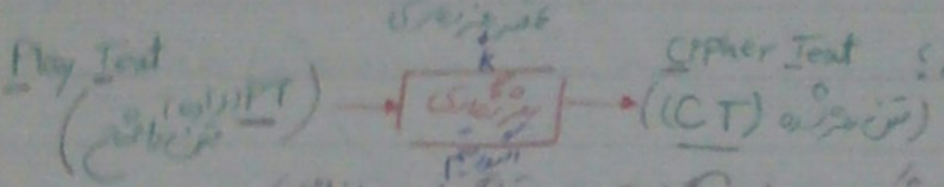
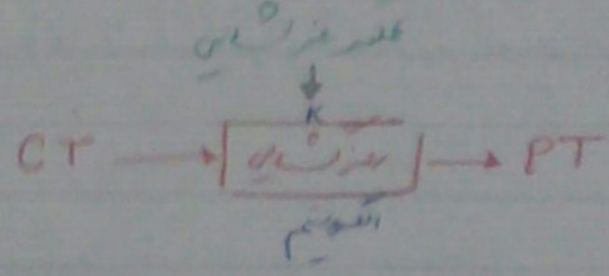
رمزنگاری متقارن

رمزهای کلاسیک : روشهایی است که می‌توان روی داده‌ها هم پیاده کرد. / رمزنگاری که در جنگ‌ها استفاده می‌کرده

رمزنگاری چه نوع سیستمی است؟



یک رمزنگاری ... داده‌ها (الگوریتم نتواند داده‌ها را خراب کند)



متغیر قطعه کلید (K) است
کلید یک ورودی ثابت است همیشه هست.

کلید : تعیین می‌کند خروجی چی باشد. / دارای محرمانه است / داده‌ها پس از رمز شده نشده محرمانه است.

رمزنگاری ← در مرحله رمزنگاری، داده محرمانه‌ها تنها کلید است.

الگوریتم را باید همه بدانند عملکردش چگونه است در غیر این صورت آن الگوریتم ایراداتش را باید پیدا کرد.

هدف رمزنگاری : کلید یک داده محدود و فشرده است

اصول و روش‌های رمزنگاری (Crypto GraPhy)

۱) رمزگشایی بدون داشتن کلید ← Crypt to Analyz

۲) رمزنگاری ← Crypt to LoGy
کوری

Subject:
Year.　Month.　Date.　( )

رمزنگاری متقارن: رمزنگاری کلید عمومی - تک کلیده - کلید خصوصی - معمولی

رمزنگاری که کلید آن خصوصی است و محرمانه / فقط مبدا و مقصد باید از آن کلید خبر داشته باشند (فرض مسئله)

باید یک کانال امن وجود داشته باشد تا کلید امن بین مبدا و مقصد منتقل شود.

کانال امن، کانالی است که در آن شنود نداریم / کانال امن پهنای باند بالا نداریم.

کانال امن با پهنای باند کم برای انتقال یک کلید کوچک استفاده می شود.

$CT = E_k(PT)$ — CT: رمز شده، E_k: رمز شده با K (کلید)

$PT = D_k(CT)$ — PT: متن واضح، D_k: رمزگشایی با کلید (K)

جلسه پنجم　۳/ اردیبهشت/ ۹۴

اگر بخواهیم الگوریتم محرمانه باشد باید ضعف ها را پیدا کرد / و پهنای باند نیز داشته باشد.

رمزنگاری را می توان از سه منظر طبقه بندی کرد:

۱) عملیات مورد استفاده

۲) تعداد کلید / تک کلیده (متقارن) یا ۲ کلیده (نامتقارن)

۳) نحوه پردازش ورودی ها / روش بلوکی

[illegible] ۱۰۰-۱۰-۱۰۰-۱۰۰ → ۱۰۰۰

روش جریانی (بدون وقفه) داده را ارسال می کند با سرعت بالا

یک قدم از کار جلوتره

(جبرانی)

Real_Time برای چه کاربردهایی خوبه؟ ۱) ارسال تصویر و صوت بدون وقفه

۲) برای جابجایی داده آماره شبکه

بعضی الگوریتم‌ها بلوکی اند بعضی‌ها جریانی اند مانند ۳۰_۵۴۸

۱۲۸ - ۵۶

انواع حملات تحلیل رمزنگاری

۱) Cyphertext only: در این نوع حمله، مهاجم (الگوریتم) را دارد به تعداد CT

CT

تعداد CT دارد: CT_1 … CT_N

(اطلاعات رمز شده)

الگوریتم رمزنگاری ✓ — کلید ؟

هم داده، ارسال کلید را کرده

۲) Known Plaintext: مهاجم الگوریتم را می‌داند به تعدادی از CT را دارد و

رمز شده CT — PT

$CT_1 \rightarrow PT_1$ … $CT_N \rightarrow PT_N$

PT را می‌داند

book: کلمه PT

CC1 #: معادل CT

۳) Chosen plaintext: این نوع حمله، بخشی از سیستم استفاده دست مهاجم

هر PT را بدهد CT را دست می‌آورد — سیستم رمزنگاری — دست مهاجم

a → *

aa → **

Subject:
Year. Month. Date. ( )

۳) Chosen Cyphertext : هر CT را داده‌اید سیستم رمزنگاری را دهد و PT مربوطه را بگیرید. (سیستم رمزنگاری دست حمله‌کننده)

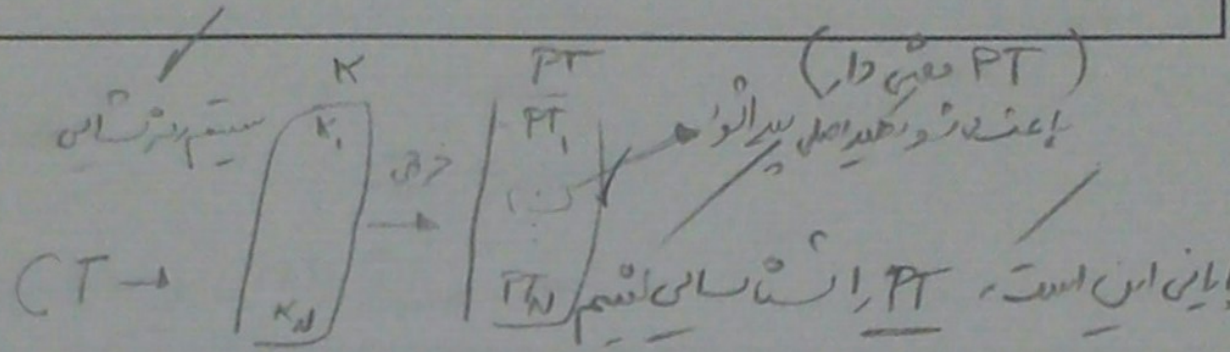
۴) Chosen Text : هر سیستم افتاده دست حمله‌کننده

رمزنگاری CT بدهد ← PT را دست می‌آورد
رمزگشایی PT بدهد ← CT " "

انواع حملات وارده بر اساس امکانات تحلیلگر

- Cipher text Only : تحلیلگر تنها متن رمزشده را دارد.
- Known Plaintext: تحلیلگر چند نمونه از متن اصلی و متن رمز شده متناظر با آن را دارد.
- Chosen Plaintext: تحلیلگر می‌تواند الگوریتم رمز را بر روی مقدار زیادی از متن واضح اعمال نماید و متن رمز شده را ببیند.

* در کلیه حالت فوق فرض شده است که الگوریتم رمزنگاری بر تحلیلگر روشن است



جستجوی تمام حالات
(Brute Force Search)

- ابتدایی ترین حمله
- فرض بر این است که متن واضح قابل شناسایی است.

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	2^{31} μs = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} μs = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} μs = 5.4×10^{24} years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 20^{50}$	2^{167} μs = 5.9×10^{36} years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} μs = 6.4×10^{12} years	6.4×10^{6} years

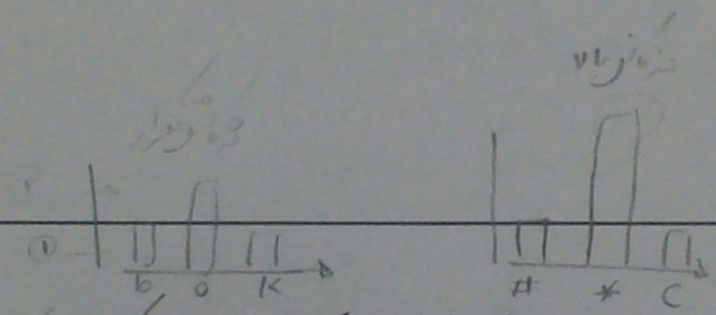
دیگر تعاریف

- امنیت مطلق
  - مستقل از قدرت محاسباتی در دسترس، متن رمز شده اطلاع کافی برای تعیین قطعی متن واضح ارائه نکند (و بنابراین الگوریتم رمز مستقل از مدت زمانی که دشمن در اختیار دارد قابل شکستن نباشد)
- امنیت محاسباتی (یک یا هر دو شرط زیر)
  - هزینه شکستن رمز بیش از ارزش اطلاعات رمز شده باشد
  - زمان مورد نیاز برای شکستن رمز از طول عمر مفید اطلاعات بیشتر باشد.

فهرست مطالب

رمزهای کلاسیک

- از زمان جنگ جهانی دوم مورد استفاده قرار می گرفتند
- قبل از به وجود آمدن سیستم های کامپیوتری امروزی بصورت دستی انجام می شدند.
- مبتنی بر دو روش اصلی جایگشتی و جایگزینی است



رمزهای کلاسیک

- ☐ جایگشتی
  - ■ جابجایی بین حروف متن اصلی
  - ■ هدف درهمریختگی بیشتر است
  - ■ شکست رمز سخت‌تر اما اگر یک **pattern** (الگو) آشکار شود، همه متن شکسته شده است.
- ☐ جانشینی
  - ■ جانشینی یک حرف با حرف دیگر
  - ■ تک الفبایی
  - ■ چند الفبایی
  - ■ حملات شناخته شده با استفاده از:
  - ■ **توزیع فرکانس‌ها**
    - ☐ تعداد رخدادها
    - ☐ حروف مشابه و احتمال کلمات
    - ☐ تحلیل pattern(الگوها)

PT = 726
K = 7
CT = 948

CT?

A →	0	1	2	3	4	5	6	7	8	9
B								K		
C →	2	3	4	5	6	7	8	9	0	1

جدول تعاونی

ادامه را خودتان تمرین کنید تا انتها

جانشینی (سزار) - رمز تک الفبایی

send another catapult ← PT

abcdefghijklmnopqrstuvwxyz

abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

K = y

C = (P + K) (mod 26)

CT → rdmc zmnsqds bzszotks

space space

رمز تک الفبایی

- تنها از یک فرمول جایگزینی مشابه فرمول فوق استفاده می شود
- به خاطر سیاری آنها آسان است
- مشاهده pattern ها به آسانی امکان پذیر است

17

PT = 633
K = 5
CT = 077

PT →	0	1	2	3	4	5	6	7	8	9
	4	5	6	7	8	9	0	1	2	3

K

جانشینی چندالفبایی

رمز چندالفبایی

- استفاده از فرمول های جانشینی مختلف بصورت متوالی
- منجر به کاهش pattern ها می شود
- همچنان می توان از توزیع حروف برای شکست رمز استفاده کرد

18

PT = 633
K_A = 5
K_B = 5 7
K_1 K_2
CT = 077

PT →	0	1	2	3	4	5	6	7	8	9
K_1	4	5	6	7	8	9	0	1	2	3
	2	3	4	5	6	7	8	9	0	1

PT = 6 3 3
K_1 K_2 K_1
0 5 7

PT: 6337

جانشینی ۲۱۳

send another catapult

2
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

1
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

3
abcdefghijklmnopqrstuvwxyz
abcdefghijklmnopqrstuvwxyzabcdefghijklmnopqrstuvwxyz

Ufqf bqqukgs fcudrvov

19

رمز جایگشتی

- جابجایی حروف در متن اصلی بدون تغییر حروف الفبا
  - با هدف ایجاد پراکندگی

امکان استفاده ترکیبی از آن با رمز جانشینی

- ایده اساسی مورداستفاده در رمزنگاری متقارن می باشد

PT = ThiS*iS*a*booK.
K = 5
CT = ?
CT = TibhSOi*oSak**.

T	h	i	S	*
i	S	*	a	*
b	o	o	k	.

20

مثال (جایگشتی ستونی)

ایده : متن را بصورت سطری بنویسیم و بصورت ستونی بخوانیم

- کلید : تعداد ستون‌ها (در اینجا ۵)
- کلید : می توان ترتیب نوشتن ستون ها را نیز تغییر داد.

SEND *
ANOTH
ER *CA
TAPUL
T * * * *

= SAETTENRA*NO*P*DTCU**HAL*

21

ایده‌های تحلیل رمز کلاسیک

- فراوانی حروف (...etanos)
- فراوانی ترکیبات حروف (th, nt)
- حروف (تشخیص) ابتدا و انتهای کلمه (th___ , ___nt, ___gh)
- نظم موجود در الفبای زبان
- متد Kasiski : این روش بر مبنای یافتن الگوهای تکراری(عموما سه حرفی) در متن رمزشده و پیدا کردن طول کلید مورداستفاده استوار است.
  - ایده : فاصله بین دو تکرار از الگوهای تکراری، باید حتما بر طول کلید مورد استفاده بخشپذیر باشد
- حملات Brute Force

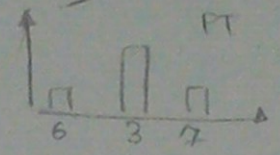
22

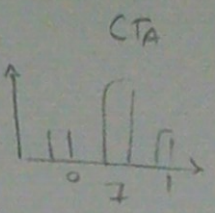
PT = 6337

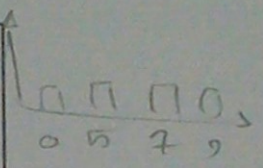
CT_A = 0771

CT_B = 0579

نمودار روش کلاسیک

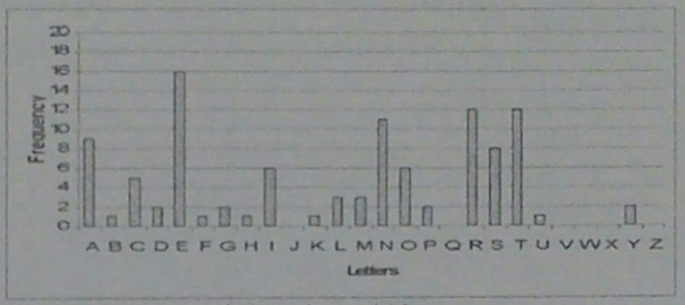






تحلیل رمز کلاسیک(مثال)

Aerial reconnaissance reports enemy reinforcements estimated at battalion strength entering your sector PD Clarke



فراوانی حروف متن اصلی

23

تحلیل رمز کلاسیک(مثال)

aerialreco		ANRMEMTNNO
nnaissance		ENEYMAAGGR
reportsene		RAPRETLTYP
myreinforc		IIOENEIHOD
ementsesti	جابگشتی (۱۰ ستونی)	ASRITDOEUC
matedatbat		LSTNSANNRL
talionstre		RASFETSTSS
ngthenteri		ENEOSBTEER
ngyoursect		CCNRTARRCK
orPDClarke		OEECITEITE

24

رمزگذاری کلاسیک-رمزگذاری مدرن

روشهای مدرن از ترکیب جانشینی و جابجایی استفاده می‌کنند

- روشهای رمزگذاری مدرن، علاوه بر اعمال جابجایی و جایگشت از توابع ساده مانند **XOR** استفاده می شود.
- مجموعه اعمال فوق طی مراحل متوالی روی متن اولیه اعمال می شوند.

Round دور ـ (هر کدام عملیات را یک دور می‌گویند)

29

۲) ساختن یک کلید با طول زیاد و تصادفی کار سختی است. (معمولاً ساختن عبارت تصادفی با احتمال یکسان نیست)

۳) هر جایی که طول PT زیاد باشد از این تابع نمی‌توان استفاده کرد. (همچنان باشد)

مشکل این تابع:

تابع رمزنگاری کامل(One-Time Pad)

شرط ۲:
۱) طول کلید با طول PT برابر باشد
۲) کلید تصادفی باشد

$P(PT) = P(K) = \epsilon$ (اپسیلون)

- ایده: برای رمزکردن یک داده به طول **n** کلیدی به طول **n** هزینه کنیم.

(هر جایی که طول PT زیاد باشد از این تابع استفاده نمی‌کنند. استراق سمعی)

- در این صورت به ازای هر **M** و **C** داریم:

P(M|C) = P(M)

طول کلید هر چه بیشتر امنیت را بیشتر می‌کند

- یعنی داشتن هر تعداد متن نمونه رمزشده کمکی به تحلیلگر نمی کند.
- امنیت این روش به تصادفی بودن کلید بستگی دارد.

30

طول PT ← ۱۲۸ (فضای PT)، طول K ← ۵۱۲ (باید ارسال کرد)

اگر کلید با ۱۲۸ ارسال شود هم امنیت با احتمال دیگر نیاز که فضای ۵۱۲ نیست جزء مرتبه شروط بود روی سیستم است.

۲ شرط این تابع دارد باعث می‌شود که احتمالات می‌توانیم PT را حدس بزنیم

استانداردهای رمزهای قطعه ای آمریکا

- رمزهای قطعه ای استاندارد
  - استاندارد رمزگذاری داده **DES**
  - استاندارد رمزگذاری پیشرفته **AES**

- تحت نظارت
  National Institute of Science and Technology (NIST)

ساختار رمزهای فایستل

- معمولا دانشوران رمزنگاری از ساختاری فیستل می کنند که توسط فایستل در سال ۱۹۷۳ در **IBM** پیشنهاد شد.

- رمزهای فایستل به انتخاب پارامترهای زیر بستگی دارند

ساختار رمزهای فایستل

- ☐ طول قطعه (بلوک)
- ☐ طول کلید
- ☑ تعداد دورها
- ☐ الگوریتم تولید زیرکلیدها
  - ■ هر چه پیچیده تر باشد، تحلیل هم سخت تر می شود.
- ☑ سرعت رمزنگاری /رمزگشایی
- ☐ تابع دور (Round function)
- ☐ سادگی تحلیل

39

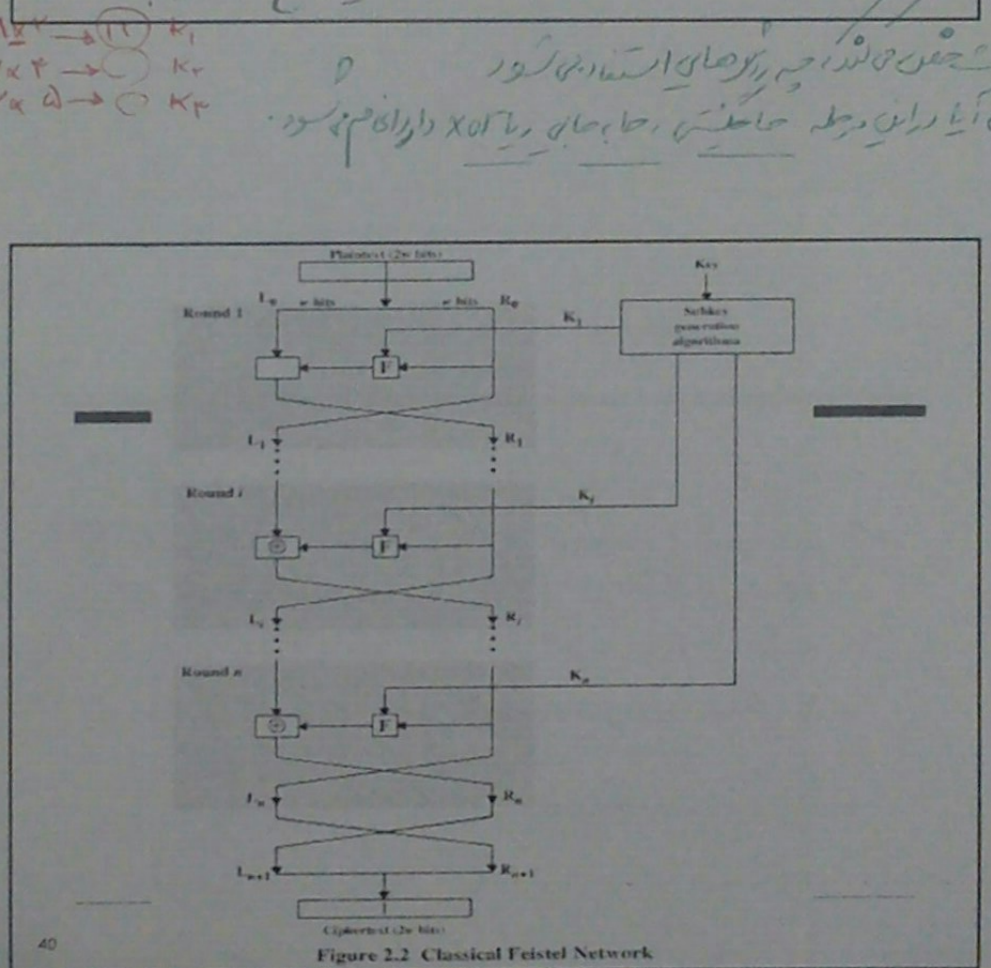


Figure 2.2 Classical Feistel Network

40

No. ۲۰

Subject:

Year Month Date ( )

رمزهای جایگشتی

PT = رمز نگاری انفورماتیک

K = 6

اسلاید ۲۱

جایگشت ستونی

م	د	ر	ز	*	ک
س	=	د	ش	*	ا
ن	ف	و	/	م	ا
ت	ی	ک	@	@	@

CT = اا@م@**@ زش/@ کردوک د=فی مسنت @@

ستونی می‌نویسیم

$K_1 \; K_2 \; K_3$

PT = ۷۴۹

(به تعداد طول PT پیش می‌رویم)

K = ۸۳۲۳

$K_1 \; K_2 \; K_3 \; K_4$

		K_3	K_2, K_4					K_1	
0	1	(2)	(3)	4	5	6	7	(8)	9
1	2	3	4	5	6	7	8	9	0
6	7	8	9	0	1	2	3	4	5
7	8	9	0	1	2	3	4	5	6

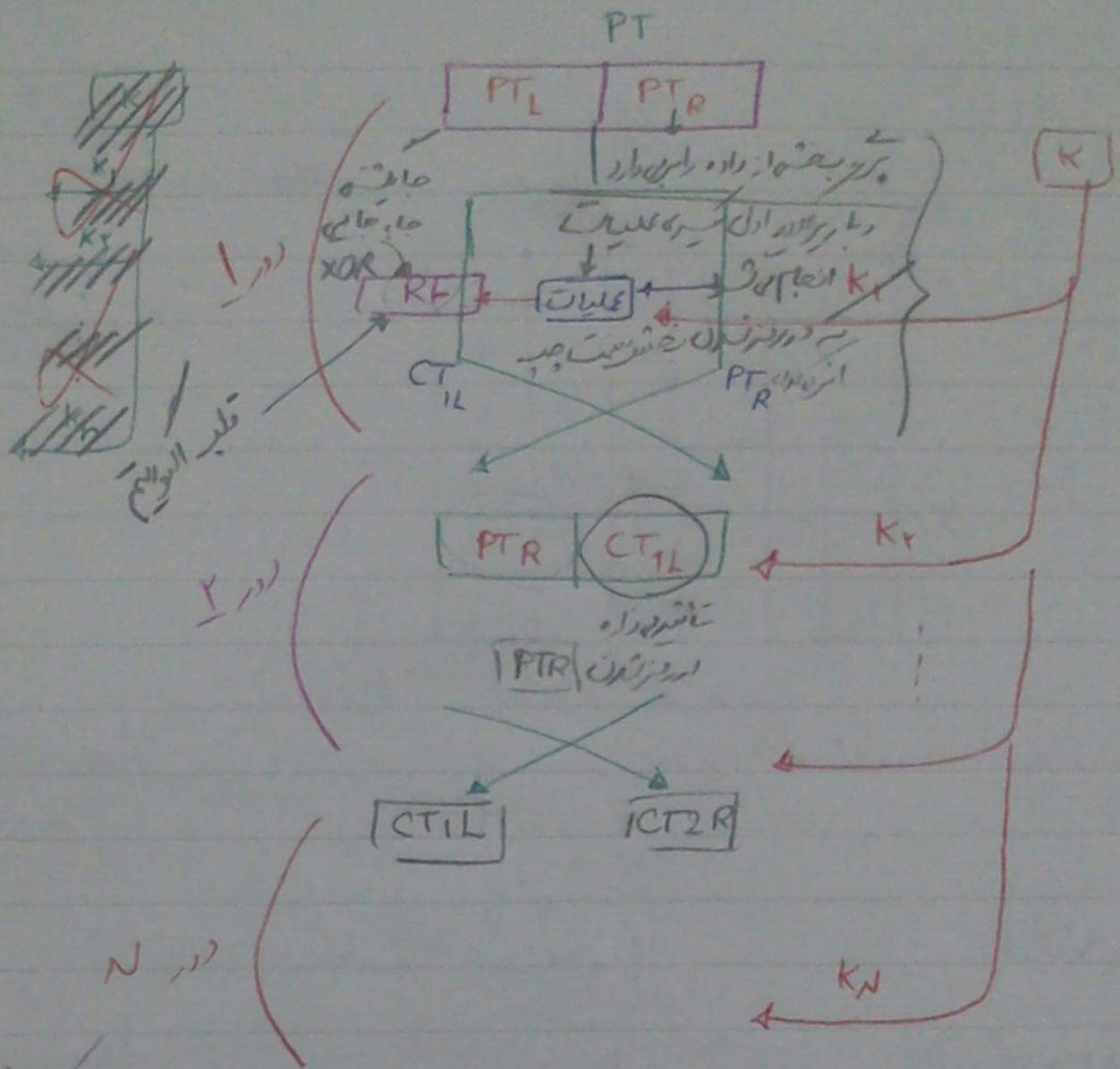
CT = ۸۰۶ 806

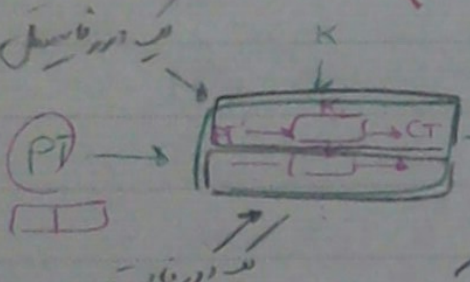
اسلاید (۲۲)

PaPCO

Subject: ساختار رفتار فایستل برای رمزگذاری

Year. Month. Date. ( )





در دور اول ابتدا داده را نصف می‌کنیم

PT

PT_L | PT_R

سمت راست داده را عیناً به سمت چپ داده ارسال می‌کند

PT_L | RTR

K_1

عملیات مثلاً K = ۱۲۳ PT = ۸۷۳۱۲۲ انجام می‌شود در نهایت خروجی را Round Function

۸۷۴
۱۲۳
-

ارسال می‌کند و باعث عوض شدن PT می‌شود در نهایت CT تولید می‌شود.

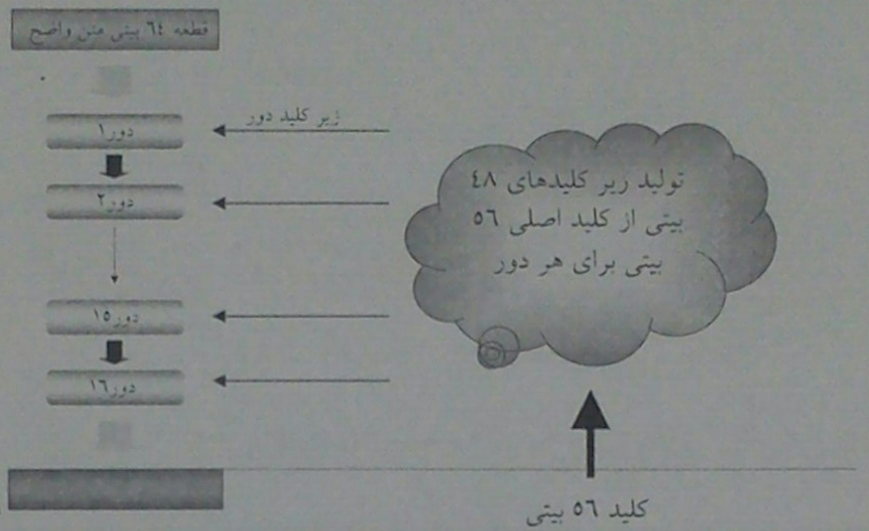
استاندارد رمزگذاری داده DES

- مرور
  - در سال ۱۹۷٤ توسط **IBM** تولید شد
  - پس از انجام تغییراتی توسط **NSA**، در سال ۱۹۷۶ **NIST** آن را پذیرفت.
- اساس الگوریتم ترکیبی از عملیات جایگزینی و جابگشت می‌باشد.
- مشخصات:
  - طول کلید ۵٦ بیت
  - طول قطعه‌های ورودی و خروجی ٦٤ بیت
  - تعداد دورها: ١٦ دور
- الگوریتمهای رمزگذاری و رمزگشایی عمومی هستند، ولی مبانی ریاضی و اصول طراحی آنها فاش نشد.
- در گذشته بسیار پر استفاده بود.
- نام دیگر آن **DEA** است. (الگوریتم به نام **DEA** و استاندارد مربوط به نام **DES**)

DES امن نیست!

- در ژانویه ۱۹۹۹ این الگوریتم توسط آزمون جامع فضای کلید در ۲۳ ساعت شکسته شد!
  - بیش از ۱۰۰۰ هزار کامپیوتر بر روی اینترنت هر یک بخش کوچکی از کار جستجو را انجام دادند.
  - منظور از آزمون جامع فضای کلید همان جستجوی کامل کلید با استفاده از روش **Brute Force** می باشد.
- به الگوریتمهای امن تر با طول کلید بالاتر نیاز داریم.
- علاوه بر این **DES** طراحی شفاف و روشن ندارد.

استاندارد رمزگذاری داده DES



43

طول امن ثبت 2^{56}

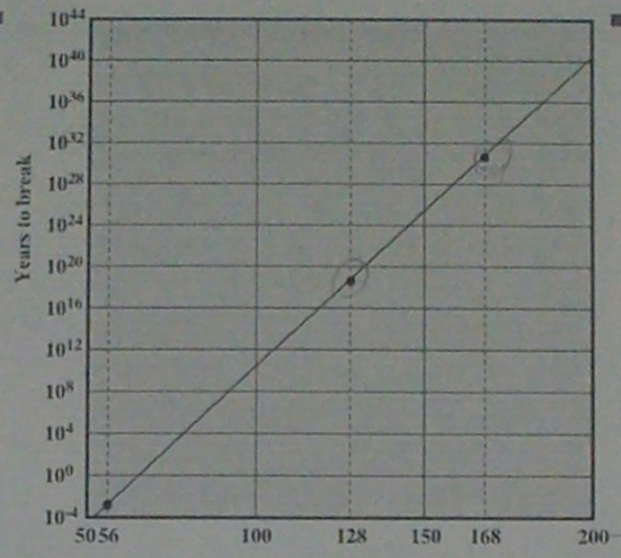
میزان توانمندی DES

- اندازه کلید
  - ٥٦ بیت دارای کل فضای حالت $2^{56} = 7.2 * 10^{16}$
  - حمله آزمون جامع هرچند مشکل، ولی امکانپذیر است
    - آخرین گزارش ثبت شده در سال ۱۹۹۹ نشان از کشف کلید تنها در عرض ۲۲ ساعت داده اند!
- حمله زمانی
  - پیاده سازی **DES** را مورد هدف قرار می دهند
  - الگوریتم برای ورودی های مختلف در زمانهای متفاوت پاسخ می دهد
  - بیشتر در کارتهای هوشمند مشکل زا می شوند

طول PT ورودی
طول CT خروجی
اعلام عملیات زمانی

44

Time to break a code (10^6 decryptions/μs)



45

حمله تحلیلی به DES

- عموما حملات آماری هستند
- از ساختار داخلی **DES** استفاده می کنند
  - تشخیص همه یا بعضی از بیتهای کلید میانی
  - جستجوی کامل روی بقیه بیتها
- شامل روش های آماری مانند: (این روش ها هنوز عملی نشده اند و جستجوی کامل به نظر عملی تر است.)
  - تحلیل تفاضلی
  - تحلیل خطی

46

فهرست مطالب

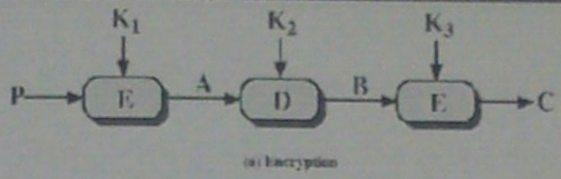
- تعاریف
- رمزهای کلاسیک
- الگوریتمهای رمزهای متقارن و رمزهای قطعه ای
- استانداردهای رمزگذاری آمریکا
- الگوریتمهای دیگر رمزنگاری

3DES
(عقب افتادن روش کند پردازش آن است)

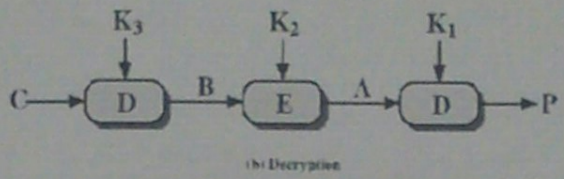
TDEA یا 3DES

- مسئله :
  - آسیب پذیری **DES** در مقابل حمله آزمون جامع
- راه حل :
  - استفاده از الگوریتم های رمزنگاری دیگر
  - پیچیده کردن الگوریتم **DES** از طریق اضافه کردن مراحل رمزنگاری و افزایش طول کلید

TDEA یا 3DES



(a) Encryption

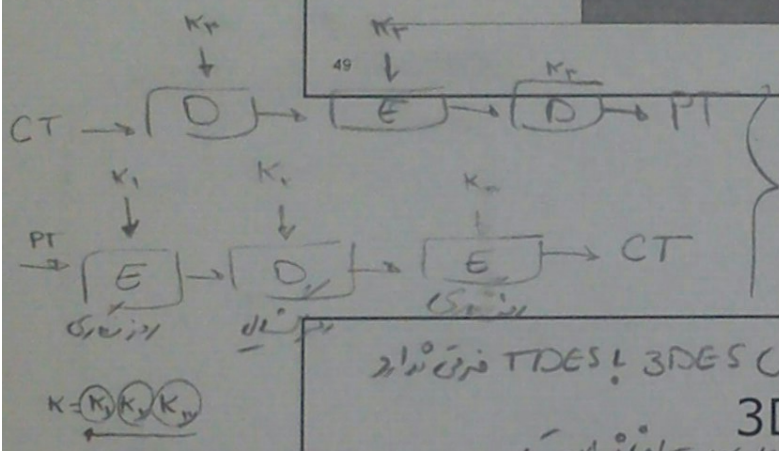


(b) Decryption

$C = E_{K3}[D_{K2}[E_{K1}[P]]]$

3DES روش رابطه

$CT = E_{K_1}(D_{K_2}(E_{K_3}(PT)))$



3DES

- استفاده از الگوریتم **3DES**
  - از دو مرحله رمزنگاری و یک مرحله رمزگشایی با سه کلید مجزا استفاده می شود
  - فضای کلید به ۱۶۸ بیت گسترش می یابد
  - در صورت استفاده از یک کلید یکسان، **3DES** با **DES** مطابقت می کند
  - نسبت به الگوریتمهای دیگر مانند **Blowfish** و **RC5** سرعت کمتری دارد
  - تا کنون حمله ای علیه آن گزارش نشده است
  - مشکل اصلی **3DES** و به طور کلی **DES** سختی پیاده سازی نرم افزاری و عدم کارآیی آن است.

مشخصات استاندارد رمزگذاری پیشرفته

AES

۱۲۸

(* طول کلید این الگوریتم متغیر است) می‌تواند ۱۹۲ یا ۲۵۶ بیت باشد.

- طول کلید ۱۲۸، ۱۹۲ و یا ۲۵۶ بیت
- طول قطعه‌های ورودی و خروجی : ۱۲۸، ۱۹۲ و یا ۲۵۶ بیت
  طول بلاک هم متغیر است. ۱۲۸ یا ۱۹۲ یا ۲۵۶ می‌شود.
- تعداد دورها به طول کلید و نیز طول قطعه بستگی دارد.
  - برای ۱۲۸ بیت: ۹ دور

(تعداد دورها متغیر است)
۱۲۸ ← ۹ دور
۱۹۲ ←

53

الگوریتم IDEA

- ابداع شده توسط **Messay** و **Lai** در سال ۱۹۹۰
- سرعت بیشتر نسبت به **DES**(در پیاده سازی نرم افزاری)
- ویژگیها
  - طول کلید : ۱۲۸ بیت
  - طول بلاک : ٦٤ بیت
  - تعداد دورها : ۸ دور
  - انجام عملیات روی عملوندهای ۱٦ بیتی

این الگوریتم روی برازنده های ضعیف خوب عمل می‌کند.

برای برنامه‌های تلفن همراه معمولاً از IDEA استفاده می‌شود

تحلیل IDEA

- تا کنون هیچ حمله عملی علیه **IDEA** شناخته نشده است.
- به نظر می رسد تا مدتها نسبت به حملات امن باشد.
- طول کلید ۱۲۸ بیتی حمله آزمون جامع را غیرممکن می کند(حداقل با تکنولوژیهای موجود)
- در **PGP** استفاده می شود. (امن سازی سرویس ایمیل)

ماهی بادکنکی

الگوریتم Blowfish

- طراحی شده توسط **Schneier** در سال ۹۴/۱۹۹۳
- وجود پیاده سازی های پرسرعت روی پردازنده های ۳۲بیتی
- فشردگی: نیاز به کمتر از 5^k حافظه
- پیاده سازی آسان
- تحلیل الگوریتم آسان
- طول کلید متغیر: درجه امنیت قابل تغییر است.

ویژگیهای Blowfish

- طول بلاک : ٦٤ بیت
- تعداد دورها : (١٦) دور
- طول کلید متغیر : ٣٢ تا ٤٤٨ بیت
- تولید زیرکلید و **S-Box** های وابسته به کلید
- ١٨ زیرکلید ٣٢ بیتی که در آرایه **P** ذخیره می شوند
- ٤ **S-Box** با اندازه **8*32** که در آرایه **S** ذخیره می شوند
- بازتولید کند زیرکلید ها : تولید زیرکلیدها به ٥٢١ مرحله رمزنگاری احتیاج دارد

الگوریتم RC5

- انطباق با نرم افزارها و سخت افزارهای مختلف
- سرعت اجرای زیاد : عملیات روی کلمه ها انجام می شوند
- انطباق با پردازنده های با تعداد بیتهای متفاوت
- طول بلاک متغیر
- طول کلید متغیر
- تعداد دورهای متغیر
- نیاز به حافظه کم
- طراحی و تحلیل الگوریتم ساده
- تعداد دورهای وابسته به داده : تحلیل رمز را مشکل می کند

الگوریتم CAST-128

- ابداع شده توسط **Adams** و **Tavares** در سال ۱۹۹۷
- طول کلید متغیر: از ۴۰ تا ۱۲۸ بیت (افزایش ۸ بیتی)
- تعداد دور : ۱۶ دور
- مشابه ساختار کلاسیک **Feistel** می باشد با دو تفاوت زیر:
- در هر دور از دو زیرکلید استفاده می کند
- تابع **F** به دور بستگی دارد
- در حال استفاده در **PGP**(امن سازی سرویس ایمیل)

59

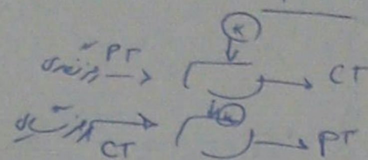
مقایسه سرعت الگوریتمها

Algorithm	Clock cycles per round	# rounds	# of clock cycles per byte encrypted	
Blowfish	9	16	18	free
RC5	12	16	23	RSA security
DES	18	16	45	56-bit key
IDEA	50	8	50	Ascom-Systec
Triple-DES	18	48	108	

فصل ۳ ← رمزنگاری نامتقارن: (جمع‌بندی رمزنگاری)

روش‌های نامتقارن ←
تعریف نامتقارن: ۲ کلید / چند کلید →
کلید عمومی
cymetric مرشد unsy

متقارن

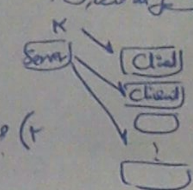


(۱)
۲ تا کلید استفاده کنیم ۱ کلید خصوصی داریم و ۱ کلید عمومی
↓
فقط یک نفر می‌دونه
(خیلی خصوصی‌تره)

(۲)
↓
همه می‌دونن

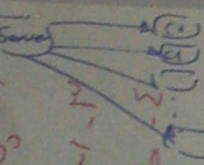
(ویژگی کلیدهای نامتقارن)
↓
۱) با هر کلیدی رمزنگاری انجام می‌دیم دیگه با اون کلید باز نمی‌شه با کلید دیگه باز می‌شه
یعنی اگر با خصوصی رمز کنیم با عمومی باز می‌شه و بالعکس
۲) زوج کلیدها (یعنی در یک لحظه تولید می‌شن (با هم حل می‌شن)
۳) از نظر محاسباتی نمی‌توان از یک کلید، کلید دیگر را رسید چون زوج کلیدن
(با هم تولید می‌شن ولی به هم وابسته نیستند)

مشکل کلید متقارن:
کلید رمزهای متقارن ۲ تا مشکل داره:
۱) کانال امن با هم باید داشته باشیم (لزوماً نداریم)
تبادل کلید توی رمزهای متقارن سخت است
۲) مدیریت کلید (یک کلید از Server بین همه Client ها در جریان تعیض می‌شود)



↑
باز
←

← برای هر کاربر یک کلید جدا تعریف کنیم
↑
خیلی زیاد

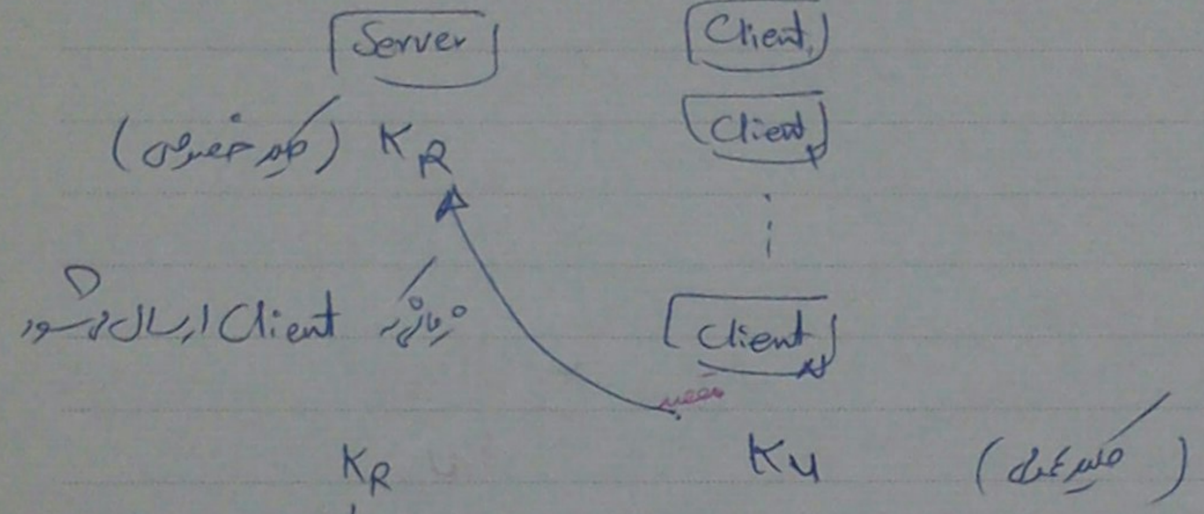


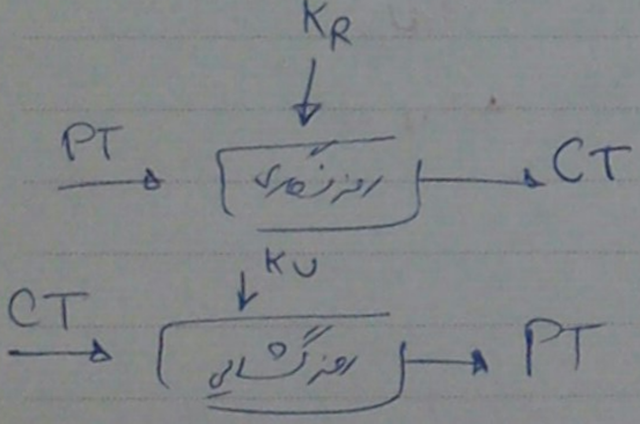
تبادل کلید به مشکل داشت در متقارن
(ویژگی نامتقارن)

۱) کانال امن نیاز نیست چون یک کلید عمومی داریم

کلید عمومی K_U Public

کلید خصوصی K_R Private

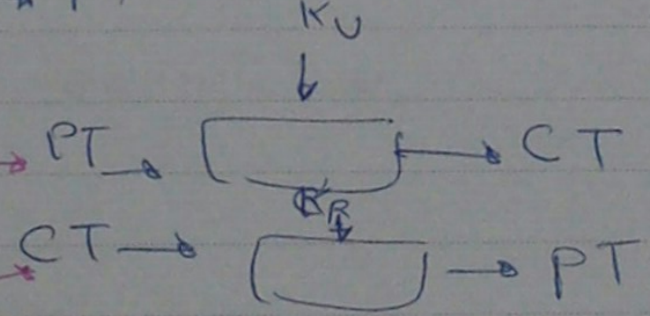




$CT = E_{K_R}(PT)$

$PT = D_{K_U}(CT)$ حل مشکل

$CT = E_{K_U}(PT)$



$PT = D_{K_R}(CT)$

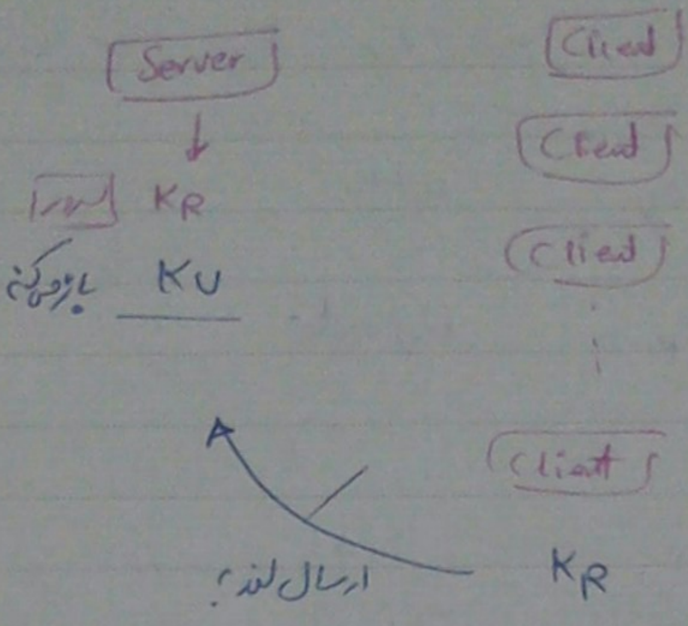
K_U مقصد ارسال کنم برای امنیت باید با K_R باز کنم

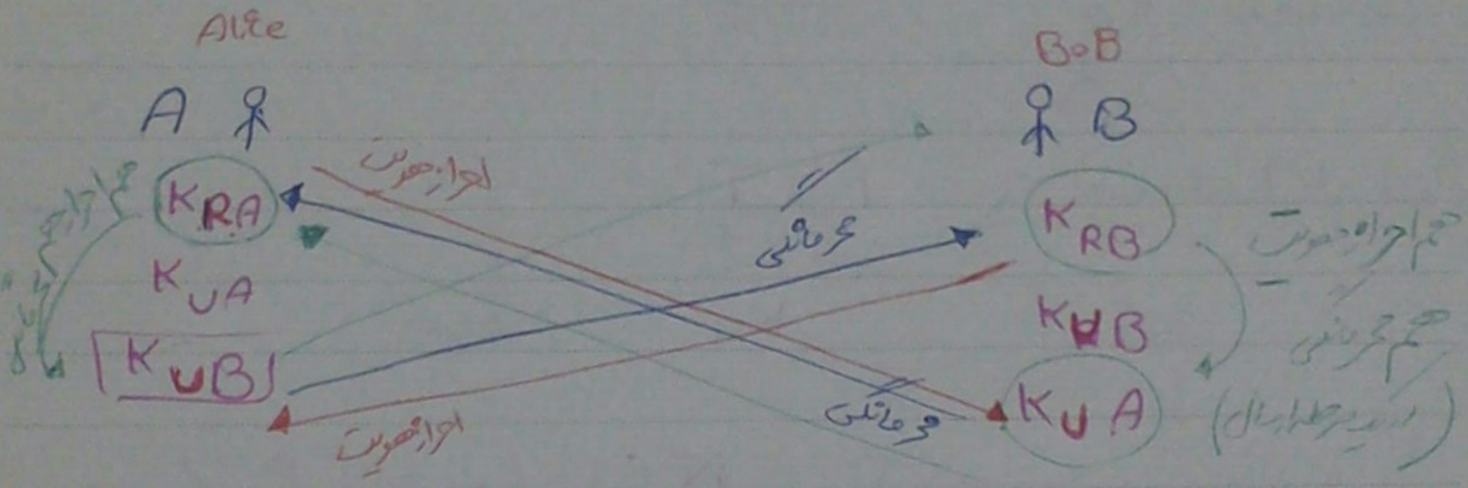
با K_U Client ارسال کنم با کلید خصوصی Server باز شود.

K_R

Subject:
Year: Month: Date:

احراز هویت





محرمانگی ← (با عمومی فرستاده شود / با خصوصی باز شود)

احراز هویت ← متن امضا شده هم بقیه را اظهار دارند توسط بازکننده می‌باشد (عمومی)

(تا آخر صفحه ۵ اسلاید ۱۰)

کاربرد رمزنگاری نامتقارن:
- امضای دیجیتال (احراز هویت)
- محرمانگی
- تبادل کلید (نامتقارن / کانال امن)

PaPCO

رمزنگاری نامتقارن

اشکالات کلید عمومی (جعل هویت)

(اعتماد) توسط شخص ثالث CA (مراجع صدور گواهی)

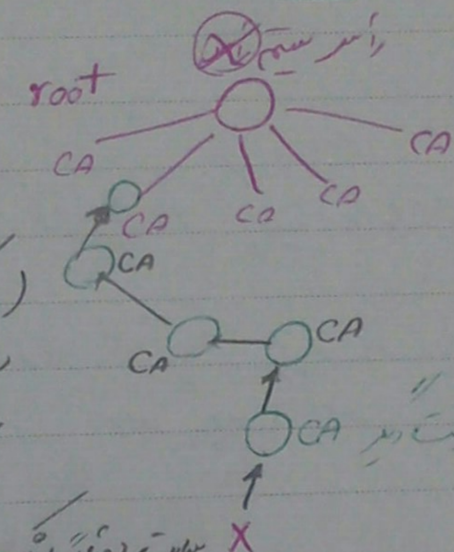
امضا با کلید ← گواهی دیجیتال

https ⟶ امضا با کلید عمومی

↓

با کلید خصوصی CA

CA های روت (ریشه) Root (۱۶ تا) یا ۲۰ تا



(اگر root برای گواهی Valid است
دیگر امضاهای بقیه CA ها را Valid
را نمیده در نتیجه به root نمیرسد،
invalid است پس Error میده)

شرکت دیگر

سایت (مثلاً بانک ملت)

(مرورگر option ⟶ Security ⟶ گواهی های نصب شده را مرورگر قابل مشاهده)

* (عکس قفل کنار Address Bar مرورگر نشان دهنده CA شرکت)

Subject:
Year: Month: Date: ( )

طول کلید

میزان امنیت با طول کلید مشخص می‌شود = ۱۲۸ متقارن
۱۲۸ نامتقارن

روشهای نامتقارن مکمل روشهای متقارن اند.
" " جایگزین " " نیستند.

تصور غلط ۱) طول کلید مدیریت کلید؟
۲) تبادل کلید مشکل داشت، حل شد

الگوریتم نامتقارن (RSA)

یکی از ویژگیهای این روش ۱۰۰۰ برابر کندتر از نسبت به متقارن هم طول خودش

چرا کندتر! چون نامتقارن از نظر پردازش سرعت پایین
محاسبات ریاضی بیشتر، آسان به کندتر تولید ۲ کلید

↓

تولید زوج کلید عمومی و خصوصی } الگوریتم نامتقارن RSA (PKCS)

(۲ تا عدد اول خیلی بزرگ انتخاب می‌کند و از حاصلضرب این دو عدد یک عدد تولید می‌شود

تجزیه ۲ تا عامل اول — که استفاده برای تولید کلید عمومی و خصوصی)

P × q →
3 × 5 → 15 ← n

(نباید از روی n ، P, q را تشخیص داد.)

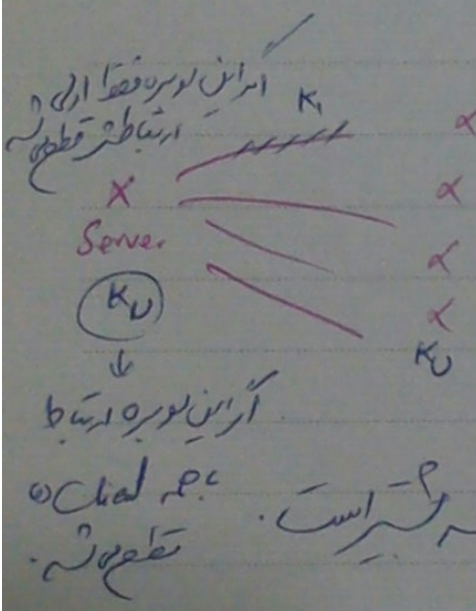
PAPCO

Subject:
Year. Month. Date. ( )

مزایای استقرار: محاسبات ساده، سرعت بیشتر
معایب استقرار: تبادل کلید، مدیریت کلید، کانال امن، گیرنده اجازه هویت ندارد
تنها کاربری که دارای محرمانگی

مزایای نامتقارن: تبادل کلید ندارد، فرض کلید امن است، مدیریت کلید امن تر، عدم انکار، محرمانگی دارد
(کلید خصوصی باعث آن عدم انکار می شود) داشتن
اجرای هویت کسی که خودش اعضای گذشته نگه نمی دارد

معایب نامتقارن: سرعت پایین، تولید کلید سخت تر، کلید عمومی نیاز به تصدیق اعتبار دارد، فضای بیشتری می خواهد
اگر کلید خصوصی لو برود خیلی خطرناک است. (مشکل مدیریت کلید دارد)



Subject :

Year . Month . Date . ( )

(تعداد سوال پاره) ۴/۵ سوال با چند جزء

۵ تا سوال (جا خالی)

کوتاه پاسخ دهید در حد یک یا ۲ خط

تشریحی