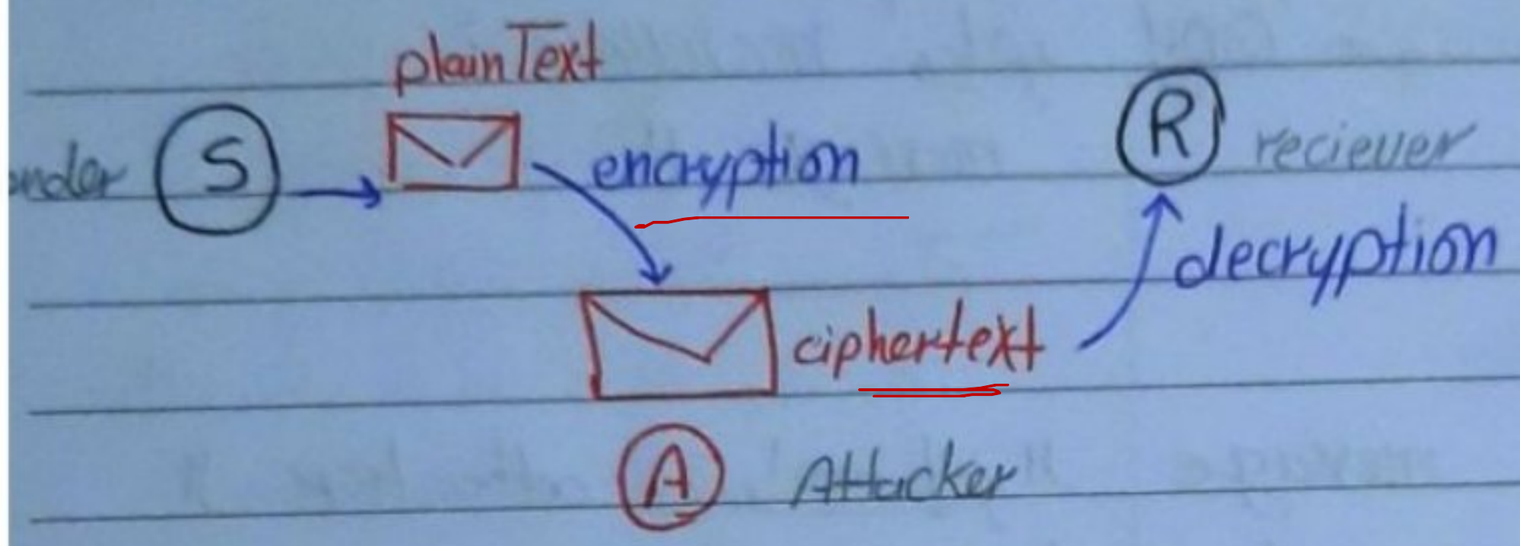
الموضوع: Section (1) التاريخ: / /

Encryption
decription
~~decryption~~

> من الآخر تغيير الكلام او محتوى بطريقة معينة



* plainText (original message) ⟶ الرسالة الأصلية message قبل ما نعملها encryption

* cipherText (encrypted message) ⟶ دى ال message الى اتعملها تشفير فلو جالك فى السؤال ومقالكش هو عايز encryption ولا decryption يبقا هتاخد ال Text دى وتفك تشفيرها

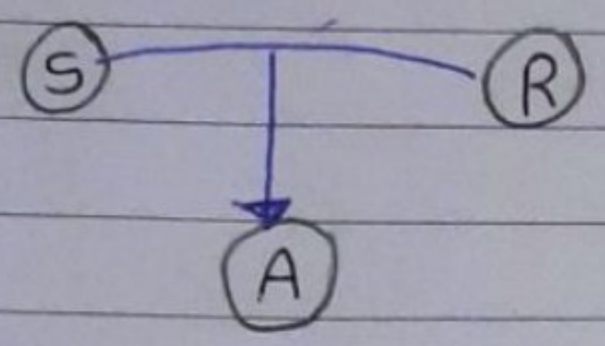
ت
٢٠٢

R. Elsha

التاريخ: / / سؤال أساسي في كل امتحان الموضوع:

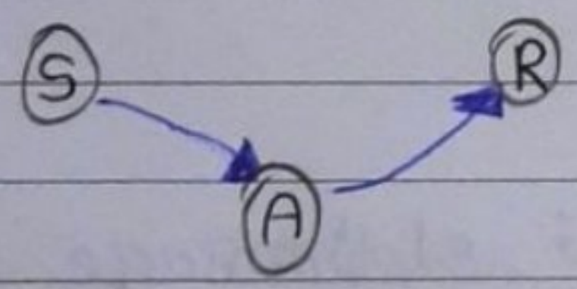
* Threads For any Message : (security threads)

1 ~~Interception~~ interception



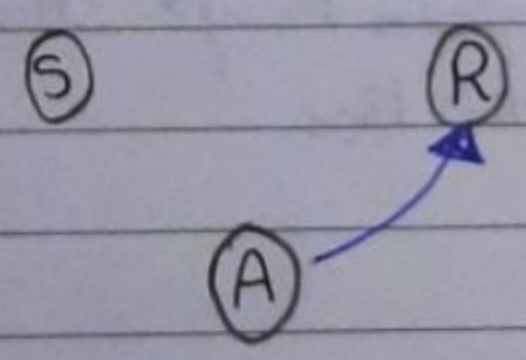
لو ال attacker قدر يوصل
لل line الي ما بين ال sender و ال
reciever وياخد copy منه
ال message

2 modification



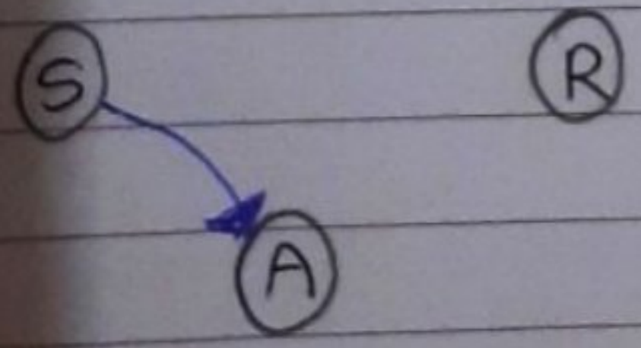
ال attacker يقدر انه ياخد ال message
ويغيرها خالص ويعدل فيها
زي ما هو عايز وبعدين يبعتها
لل reciever (يعني الرسالة مش بتتغير
لما تطول لل reciever)

3 ~~Fabrection~~ Fabrication



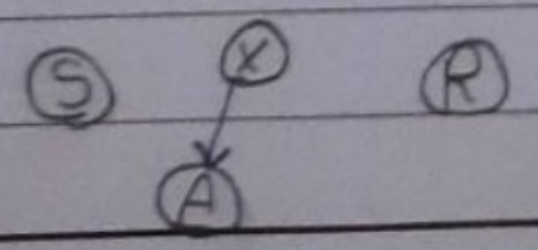
ال attacker بيبعت رسالة لل reciever
من غير ما يكون ال sender بعتت
حاجة ولا قال حاجة أصلا

4 ~~interption~~ interruption



ال attacker بيقدر يسرق ال message
و ميوصلهاش أصلا لل
reciever.

(or)



Scanned with CamScanner

الموضوع: _____ التاريخ: / /

طيب ال attacker بيستخدم ايه عشان يقدر يعدل محتوى رسالتي؟

Key ← بيستخدم

في نوعين

private key (semetric)

بيكون عندك key واحد هو هو الي تستخدمه في encryption ال عليه هو هو الي تستخدمه في decryption ال

public key (asemetric)

بيكون معاك 2 keys واحد لل encryption وواحد لل decryption.

كام نفرق بين هاتين

* Supstitution تعويض AH → XH

شلت لاعب ونزلت لاعب تاني

* transposition تبديل Kill → lilK

الكلمة زي ماهيا بس بدلت اماكن الحروف

R. Etsha

الموضوع: لو جه قالك في السؤال الهتش English alphaptic

التاريخ: / /

A	B	C	D	E	F	G	H	I	G	K	...	Z
0	1	2	3	4	5	6	7	8	9	10	....	25

N (عدد الحروف اللي بتتعامل معاها) = 26

لو جه في الامتحان

وقالك ان ال space معاك فال Alphabet

$\therefore N = 27$

وتكون ال space هيا رقم 0

A → 1

B → 2

C → 3

⋮

Z → 26

** لو قالك طريقة تانية / الهتش

بترتيب ارقام تانية اصلا زي ما هيقولك

في الامتحان

لو قالك معاك فال Alphaptic ال lower & upper

$\therefore N = 52 = 26 + 26$

مهم

الهتش حروف الكابتل كلها من A → Z الاول

وبعدين ال small كلها من a → z

التاريخ: / / For general الموضوع:

For Encryption:

ct. ciphertext K: Key
pt. plain text N: ✓

$$C = (P + K) \bmod N$$

For decryption

$$P = (C - K) \bmod N$$

آخر كلمتين في السكشن

* cryptography

هي عملية التشفير لغرض إرسال رسالة
تنفذ عليها مجموعة processes معينة
وتتغير شكل / محتوى الرسالة
(طويل p.t إلى c.t)

p.t $\xrightarrow{\text{encryption}}$ c.t

* Crypto anlysis

معناها معايا الـ ciphertext وعايز أوصل
للـ plain text بس مش معايا الـ key ولا أعرف
طريقة التشفير

End of section (1)

R. Elsho

لو اداليه Key حرفه ← هشوفه بكافي كام فال Alphabit واشتغل ✓

الموضوع: سكشن التحاسب (2) التاريخ: / /

« Algorithms »

Transposition :-

[Encryption] [1]

← بتعتمد على private Key ← عبارة عن كلمات كل الي عليك انك تعمل matrix عن طريق ال Key ده وبعد كده [2] تبدأ ترص ال p.t ولو ال matrix اتفضل فيها cells فاضية كاملهم الحروف جايه بالترتيب A,B,C,D..... ✓

Example: Key = Securit

p.t = we need more snow now

5	2	1	7	4	3	6
S	e	c	u	r	i	t
w	e	n	e	e	d	m
o	r	e	s	n	o	w
n	o	w	a	b	c	d

هعمل matrix بحروف ال Key

[3] ايه اول حرف Alphpet قابلك فال Key

c → 1

e → 2 i → 3 r → 4

s → 5 t → 6

تروح لل matrix وتحط لكل واحد فيهم رقمه

[4] الحل النهائي ← ابدأ آخذ colum colum بالترتيب واكتبه

∴ C.t = new ero doc enb won mwd esa ※

← اعكس بقا اجيب ال decryption ازاي

الموضوع: _____ التاريخ: / /

[decryption]

1 هشان اعرف كل column فيه كام حرف = [عدد حروف c.t / عدد حروف ال key]

c.t = new ero doc enb won mwd esa = 21

key = security = 7

$\therefore \frac{21}{7} = 3$

2 هقسم كل ٣ حروف وتبدأ ترص وبرضو هكتبه ال key وهترقمهم بالترتيب

بس هتبدأ رص من ترتيب الأعمدة

يعني هتروح ترص الحروف

من عند ال c الأول وبعدين ال e

وهكذا بالترتيب

5	2	1	7	4	3	6
s	e	c	u	r	i	t
w	e	n	e	e	d	m
o	r	e	s	n	o	w
n	o	w	a	d	c	d

p.t وتطلع بالحروف منه هنا

∴ p.t = we need more snow now abcd

انت هتفهم انهم ملهمش لازمة

هشلهم او خليهم براحتك [أهم حاجة انك طلعت ال p.t]

R. Elshal

الموضوع: _____ التاريخ: / /

playFair

الخطوات :

١) هتعمل matrix 5X5 = 25 وهو مديك Key f

٢) هتحط ال Key جوا ال matrix

وتكمل بالحروف ال Alphapit (ما عدا اللي جه معاك فال Key)

كل حرف فال matrix ليه unique

حلبي هو كدا 5X5 = 25 وانا عندي حروف Alphapit = 26

هتحط i, J مع بعض في الـ واحدة

٣) هتشيل ال p.t وتقسمه لـ blocks كل block يكون حرفين

** ← لو جه في block حرفين متشابهين ← افصل بينهم بـ x

** ← لو جه حرف فالآخر لوحده ← خليه x

مثال

p.t = Million

Mi ll io n

↳ = Mi Lx Li on

p.t = Millions

↳ = Mi Lx Li on Sx

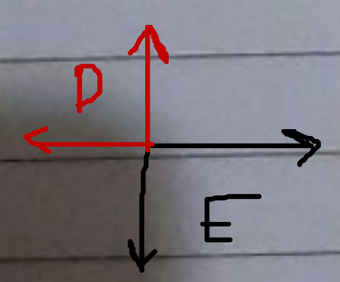
في نفس ال block بسيطا مرتين جم جنب بعض فالحل بقا افصل بينهم لما لو الخطوة بلوك واحد مع بعض

٤) عندك ٣ احتمالات : بالنسبة لكل block (الحرفين اللي في كل block)

① ان الحرفين في نفس ال row

لو Encryption هعمل : shift right

لو decryption هعمل : shift left



② ان الحرفين في نفس ال clown

لو Encryption هعمل : shift down

لو decryption هعمل : shift up

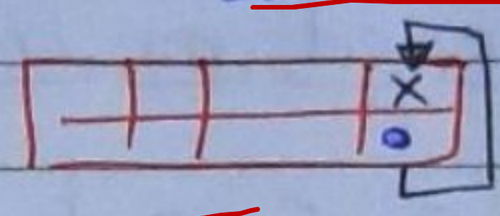
الموضوع: _____ التاريخ: / /

③ لو هما الاتنين نفس الخط ولا نفس العمود

corner | هما بكونوا ← هرسم شكل هندسي

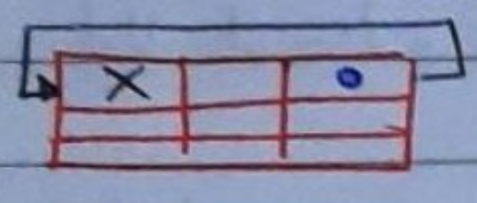
كان ٢ يكونوا مقابلين بعض

لو انا هنا وعايزه اعمل shift down



=

لو انا هنا وعايزه اعمل shift right



---

* لو انت فال decryption وقابلتك ال الف ياعمة (ا/ج)

هتاخد انهي فيهم ← هتاخد الي هيديلك معنى (ايجي)

p.t

R. Elshal

الموضوع: _____

التاريخ: / /

اهو انا غلطت هنا المفروض الحرف unique حتا لو حرف اتكرر في Key متكرهوش المفروض مكنش كتب في n تاني هنا

« Example For playFair »

pt = we need million

Key = since by plan

Answer

اول حاجة

we ne ed mi lx li on

s	i/j	n	c	e
b	y	u	a	n
~~a~~	~~d~~	~~f~~	~~g~~	~~h~~
*				

اولا بلوكات ال pt

matrix 5X5

هط الاول ال Key

اوعي تكرر حرف

s	i/j	n	c	e
b	y	u	a	d
f	g	h	k	l
o	p	q	r	t
u	v	w	x	z

بتجيب ف اول طريقة بقي الـ الي قصادو ا ف الروووووو

انا هنا بعمل encryption

اول block كان we

مش في نفس الصف ولا العمود ارسم ↳

∴ e → n

w → z

∴ [we] → [~~nz~~] zn

∴ [ne] → [cs] shift right

∴ [ed] → [dl] shift down

∴ [mi] → [yn]

∴ [lx] → [kz]

∴ [li] → [qe]

∴ [on] → [qs]

∴ c.t =

↳ nz cs dl yn kz qe qs *

بس كدا

* اهدى وبراحة كمل جزء اللي بس

رتب افكارك في ورقة خارجية

الموضوع: _____ التاريخ: / /

Poly Alphapetic

ال Key بتاعها عبارة عن جملة

① هتمسك ال p.t و تبدأ تزود ال Key تحته (لو خلص عيده تاني)

X X X X X
4 4 4 4 4

② هتطبق قانون ال Encryption العادي

$c(p) = (p + K) \bmod n$

او ال dycryption

$p = (c - K) \bmod n$

طبعاً الارقام دي الي هيا كل حرف فال Alphapit تحسبها
وتشوف لبنائي ده حرف ايه فال Alphabet وتكتبه

Example:-

p.t = we need Million

Key = Ytirvces

p.t = 22 W, 4 e, n, e, e, d, M, i, l, l, i, o, n

24 y, 19 t, i, r, u, c, e, s, y, t, i, r, u

$c(w) = (22 + 24) \bmod 26 = 20 \rightarrow u$

$c(e) = (4 + 19) \bmod 26 = 23 \rightarrow X$

وهكذا هكمل بقا يسطا عشان تعب #

ولو decrypt

$(c - K) \bmod n$

End of section (2) #

R. Etshal

الموضوع: تشكشن الخاص (3) التاريخ: / /

Combination between Transposition and subsititution

* مفيهاش Key خالص (بتعتمد على التعويض)

ملاحظات:

1. بتبني squar matrix من E J A (العناوين لل Colums) 5x5
2. وتملي ال 25 cell الي عندك حروف ال Alphabitt العادية هنا هتدمج (Q, Z) مع بعض
3. بيبان p.t (ومش محتاج Key فالي بيحركك هنا هيا ال matrix مش ال Key)

هتشيل على p.t واملي كل حرف فيها وشوف التقاطع row x coloum

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I	J
C	K	L	M	N	O
D	P	Q/Z	R	S	T
E	U	V	W	X	Y

R. Elshal

التاريخ: / / الموضوع:

Example:- [Encryption]

pt = Take me to your leader

Answer

pt = T a k e m e to your leader

D E a a c c A A E D E C E E E E C E D C A E a a A E

كل حرف طلعلي حرفين

يعني بقا عندي 36 حرف هستهم جزبنه

DE AA CA AE CC AE DE CE EE CE EA DC C bA E AAA D A E D C

هنا ال Encryption هنحط أول نص على سطر والنص التاني تحته

Row

Colum

D E A A C A A E C C A E D E C E E E

C E E A D C C b A E A A A D A E D C

وها خدهم كل حرفين تحت بعض [Colum] واروح اشوف فال Matrix ها التقابل

[row & colum] كان ايه وهو ده ✓ c.t

c.t =

R Y E A n C C V K o A u p x K y X W.

---

encryption ده بالنسبة لل

بالنسبة لل decryption في اختلاف في حتة معينة

R y E A

D C E E A E A A خالص

* لحظ c.t واطلع بصوا هو التقاء حرفين ايه هنا بقا

كتبه كل حرفين تحت بعض

D E A A → وهسلف كل حرفين جنب بعض

C E E A

واشوفهم التقاء حرف ايه, اطلعه

وهو ده pt

التاريخ: / /

الموضوع:

Example « For Dycryption »

c.t = R Y E A n C C V K O A U P X ...

D C E E A E A A C D A C A C E B

t a K E

D E A A C A A E

C E E A D C C B

ipt = take me ✓ بس كدا *

لو حالت ال Q/Z

عادي اكتبها كما Q/Z

R. Elshel

Scanned with CamScanner

التاريخ: / / الموضوع:

قبل اي حاجة * هاين حفظ ازاي طبق ال gcd

gcd

eclidean ✓✓

$m > n$

$\gcd(m, n)$

$= \gcd(n, m \bmod n)$

$= \gcd(m \bmod n, n \bmod (m \bmod n))$

$\gcd(\square, \square)$

$= \gcd(x, \square \bmod x)$

$= \gcd(\square, x \bmod \square)$

مثال

$\gcd(162, 15)$

162 mod 15

$= \gcd(15, 12)$

15 mod 12

$= \gcd(12, 3)$

$= \gcd(3, 0)$

$\therefore \gcd = 3$

R.Etshal

m n $m > n$

$\gcd(270, 192)$

$= \gcd(192, 270 \bmod 192)$

$= \gcd(192, 78)$

$= \gcd(78, 192 \bmod 78)$

$= \gcd(78, 36)$

$= \gcd(36, 78 \bmod 36)$

$= \gcd(36, 6)$

$= \gcd(6, 36 \bmod 6)$

$= \gcd(6, 0)$

$\therefore \gcd = 6$ *

عبدالله بارب نفهم

الموضوع: _____ التاريخ: / /

modulo multiplicated inverse

بحاول سد الضرب

بحث مقدرش ادخل واجيب أحتلا غيرها اتأكد ان ال GCD

بين الرقمين = 1 **

متحلش و متحطش القلم في طبالات غيرها تتأكد

ان GCD = 1 ✓

No result ⇐ ≠ 1 لو

Example

$f^{-1} \bmod 26$

m n

GCD انا كد الاول انه

~~gcd(f, 26)~~

gcd(26, f)
= gcd(f, 5)
= gcd(5, 2)
= gcd(2, 1)
= gcd(1, 0)

∴ gcd = 1 ✓✓✓✓✓✓

يبقا ادخل المعادلة وحسب الحل

R.Elshal

التاريخ: / /

الموضوع:

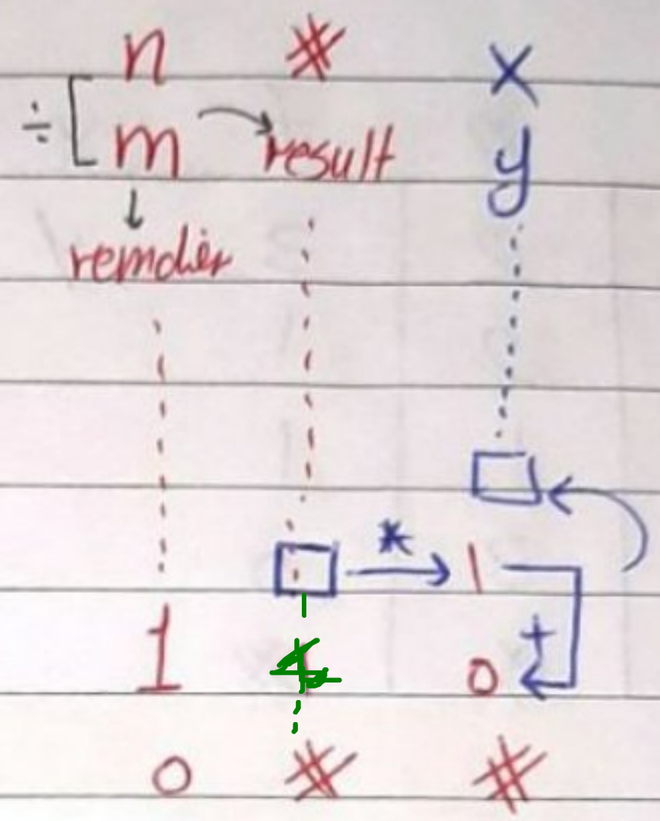
« modulo multiplicated inverse »

$\mu^{-1} \bmod n = 1$ $\qquad$ $n > m$

μ $\quad$ ν

$f^{-1} \bmod 26$

26	*	11 → x
7	3	3 → y
5	1	2
2	2	1
1	2	0
0	*	*



$Ny \qquad x\mu = 1$

وتشوف مين يخط قدامك

كل الكلمات الاول انا
عايزة اعرف اشارة الـ x

لو ال x موجبة

$\therefore Ny \qquad x\mu = 1$

$\therefore$ x = modulo multipl. inverse الـ

وخلاص

لو سالبة

$26 * 3 \qquad 11 * 7 = 1$

$+ \; 78 \qquad - \; 77 = 1$

السالبة ناقص الـ x

$\therefore$ x سالبة

روح حولها
mod n

$-11 \bmod 26 = 15 \bmod 26 = \boxed{15}$

$\therefore$ Modulo Multipli Cated inverse = 15

التاريخ: / / الموضوع:

مثال كمان لتأكد منه فهمك

* Find modulo Multiplicated inverse

11 mod 26 = 1

M N

26	*	f → x
11	2	3 → y
4	2	1
3	1	1
1	3	0
0	*	*

gcd (26 , 11)
= gcd (11 , 4)
= gcd (4 , 3)
= gcd (3 , 1)
= gcd (1 , 0)

∴ gcd = 1 ✓✓✓✓
يلا بينا ✓

yN xM
3*26 f*11
+ f8 − ff

∴ x = -f

-f mod 26 = $\boxed{19}$ *

بعد كده

هات الآلة

آخر حاجة في السكشن هو Affine

التاريخ: / / الموضوع:

Affine

For Encryption :-

$$C = ([\mathcal{M} * P] + S) \bmod N$$

- $\mathcal{M}$ → decimal Factor (معطى)
- P → plain text (حرف الموجود فالـ alphpet) (رقم الحرف)
- S → Key
- N → Size عدد الحروف الموجودة في الـ alphpet ولازم 26 ولا 27 والحد ايه

✓ $1 = \gcd(m, n)$ برضوا نفس اللي قلت كام ؟ كل اول

For decryption :-

$$P = [\mathcal{M}^{-1} * (C - K)] \bmod N$$

- $\mathcal{M}^{-1}$ → modulo multiplicated inverse
  لازم m هتبقى وتيجي تصلي عالبتي وتبدأ طل ✱
- $C - K$ → برضوا رقم الحرف فالـ Alphbet

R. Elshal

$w=22$ $r=17$ $s=18$
$a=0$ $L=11$ $t=19$

الموضوع:

التاريخ: / /

Example use Affine
Encrypt plainText = war last
$c = K = 10$
$m = 7$ $n = 26$

$\gcd(26, 7)$
$= \gcd(7, 5)$
$= \gcd(5, 2)$
$= \gcd(2, 1)$
$= \gcd(1, 0)$ ✓✓ تمام

Encryption $\Rightarrow C = Mp + K \bmod n$

$C(w) = (7 * 22 + 10) \bmod 26 = 8 \rightarrow I$ (154)
$C(a) = (7 * 0 + 10) \bmod 26 = 10 \rightarrow K$
$C(r) = (7 * 17 + 10) \bmod 26 = 25 \rightarrow Z$

✓ وهكذا

عمل وكتبه الكلمة

Example use Affine
decrypt cipher text = IKZJKGN
$n = 26$ $m = 7$ $S = 10$

decryption
$\Rightarrow p = [M^{-1}(C - S)] \bmod n$

$p(I) = (15 * (8 - 10)) \bmod 26 = 22 \Rightarrow w$

✓ إيش

$M = 7$ $n = 26$
$\gcd = 1$ ✓

M^{-1}

26	*	11
7	3	3
5	1	2
2	2	1
1	2	0
0	*	*

$x = 15$

إذن $M^{-1} = 15$ ✓

End of Section (3)

✓ لا ربه يا معين

go to hell

التاريخ:

الموضوع: سكشن التخاسر (4)

Hill Cipher

3X3
2X2

الـ Key بيكون matrix
plain Text → block in size 2 او 3
هو بيحددلك

For encryption: if matrix 2X2

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \right] \bmod n$$

n → size

cipher chars — key matrix — block of plain text (ارقامهم في ترتيب الحروف)

if matrix 3X3

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \left[\begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} * \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \right] \bmod n$$

* لازم الأول قبل اي حاجة

$\gcd(\text{determisk of key matrix}, n) = 1$

$$\begin{pmatrix} x & a \\ b & z \end{pmatrix}$$

$\boxed{xz - ab}$ ✓ =

3X3 Key ولا

$$\begin{array}{ccc} + & - & + \end{array}$$
$$\begin{bmatrix} 3 & 5 & 3 \\ 2 & 7 & 8 \\ 9 & 10 & 20 \end{bmatrix}$$

$= 3*(7*20 - 8*10) - 5*(2*20 - 8*9) + 3*$ وهكذا

انا هفكرك بس بالطريقة بس

التاريخ: / /

$h \to f$
$e \to 4$
$l \to 11$
$p \to 15$

الموضوع:

Example For Encryption

$$Key = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} \qquad p.t \Rightarrow HELP \qquad n = 26$$

الحل

$det = 3 \times 5 - 3 \times 2$ $\qquad gcd(det, n)$ ← اولاً

$= 15 - 6 = 9$

$gcd(26, 9)$

$= gcd(9, 8) = gcd(8, 1) = gcd(1, 0)$ ✓

$gcd = 1$ ✓✓✓

∴ For Encrypt:-

أول حرفين وبعدين تاني حرفين

H ترتيب حرف ال

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \left[\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix} * \begin{pmatrix} f \\ 4 \end{pmatrix} \right] \bmod 26$$

$$= \begin{pmatrix} 33 \\ 34 \end{pmatrix} \bmod 26 = \begin{pmatrix} f \\ 8 \end{pmatrix} = \begin{pmatrix} H \\ I \end{pmatrix}$$

$\begin{pmatrix} L \\ P \end{pmatrix}$ وبعدين شوف الحرفين اللي بعدهم ✓

وهكذا بسيطا

R.Elshal

التاريخ: / / الموضوع:

For decryption

if matrix (2×2)

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} * \det{}^{-1} * \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \right] \bmod n$$

هتحسب الرقم وتروح تجيب
modulo multiplicated inverse with n=26
او 27 حسب الحالة

The inverse of the Key Matrix

if the matrix 2X2

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$$

بدل a و d مع بعض وغير اشارة b, c

$$= \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

if the matrix 3X3

$$\begin{pmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{pmatrix}$$

3 خطوات :

① هتحسب ال matrix بالطريقة
انك تحذف الصف والعمود متقربن بالرقم
بعدين وحط النواتج زي ما هيا مش عكس

$9 \times 17 - 4 \times 17 = 85$

$20 \times 17 - 9 \times 17 = 187$

$20 \times 4 - 9 \times 9 = -1$

وتكمل

$$\begin{pmatrix} 85 & 187 & -1 \\ 90 & -129 & -78 \\ -10 & -349 & -173 \end{pmatrix}$$

$$\begin{matrix} + & - & + \\ - & + & - \\ + & - & + \end{matrix}$$

② حط العلامات على ال Matrix اللي طلعت

$$\begin{pmatrix} \overset{+}{85} & \overset{-}{-187} & \overset{+}{-1} \\ \overset{-}{-90} & \overset{+}{-129} & \overset{-}{78} \\ \overset{+}{-10} & \overset{-}{349} & \overset{+}{-173} \end{pmatrix}$$

هتغير الإشارات

③ اقلب الصف عمود والعمود صف

$$\begin{pmatrix} 85 & -90 & -10 \\ -187 & -129 & 349 \\ -1 & 78 & -173 \end{pmatrix}$$

بس كده بسيطا

R.Elsheh

ونفس الطريقة بسيطا

الموضوع: سكشن التخاسة (5)

التاريخ: / /

Full Viginier :-

طريقة سهلة جداً جداً

هتعمل 26X26 matrix فيها حروف كلها هيا دي هتكون بدل key بتاعك

ده key بتاعك

	A	B	C	D	E	F	.....	Z
A	A	B	C	D	E	.....		Z
B	B	C	D	.....			Z	A
C	C	D	E	.....		Z	A	B
D								
E								
F								
⋮								
Z								

ده p.t بتاعك

وهكذا

c.t ده بقى

For Encryption:

يلا

p.t = BeDA

Key = DF

BeDA

DFDF

وتحيث نيجي نقارنهم في الـ Matrix

For decryption:

يلا c.t = EJ9F

key = DF

EJ9F

DFDF

نفس الكلام بس هتدخل في عمود الـ c.t في matrix وتجيب التقاطع مع الـ key

وتطلع الـ p.t بسهولة

وكل سنة وانتم طيب والف الف مبروك #

الموضوع: _____ التاريخ: / /

سهلت بصوا بس افهم الليه
مارشيت ازاى هتانه
خلص

RSA Algorithm

والسكشن هيكون خلص *

Ali → Ahmed

الموضوع: _____ التاريخ:

الحكايه وما فيها

← Ali عاوز يبعت message لـ Ahmed
← الـ public key shared

← Ali هيجيب الـ public key بتاع Ahmed
يشفر بيه الـ message ويبعتها

← Ahmed استلم الـ message متشفرة

هيفك التشفير ده بالـ private key بتاعه

← طالبين بالـ الـ امتحان بيخليك جيب الـ keys لـ user واحد *

التاريخ: / /

الموضوع:

سهلات برضوا بس افهم الليه
مارشيت ازاى عوانه
خلاص

والسكشن هياخوه خلاص *

RSA Algorithm

2 users — Sender / reciever

1. generate 2 large prime numbers (p, q)

دي رقم عشوائي بخلاف
الي تحت بتاع ترتيب
الحرف اوعي تتلغبط !!

2. $n = p * q$

3. $Z = (p-1) * (q-1)$

4. E relative prime with $Z \rightarrow \gcd(E, Z) = 1$

5. $d = E^{-1} \bmod Z$

public key $= (E, n)$
secret key $= (D, n)$

ركز : الإيي مش عدد حروف اللغة ولكن هي
الخطوة رقم 2 فووووق

* For Encryption:

$C = P^E \bmod n$

R.Elshee

* For decryption:

$P = C^D \bmod n$

Scanned with CamScanner

$(52)^9 \bmod 55$

التاريخ: / / الموضوع:

Example

Ali send → Ahmed

∴ p.t → secret key for Ahmed

∴ c.t → public key for Ahmed

Ali

$p=3$

$q=11$

$n=3*11=33$

$Z=2\times10=20$

$E=7$

$\rightarrow \gcd(7,20)=1$

$1<E<Z$

∴ public key $=(7,33)$ (E, n)

$D=7^{-1} \bmod 20$ (Z)

20	*	3
7	2	1
6	1	1
1	0	0
1	#	#

$x=3$

∴ $D=3$ (D, n)

∴ Secret key $=(3,33)$

Ahmed

$p=5$

$q=11$

بنفس الخطوات

public key $=(9,55)$

secret key $=(9,55)$

صيغة مش أكتر

p.t = Help

$7^{33} \bmod 1$

$c(H)=p^E \bmod n$

$=7^9 \bmod 55$

$40353607 \bmod 55$

$=52$ ✓

40353555

$c(e)=p^E \bmod n$

$4^9 \bmod 55$ ✓

decrypt (H)

$p^{(H)}=c^d \bmod n$

$=52^9 \bmod 55 = 7 \rightarrow h$

الموضوع: _____

التاريخ: / /

مسألة كدا هعملها

$n = 3599$ $E = 31$ Find D

$D = E^{-1} \bmod Z$

$n = p \times q = 3599$ $p = 59$ $q = 61$

$Z = 58 * 60 = 3480$

$d = 31^{-1} \bmod 3480$

$\boxed{d = 3031}$

N		
3480		449
31	112	4 4
8	3	1
7	1	1
1	7	0
0		

~~3480 * 449 31 * 4~~

$\ominus 449 * 31 \oplus 3480 * 4$

$X \Rightarrow -$

$-449 \bmod 3480$

$X = 3031$

R. Elshell

Scanned with CamScanner

الموضوع:

التاريخ: معناه

E

public key = 5 $\quad n = 35 \quad C = 10 \quad \boxed{p + ??}$

p = 7 $\quad q = 5$

decryption :

$Z = 24$

$E = 5$

$d = 5^{-1} \bmod 24 = 5$

لو ال $D = E$ زود عدد D دورة Z

$d = 5 + 24 = 29$

دورة

$\boxed{E \neq d}$

ال algorithm نفسه بيقولك متجليش *

$d = E$

الدورة الجاية عندك هنا إلجي هيا

ال Z

الموضوع:

التاريخ:

مسألة الإثبات الي قالها في آخر السكشن *

هلعبه شوية بالارقام على جنب

$p = ff$
$q = 1f$
$e = 5$

$N = 119$

$d = 19$

96	*	19
5	19	1
1	5	0
0	*	*

معناها يقبل القسمة على E

$E \rightarrow$ odd number

$p, q \rightarrow$ two prime number

when

$(p-1)(q-1) - 1 \;/\; E$

$p * q = n$

$D = [(p-1)(q-1)(E-1) + 1] \;/\; E$

الحل

Z	d
E	α

$\therefore d = E^{-1} \bmod Z$

$\pm \alpha Z \pm E d = 1$

هفترض

$-\alpha Z + E d = 1$

$\therefore E d = \alpha Z + 1$

$d = \dfrac{\alpha Z + 1}{E}$ $\quad \because Z = (p-1)(q-1)$

$\therefore d = \dfrac{\alpha (p-1)(q-1) + 1}{E}$

96 ff

5 α هفترض ارقام $\alpha = (E-1)$ فاضل الي اثبته انه

$\therefore -96\alpha + 5 * ff = 1$

$\cancel{-96\alpha = 1 - 385}$ $-96\alpha + 385 = 1$

$\alpha = E - 1$

$\therefore D = [(p-1)(q-1)(E-1) + 1] \;/\; E$

End section (5)

①

① بعد كيدتي م اللعيز

الموضوع: الكشف الخاص (6) التاريخ: / /

EST « Excepted safe time »

✓ عدد الحروف الي انت شغال عليها
✓ عدد المحاولات
✓ زمن المحاولة الواحدة
password length ✓

$$EST = \frac{1}{2} A^S * E/R$$

عدد الاحتمالات ال password

one trial time
زمن المحاولة الواحدة

* (A) → عدد الحروف الي انت شغال عليها

* (S) → length password
(عدد حروف ال password بس)

* (E) → login عدد الحروف الي انت بتكتبها وانت بتعمل كلمة (عدد حروف ال username + عدد حروف ال password)

* (R) → Transmition rate
انت بتعمل / بتكتب الحرف الواحد في وقت أد ايه

$$EST = \frac{1}{2} A^2 * E/R$$

ABC

$S = 2$ ⟶ ∴ عدد المحاولات $= 3^2$

length password

Example 1

عدد حروف اللغة = 26

$S = 3$

الـ username = 10 حروف

وبنتقل حرف في 2 ثانية

* رسالة الـ error بعد كل حرفه

← عدد المحاولات اللي تقدر تعملها

$26^1 + 26^1 + 26^1 + 2$

← الوقت اللي تقدر تنتقل فيه حروف الـ username

$2 = 2 \times 10 = 20$

* لو الرسالة الـ error بعد كل حرفين

∴ $EST = 26^2 + 26^2 + 26^2 + 20$ #

* لو الرسالة الـ error بعد كل 3 حروف

∴ $EST = 26^3 + 26^3 + 26^3 + 20$ #

Sec_f الاسئلة مكتوبة كاملة في ملف خلود ✓

Example 2

user write his name in 3 s

A = 100

(5) length password = 3

وشان يكتب ال password

1 character / 1 second بيكتب

ظهلها رسالة error خدته ← 5 ثواني

ورجع تاني عشان ال password

« هياخد اد ايه عشان يعتاله »

وظهر غلط

وظهلها رسالة error ← خدته 5 ثواني

فكتب ثالث مرة وبرضوا ظهر غلط X

ال system هيعمل logoff ← اخد 3 ثواني

بكتب ال password

1c/s

وال length password بتاع = 3 ∴ 3X1 = (3)

ازن كتابة ال password

احسب ال Est

الحل

name → pass → error → pass → error → pass → logoff

3s 1c/s 5s 1c/s 5s 1c/s 3s

Total Time For these three trial

$2 = 3 + 3 + 5 + 3 + 5 + 3 + 3 = 25$

pass 1X3

∴ Time For one trial = 25/3 = 8.3 second

∴ $Est = \frac{1}{2} A^3 * 8.3$

$= [\frac{1}{2} \times 100^3] * 8.3 = 4166 \ldots\ldots$ second

= 48 days

بسم الله

وحدي لكن خوفي ساكن جوا روحي مبينتهيش

التاريخ: / /

الموضوع:

Example 3

length password = 32

اللغة الحاسبة/الشمال عليها = 2 = bit كام ?

File has internal 32 bit key

the call and test to open the File take 20 microsecond

20×10^{-6} Second

زمن المحاولة الواحدة بسيطا

what th Excepted save time?

الحل

$$EST = \frac{1}{2} A^S * E/R = \frac{1}{2} * 2^{32} * (20 \times 10^{-6}) = \checkmark$$

لا وهو دكتور حاتم اللهم صلي على النبي بيجيبلنا مسائل سهلة خالص زي دي

واكبر دليل على ترم العينة

« cry and cry and cry »

G.R. Elsha

التاريخ: / /

الموضوع:

* طالما هكتب الـ R والـ E هريحة شوية جيب الـ Trial Time فهنستعوض ابنا فالمسالة وجيبها بدماغك

Example 4

username = 12 حرف

كل حرف بيكتب في ثانية واحدة

* لو حط login غلط

هيرجع يكتب الـ username تاني

* لو دخل الـ password غلط

هيعمل ignore 5 s اعتبر error

الـ Field اللي بيكتب فيها مدتها

* ايه الافضل الجيه الـ Est كبر

* ايه الافضل في الحالتين

① هل الـ password length يكون 6 حروف وعدد حروف اللغة = 26

ولا

② S=5 والـ A=28

الحل

1

S=6 & A=26

Trail Time = 12*1 + 6*1 + 5 = 23

∴ Est = $\frac{1}{2} * 26^6 * 23$ = 112 years → the best

2

S=5 A=28

Trail time = 12*1 + 5*1 + 5 = 22

∴ Est = $\frac{1}{2} * 28^5 * 22$

= 6 years

واجعلك زي ما رضيا

الموضوع: _____ التاريخ: / /

طالما جاية سيرة الـ probability

يبقى كشغل ← underson Formula

* الناتج هنا نسبة مئوية

* لكن الـ EST كان كام seconds

$$P \geq \frac{T.G}{N}$$

T → Time unit (كام الـ password دي في أد ايه)

G → number of gesus that can be tested in one time unit

التخمينات $G = R/E$

N → number of possible passwords $= A^S$

$N = A^S$

حسب معطيات المسألة بقا بسيطا هيكون القانون

* $P \geq \frac{T.G}{A^S}$

* $P \geq \frac{T.R}{A^S.E}$

(لا تبكي يا صغيري لا انظر نحو السماء)

(بص في كتابك يا بابا بص في كتابك)

« اللهم إني أشكو إليك ضعف قوتي وقلة حيلتي وهواني على الناس »

التاريخ: / /

الموضوع:

Example 1

ال password بتتكون من 96 حرف

assume that

عدد المحاولات $= 10^4$ guess in 1 second

probability $= \frac{1}{2}$

over 1 year $\rightarrow$ $T = 365$ day

عايز ال length (S)

الحل

$$P \geq \frac{T \cdot G}{A^S}$$

$$0.5 \geq \frac{\overbrace{[365 * 24 * 60 * 60]}^{\text{second}} * 10^4}{96^S}$$

[redacted]

$$96^S \geq 6.3 \times 10^{11}$$

$\log_{10}$

[redacted]

$$S \log_{10} 96 \geq \log_{10} 6.3 \times 10^{11}$$

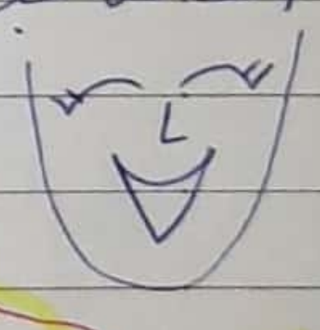
$$S \geq 5.9$$

$$S \simeq 6$$

لازم نقرب بسطا

#

حوش أمل
خش نام اسهل
صدقني
او غيط
اي ما تحبي



التاريخ: / /

الموضوع:

Example 2

$S = f$ $\quad A = 28$

$T = 100$ day $\quad R = 40$ character per second

$E = 30$

what's the probability?

$$P \geq \frac{T \cdot R}{E \cdot A^S}$$

$$P \geq \frac{[100 * 24 * 60 * 60] * 40}{30 * 28^f}$$

$$P \geq 8.5 \times 10^{-4}$$

Example 3

$A = 26$ $\quad T = 90$ day $\quad E = 30$

$P = 0.0005$ $\quad R = 40$ $\quad$ Calculate S

$$P \geq \frac{T \cdot R}{E \cdot A^S}$$

$$0.0005 \geq \frac{(90 * 24 * 60 * 60) * 40}{30 * 26^{S}}$$

$$26^S \geq \frac{90 \times 24 \times 60 \times 60 \times 40}{30 \times 0.0005}$$

$\therefore S = 7.2 \simeq 8$

انا اكتر حاجة مخوفاني
ان مسائل سهلة وبسيطة
وده بوكدلي
ان ليلتنا فلة فالفاينل
فلة فلة

يارب هوزن

التاريخ: / /

الموضوع:

Example

$S=4$
$A=26$
$R=1$

في حالتين :

① مفيش رسالة error هتطلع بعد كتابة ال password
حتا لو غلط

② لو في رسالة error هتطلع بعد كل حرف

يبقا هاتحسب

$\sum St$

$\sum St = \frac{1}{2} A^2$

لان مفيش اي حاجة اقدر اطلعها
ال Trial time

① No error Message

$Est = 1/2 * 26^4$ ✓

② there is error Message

⇐ اوقص عدد المحاولات = $26+26+26+26$

$Est = 26^4 * 0.5$ ✓

$L_n = R_{n-1}$ و $R_n = L_{n-1} \oplus f(R_{n-1} \oplus K_n)$

التاريخ: / / الموضوع: شرح DES

DES

Data 64 bit

هتدخل الـ Message على matrix اسمها
intial permutation matrix (I_p)
والحد يطلع قسمين

L_0 R_0

دي لليلي لوحدها

L_1 $R_1 = L_0 \oplus f(R_0 \oplus K_1)$

L_2 $R_2 = L_1 \oplus f(R_1 \oplus K_2)$

L_{16} R_{16}

وبعدها هنعمل Swaping

L_{16} R_{16}

حاتقم مع بعض وتدخلهم على matrix
Final permutation Matrix (I_p^{-1})
64 bit

والحد يطلع خلاص ده Encrypted Message

Hexadecimal حوله لـ
بقا بسيطا

Key

انه هتدخله على matrix
PC-1
والحد هيطلع (K_+) هتقسمه نصين
C_0 & D_0
وتطبق الـ shifting
1, 2, 9, 16 → ①
الباقي → ②
لحد ما توصل لـ C_{16} & D_{16}

وبعدين تاخد كل CD مع بعض
وتدخلهم على matrix
PC-2

$C_1D_1 \rightarrow PC\text{-}2 \rightarrow K_1$
$C_2D_2 \rightarrow PC\text{-}2 \rightarrow K_2$
⋮
$C_{16}D_{16} \rightarrow PC\text{-}2 \rightarrow K_{16}$

ده الطلوب

(الدعاء ربي اجعلك تعيشين لأشياء جميلة)

R.Elshal

الموضوع: _____ التاريخ: / /

$MF(R_0 \oplus K_1)$

↳ Mangler Function

32bit ⊕ 48bit ⟹ مش هينفع هندخل ال R

$MF(R_0 \oplus K_1)$ Expasion to 48bit

block R

4bit [0110] [1111] [0101] [1011] ⟹ كل واحد هياخد آخر الحرف قبله واول الحرف بعده

6bit 101101 011110 101011 110110

↳ E(R) 48bit ده مرحلة اسمي خطوة ال Expasion انك بتدخل ال R عن matrix اسمها «E-bit Selection Table»

فكرة خلاص تاخد

48bit E(R) ⊕ 48bit K

⊕

48bit

الى يطلع

دخله على

S-box (reduction box)

32 bit

P matrix

32 bit ✓ * output For Mangler function

Sbox

انت بتاخد ناتج ال ⊕ الى طلع 48bit

[6bit] [6bit] [6bit] [ ] ...

① ② ③ ④

هتاخد كل بلوك تدخله على ال Sbox تباعه (الاول والثاني والثالث بالترتيب)

هتمسك كل بلوك

011011

0 → رقم الـ Row

1101 → Clom

Scanned with CamScanner

DES Modes of operation:

ECB (electronic code book)
CBC (chain Block coding)
CFB (cipher Feedback)

Weak & Semi weak keys

يقول انه سؤال فاينل

weak Key => Consist of either all zeros
or all ones or
alternating 1s and zeros
or alternating zeros and 1s
(4 possible probability)

Semi Weak Key => th remaing 12 possible probability
From 16 subkeys.

Triple DES: 56 bit key applied

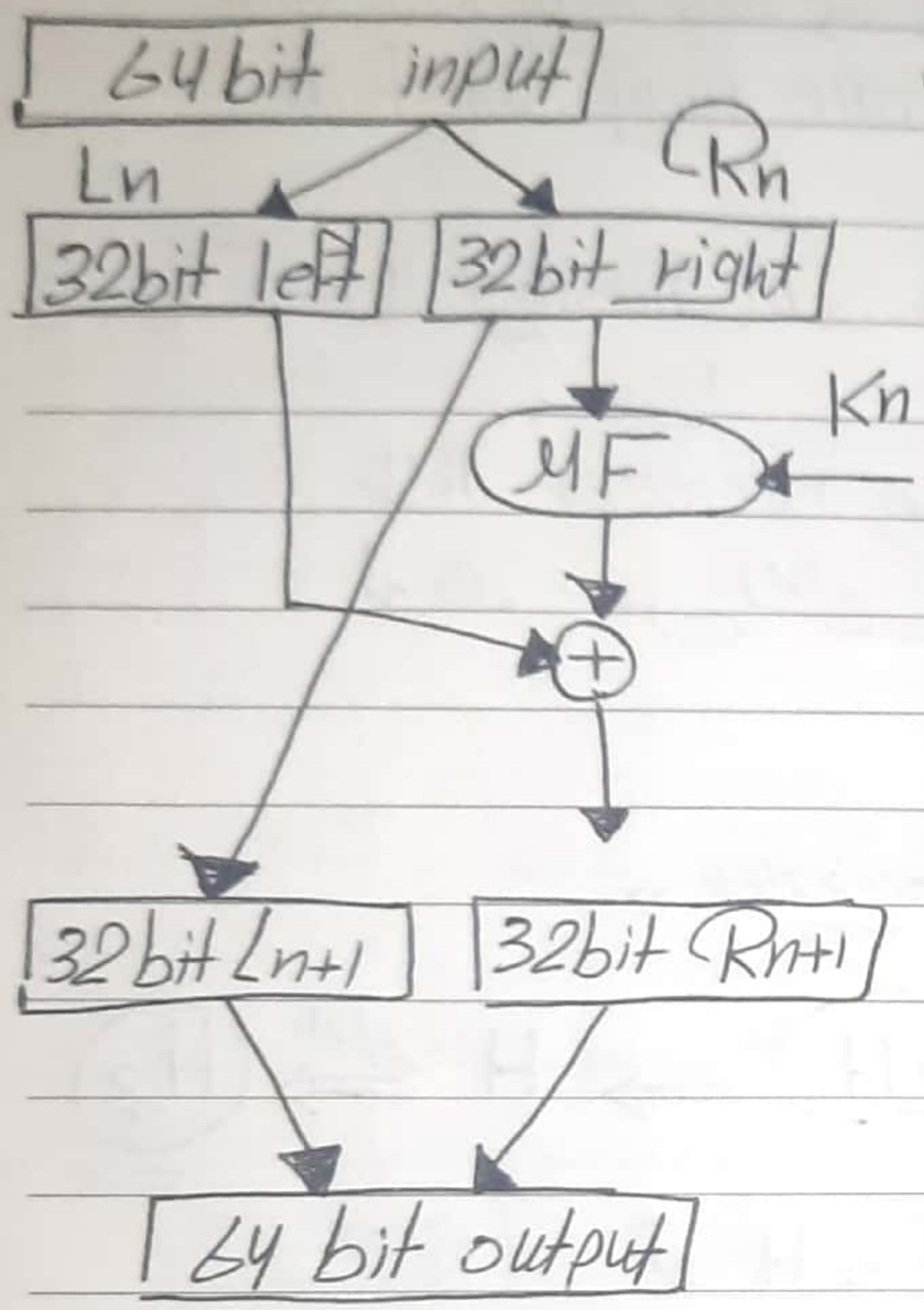
↳ is just DES done three with Two keys used in a particular order.

[Triple DES can also done with 3 Separate keys instead of only 2.
incase the resulatant key space is about 2^112]

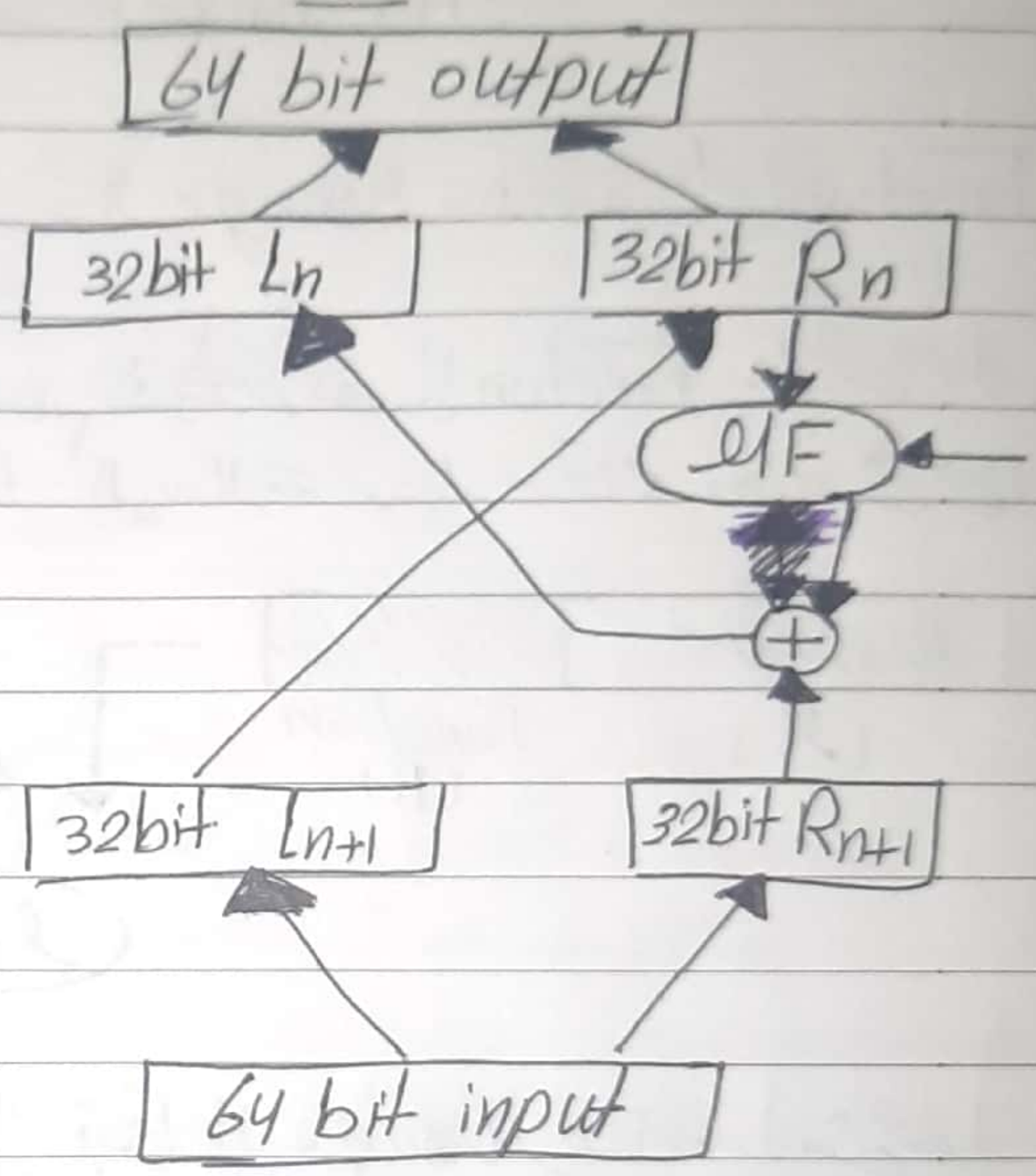
DES

DES Round

Encryption



Decryption



لا يستطيع الجميع ان يحاربوا

هو بيقول ان مفيش مسائل كبيرة بتيجي على الـ DES أو الـ hashing
فانت تفهم بس # وتعرف الدنيا لاي سؤال #

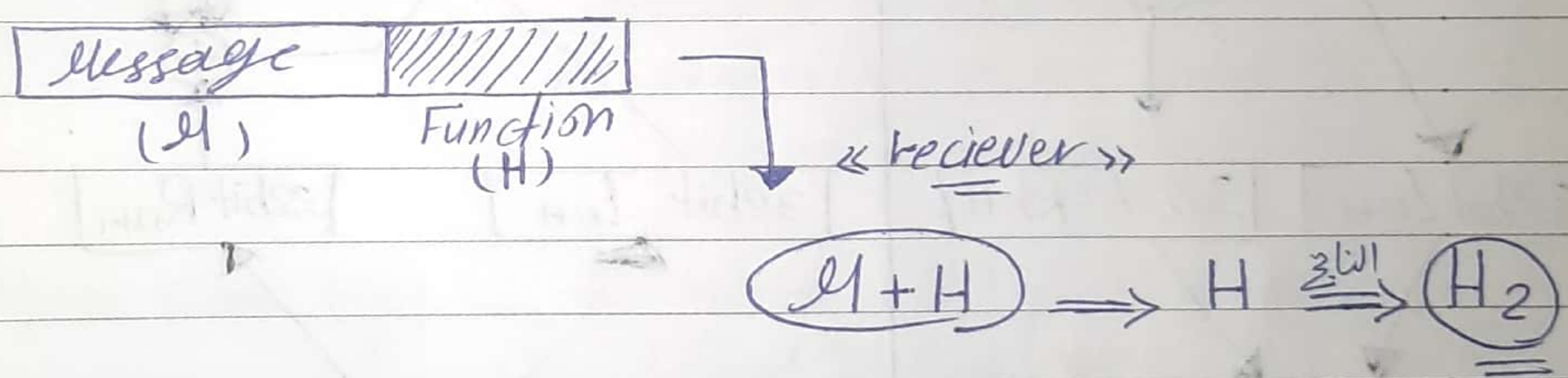
الموضوع: / / التاريخ:

« Hashing »

بحث الـ hashing

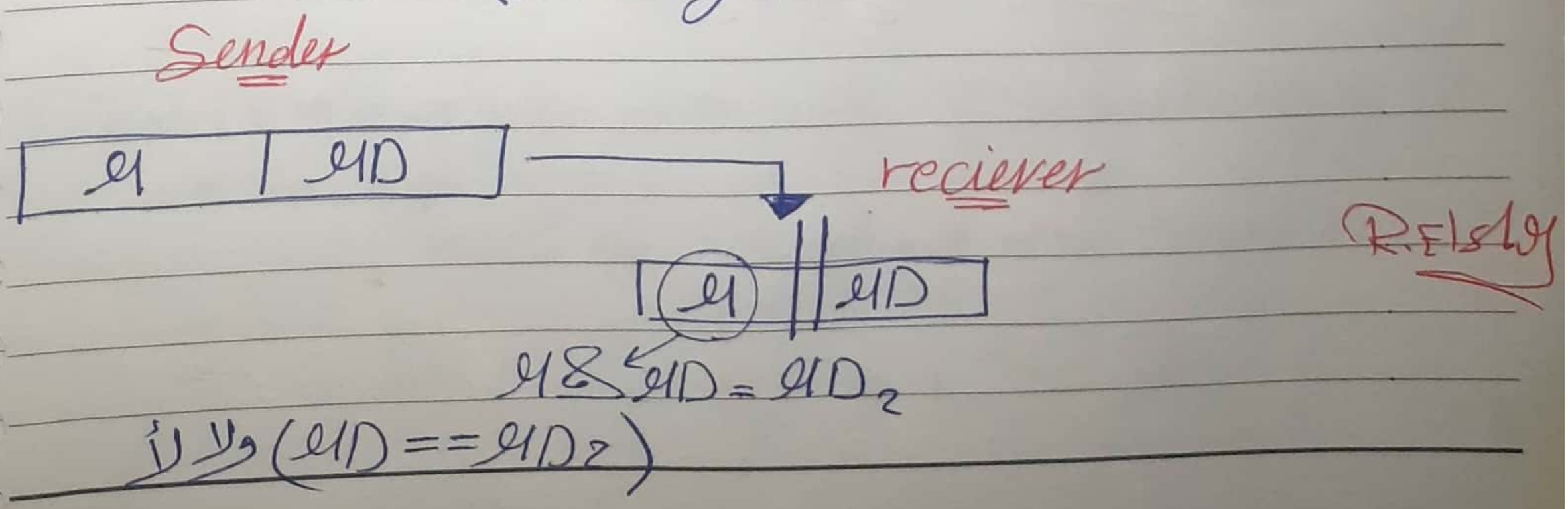
hashing : not Two way Function For check Data integrity
(Encryption & decryption) → Two way Function
(Hashing) → one way Function

فكرة الـ hashing انك هتاخد الـ Message وتبعتها هتضيف عليها Function
طالما الـ reciever يستلمها هيطبق نفس الـ Function على الـ message
لو هو نفس الناتج تبقا الرسالة وصلت تمام ومتلعبش فيها



لو H = H2 تبقا الـ Message فاضل ومتلعبش فيها
الـ H دي اسمها
(Message digest) MD

« Hashing »



#

19-1-2021
الاكتاب هياكل من دماغي
حتى

R.Elshal

التاريخ: / /

الموضوع:

Collegien ⇒ 2 Messeuge have the Same digiest

birthday problem ⇒ مشكلة ليها قانون (ايش ليهم نفس تاريخ الميلاد)

$$nsd = p = \frac{n!}{n^r (n-r)!}$$

n ⇒ عدد الايام

r ⇒ عدد الاشخاص

not have Same birthday

$$sd = p = 1 - nsd = 1 - \frac{n!}{n^r (n-r)!}$$

مثال year = n = 365 & r = 100

$$\therefore sd = 1 - \frac{365!}{(365)^{100} * (365-100)!}$$

لو قالك كدا

احتمال ان شخصين يتولدوا في نفس اليوم والشهر ⟸ $\therefore n = 31 * 12$

احتمال ان الشخصين يتولدوا في نفس اليوم والشهر والسنة ⟸ $\therefore n = 365$

لو شهر بس ⟸ $\therefore n = 12$ ، لو day بس ⟸ $\therefore n = 31$

(Hashing) md2, md4, md5 → كلمة وخلاص

md2: have 3 phases ① padding ② checkSum ③ Final pass

padding

msg must be octed → bytes ✓ → 8 bits ✓

عشان نخلص ⟸ ال msg لازم يكون عدد ال bits منه مضاعفات ال 8

وال octed ⟸ منه مضاعفات ال 16

وتشوف هتزود على الرسالة كام عشان تبقى multiple of 16 وتزود

مثال

msg = 512 bit

md2 بال padding عايز اعملها

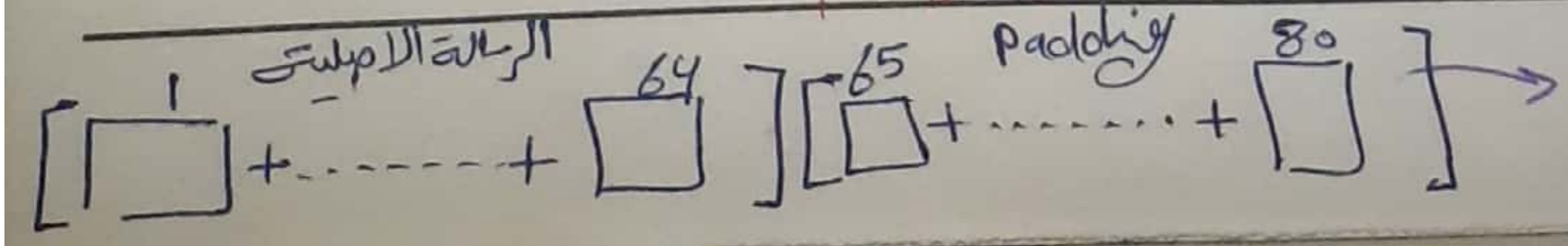
$\therefore 512/8 = 64$ $\therefore$ number of octed = 64 octed

$\therefore 64/16 = 4$ ✓ خلص تمام

هزود على الرسالة 16 octed

اعملها padding ⇐

الرسالة الاصلية



كل واحد فيهم هيحط فيه 16 بال binary

8 bit والباقي اصفار

* لو عايز تضيف 8 octed يبقا كل block يتكتب فيه 8 بال binary والباقي اصفار
* لو محتاج اضيف 2 octed يبقا كل block يتكتب فيه 2 بال binary

الموضوع: _____ التاريخ: / /

1

مثال

msg = 500 bytes
↳ = 500 octed يعني

جايالي جاهزة انها octed
اتأكد بقا انها مش
multiple of 16

500/16 = 31.25 XX

واقرب مضاعف لل 16
اكبر من ال 500 هو 512
يعني هزود الرسالة بتاعتي
12 blocks

[1 + ... + 500] + [501 + ... + 512]
الرسالة الاصلية — padding

كل واحد فيهم
مكتوبة فيه 12 بال binary
وباقي ال 8bit اصفار

2

مثال

msg = 480 bit

480/8 = 60 ✓ octed

60/16 = 3.75 XX

واقرب مضاعف لل 16
اكبر من ال 60 هو 64
هضيف 4 بلوكات

[1 + ... + 60] + [61 + ... 64]
الرسالة الاصلية — padding

كل واحد فيهم مكتوبة
فيه 4 بال binary

بتاخد الخطوة اللي فاتت الخطوة دي كمان
بعضها، وهنا خلصنا على طرح
حاجات من ال md2
وهو ال checksum

Padding في MD2

الي هو ده
على بعضه بعض

original message	r bytes ($1 \leq r \leq 16$)

→ multiple of 16 bytes

R. Elshal

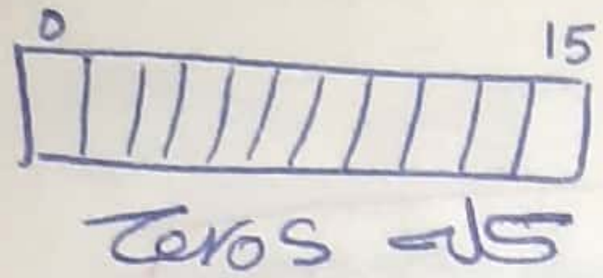
مش هننتحر بقا ولا ايه؟!

md2 → 1 padding 2 checkSum 3 Final pass

تم

هنا خد الحاجة من خطوة ال padding وهو

checkSum → $\boxed{\text{msg أصلية} + \text{padding}}$



← (initial checkSum) وهيكون معانا حاجة اسمها

هتخزنه وتشتغل على

كل مرة 16 تم 16 لحد ما تخلص *

مثلا انا عاوزة اعرف اجيب الداتا الي هتحط في كلمات رقم 5 فار initial checkSum

هعمل ايه ↓

هتاخد الداتا الموجودة في — الداتا الموجودة في

octed(n-1) ⊕ octed(n) = ناتج

initial checkSum — الداتا الأصلية

هتحطه على جدول bi substitution Table

ولكن الناتج ده بـ 12 هتروح تجيب الرقم الي في العمود رقم 12 وحوله binary وحطها

⊕ octed(n) = ناتج

initial checkSum

تاخده تروح تحطه فار octed(n) من الـ initial checkSum

وهكذا لحد ما تخلص الـ initial checkSum وتدخل على 16 من الداتا تم ال 16 bit

الي بعدهم وهكذا * لحد ما تخلص *

بقا الحاجة خلاص بقا checkSum

خلصت؟

تاخد ال checkSum النهائي وتدخله على أم خطوة الي هيا

CS

Final pass

PM	CS

Final pass

هتخدهم وتقسمهم

كل بلوك فيهم 16 octed

ومعاك خانات اسمها mdi ← mdintermediant

كلهم zeros فالاول

0 — 15

هاخد أول بلوك منها وابدأ شغل

mdi ⊕ [ ] = [ ]

16 16 16

= 48 octed

حطهم كلهم هنا

0 — 47

انا هلا عايز اعرف ايه الداتا الحالي فرضت تحطها فال octed اقم 5

(n)

هاخد الداتا الموجودة في

oct (n-1) → وارجع اشوف قيمتها في substitution Table

واخد الداتا الي طلعت منه

⊕ octed (n) = فاتي

اخده اخزنه في مكانه فال octed

(n)

الرحمة

③ وهكذا الحدما تخلص على اول 16 oct من الداتا الى داخلت لـ Finalpass
وهيطلعلك كل مرة mdi جديد
وهكذا

$$\underbrace{\underset{\text{16oct Data}}{\boxed{}} \oplus \underset{\text{16oct mdi}}{\boxed{}}}_{\text{48 octed}} = \boxed{}_{16}$$

ونفس الطريقة
18 خطوة

لما توصل للآخر وخلاص توصل لآخر 48 octed هتقسمهم

16	32

الهلها XX

هاها دول
ال

Message digest

الحدانا عايزة اجيبهم من الصبح

سؤال بيجي بسيط هو طلب عدد الخطوات فال

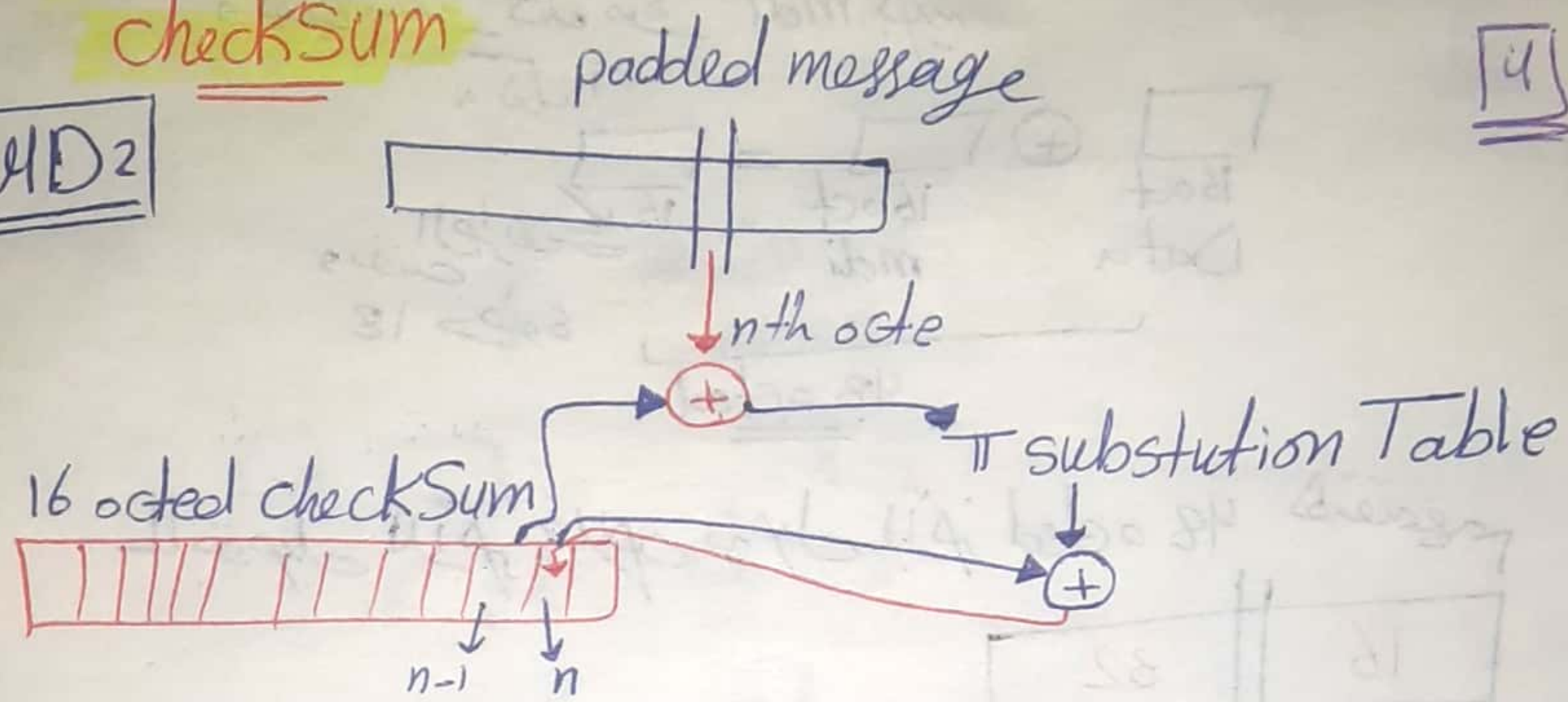
⊛ checkSum = 16 * m

m × 16
عدد البلوكات

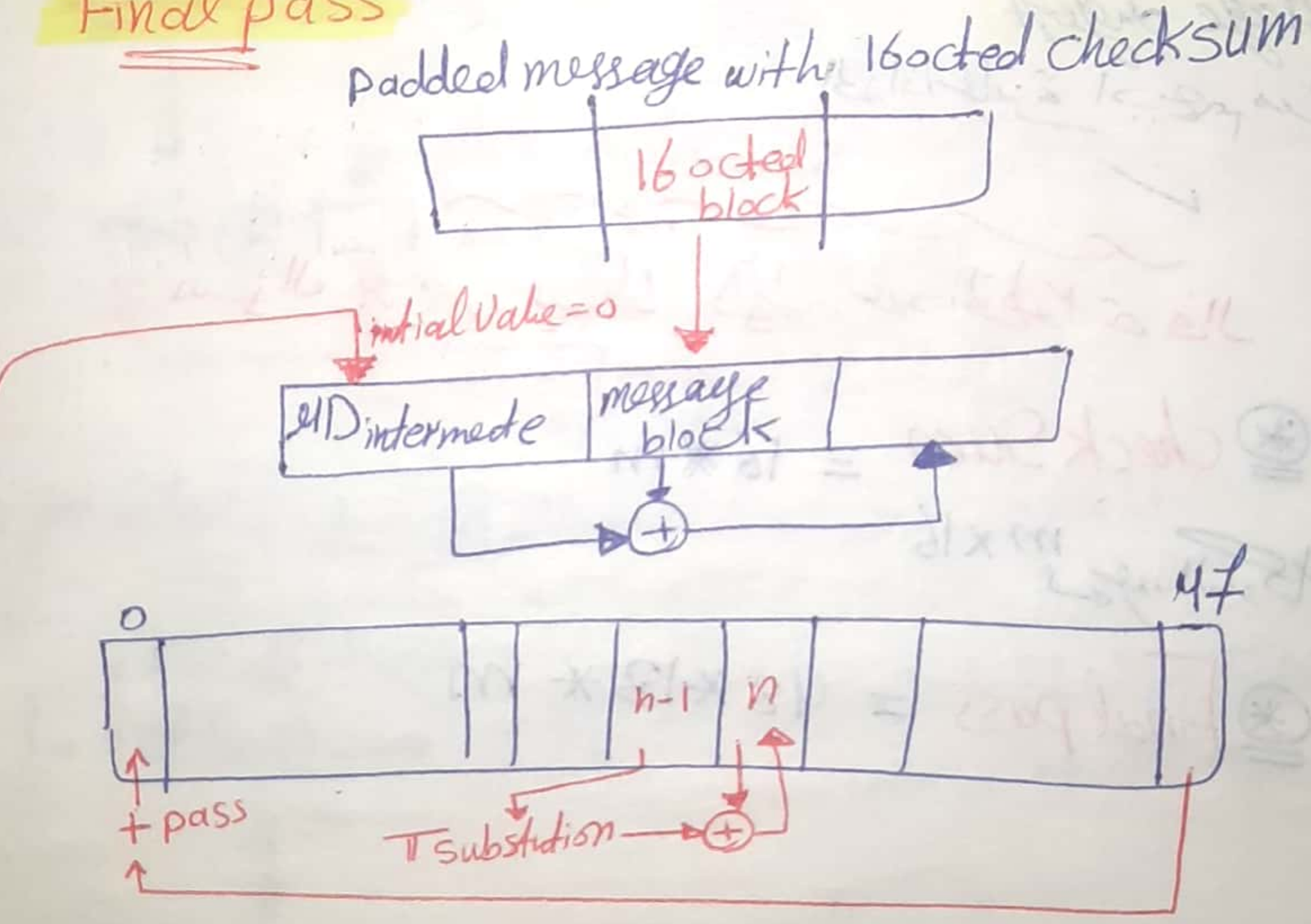
⊛ Final pass = 48 * 18 * m

checksum

MD2



Final pass



For next message block | discarded

Final MD2 after checksum processed #

md 5 & md 4 هنقول كلمتين سريعين

md 4

خطوتين → padding = padding For md5
→ passes

padding

original message	512 bits (Padding)	64 bits message length ثابتة

multiple of 512 bits

مثال

msg = 400 bit

قبل اي حاجة ضيف 64 وانت مغمض

$400 + 64 = 464 \Rightarrow X$ لسة مش مضاعف لـ 512

واقرب مضاعف ليه هو 512

فهزود 48 bits هزودها ازاي بقا هنا md 4

هنقول كدا هضيف 48 bits

$1\underbrace{000\cdots0}_{47}$

هنحط واحد وجنبه 47 صفر

مثال

msg = 1000 bits

$1000 + 64 = 1064$ لسه واقرب مضاعف ليها 1536

$1\underbrace{00\cdots0}_{471 \text{ zeros}}$ يعني 472 هزود

* For Padding

مثال

msg = 500 bytes

↳ 500 X 8 = 4000 bits

4000 + 64 = 4064

اقرب مضاعف

هو 4096

32 bit ∴ محتاج

∴ For Padding ⟹ 1 000.....0

↓

31 zeros

الخطوة الثانية ⟸ لـ md 4 هيا

Final passes

ويتكون من 3 Functions

1. selection Function
2. Majority Function
3. X-or Function

هي سؤال مهم جداً بيجي فالفاينال

md4 Vs md 5 الفرق بينهم

MD4	MD5
3 passes	4 passes
2 Constriant (pass 2, pass 3)	64 constriant

Functions

MD2	MD5
*worked on octed /byte	*worked on bits
* 16 octed	* 512 bit and 64 bit recerved

original message	r bytes $1 \leq r \leq 16$

multiple of 16

original message	100...00 512 bit	original length 64 bits

multiple of 512 bit

نصيحة لازم تحل الامتحانات وتشوف الرسومات والاسئلة
النظرية والحلول على درايف خلود

وربنا ييسر علينا كلنا

MEXICO
WHERE THE CULTURE CAN SPEAK

Scanned with CamScanner

نسخة محاضرة

① هتشوف الاسئلة النظرية الجاية على درايف خلود

② سكشن EST لازم تقرأ المسائل اللوغاريتمية
عشان تعرف تطلع طرحيات وتشتغل
فروح في سكشن (7) بتاع خلود هتلاقي الاسئلة
مكتوبة بحلولها #

عشان النحاس كان بيعرفنا القوانين
والحلول بعد فالسكشن وملحقناش

③ شوف حل ال gcd بطريقة ال euclidean

④ هشرح دلوقتي Diffie Hellman عشان كان واقع
مني قبل كده

⑤ حطرتك لازم تشوف وتحل على الاقل مثال واحد بعد عن
ال DES عشان تفهم الليلة صح
وهتلاقيه فالفولدر بتاع النحاس الي منزله
مني كام ورقة كدا فيهم مثال واخد بس
بص فيه عشان تبقا عاملة الي عليك

⑥ آخر حاجة
لازم تبص على الامتحانات المحلولة في درايف خلود
عشان ربنا يستر #

* (Diffe Hellman) *

* * *

public
private > 2 Keys ليه Sender ال
وكذلك ال reciever

⇐ الي بيتبعت على الشبكة هو ال (public Key)

⇐ هيبدلو ال public Key مع بعض

⇐ وال Sender هيطبق algorithm معين عليه وتجيب منه private Key
وال reciever نفس الكلام ~ ~ ~ ~ ~ ~ ~ ~

ايه ال algorithms دي

هو رقمين بيوا فدماغ كل واحد منهم وبتاخد منهم معلومات

$A, X, \alpha, q \Rightarrow$ معطيات أساسية

A

$$\text{public Key}(A) = \alpha^{XA} \bmod q$$

B

$$\text{public Key}(B) = \alpha^{XB} \bmod q$$

لازم ال

$$\gcd(\alpha, q) = 1$$

$$\text{private Key}(A) = y(B)^{XA} \bmod q$$

$$\text{private Key} = y(A)^{XB} \bmod q$$

لازم يطلعوا متساويين

تعالى مثال

example

$q = 71$ & $\alpha = 7$ & $XA = 5$ & $XB = 12$

Find $K \Rightarrow K$ is private key

$q \nmid$

check For gcd

$$\gcd(\alpha, q) = (7, 71)$$
$$= \gcd(71, 7 \bmod 71)$$
$$= \gcd(7, 71 \bmod 7)$$
$$= \gcd(1, 7 \bmod 1)$$
$$= 1 \quad \checkmark$$

$$y(A) = \alpha^{XA} \bmod q$$
$$= 7^5 \bmod 71$$
$$= 51$$

$$y(B) = \alpha^{XB} \bmod q$$
$$= 7^{12} \bmod 71$$
$$= 4$$

$$Key = y(B)^{XA} \bmod q$$
$$= 4^5 \bmod 71 = 30$$

$$Key = y(A)^{XB} \bmod q$$
$$= 51^{12} \bmod 71$$
$$= 30$$

private key = 30

R.Etshal

دعوة دخول الغنيد

End of Security

مع السلامة بسيطا

Scanned with CamScanner