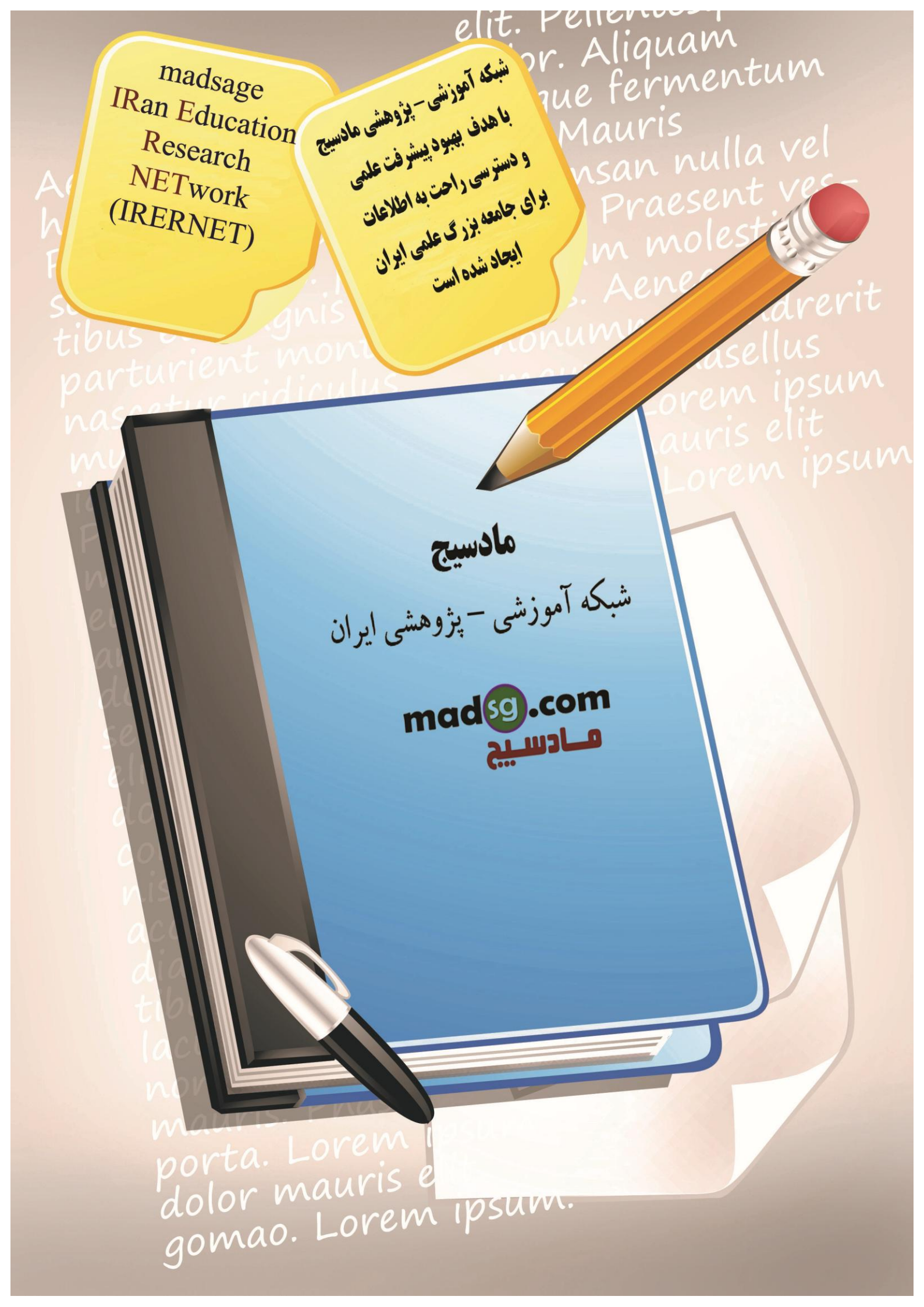

madsage
IRan Education
Research
NETwork
(IRERNET)
شبکه آموزشی-پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است
مادسیج
شبکه آموزشی - پژوهشی ایران
madsg.com
مادسیج

یا ذاالامن والامان

امنیت داده و شبکه

رمزنگاری نامتقارن (کلید عمومی)

مرتضی امینی - نیمسال اول ۹۱-۹۰

مرکز امنیت داده و شبکه شریف
http://dnsl.ce.sharif.edu

فهرست مطالب

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

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

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

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.

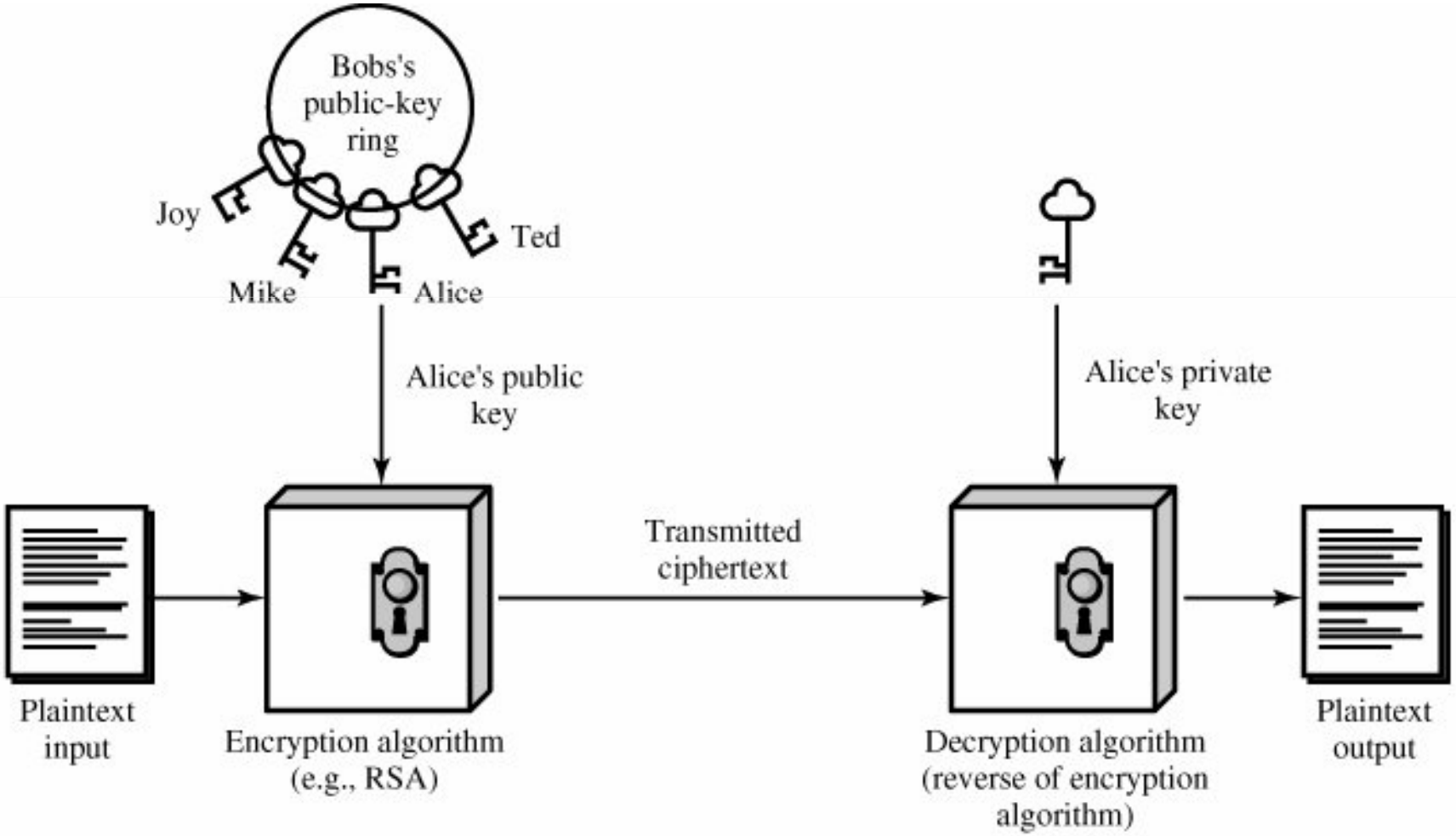
$$M = D_{PR_b}[E_{PU_b}(M)] = D_{PU_b}[E_{PR_b}(M)]$$

رمزگذاری کلید عمومی

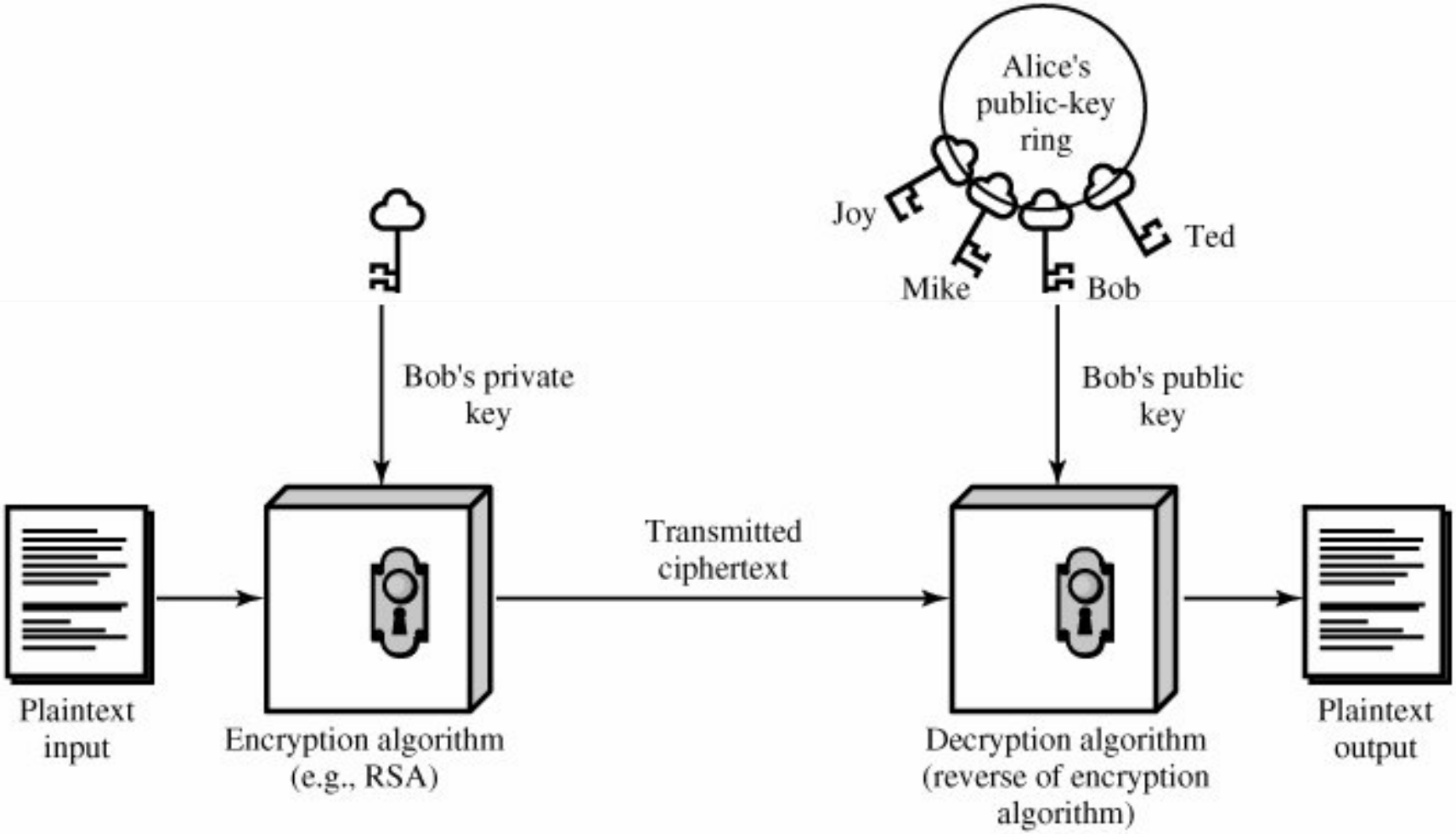
- برای رمز نگاری کلید عمومی گام‌های زیر را برمی‌داریم:

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



رمزگشایی با کلید عمومی

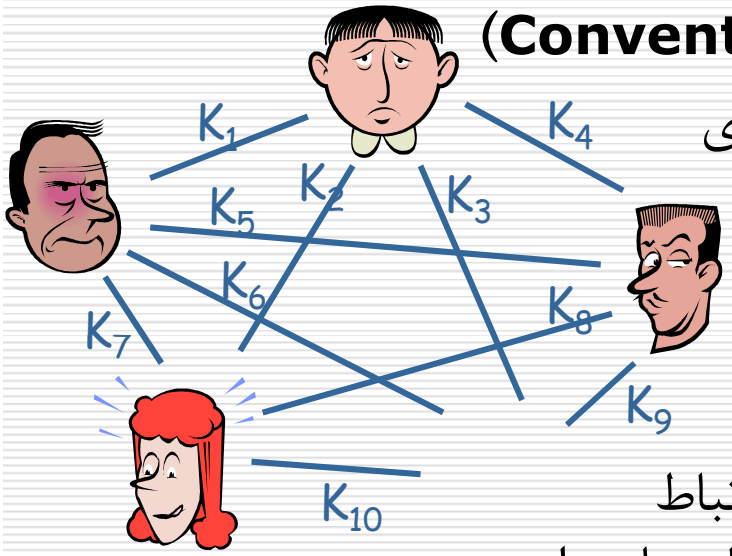


فهرست مطالب

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

مقایسه رمزنگاری مرسوم و رمزنگاری کلید عمومی

رمزنگاری مرسوم (Conventional Cryptography)



- 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 الکترونیکی

مزایا

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

مقایسه رمزنگاری مرسوم و رمزنگاری کلید عمومی

- در **رمزگذاری مرسوم** 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 مرسوم 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 مرسوم 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 نیست.

محرمانگی و احراز اصالت به صورت همزمان

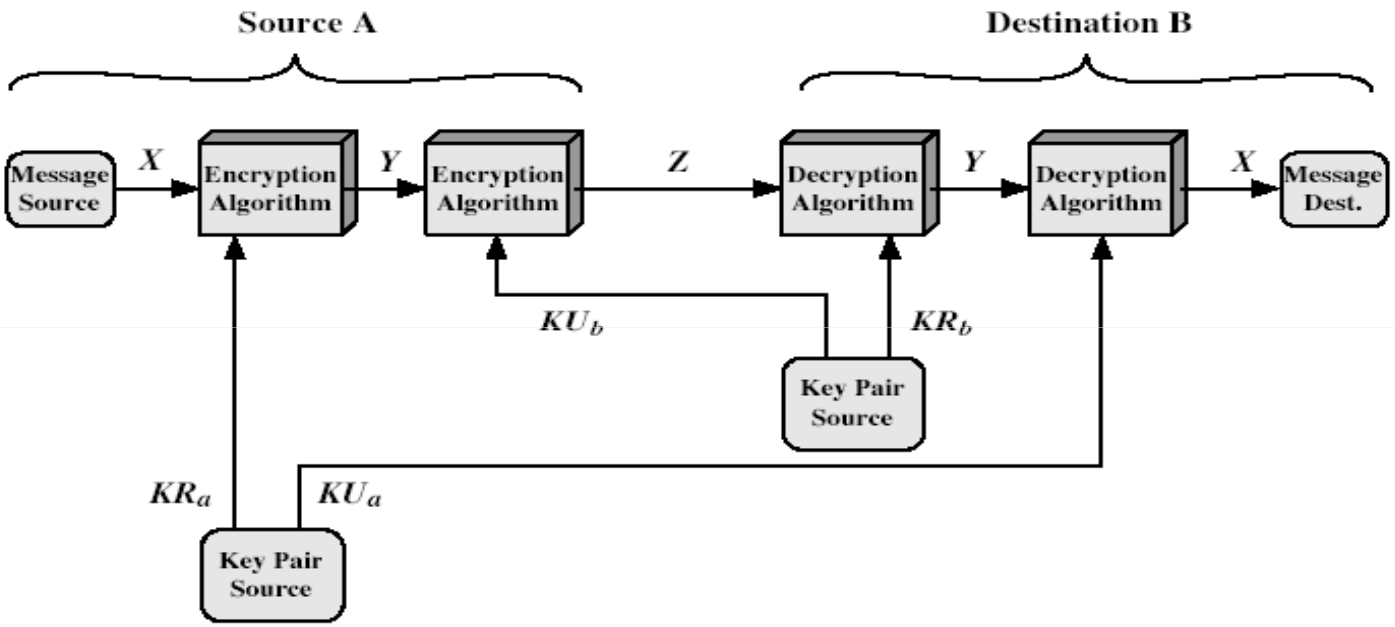


Figure 9.4 Public-Key Cryptosystem: Secrecy and Authentication

رمزگذاری کلید عمومی: محرمانگی و احراز اصالت به صورت همزمان

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)
- **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 مرسوم (کلید خصوصی) هستند.
  - الگوریتم RSA با پیمانه ۱۰۲۴ بیتی امنیتی در حد الگوریتم‌های متقارن با کلیدهای ۸۰ بیتی دارد.

- سرعت الگوریتم‌های کلید عمومی از الگوریتم‌های رمزگذاری مرسوم 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

- 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.

Public Key Cryptography Standards

نمادگذاری RSA

- n : پیمانه محاسبات
- e: نمای رمزگذاری
- d: نمای رمزگشایی
- M: پیام، عدد صحیح متعلق به Z_n^*
- تابع RSA: تابع یکطرفه $C = M^e \bmod n$
- تابع معکوس: $M = C^d \bmod n$

مبانی ریاضی 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}

$$n = p.q$$

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

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

$$d.e \equiv 1 \mod \phi(n), \quad d \equiv e^{-1} (\mod \phi(n))$$

$$C = M^e \mod n, \qquad M < n$$

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

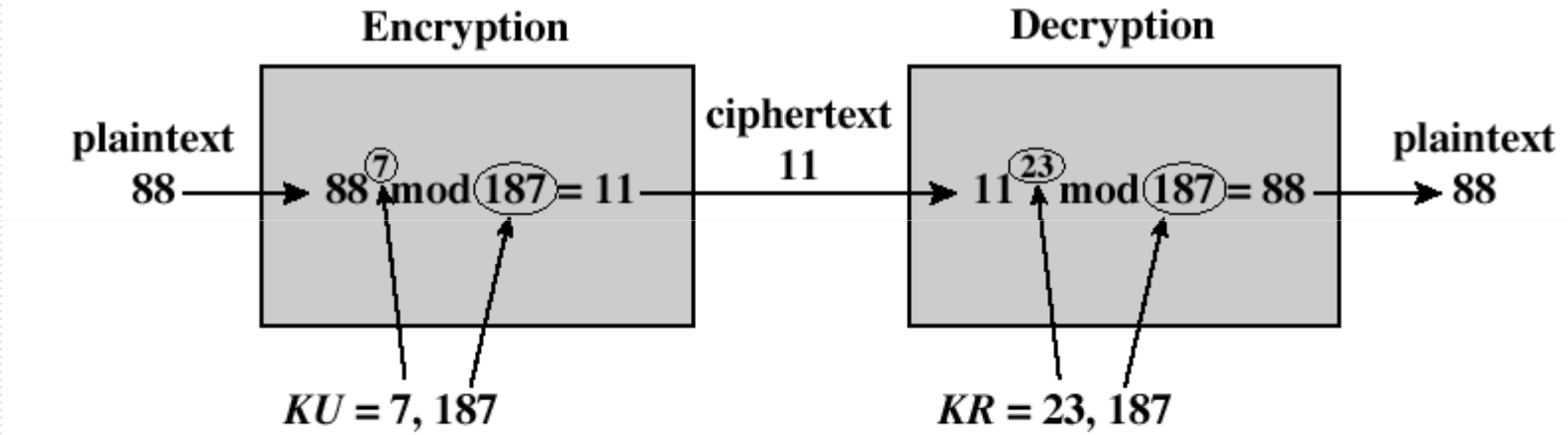
روند تولید کلید در RSA

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.

مثال–RSA



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

- بر این مبنا می‌توان الگوریتم زیر را طراحی نمود:

$c \leftarrow 0; d \leftarrow 1$

for $i \leftarrow k$ *downto* 0

do $c \leftarrow 2.c$ ⟹ c is prefix of b

$d \leftarrow d^2 \bmod n$

if $b_i = 1$

then $c \leftarrow c + 1$

$d \leftarrow (d.a) \bmod n$ ⟹ $d = a^c \bmod n$

return d

مثال عددی الگوریتم توان و ضرب

اگر a، b و n با β بیت قابل نمایش باشند،

- نیاز به O(β) عمل ریاضی

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

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
d	7	49	157	526	160	241	298	166	67	1

Figure 9.8 Result of the Fast Modular Exponentiation Algorithm for $a^b \bmod n$, where $a = 7$, $b = 560 = 1000110000$, $n = 561$

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)
  - محاسبه φ(n) به صورت مستقیم
  - محاسبه d بدون استفاده از φ(n)
- در حال حاضر سختی همه راه‌های فوق معادل سختی مساله تجزیه اعداد بزرگ حاصل از ضرب دو عامل اول است.
- الگوریتم‌های مختلفی برای مساله تجزیه ارائه شده است (بهترین آنها LS 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 رمز 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

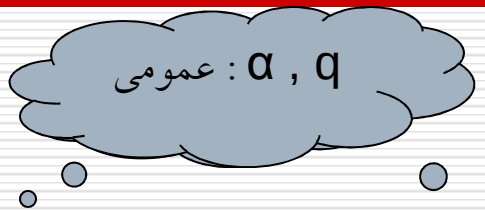
فهرست مطالب

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

الگوریتم دیفی–هلمن

- توسط Diffie و Hellman در سال ۱۹۷۶ ارائه شد.
- برای تبادل کلید مورد استفاده قرار می‌گیرد.
- طرفین بر روی مقادیر q و α توافق می‌کنند.
- q یک عدد اول و α یک مولد برای این عدد است.
- امنیت روش مبتنی بر مشکل بودن لگاریتم گسسته است.

الگوریتم دیفی–هلمن



A

B

مقدار تصادفی X_A را انتخاب می‌کند

مقدار تصادفی X_B را انتخاب می‌کند

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

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

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

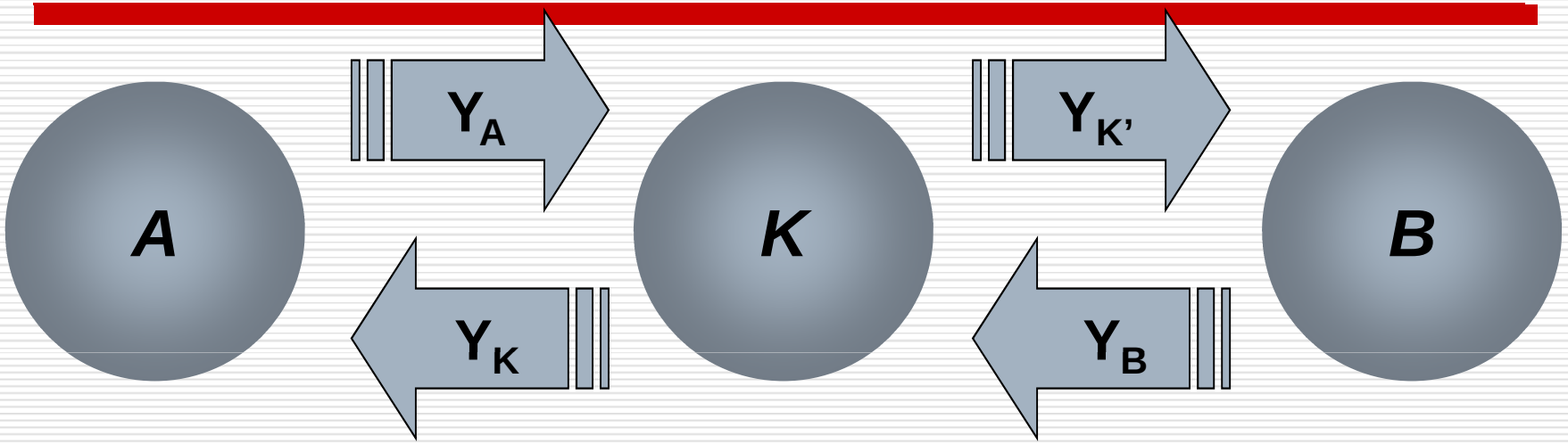
$$K_{AB} = (Y_A)^{X_B} \bmod q$$

کلید مشترک عبارت است از $\alpha^{(X_A \times X_B)} \bmod q$

حمله مرد میانی

- مهاجم به عنوان کانال ارتباطی میان طرفین عمل می‌کند.
- از نوع حملات فعال محسوب می‌شود.
- الگوریتم دیفی-هلمن را تهدید می‌کند.

حمله مرد میانی



$$K_1 = \alpha^{(X_A \times X_K)} \bmod q$$

$$K_2 = \alpha^{(X_A \times X_{K'})} \bmod q$$

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

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

کاربردهای برخی الگوریتم‌های کلید عمومی

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

پایان

مرکز امنیت داده و شبکه شریف

http://dnsl.ce.sharif.edu

پست الکترونیکی

m_amini@ce.sharif.edu

درستی RSA

- بر اساس تئوری اولر
  - اگر $gcd(a,n)=1$ باشد، آنگاه $a^{\phi(n)} \bmod n = 1$
- در RSA داریم:
  - $n=p.q$
  - $\phi(n)=(p-1).(q-1)$
  - $d \equiv e^{-1} \pmod{\phi(n)}$ و لذا $e.d=1+k.\phi(n)$
- بنابراین
  - $C^d = M^{e.d} = M^{1+k.\phi(n)} = M^1.(M^{\phi(n)})^k = M^1.(1)^k = M^1 = M \bmod n$

شبکه آموزشی- پژوهشی مادسیج
با هدف بهبود پیشرفت علمی
و دسترسی راحت به اطلاعات
برای جامعه بزرگ علمی ایران
ایجاد شده است

madsg.com

مادسیج

IRan Education & Research NETwork
(IRERNET)