امنیت شبکه

علی فانیان
a.fanian@cc.iut.ac.ir

فهرست مطالب

- مبانی رمزنگاری کلید عمومی
- کاربردهای رمزنگاری کلید عمومی
  - توزیع کلید
  - امضای دیجیتال
- توابع یک طرفه
- توابع یک طرفه دریچه ای

مبانی رمزنگاری کلید عمومی

- رمزنگاری کلید عمومی اساساً با انگیزه رسیدن به دو هدف طراحی شد:
  - حل مساله توزیع کلید
  - امضای رقمی (دیجیتال)

➢ دیفی و هلمن توصیف کلی و اولین راه حل را در ۱۹۷۶ ارایه دادند.

رمز نگاری کلید عمومی

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

نمادها و قراردادها

- کلید عمومی : کلید رمز گذاری
  - این کلید را برای شخص A با PU_a نشان می دهیم
- کلید خصوصی: کلید رمز گشایی
  - این کلید را برای شخص A با PR_a نشان می دهیم

نیازمندیهای رمزنگاری کلید عمومی

- از نظر محاسباتی برای طرف B، تولید یک زوج کلید آسان باشد
- برای فرستنده، تولید متن رمز آسان باشد:

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

- برای گیرنده، رمزگشایی متن با استفاده از کلید خصوصی آسان باشد

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

نیازمندیهای رمزنگاری کلید عمومی

- از نظر محاسباتی تولید کلید خصوصی با دانستن کلید عمومی غیر ممکن باشد
- بازیابی پیام M، با دانستن PU_b و C غیر ممکن باشد

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

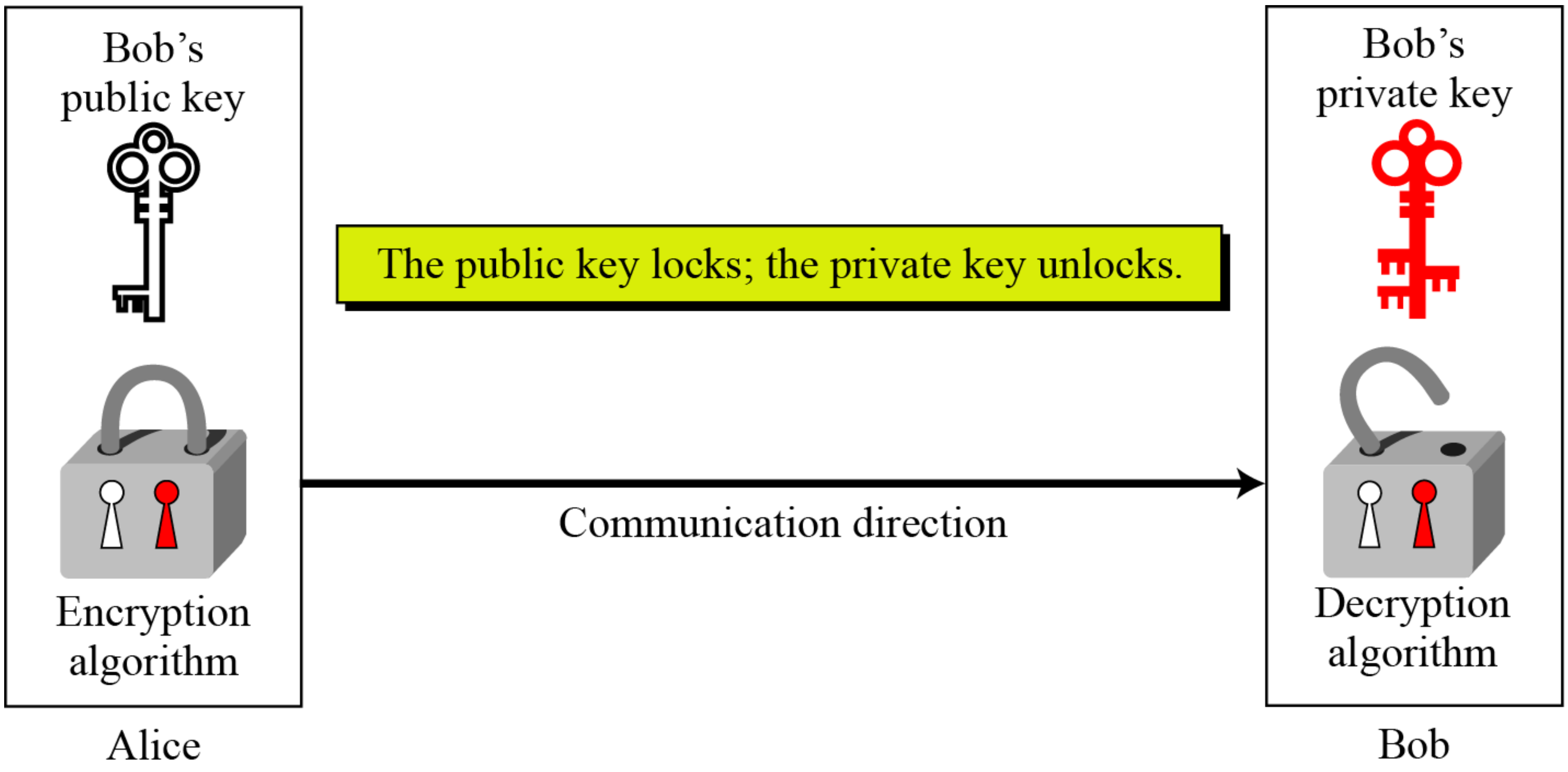
- ویژگی تقارنی: از هر یک از کلیدها می توان برای رمزکردن استفاده نمود. در این صورت از کلید دیگر برای رمزگشایی استفاده می شود.

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

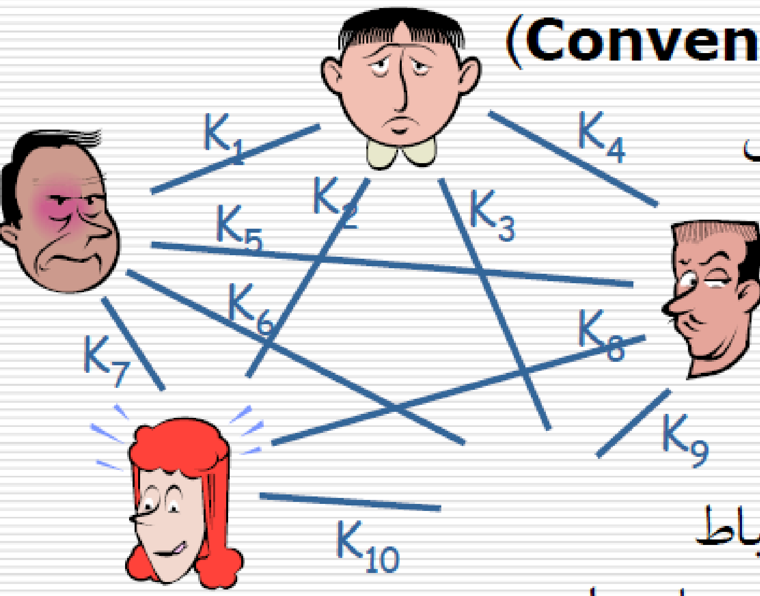
رمزگذاری کلید عمومی

- برای رمز نگاری کلید عمومی گامهای زیر را برمیداریم:
  - هر کاربر یک زوج کلید رمزگذاری و رمز گشایی تولید میکند.
  - کاربران کلید رمزگذاری خود را به صورت عمومی اعلان میکنند درحالی که کلید رمز گشایی 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.

رمزگذاری با کلید عمومی



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.

جایگزینی یا تکمیل؟

از نظر کاربردی، رمزگذاری با کلید عمومی بیش از آنکه جایگزینی برای رمزگذاری مرسوم باشد نقش مکمل آنرا برای حل مشکلات توزیع کلید بازی می کند.

Misconceptions!

دو تصور اشتباه دیگر درباره کلید عمومی

– رمزنگاری با کلید عمومی امن تر است!

- در هر دو روش رمزنگاری امنیت به طول کلید وابسته اس

– مسئله توزیع کلید در رمزنگاری با کلید عمومی برطرف شده است

- چگونه مطمئن شویم کلید عمومی لزوما متعلق به شخص ادعاکننده است؟!
- توزیع کلید عمومی آسانتر است، ولی بدیهی نیست.

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

محرمانگی و احرازاصالت بطور همزمان

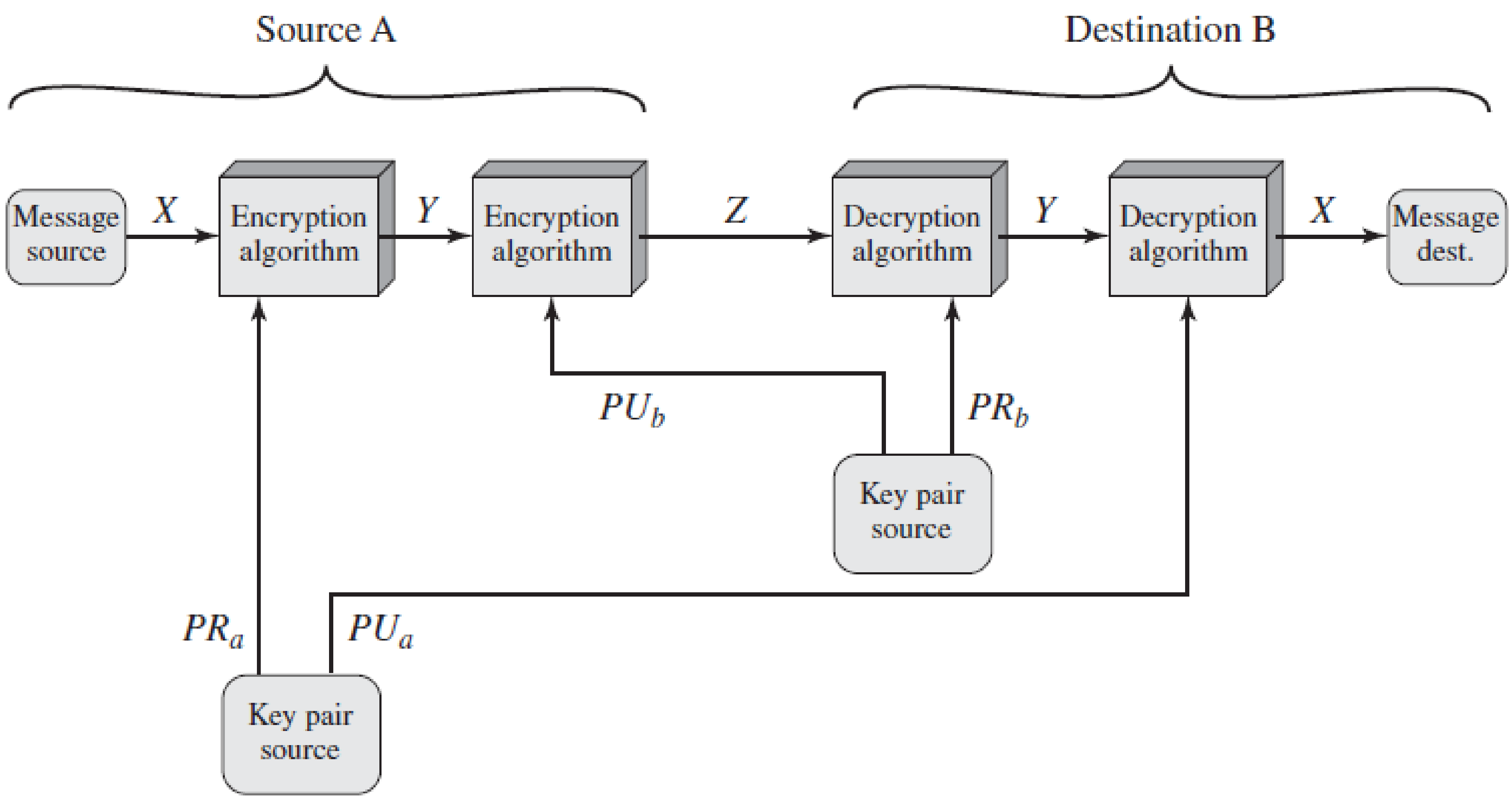


Figure 9.4 Public-Key Cryptosystem: Authentication and Secrecy

توابع یک طرفه

- تابع یک طرفه: تابع $f(.)$ را یک طرفه گوییم اگر یافتن مقدار ورودی تابع از روی مقدار خروجی از لحاظ محاسباتی ناممکن باشد.
- یک تابع یک طرفه همانند ماشین چرخ گوشت عمل میکند!

  – از روی خروجی (گوشت چرخ شده)

  عملا نمی توان ورودی را بازسازی کرد.

توابع یک طرفه

- تعریف: تابع $f(.)$ را یک طرفه گوییم اگر:
  - طول ورودی و خروجی یکسان باشد.
  - $f(.)$ در زمان چند جمله ای قابل محاسبه باشد.
  - $f^{-1}(.)$ در زمان چند جمله ای تصادفی قابل محاسبه نباشد.

توجه:

- تابع $f(.)$ لزوماً یک به یک نیست.

مثال: لگاریتم گسسته

q یک عدد اول و α یک مولد برای این عدد میباشد.

(یعنی هر عدد بین 1 تا q را میتوان به صورت توانی از α نشان داد.)

اگر $a = \alpha^b \bmod q$ باشد آنگاه یافتن b از روی a را محاسبه لگاریتم گسسته گویند.

فرض: محاسبه لگاریتم گسسته با بزرگ شدن پارامترها از لحاظ محاسباتی ناممکن است در حالی که نمارسانی گسسته همچنان به سادگی میسر است.

محاسبه نمای گسسته

- 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 Diffie - Hellman

توافق بر روی مقادیر q و α

Alice

عدد تصادفی X_A را انتخاب میکند

Bob

عدد تصادفی X_B را انتخاب میکند

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

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

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

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

کلید مشترک برابراست با $\alpha^{(X_A \times X_B)} \bmod q$

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
    - $y_A=3^{97} \bmod 353 = 40$
    - $y_B=3^{233} \bmod 353 = 248$
  - محاسبه کلید جلسه مورد توافق
    - $K_{AB}= y_B^{x_A} \bmod 353 = 248^{97} = 160$
    - $K_{AB}= y_A^{x_B} \bmod 353 = 40^{233} = 160$

دریچه

- وجود یک دریچه در تابع: اطلاعات اضافی که با دانستن آنها میتوانیم تابع را به روشی کارا معکوس کنیم.

توابع یک طرفه دریچه ای

- مجموعه ای از توابع معکوس پذیر $f_k(.)$ به طوریکه :
  - محاسبه $y= f_k(x)$ با دانستن k و x آسان باشد
  - محاسبه $x= f_k^{-1}(y)$ با دانستن k و y آسان باشد
  - محاسبه $x= f_k^{-1}(y)$ با دانستن y و مخفی بودن k امکانپذیر نباشد

توابع یک طرفه دریچه ای

- توابع یک طرفه دریچه ابزارهای مناسبی برای طراحی الگوریتمهای رمزگذاری و امضای دیجیتال میباشند.
- در حقیقت ثابت میشود وجود توابع یک طرفه دریچه شرط لازم و کافی برای وجود الگوریتمهای رمزگذاری و امضای دیجیتال امن میباشد.

مثال: RSA

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

نمادگذاری RSA

- N : پیمانه محاسبات
- e: نمای رمزگذاری
- d: نمای رمزگشایی
- M: پیام ، عدد صحیح متعلق به $\mathbf{Z}_N^*$
  - $\mathbf{Z}_N^*$ گروه ضربی Z_N (شامل کلیه عضوهای که نسبت به N اول می باشند
- تابع RSA: $x \to x^e \bmod N$
- تابع معکوس: $x \to x^d \bmod N$

الگوریتم Pohling-Hellman

- مفروضات:
  - N عدد بزرگ می باشد.
  - $d \times e \equiv 1 \bmod \varphi(N)$
- رمزگذاری:

$$C = M^e \bmod N$$

- رمزگشایی :

$$\begin{aligned} C^d \bmod N &= \left(M^e\right)^d \bmod N \\ &= M^{ed} \bmod N \\ &= M \bmod N = M \end{aligned}$$

مبانی ریاضی RSA

- p و q دو عدد اول می باشند.
- $\varphi(N)$: تعداد اعداد(کوچکتر ازN) که نسبت به N اول است.

$$\boldsymbol{N = p \times q}$$

$$\boldsymbol{\varphi(N) = (p-1) \times (q-1)}$$

$$\mathbf{gcd}(\boldsymbol{\varphi(N), e}) = 1$$

$$\boldsymbol{d \times e \equiv 1 \bmod \varphi(N)}$$

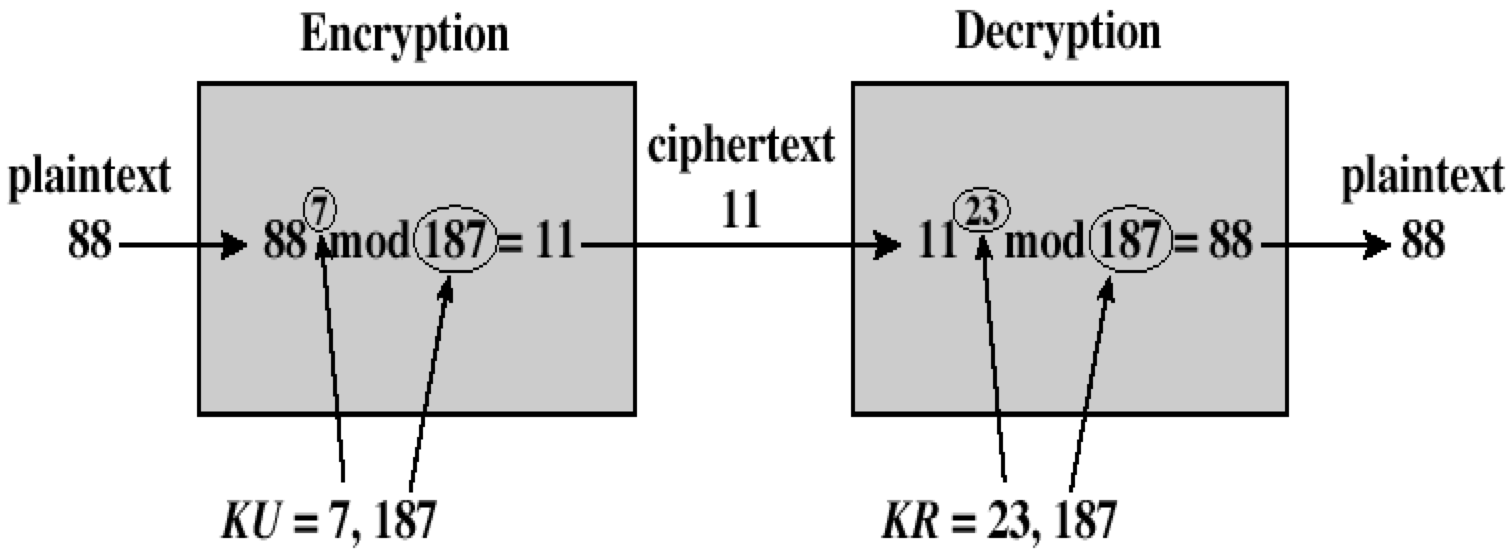
$$\boldsymbol{C = M^{e} \bmod N}$$

$$\boldsymbol{M = C^{d} \bmod N = \left(M^{e}\right)^{d} \bmod N}$$

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

RSA–مثال



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

Φ(n) = 16*10 =160, pick e=7, d.e=1 mod Φ(n) ➔ d = 23

کاربردهای رمزنگاری کلید عمومی

- دسته بندی کلی کاربردها
  - رمزگذاری/ رمز گشایی : 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 جلسه مخفی

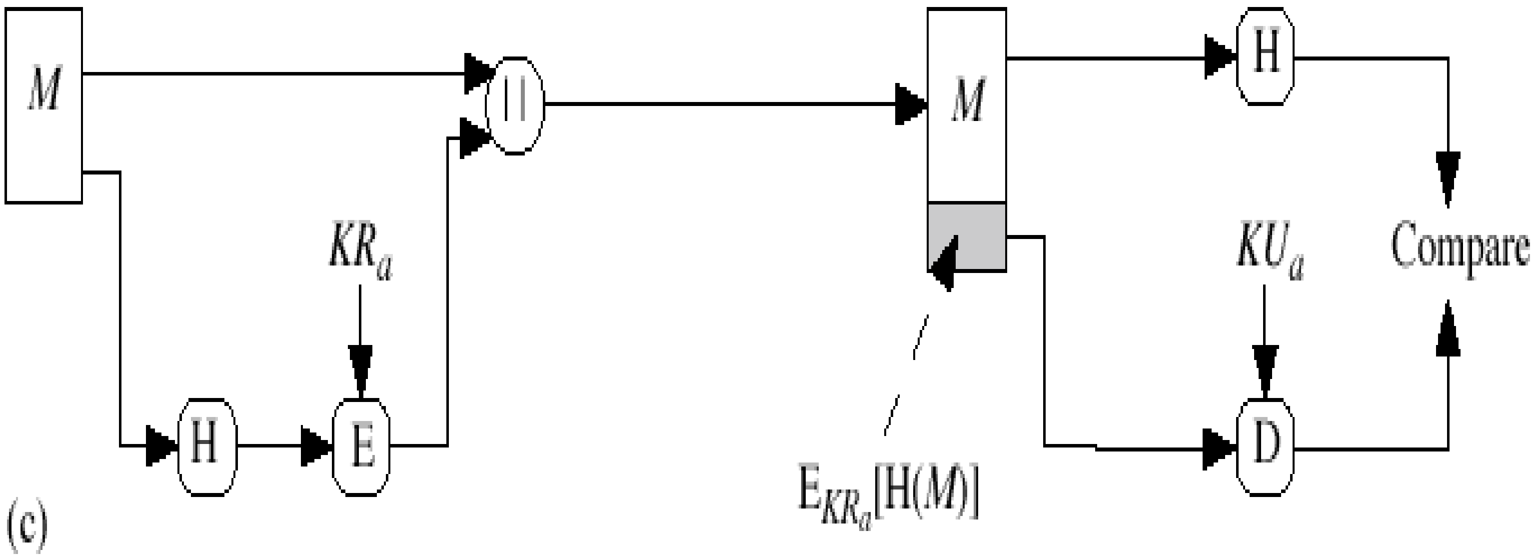
جایگاه عملی رمزنگاری کلید عمومی

- کلیدهای این نوع از الگوریتمها بسیار طولانی تر از الگوریتمهای مرسوم (کلید پنهان) میباشند.
  - الگوریتم **RSA** با پیمانه ۱۰۲٤ بیتی امنیتی در حد الگوریتمهای متقارن با کلیدهای ۸۰ بیتی دارد.

- سرعت الگوریتمهای کلید عمومی از الگوریتمهای رمزگذاری مرسوم پایین تر است.
  - **RSA** تقریباً ۱۰۰۰ بار کند تر از رمزهای کلید پنهان (با امنیت یکسان) میباشد.

امضاء رقمی

RSA



توزیع کلید

الگوریتم Diffie - Hellman

Alice

عدد تصادفی X_A را انتخاب میکند

Bob

عدد تصادفی X_B را انتخاب میکند

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

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

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

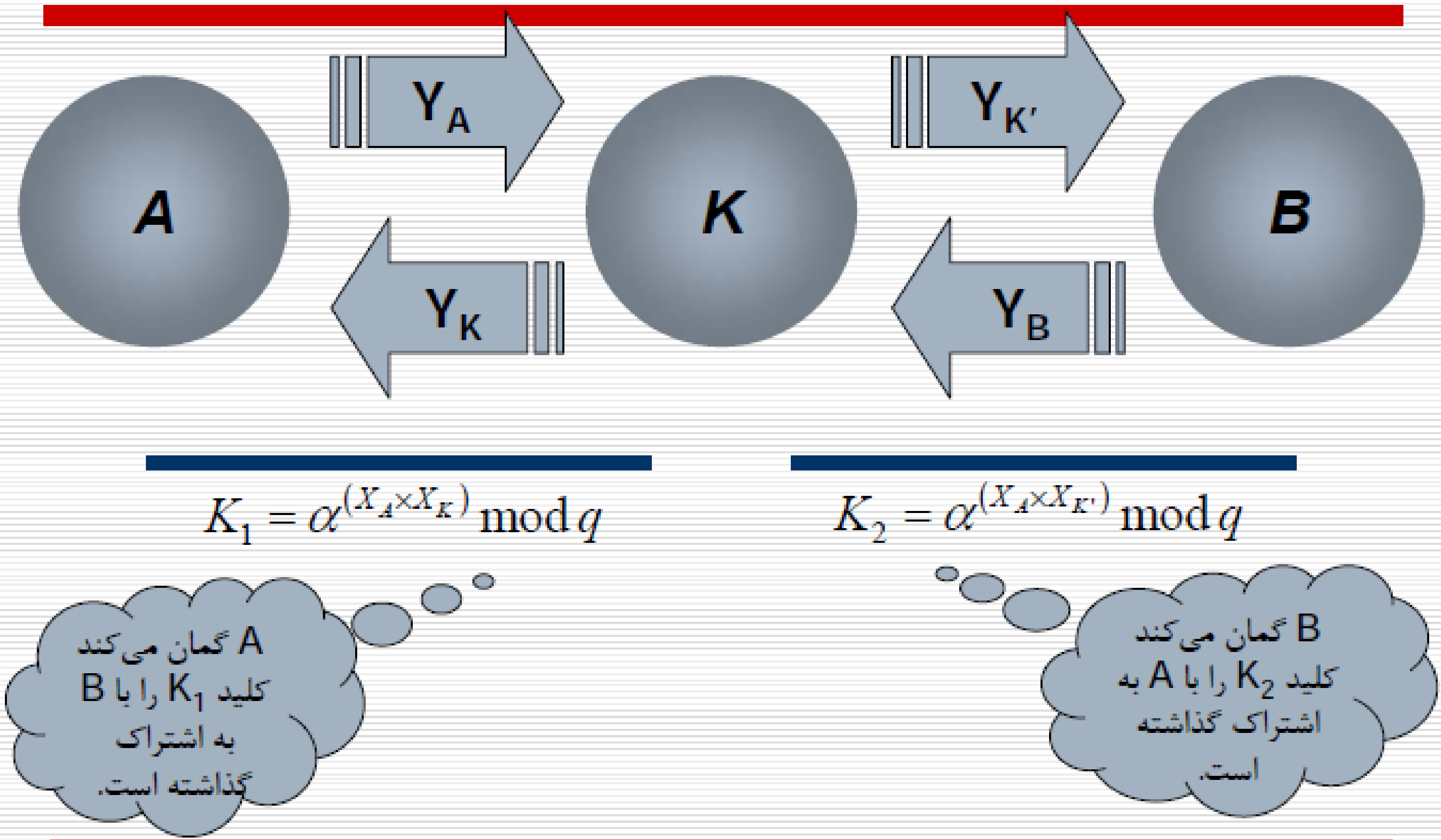
$$K_{AB} = (X_A)^{Y_B} \bmod q$$

کلید مشترک برابراست با $\alpha^{(X_A \times X_B)} \bmod q$

حمله مردی در میان

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

حمله مردی در میان



کاربردهای برخی الگوریتم های کلید عمومی

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

لغت نامه

Public Key	کلید عمومی
Authentication	احراز اصالت
Message Integrity	اصالت پیام
Cipher Text	پیام رمز شده
Plain Text	پیام واضح
Binding	پیوند دادن
Modulus	پیمانه
One Way Function	تابع یک طرفه
Factorization	تجزیه
Modular Exponentiation	نما رسانی پیمانه ای

Probabilistic Polynomial Time	زمان چندجمله ای تصادفی
Trapdoor	دریچه
Decryption	رمز گشایی
Encryption	رمزگذاری
Factor	عامل
Session Key	کلید جلسه
Confidential	محرمانه
Man In The Middle	فردی در میان
Conventional	مرسوم
Infeasible	ناممکن
Exponent	نما
One to One	یک به یک