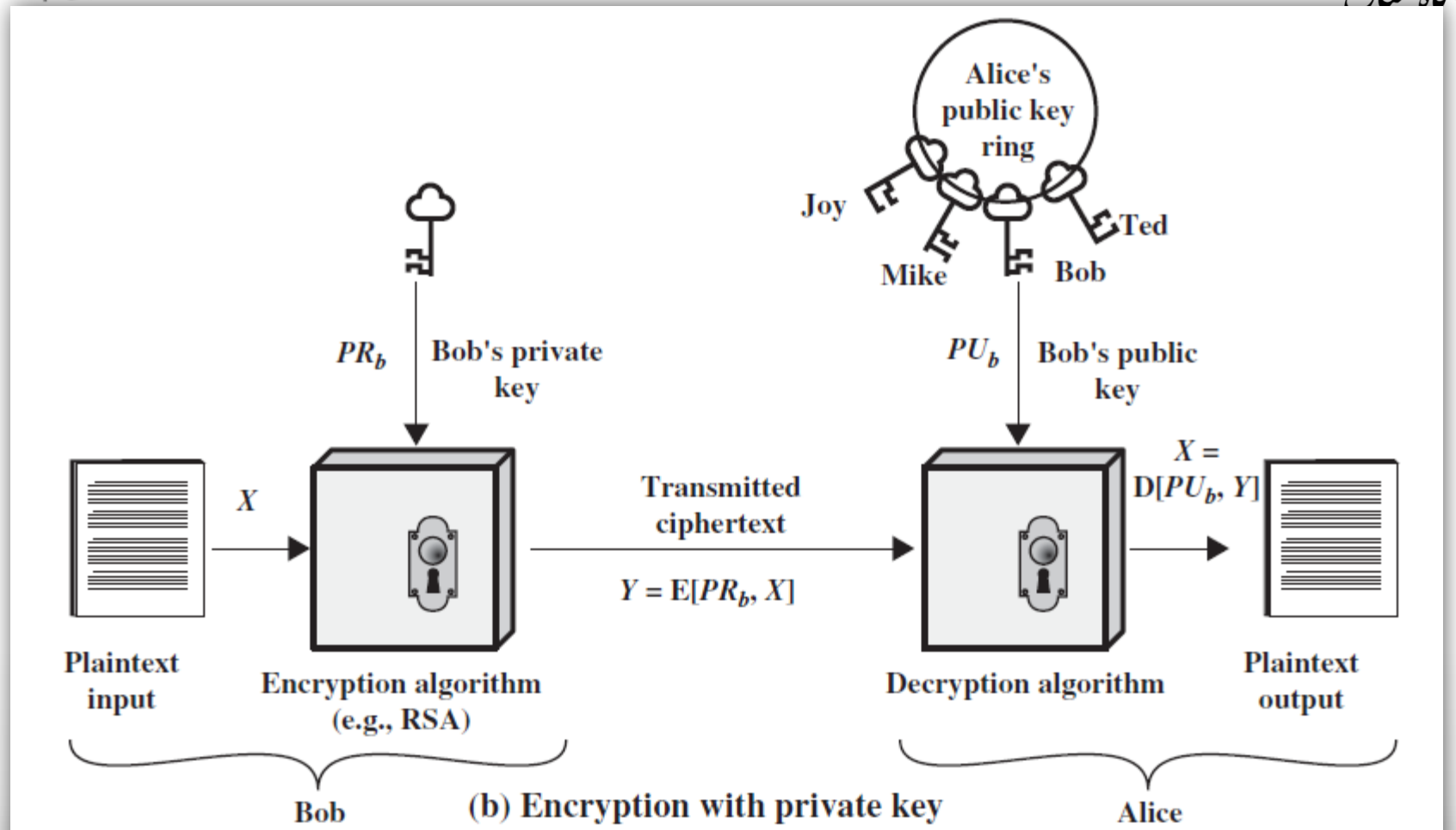
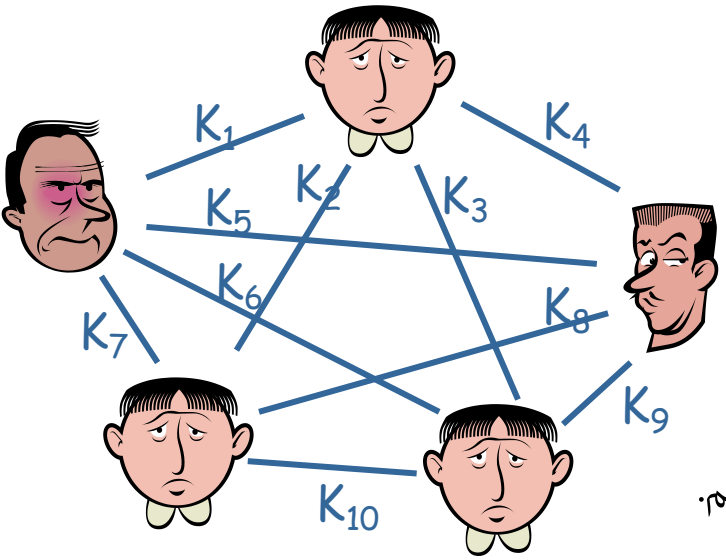


Figure 9.1 Public-Key Cryptography

فهرست مطالب

- مبانی رمزنگاری کلید عمومی
- **مقایسه با رمزنگاری سنتی و متقارن**
- کاربردهای رمزنگاری کلید عمومی
- الگوریتم رمز RSA
- الگوریتم رمز دیفی-هلمن

مقایسه رمزنگاری متقارن و رمزنگاری کلید عمومی



رمزنگاری متقارن

- استفاده از یک کلید یکسان و مخفی برای رمزنگاری

معایب

- مشکل مدیریت کلیدها
  - نیاز به توافق بر روی کلید پیش از برقراری ارتباط
  - برای ارتباط n نفر باهم به $n(n-1)/2$ کلید احتیاج داریم.
- عدم پشتیبانی از امضاء رقمی (دیجیتال)

مزایا

- **با این وجود از الگوریتم‌های رمزنگاری با کلید عمومی سریع‌تر است.**

مقایسه رمزنگاری متقارن و رمزنگاری کلید عمومی

- در **رمزگذاری متقارن** برای امن بودن باید:
  - کلید سری، مخفی نگه داشته شود.
  - رسیدن به پیام آشکار از روی متن رمزشده از نظر محاسباتی ناممکن باشد.
  - اطلاع از الگوریتم و داشتن نمونه‌هایی از پیغام رمزشده برای تعیین کلید کافی نباشد.

مقایسه رمزگذاری متقارن و رمزگذاری کلید عمومی

- ملزومات امنیتی **رمزگذاری با کلید عمومی**
  - تنها یکی از دو کلید باید مخفی بماند.
  - رسیدن به پیام آشکار از روی متن رمز شده حتی با داشتن کلید عمومی از نظر محاسباتی ناممکن باشد.
  - اطلاع از الگوریتم، داشتن یکی از کلیدها و نیز دراختیار داشتن نمونه پیغام‌های رمزشده برای تعیین کلید دوم کافی نباشد.

جایگزینی یا تکمیل؟

از نظر کاربردی، رمزگذاری با کلید عمومی بیش از آنکه **جایگزینی** برای رمزگذاری متقارن باشد, نقش **مکمل** آن را برای حل مشکلات توزیع کلید بازی می‌کند.

سوء برداشت!

- دو تصور اشتباه دیگر درباره الگوریتم‌های کلید عمومی
- رمزنگاری با کلید عمومی امن‌تر است!
  - در هر دو روش رمزنگاری امنیت به طول کلید وابسته است.
- مسئله توزیع کلید در رمزنگاری با کلید عمومی برطرف شده است!
  - چگونه مطمئن شویم کلید عمومی لزوما متعلق به شخص ادعاکننده است؟!
  - پس توزیع کلید عمومی آسانتر است، ولی بدیهی و بدون مشکل نیست.

فهرست مطالب

- مبانی رمزنگاری کلید عمومی
- مقایسه با رمزنگاری سنتی و متقارن
- **کاربردهای رمزنگاری کلید عمومی**
- الگوریتم رمز RSA
- الگوریتم رمز دیفی-هلمن

کاربردهای رمزنگاری کلید عمومی

- **رمزگذاری/ رمزگشایی:** برای حفظ محرمانگی
- **امضاء رقمی:** برای حفظ اصالت پیام و معین نمودن فرستنده پیام (پیوند دادن پیام با امضاء کننده) یا همان عدم انکار
- **توزیع کلید:** برای توافق طرفین روی کلید مخفی جلسه، قبل از برقراری ارتباط

جایگاه عملی رمزنگاری کلید عمومی

- کلیدهای این نوع از الگوریتم‌ها بسیار طولانی تر از الگوریتم‌های رمز متقارن هستند.
  - الگوریتم RSA با پیمانه ۱۰۲۴ بیتی امنیتی در حد الگوریتم‌های متقارن با کلیدهای ۸۰ بیتی دارد.

- سرعت الگوریتم‌های کلید عمومی از الگوریتم‌های رمزگذاری متقارن پایین‌تر است.
  - RSA تقریباً ۱۰۰۰ بار کندتر از رمزهای متقارن (با امنیت یکسان) است.

جایگاه عملی رمزنگاری کلید عمومی

- امروزه کاربرد این الگوریتم‌ها به حل مساله توزیع کلید و امضای دیجیتال محدود می‌شود.
(مطابق اهداف و انگیزه های اولیه طراحی)

حملات به رمزنگاری کلید عمومی

- جستجوی فراگیر (Brute force)
- محاسبه کلید خصوصی از کلید عمومی
  - اثبات نشده که غیر ممکن است!
- حمله پیام احتمالی (Probable-message attack)
  - مخصوص رمزنگاری کلید عمومی
  - در صورت کوچک بودن پیام (مثلا پیام، یک کلید ۵۶ بیتی DES باشد) می‌توان همه کلیدهای ممکن DES را با کلید عمومی رمز کرد و کلید رمز شده را پیدا کرد.

فهرست مطالب

- مبانی رمزنگاری کلید عمومی
- مقایسه با رمزنگاری سنتی و متقارن
- کاربردهای رمزنگاری کلید عمومی
- **الگوریتم رمز RSA**
- الگوریتم رمز دیفی-هلمن

کلیات الگوریتم رمزنگاری RSA

آپا دانشگاه سمنان

- کلیات

- توسط Rivest–Shamir –Adleman در سال ۱۹۷۷ در MIT ارائه شد.
- مشهورترین و پرکاربردترین الگوریتم رمزگذاری کلیدعمومی
- مبتنی بر توان رسانی پیمانه‌ای
- استفاده از اعداد طبیعی خیلی بزرگ
- امنیت آن ناشی از دشوار بودن تجزیه اعداد بزرگ، که حاصلضرب دو عامل اول بزرگ هستند، می‌باشد.
- مستندات مربوط به آن تحت عنوان PKCS استاندارد شده است.

- $\mathbb{Z}_n$: مجموعه اعداد نامنفی کمتر از n.
- $\mathbb{Z}_n^*$: مجموعه اعداد طبیعی کمتر از n و اول نسبت به آن.
- مثال:

$$\mathbb{Z}_{۱۲} = \{۰,۱,۲,۳,۴,۵,۶,۷,۸,۹,۱۰,۱۱\}$$

$$\mathbb{Z}_{۱۲}^* = \{۱,۵,۷,۱۱\}$$

- تابع $\varphi(n)$ اویلر: تعداد اعضای $\mathbb{Z}_n^*$
- مثال: $\varphi(۱۲) = ۴$
- اگر n عددی اول باشد: $\varphi(n) = n - ۱$
- اگر n حاصل ضرب دو عدد اول p و q باشد:

$$\varphi(n) = \varphi(pq) = (p-۱)(q-۱)$$

❑ قضیه کوچک فرما (Fermat):

☜ p عددی اول و a عددی صحیحی که مضرب p نیست:

$$a^{p-۱} \equiv ۱ \pmod{p}$$

❑ مثال:

$$p = ۱۱, \qquad a = ۷$$

$$۷^{۱۱-۱} = ۲۸۲۴۷۵۲۴۹$$

$$= ۲۵۶۷۹۵۶۸ \times ۱۱ + ۱$$

$$\equiv ۱ \pmod{۱۱}$$

❑ قضیه اویلر (تعمیم قضیه فرما):

☜ اگر a و n اعداد طبیعی و نسبت به هم اول باشند:

$$a^{\varphi(n)} \equiv ۱ \pmod{n}$$

❑ مثال:

$$n = ۱۲, \qquad a = ۷$$

$$۷^{\varphi(۱۲)} = ۷^{۴}$$

$$= ۲۴۰۱ = ۲۰۰ \times ۱۲ + ۱$$

$$\equiv ۱ \pmod{۱۲}$$

نمادگذاری RSA

- n: پیمانه عمومی (Public Modulus)
  - ☜ حاصل ضرب دو عدد اول p و q بسیار بزرگ
- e: نمای عمومی (Public Exponent)
- d: نمای خصوصی (Private Exponent)
  - ☜ داریم: $d \leftarrow e^{-1} \pmod{\varphi(n)}$
- m: پیام، عددی متعلق به $\mathbb{Z}_n$
- **تابع RSA**: تابع یکطرفه $c \leftarrow m^e \pmod{n}$
- **تابع معکوس**: $m \leftarrow c^d \pmod{n}$

عدد صحیح k وجود دارد که:

$$ed = k\varphi(n) + 1$$

مثال از RSA

$$p = ۶۱, \quad q = ۵۳$$

$$n = pq = ۳۲۳۳$$

$$\varphi(n) = (۶۱-۱)(۵۳-۱) = ۳۱۲۰$$

$$\left.\begin{array}{l} e = ۱۷ \\ d = ۲۷۵۳ \end{array}\right\} \rightarrow ed \equiv ۱ \pmod{\varphi(n)}$$

$$m = ۶۵$$

$$c = E(m) = ۶۵^{۱۷} \pmod{۳۲۳۳} = ۲۷۹۰$$

$$c = ۲۷۹۰$$

$$m = D(c) = ۲۷۹۰^{۲۷۵۳} \pmod{۳۲۳۳} = ۶۵$$

روند تولید کلید در RSA

1. ابتدا دو عدد اول بزرگ p و q را به طور تصادفی انتخاب کن به گونه‌ای که $p \neq q$
2. عدد n و $\phi(n)$ را محاسبه کن $n=p.q$ و $\phi(n)=(p-1).(q-1)$
3. عدد صحیح فرد e کوچکتر از $\phi(n)$ را به گونه ای انتخاب کن که $\gcd(e, \phi(n))=1$ باشد.
4. d را محاسبه کن $d \equiv e^{-1} \pmod{\phi(n)}$
5. زوج $PU=(e,n)$ را به عنوان کلید عمومی اعلام کن.
6. زوج $PR=(d,n)$ را به عنوان کلید خصوصی ذخیره کن.

قراردادها و پروتکل RSA

- هم فرستنده و هم گیرنده مقدار n را می‌دانند.
- فرستنده مقدار e را می‌داند.
  - کلید عمومی : (n , e)
- تنها گیرنده مقدار d را می‌داند.
  - کلید خصوصی : (n, d)
- نیازمندی‌ها:
  - محاسبه M^e و C^d آسان باشد.
  - محاسبه d با دانستن کلید عمومی غیرممکن باشد.

- اعداد صفرم تا سوم فرما (۳ ، ۵ ، ۱۷ ، ۲۵۷) کوچک هستند و به آنها حمله وارد است. استفاده بسیار متداول از عدد چهارم فرما 65537

Figure 9.5 The RSA Algorithm

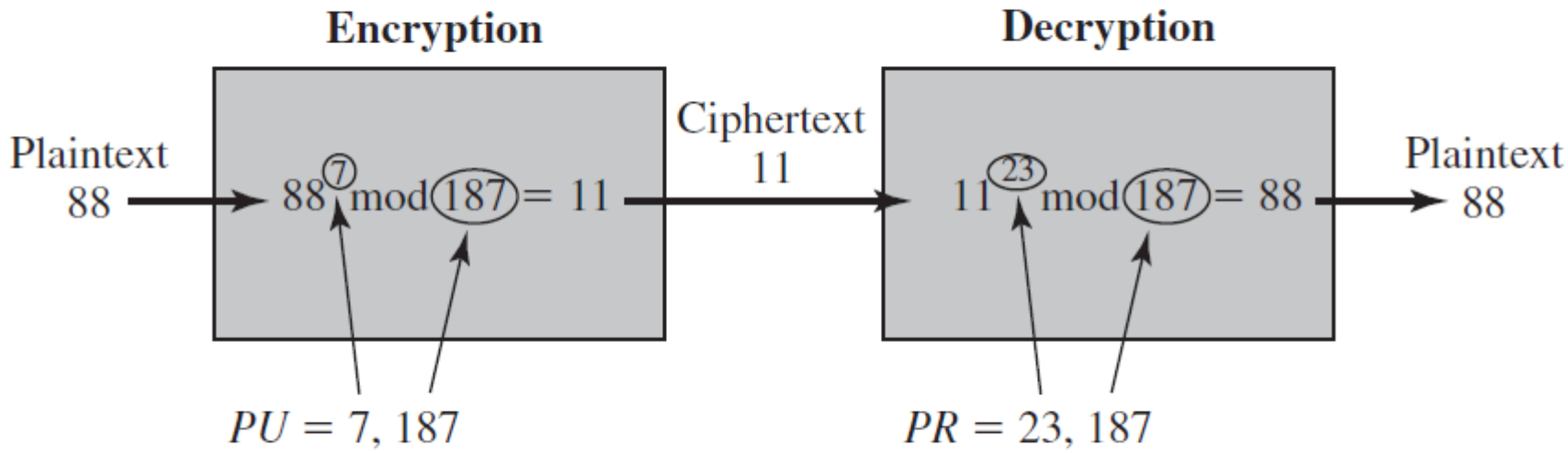


Figure 9.6 Example of RSA Algorithm

p = 17, q = 11, n = p.q= 187

φ(n) = 16.10 =160, pick e=7, d.e≡1 [mod φ(n)] ➔ d = 23

روشهای کارا برای محاسبه نما

- برای محاسبه $a^b \pmod n$ الگوریتم‌های متفاوتی ابداع شده است...
  - فرض کنید $b_k b_{k-1} \ldots b_0$ نمایش مبنای ۲ عدد b باشد.
  - بنابراین خواهیم داشت:

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

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

الگوریتم توان و ضرب

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

Note: The integer b is expressed as a binary number $b_k b_{k-1} \ldots b_0$.

Figure 9.8 Algorithm for Computing a^b mod n

- بر این مبنا می‌توان الگوریتم شکل مقابل را طراحی نمود:


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

Note: The integer b is expressed as a binary number $b_k b_{k-1} \ldots b_0$.

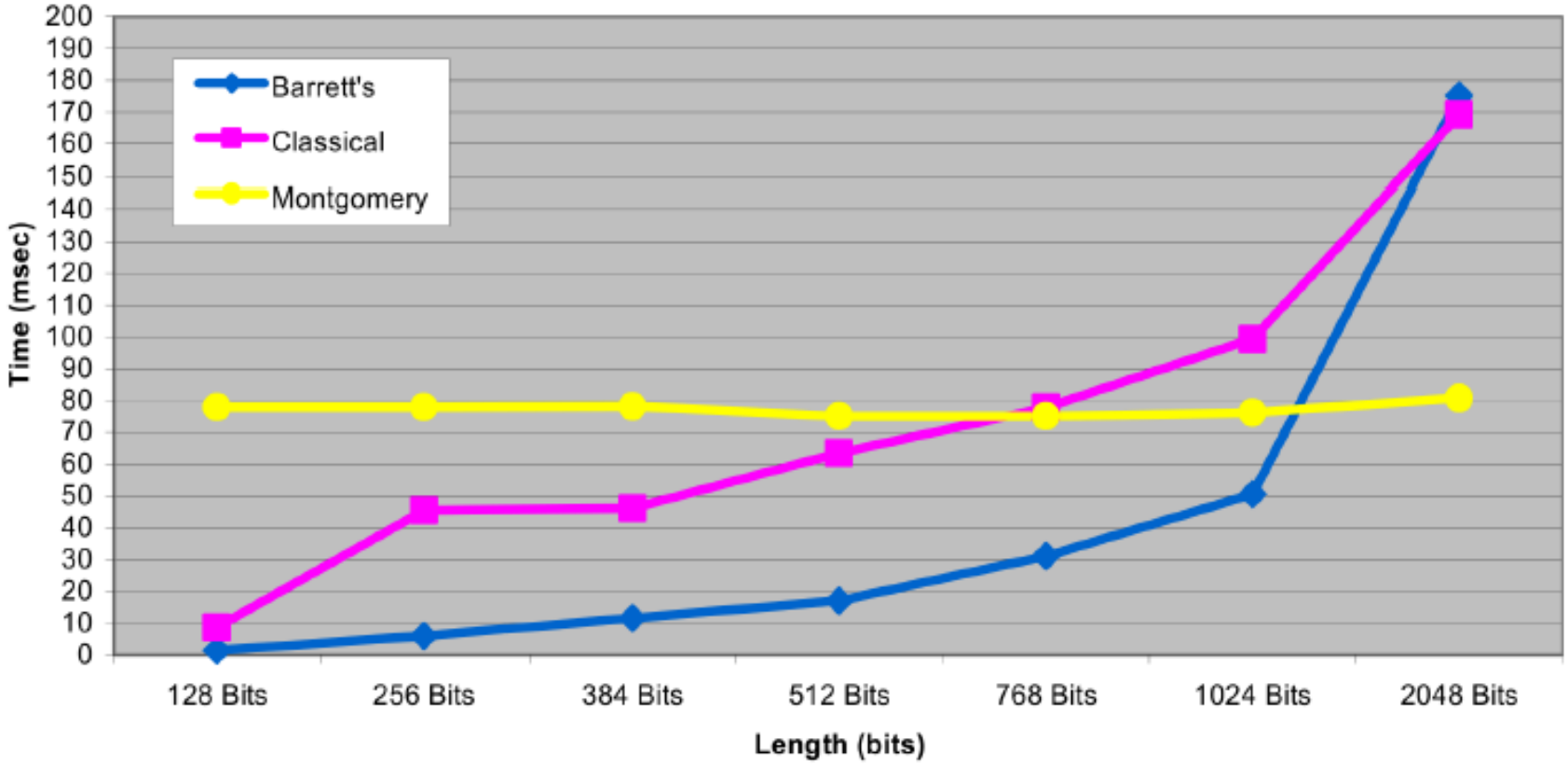
Figure 9.8 Algorithm for Computing a^b mod n

- اگر a، b و n با β بیت قابل نمایش باشند، نیاز به O(β) عمل ریاضی است.

Table 9.4 Result of the Fast Modular Exponentiation Algorithm for a^b mod n, where $a = 7$, $b = 560 = 1000110000$, and $n = 561$

i	9	8	7	6	5	4	3	2	1	0
b_i	1	0	0	0	1	1	0	0	0	0
c	1	2	4	8	17	35	70	140	280	560
f	7	49	157	526	160	241	298	166	67	1

سرعت سه الگوریتم توان‌رسانی پیمانه‌ای (Pentium III)



M. Johnson, B. Phung, T. Shackelford, S. Rueangvivatanakij. **Modular Reduction of Large Integers Using Classical, Barrett, Montgomery Algorithms**, Tech. Report, 2002.

مبانی ریاضی و درستی RSA

- p و q دو عدد اول می‌باشند.
- φ(n): تعداد اعداد (کوچکتر از n) که نسبت به n اول است.
- کلید عمومی:{e,n}
- کلید خصوصی: {d,n}

$n = p.q$

$\varphi(n) = (p-1).(q-1)$

$gcd(\varphi(n), e) = 1, \quad 1 < e < \varphi(n)$

$d.e = 1 \ [mod \ \varphi(n)], \quad d = e^{-1} \ [mod \ \varphi(n)]$

$C = M^e \bmod n, \quad M < n$

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

درستی RSA

- **Chinese Remainder Theorem**
  - If $n_1, n_2, \ldots, n_k$ are pairwise relatively prime and $n = n_1 n_2 \ldots n_k$, then for all integers x and a:
  - $x \equiv a \pmod{n_i}$ for $i = 1, 2, \ldots, k$

    if and only if

    $x \equiv a \pmod{n}$

- **Fermat's Theorem**
  - If p is prime, $a^{p-1} \equiv 1 \pmod{p}$

درستی RSA

- Since *e* and *d* are multiplicative inverses modulo
- $\Phi(n) = (p-1)(q-1)$, So $ed = 1 + k(p-1)(q-1)$

- We prove that $M^{ed} = M \pmod p$, for all M
  - If $M \neq 0 \pmod p$
    - $M^{ed} = M\,(M^{p-1})^{k(q-1)} \pmod p$
    - $= M\,(1)^{k(q-1)} \pmod p$
    - $= M \pmod p$
  - If $M = 0 \pmod p$, then $M^{ed} = M \pmod p$
- In the same way: $M^{ed} = M \pmod q$, for all M
- Thus: $M^{ed} = M \pmod n$ based on Chinese remainder theorem

حملات ممکن بر RSA

- **حمله آزمون جامع(Brute Force)**
- طول کلید با پیدایش هر نسل جدید از پردازنده‌ها افزایش می‌یابد، ضمن اینکه قدرت پردازشی هکرها زیاد می‌شود!
- طول کلید معادل تعداد بیتهای پیمانه محاسبات (n) است.

حملات ممکن بر RSA

- **حملات ریاضی**
  - تجزیه پیمانه n و در نتیجه محاسبه φ(n)
- در حال حاضر سختی مساله فوق معادل سختی مساله تجزیه اعداد بزرگ حاصل از ضرب دو عامل اول است.
- الگوریتم‌های مختلفی برای مساله تجزیه ارائه شده است (بهترین آنها GNFS است).
- در حال حاضر RSA با کلید ۱۰۲۴ تا ۴۰۹۶ بیت امن است.

Twenty Years of Attacks on the RSA Cryptosystem 1999, by Dan Boneh

حملات ممکن بر RSA

- **حمله زمانی**
  - زمان اجرای عملیات رمزگذاری یا رمزگشایی می‌تواند اطلاعاتی را در مورد کلید افشاء کند.
- **راه‌های مقابله با حملات زمانی**
  - استفاده از توان رساندن با زمان ثابت محاسباتی
  - اضافه کردن تاخیرهای تصادفی
  - قرار دادن اعمال اضافی و گمراه کننده در بین محاسبات

فهرست مطالب

- مبانی رمزنگاری کلید عمومی
- مقایسه با رمزنگاری سنتی و متقارن
- کاربردهای رمزنگاری کلید عمومی
- الگوریتم رمز RSA
- **الگوریتم رمز دیفی-هلمن**

مبانی ریاضی – ۱

- فرض کنید p عددی اول باشد.
- مجموعه توانهای مختلف عدد a به پیمانه p را با $<a>_p$ نمایش می‌دهیم.
- مثال: $p = ۷$

$$\langle ۳ \rangle_۷ = \{۱, ۳, ۲, ۶, ۴, ۵\} \qquad \langle ۲ \rangle_۷ = \{۱, ۲, ۴\}$$

- g را یک مولد (Generator) برای $\mathbb{Z}_p^*$ می‌خوانیم اگر:

$$\langle g \rangle_p = \mathbb{Z}_p^*$$

- قضیه ۱: $\mathbb{Z}_p^*$ حتماً مولد دارد.
- قضیه ۲: مولد $\mathbb{Z}_p^*$ الزاماً یکتا نیست.
- عدد اول p و مولد دلخواه g از $\mathbb{Z}_p^*$ را در نظر بگیرید.
- عدد α را به تصادف از $\mathbb{Z}_p$ انتخاب کنید.
- مسئله لگاریتم گسسته (DL): پیدا کردن α با داشتن مقادیر:

$a^x \equiv b \bmod p$

$$p, \quad g, \quad g^{\alpha} \pmod{p}$$

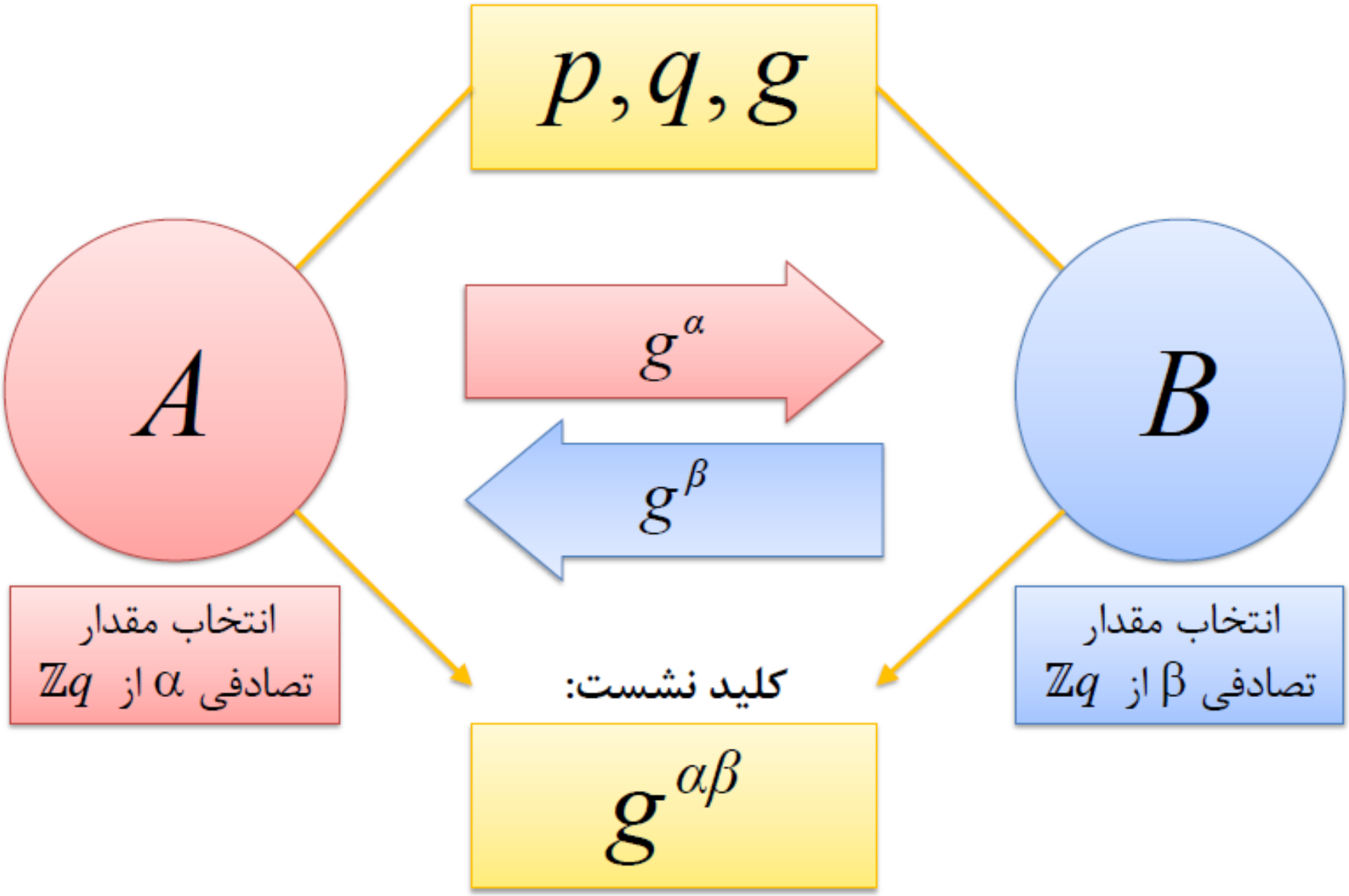
الگوریتم دیفی–هلمن

- توسط Diffie و Hellman در سال ۱۹۷۶ ارائه شد.
- برای تبادل کلید مورد استفاده قرار می‌گیرد.
- کلید نشست باید غیر قابل تمایز از یک مقدار تصادفی باشد.
- امنیت روش مبتنی بر دشواری شکستن DDH است.

- طرفین از قبل روی مقادیر p، q و g توافق می‌کنند.

☜ کلیه محاسبات به پیمانه p

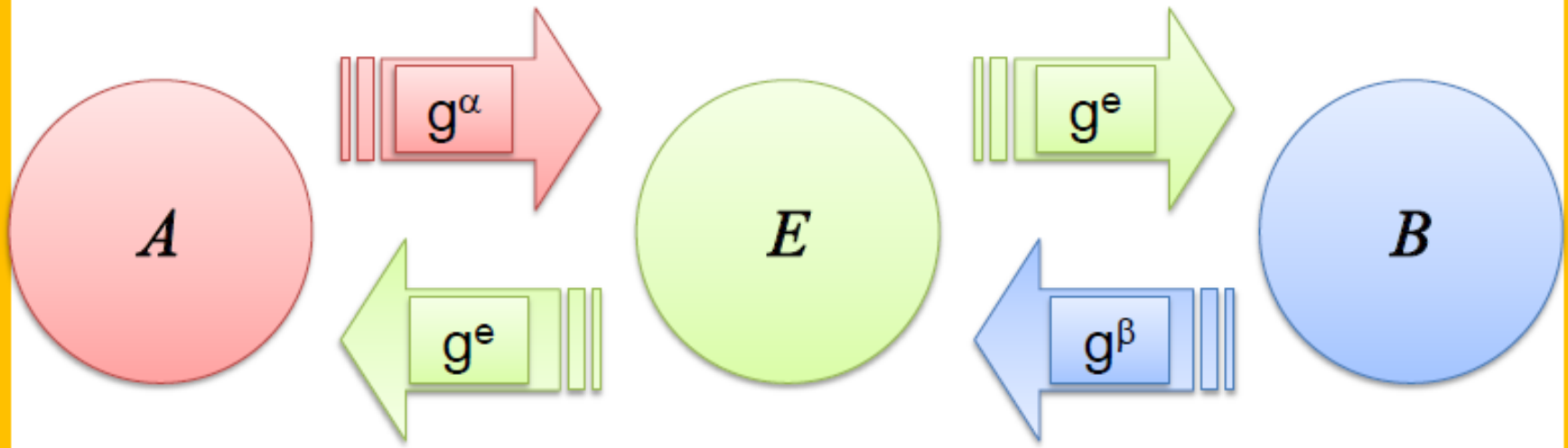
تبادل کلید دیفی–هلمن



حمله مرد میانی

- با فرض دشواری DDH، پروتکل دیفی-هلمن در برابر حملات منفعلانه (passive) امن است.
- اما این پروتکل در برابر حملات فعال (active) امن نیست.
- **حمله مرد میانی (MITM)**
  - مهاجم برای A وانمود می‌کند که B است.
  - مهاجم برای B وانمود می‌کند که A است.

حمله مرد میانی



$$K_1 = g^{\alpha e}$$

$$K_2 = g^{\beta e}$$

A گمان می‌کند کلید K_1 را با B به اشتراک گذاشته است.

- A پیامهای به مقصد B را با K_1 رمز می‌کند.
- B پیامهای به مقصد A را با K_2 رمز می‌کند.
- E می‌تواند همه پیامها را بخواند، و با کلید مناسب برای فرد منظور رمز نماید.

B گمان می‌کند کلید K_2 را با A به اشتراک گذاشته است.

رفع مشکل تبادل کلید دیفی–هلمن

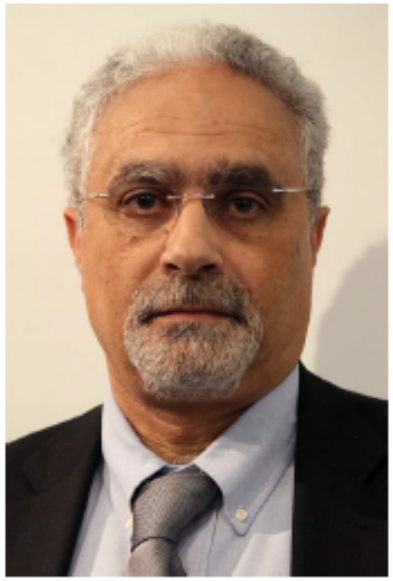
- طرفین باید قبل از شروع پروتکل، یک کلید طولانی مدت (LTK) را به اشتراک گذاشته باشند.
  - LTK می‌تواند متقارن یا نامتقارن باشد.
  - در حالت نامتقارن، طرفین کلید عمومی یکدیگر را دارند.
- از LTK برای حفظ صحت g^{α} و g^{β} استفاده می‌شود.
  - (ADH) Authenticated Diffie–Hellman
  - در صورت حفظ صحت، مهاجم نمی‌تواند MITM را اجرا کند.

فهرست مطالب

- مبانی رمزنگاری کلید عمومی
- مقایسه با رمزنگاری سنتی و متقارن
- کاربردهای رمزنگاری کلید عمومی
- الگوریتم رمز RSA
- **الگوریتم رمز دیفی-هلمن**
- **الگوریتم رمز الجمل**

رمز الجمل (ElGamal)

- ابداع توسط الجمل، رمزنگاری مصری-آمریکایی، در سال ۱۹۸۵
  - ☜ در ایران بیشتر با نام «الجمال» شناخته می‌شود.
  - ☜ الجمال دانشجوی دکترای هلمن در دانشگاه استنفورد بود.
- امنیت رمز الجمل مبتنی بر دشواری DDH



طاهر الجمل
(۱۹۵۵ –)

تولید کلید الجمل

- انتخاب عدد اول بزرگ p
- انتخاب $g \in \mathbb{Z}_p^*$ به گونه‌ای که $|\langle g \rangle_p| = q$.
  - q باید اول و بزرگ باشد.
  - کلیه محاسبات به پیمانه p.
- انتخاب عدد تصادفی α از $\mathbb{Z}_q$ و محاسبه $h = g^\alpha$.
- p، q و g پارامترهای عمومی (همه مقادیر آنها را می‌دانند).
- α کلید خصوصی و h کلید عمومی.

رمزگذاری و رمزگشایی الجمل

- رمزگذاری عدد $m \in \langle g \rangle_p$:
  - انتخاب عدد تصادفی r از $\mathbb{Z}_q$.
  - مقدار رمز عبارت است از زوج: $c = (g^r, mh^r)$.
- رمزگشایی از زوج $c = (c_1, c_2)$ با استفاده از کلید خصوصی α:

$$m = \frac{c_2}{(c_1)^{\alpha}}$$

- $Z_p^* = \langle g \rangle$, $m \in Z_p$ message
  - B encrypts a message to A.
- Alice: a random, $h = g^a$, public key = (p, g,A)
- Bob: k random (ephemeral key), $c_1 = g^k$, shared key $K = A^k = g^{ak}$
  - $E_A(m) = (c_1,c_2)$, $c_2 = mK \bmod p$.
  - $D_A((c1,c2)) = c_2 * (1/K) \bmod p$, $K = c_1{}^a = g^{ak}$
- Security depends on Computational Diffie-Hellman (CDH) assumption: given (g, g^a, g^b) it is hard to compute g^{ab}
- Do not use same k twice

کاربردهای برخی الگوریتم‌های کلید عمومی

الگوریتم	رمزگذاری/ رمز گشایی	امضاء رقمی	توزیع کلید
RSA	√	√	√
Diffie-Hellman	×	×	√
DSS	×	√	×
Elliptic Curve	√	√	√

منابع

- اسلایدهای دکتر مرتضی امینی (منبع اصلی) – درس امنیت داده و شبکه
- اسلایدهای درس امنیت داده و شبکه دکتر دوستی – درس امنیت داده و شبکه
- جزوه درس رمزنگاری دکتر عارف
- Cryptography and Network Security Principles and Practices, By William Stallings 5th Edition