Project title choices deadline
1st Assignment

امنیت شبکه – رمزنگاری – بخش ۴

محمد صیاد
دانشگاه تهران

1

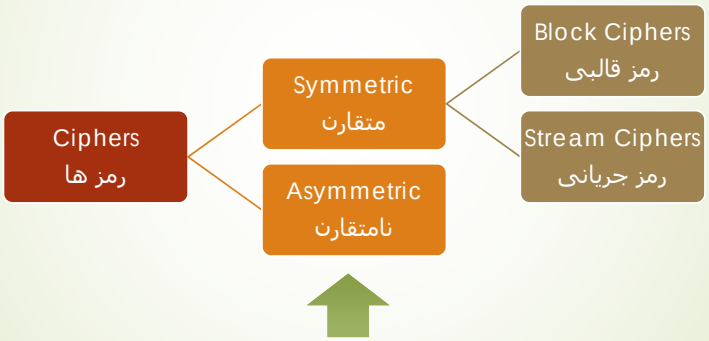
رمزنگاری نامتقارن

Asymmetric Cryptography (Public Key Cryptography)

2

ابزار مورد نیاز برای امن سازی شبکه

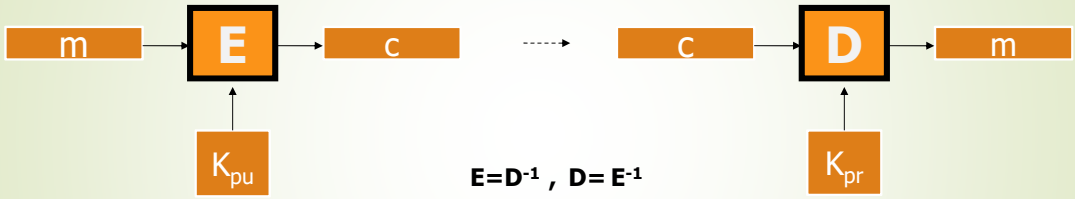
۲- رمز کننده کلید نامتقارن Asymmetric Encryption



3

شکل کلی رمز کننده نامتقارن

رمز کنند های نامتقارن (کلید عمومی) Asymmetric Encryption



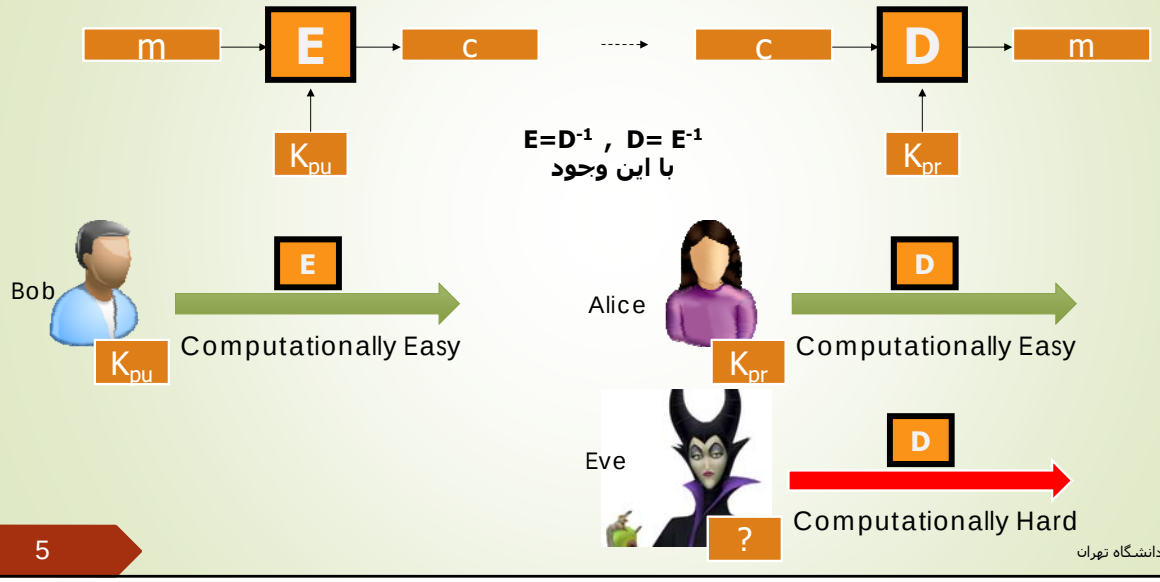
کلید عمومی
(همه میتوانند برای کسی که کلید عمومی اش در دسترس است پیام رمز شده بفرستند)

کلید خصوصی
(تنها و تنها گیرنده میتواند پیامهای رمز شده را باز کند چون کلید خصوصی متناظر، فقط در دست اوست)

مثال الگوریتم های رمز نامتقارن : RSA، Elgamal، Elliptic Curve C.،

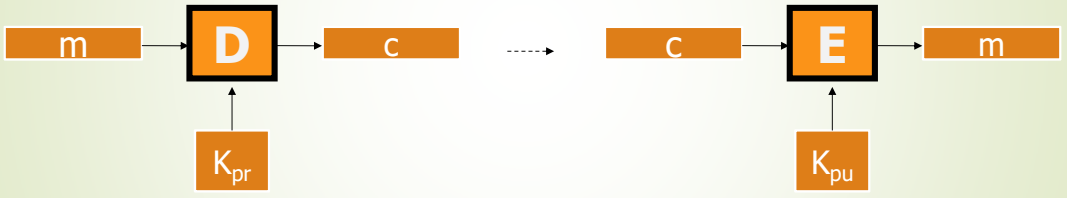
4

سختی رمز کننده نامتقارن



شکل کلی رمز کننده نامتقارن

$$E=D^{-1} , D= E^{-1}$$



این شکل بیشتر در امضای دیجیتالی استفاده میشود که در آینده خواهیم دید.

محاسبات همنهشتی – Modulo Computation

Mod مانده یک عملیات تقسیم است.

مثال:

8 mod 4 = 0

6 mod 4 = 2

1 mod 4 = 1

13 mod 4 =1

اگر دو عدد a و b مانده یکسانی در تقسیم بر یک عدد c داشته باشند، هم نهشت در پیمانه c خوانده میشوند.

$$a \equiv b \pmod{c}$$

رمزنگار نامتقارن RSA

- Introduced by Rivest, Shamir, Adleman at MIT in 1978.
- How do we make an RSA cryptosystem? :

۱- دو عدد اول p و q (بزرگ) انتخاب می کنیم

۲- n=pq را بدست می آوریم (پیمانه)

۳- تابع فی اویلر را محاسبه میکنیم $\varphi(n) = (p-1)(q-1)$

نکته: تابع $\varphi(n)$ تعداد اعداد طبیعی کوچکتر از n ای است که نسبت به n اول هستند (ب م م/gcd آنها یک است).

رمزنگار نامتقارن RSA

۴- کلید رمزنگاری (عدد e) را طوری انتخاب میکنیم که نسبت به $\varphi(n)$ اول باشد.

۵- معکوس آن را در پیمانه $\varphi(n)$ محاسبه میکنیم و آنرا d (کلید رمزگشایی) مینامیم (با الگوریتم اقلیدسی امکان پذیر است)

$$e.d \equiv 1 \pmod{\varphi(n)}$$

پارامتر های عمومی: PU={e, n}

پارامترهای خصوصی: PR={d}

فرآیند رمزنگاری:

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

فرآیند رمزگشایی:

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

امنیت رمزنگار نامتقارن RSA

از نظر ریاضی مساله فاکتور گیری مساله سختی است :

28=2*2*7

ثابت میشود که با این فرض، بدون دانستن p و q و تنها با داشتن n، محاسبهٔ d از روی e مساله ریاضی سختی است و معادل فاکتور گیری n است. در حالی که کسی که p و q را داشته باشد براحتی $\varphi(n)$ را میتواند محاسبه کند و معکوس e را در پیمانه $\varphi(n)$ بدست آورد.

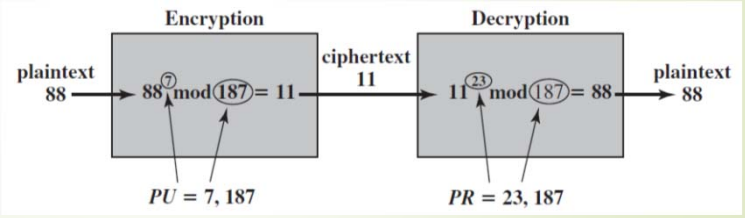
Example:

p=11, q=17

n=11*17=187

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

e=7 (notice that gcd(e, $\varphi(n)$)=1) => d=23



ب م م

Encryption

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$
$$88^1 \bmod 187 = 88$$
$$88^2 \bmod 187 = 7744 \bmod 187 = 77$$
$$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$$
$$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$$

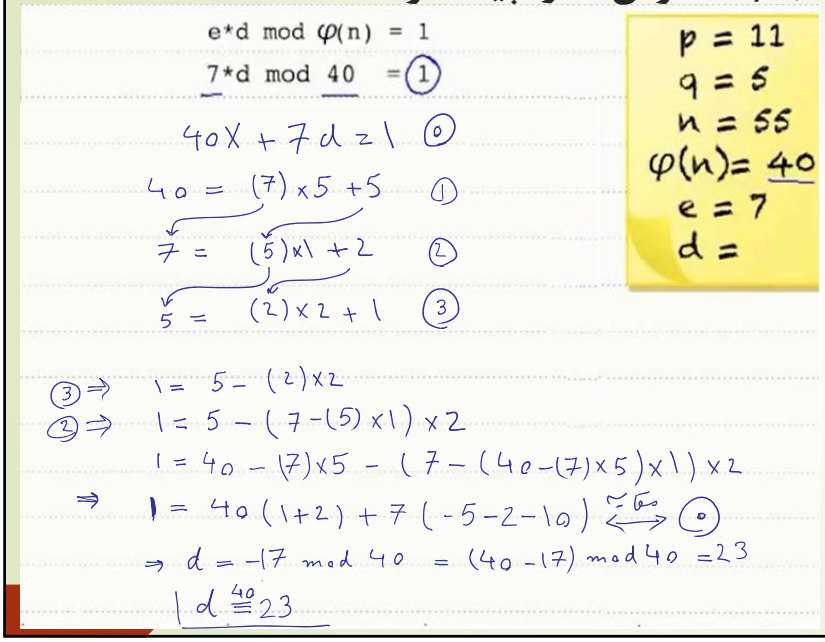
Decryption

$$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$$
$$11^1 \bmod 187 = 11$$
$$11^2 \bmod 187 = 121$$
$$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$$
$$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$$
$$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$$

چگونه باید در پیمانه $\varphi(n)$ معکوس e را پیدا کرد؟

- برای اینکار از الگوریتم اقلیدسی استفاده میشود.

مثال:



Another Example مثالی دیگر

p=5, q=11, N=55 and e=17

Therefore, $\varphi(n)$=40. Write our main equation:

$$17x+40y=1$$

We need to solve this for x. So apply the ordinary Euclidean algorithm:

$$40=2\times17+6$$
$$17=2\times6+5$$
$$6=1\times5+1$$

Write that last one as:

$$6-1\times5=1$$

Now substitute the second equation into 5:

$$6-1\times(17-2\times6)=1$$

Now substitute the first equation into 6:

$$(40-2\times17)-1\times(17-2\times(40-2\times17))=1$$

Note this is a linear combination of 17 and 40, after simplifying you get:

$$(-7)\times17+3\times40=1$$

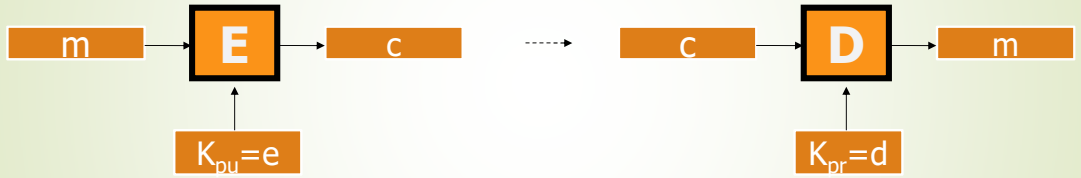
We conclude d=−7, which is in fact 33 modulo 40 (since −7+40=33).

Proof of Euler Phi Function
was given here

پایان RSA

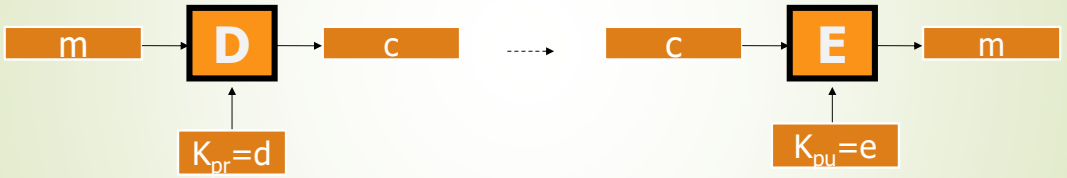
یادآوری

رمز کننده نامتقارن (کلید عمومی) Asymmetric



شکل کلی رمز کننده نامتقارن

$$E=D^{-1}\ ,\ D=E^{-1}$$



گفتیم این شکل بیشتر در امضای دیجیتالی استفاده میشود.

امضای دیجیتال

مثال: الگوریتم های امضای دیجیتال : DSS (شبیه RSA)

نکات

- امضای دیجیتالی سرویس Integrity و Authentication و Non-repudiation را ارائه میدهد.
  - توجه کنید که با رمز کننده متقارن این همان MAC بود اما non-repudiation را نمیتوانست ارائه کند.
- امکان جعل امضا وجود ندارد چراکه کلید خصوصی تنها در دست A است. از روی کلید عمومی نیز که در دسترس همه هست نمیتوان به کلید خصوصی رسید (از نظر محاسباتی سخت است)
- دستکاری در پیام موجب عدم تطابق H(m) ها در گیرنده شده و دستکاری آشکار میشود.
- هیچ کس دیگری کلید خصوصی A را ندارد پس هر آنچه وی امضا کند غیر قابل انکار توسط او در آینده است. همه میتوانند چیزی که A امضا کرده را بررسی کنند.

الگوریتم تبادل کلید Diffie-Hellman (DH)

الگوریتم تبادل کلید Diffie-Hellman (DH)

- هدف DH آنست که دو نفر A و B که هیچ توافق قبلی با هم در مورد کلید نداشته اند و بدون آنکه خود کلید را هم روی کانال بفرستند بتوانند یک کلید مشترک متقارن بسازند و داده های ارسالی اشان برای هم را با آن رمز کنند.
- RSA بر مبنای سختی فاکتور گیری بنا نهاده شد بود.
- DH بر مبنای یک مساله ریاضی سخت دیگر یعنی محاسبه لگاریتم گسسته ساخته شده است.
- پایه خود DH یک الگوریتم نامتقارن است، اما برای ساخت یک کلید متقارن از این الگوریتم استفاده میشود.

لگاریتم گسسته Discrete Logarithm

- عدد اول q را در نظر بگیرید. بین اعداد q-1 ... 1 برخی را primitive root عدد q میخوانند چرا که با توانهای متعدد خود تمام اعداد 1 تا q-1 را در پیمانه q تولید میکنند:

q=5, a=2

a=2,

a^2 mod q = 4,

a^3 mod q = 3,

a^4 mod q = 1

For any $1 \le b \le q-1$

$b = a^i \bmod q$ (آسان؛ i در پیمانه q نیست)

$i = dlog_a b$ (سخت)

Diffie-Hellman Protocol

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

User B Key Generation

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

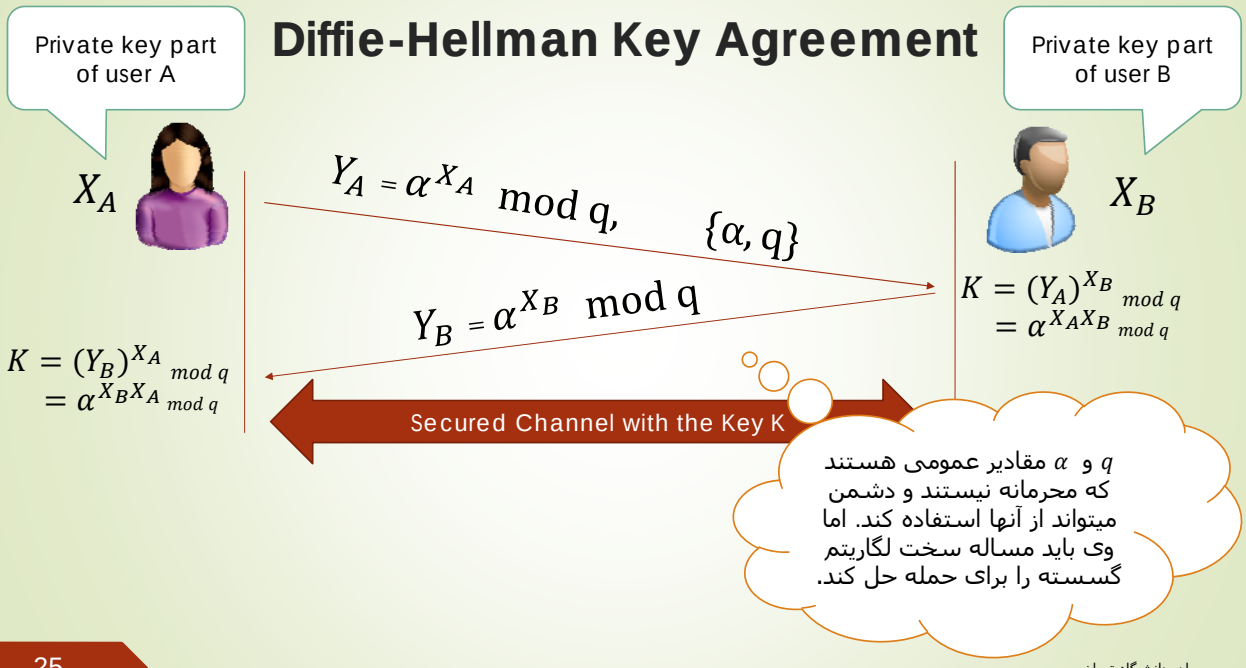
Generation of Secret Key by User A

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

Generation of Secret Key by User B

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

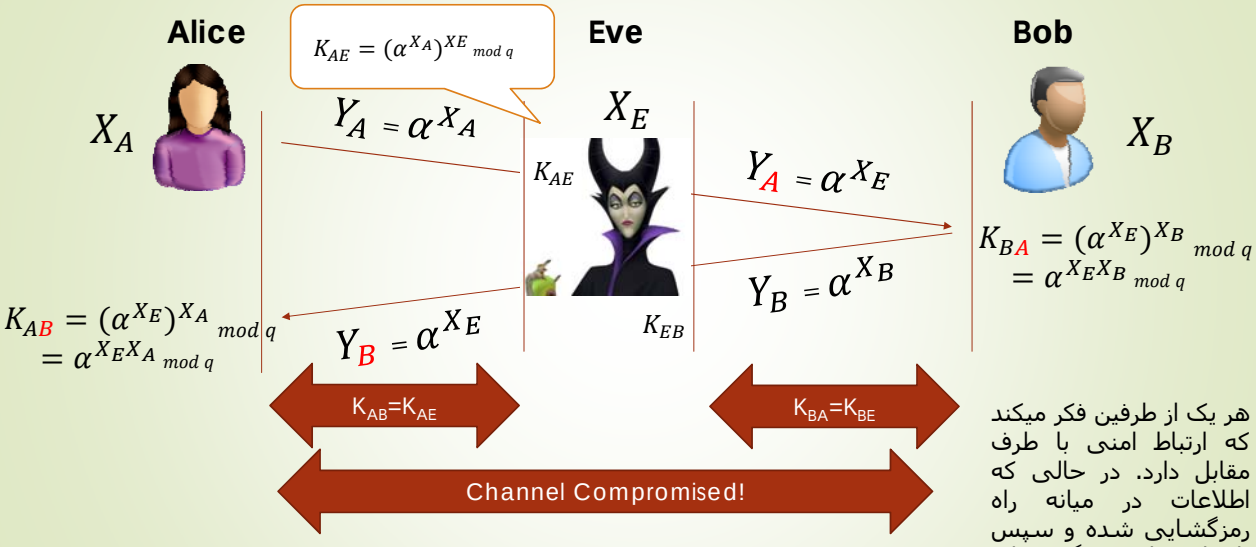
Diffie-Hellman Key Agreement



Man in the Middle Attack - حمله مردی در میانه

- این حمله احراز هویت را مورد هدف قرار می دهد و هکر یا دشمن در میانه راه و بین دو طرف نشسته و سعی میکند در هر طرف خود را جای طرف دیگر جا بزند.
- وقتی اتفاق می افتد که دو طرف از قبل هیچ اطلاعات محرمانه ای بین خودشان به اشتراک نگذاشته باشند و یا شخص سوم قابل اعتمادی موجود نباشد.

Man in the Middle Attack



هر یک از طرفین فکر میکند که ارتباط امنی با طرف مقابل دارد. در حالی که اطلاعات در میانه راه رمزگشایی شده و سپس با کلید طرف دیگر دوباره رمز میشود

صیاد- دانشگاه تهران

27

پایان بحث رمزنگاری

28

صیاد- دانشگاه تهران