Example:-

ciphertext: EHJLQWKHDWWDFNQRZ.

plaintext: begintheattacknow.

the key is $\underline{\underline{3}}$.

- Plain - cipher = key.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| cipher text : | L | A | H | Y | C | X | key = 9 |
| cipler num : | 11 | 0 | 7 | 24 | 2 | 23. | |
| X = cipler - key : | 2 | -9 | -2 | 15 | -7 | 14 | ⇒ Mod for $\underline{\underline{+ve}}$ num |
| X % $\underline{\underline{26}}$ : | 2 | 17 | 24 | 15 | 19 | 14 | ⇐ إذا كان الرقم أقل من المقسوم |

عليه يكون الناتج الرقم نفسه

عدد أحرف اللغة.

|k| = 26!

⇐ وإذا كان سالب يكون

so the plain text : C R Y P T O.

المقسوم عليه - ال key

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Plaintext: | B | E | S | T | S | T | U | d | e | n | t | s. |
| plain num: | 1 | 4 | 18 | 19 | 18 | 19 | 20 | 3 | 4 | 13 | 19 | 18. |
| x = plain + key : | 18 | 21 | 35 | 36 | 35 | 36 | 37 | 20 | 21 | 30 | 36 | 35 |
| X - key : | | | 9 | 10 | 9 | 10 | 11 | | | 4 | 10 | 9 |
| so the cipher text : | S | V | J | K | J | K | L | U | V | E | K | J. |

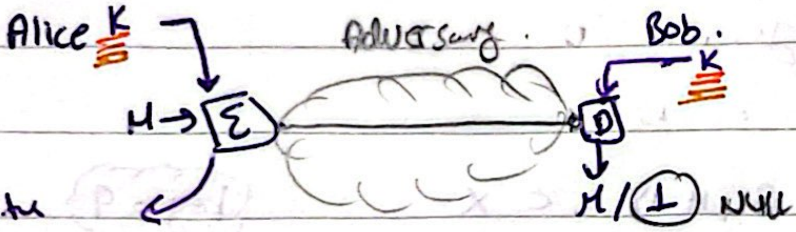
key = 17

not secure. غير آمن ⇐ deterministic encription ⇐ يوجد تكرار

note :-

E : (key + Mess) mod 26.

D : (ciph - key) mod 26.



- Subsitu

شيء محل شيء.

- Transpos.

تبديل.

⇐ عند عمل التشفير من طرف المرسل يتم عمله على المفتاح العام للمستقبل Kpu . وفي الطرف الآخر يتم فك التشفير بواسطة المفتاح الخاص للمستقبل Pri .

1) private (symmetric) " key crypto "

⇒ save key.

2) public (Asymmetric).

⇒ there is public and private key for even one.

- kepu , kpr.

## vigenere cipler:

**Example:**

- the MOGZD was encrepted using vigenere cipher with key Fork, what is the plaintext.

C: M O G Z D

12 14 6 25 3

key: F o r k F.

5 14 17 10 5.

Plain = c-key: 7 0 $\boxed{-11}$ 15 $\boxed{-2}$.

15. 24

so the plain text is HAPPY.

- You have intercepted a message encrypted with vigener Algoritem and have managed to determine the corresponding plaintext. the ciphertext is " kcszjwvf|abdlzgzslsygym " and the corresponding plain text is " sallywenttotheseashore ". what is the key?

C: 10 2 18 25 9 22 21 5 0 1 3 11 25 6 25 18 11 18 24 ...

P: 18 0 11 11 24 22 4 13 19 19 14 19 7 4 18 4 0 18 ....

$\boxed{-8}$ 2 7 14 11 0 17 -8 -19 -18 -11 -8 ....

18 18 7 8 15 18.

∴ the key is SCHOLARSHIPS. key = (C-P)mod 26.

$\Rightarrow$ GCD (888, 54) = 6

$888 = 54(16) + 24.$

$54 = 24(2) + 6$

$24 = \underline{\underline{6}}(4) + \boxed{0}.$ "linear combination"

from the last one :-

$6 = 54 - 24(2)$

$6 = 54 + 24(-2)$

$6 = 54 + [888 - 54(16)](-2).$

$6 = 54 + 888(-2) + 54(32)$

$6 = 54(33) + 888(-2).$ "linear combination".

$\Rightarrow$ $27^{-1}$ mod 392.

$392 = 27(14) + 14$. ⇐ تحليل الرقم المقسوم عليه

$27 = 14(1) + 13$. بالنسبة له نفسه، حتى الوصول

$14 = 13(1) + \boxed{1}$. إلى 1

• GCD (392, 27) = 1 ⇐ نأخذ آخر معادلة تم التوصل إليها.

greater comon diviser.

$14 - 13(1) = 1$

$13 = 27 - 14(1)$ ⇐ $14 + 13(-1) = 1$. لأنه يوجد سالب أمامي وسالب موزع.

$14 + 27(-1) + 14(1) = 1$

$14 = 392 - 27(14)$. ⇐ $14(2) + 27(-1) = 1$

$14 = 392 + 27(-14)$. $[392 + 27(-14)](2) + 27(-1) = 1$.

$392(2) + 27(-28) + 27(-1) = 1$.

$392(2) + 27(-29) = 1$.

$392 \times 2 \ \% \ 392 = 0$

$\frac{\cancel{27}(-29)}{\cancel{27}}$ mod $392 = \frac{1}{27}$.

$-29$ mod $392 = 27^{-1}$ mod 392

∴ $27^{-1}$ mod $392 = \boxed{362}$.

$392 - 29$

⇒ perfect secrecy :-

Regardless of any prior information, the attacker has about the plaintext , the ciphertext should has no additional information

$$Pr[M=m] \equiv Pr[M=m \mid C=c].$$

" prior info "  " posterior "

notes :-

- one time pad.

  $\mathcal{E} = M \otimes key.$

- cipher :

  1) stream cipher. " bit by bit "

← يتم عمل التشفير لبت واحدة كل مرة ، مثال عليه كل الاساليب الى الآن .

.Vigenere cipher . OTP . ceasar . Substitution.

  2) Block cipher.

← يتم تقسيم المسج لـ blocks كل واحدة منها 64 bit ، ثم عمل التشفير مجموعة مجموعة

ويتم تشفير كل مجموعات باستخدام ال key نفسه ونفس وسيلة التشفير ،

ممكن ان تكون عدد بتس

مختلف ، ليس شرط ان تكون

64 bit .

e) crypto needs twee scinese :-

1) Number theory.

2) group theory. $\underline{\underline{3}} \% 5 = \underline{\underline{8}} \% 5 = 3$. "group".

3) probability.

$\rightarrow$ ex:-

head $\rightarrow$ 0

tail $\rightarrow$ 1 $\quad X \in [0, 1]$.

$$Pr\{X\} = \begin{cases} 0.5 & , \text{tail} \\ 0.5 & , \text{head} \end{cases}$$

ex:

Die " حجر نرد ".

$Pr[X = 4] = \frac{1}{6}$

$Pr[X = 4 \mid \text{number is odd}] = 0$.

$Pr[X = 4 \mid$ ″ ″ $\text{even}] = \frac{2}{6} = \frac{1}{3}$

- $$P(A/B) = \frac{P(A \cap B)}{P(B)} = \frac{P(B|A)\, P(A)}{P(B)}$$

- Two R.V are independent : $P(A/B) = P(A)$ " perfect "

$P(M = m \mid C = c) = \underset{\smile}{P(M = m)}$ prior info.

ex:-

$$P[M = \text{one}] = Pr[M = \text{one} \mid C = xyz] = \frac{1}{2}.$$

Total prob theorem:-

$$P(A) = \sum_{B} P(A/B)P(B).$$

ex:-

Person has undertaken a mining Job the probability of compliation of the Job on time with and without rain is 0.42, 0.9. probability of rain is 0.45. determine the probability that the mining Job will be compleation in time:

$P(B) = P(rain) = 0.45$

$P(B') = 0.55$

$P(A/B) = 0.42$

$P(A/B') = 0.9.$

$\therefore P(A) = P(A/B)P(B) + P(A/B')P(B').$

$= 0.42 \times 0.45 + 0.9 \times 0.55 = 0.684.$

" note "

عند استخدام نفس المفتاح في ال OTP

يكون السستم غير آمن " not perfect secrice "

## perfect privicy:-

ex!- shift cipher.

Ataker : $pr[M = one] = \frac{1}{2}$

$pr[M = ten] = \frac{1}{2}$.

sender                                   reciver.

$\underset{\text{prior}}{pr[M = ten] = \frac{1}{2}} \equiv \underset{\text{posterion}}{pr[M = \boxed{t}\underline{e}n \mid c = \overset{12}{\underset{24}{\boxed{o}}}q\underline{u}]} = 0.$

ع ال shif ليس بنفس المقدار لكل الأحرف وبالتالي احتمالية المعرفة اذا كان هذا
هو المبع او لا تساوي $\underline{0}$ .      " not secricy ".

ex:-

$Enc(M) = (K+M) \bmod 5$.

$Dec(M) = (c-m) \bmod 5$      $pr[\underline{Enc(0)} = 0] = \boxed{\frac{2}{6}}$ $\underline{m=0}$ . ⇐

$M = [0, 1, 2, 3, 4]$      should be =

$k = [0, 1, 2, 3, 4, 5]$      $pr[\underline{Enc(1)} = 0] = \boxed{\frac{1}{6}}$ $\underline{m=1}$

perfect secrece??      ⇒ " not perfect secrice "

| m = 0 | m = 1 |
|---|---|
| $(0+0) \bmod 5 = \boxed{0}$. | $(0+1) \bmod 5 = 1$ |
| $(1+0)$ " $= 1$ | $(1+1)$ " $= 2$ |
| $(2+0)$ " $= 2$ | $(2+1)$ " $= 3$ |
| $(3+0)$ " $= 3$ | $(3+1)$ " $= 4$ |
| $(4+0)$ " $= 4$ | $(4+1)$ " $= \boxed{0}$ |
| $(5+0)$ " $= \boxed{0}$ | $(5+1)$ " $= 1$ |

Example:-

$M = C = K = \{0, 1, \dots, 1023\}$

$E(M) = (M + K) \bmod 1024$

$D(C) = (C - K) \bmod 1024$ .

perfect secrecy?

| $M=0$ | $M=1$ |
|---|---|
| $(0+0) \bmod 1024$ | $(1+0) \bmod 1024$ . |
| $(0+1)$ 〃 | $(1+1)$ 〃 |
| $(0+2)$ 〃 | $(1+2)$ 〃 |
| ⋮ | ⋮ |
| $(0+1023)$ 〃 | $(1+1023)$ 〃 |

⇒ perfect seclecy.

- key space is long as the message so the key is used only once.

note!:

$(5 \times 10) \bmod 7 = 1$

$$\overset{\equiv}{\left[(5 \bmod 7) \times (10 \bmod 7)\right] \bmod 7}$$

⇐ ال mod بتوزع .

$\Rightarrow (345^{28567} \times 23^{567} + 1078) \bmod 29.$

$(345^{1020 \times 28 + 7} \times 23^{20 \times 28 + 7} + 1078) \bmod 29$ Fermat theorem:

$(345^{7} \times 23^{7} + 1078) \bmod 29.$ $\alpha^{p-1} \bmod \underline{\underline{p}} \equiv 1.$

prime number

$((23 \times 3 \times 5)^{7} \times 23^{7} + 1078) \bmod 29.$

$(23^{14} \times (3 \times 5)^{7} + 1078) \bmod 29.$ $\cdot\ 9000^{28} \bmod 29 = 1.$

$\left[(23^{14} \bmod 29)((3 \times 5) \bmod 29) + 1078 \bmod 29\right] 4{,}29$ $9000^{9000 \times 28} \bmod 29 = 1$

**Block cipher:-**

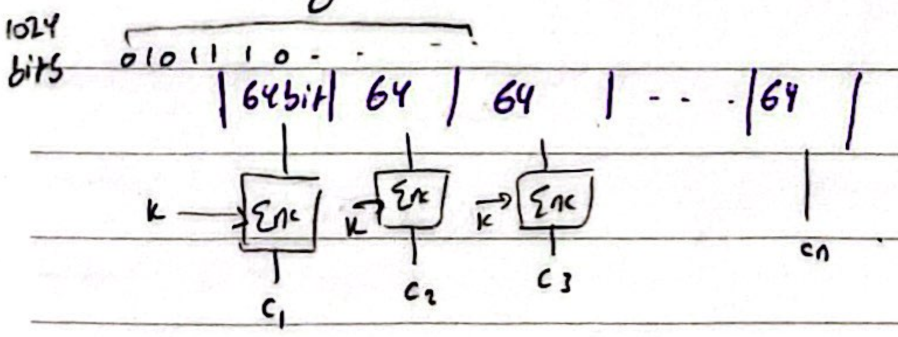
Sender:

Email:

Hi Ahmad - - -

Regards.

↓ coding.



o same key.

o eg. 64 . it's can be 128bit - - .

**Confusion:-**

Refer to make relationship between ciphertext and key as complex as possible "change one bit in key completly change cipher text". "-تحقق بواسطة ال XOR".

**Diffusion:-**

Dissipating the statistical structure of the plain text over bulk of ciphertext.

"the relationship between the message and the cipher text".

notes about otp:-

to be perfect secrecy the key lenght should be equale to the message, and it's should be use one time only, Finally it's not allowed to be $\underline{\underline{0}}$.

b/z the ciphertext become same as the message

$0 \otimes M = M$

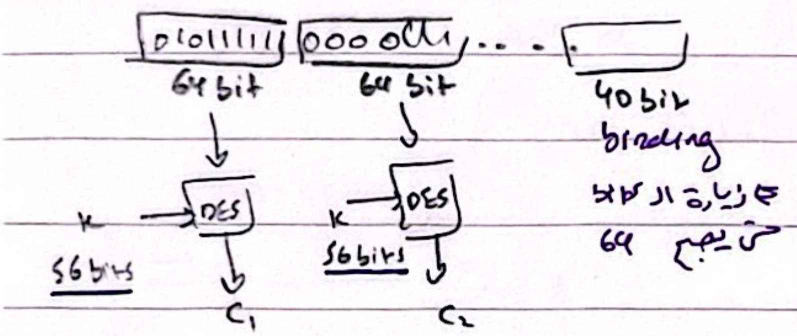
Sender                                                                 Reseuer.

game1 / App layer.

HI Hada. I will...

↓

coding.



Block encryption.

. DES "Data encryption standard"

. AES
↓
Advance.

"not CPA secure"

ع لأنه عند ادخال المسج وهو
يحتوي على blocks متشابهة ينتج
نفس ال cipher text.

o the same key for all blocks.

=> key space = $2^{56}$

o ليس رقم كبير جداً على بعض الاجهزة
وبالتالي يمكن الحصول عليه ركى ابسح.

"not secure"

CPA secure: "chosen-plaintext attacks."

o the symmetric cipher must not be
vulnerable to chosen plaintext attacks.
عرضة

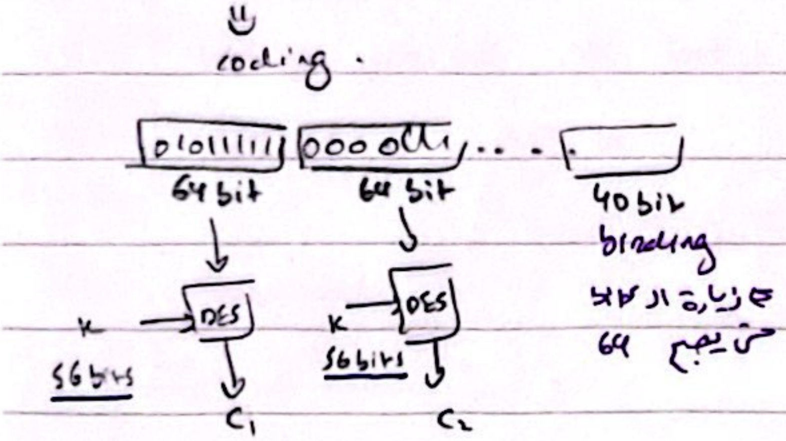
CCA secure: "chosen-ciphertext attacks".

o is an attack model for cryptanalysis where
the cryptanalyst can gather info by obtaning the
decryption of chosen cipher text.

Sender                                        Resever.

gamil / App layer.

HI Hada. I will. . .



Block encryption:

- DES "data encryption standard"
- AES
  Advance.

"not CPA secure"

لأنه عند ادخال المسج وهو يحتوي على blocks متشابهة ينتج نفس ال-cipher text.

=> key space = $2^{56}$

وليس رقم كبير جداً على بعض الأجهزة وبالتالي يمكن الحصول عليه وكلى ابيح.

"not secure"

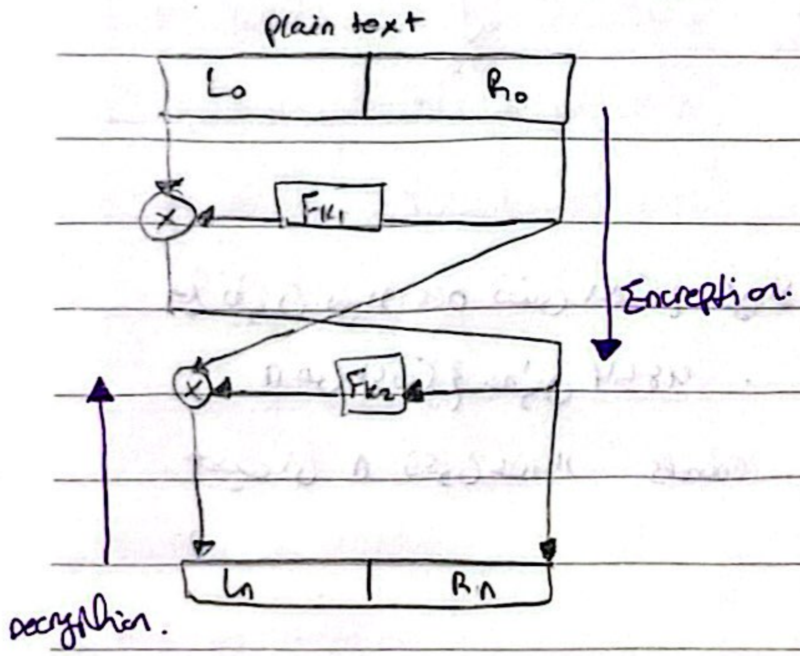
- the same key for all blocks.

From tese pieces of info the adversary can attempt to recover the hidden secret key used for decryption.

## Feistal

- PRP "input bits = output bits" .
- the first impliminatetion about the block cipher but not one of it's basics .
- DES ✓ AES α .

⇐ كل ما زاد عدد ال Round يكون أكثر أمان



note:

- transposition:

تغير أماكن الداتا .

- permotation:

تغير أماكن ال bits .

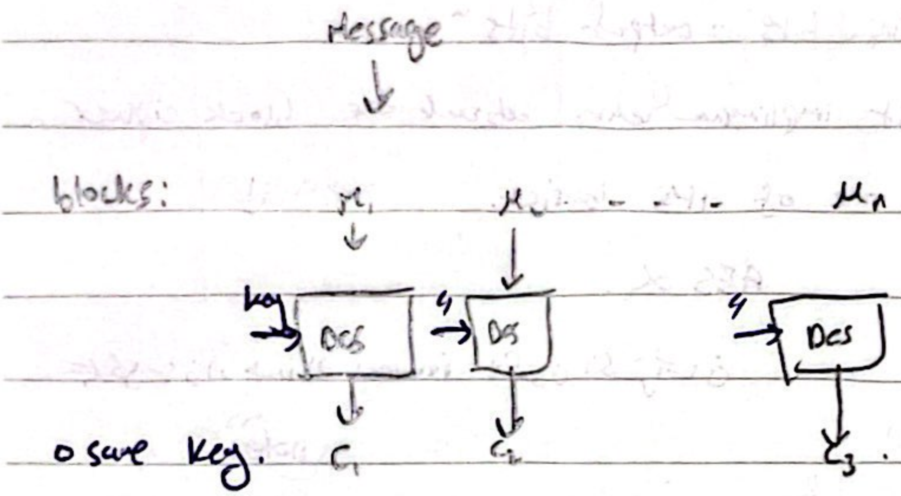
**one cycle Encreption:**

1) Split the plain text into 2 halves.
2) $L_1 = R_0$
3) $R_1 = L_0 \otimes f_k(R_0)$ .

**one cycle Decreption:**

1) $R_0 = L_1$
2) $L_0 = R_1 \otimes f_k(R_0)$ .

## DES:



- same key.

56 bit .

Key space $2^{56}$ .

ع يكون في ال DES نفس المفتاح لكل ال blocks ولكن عند دخوله يتحول لـ

n من المفاتيح بطول 48 bit .

حيث ان n تكون عدد ال rounds .

## AES:

- non - Feister.

**Note:-**

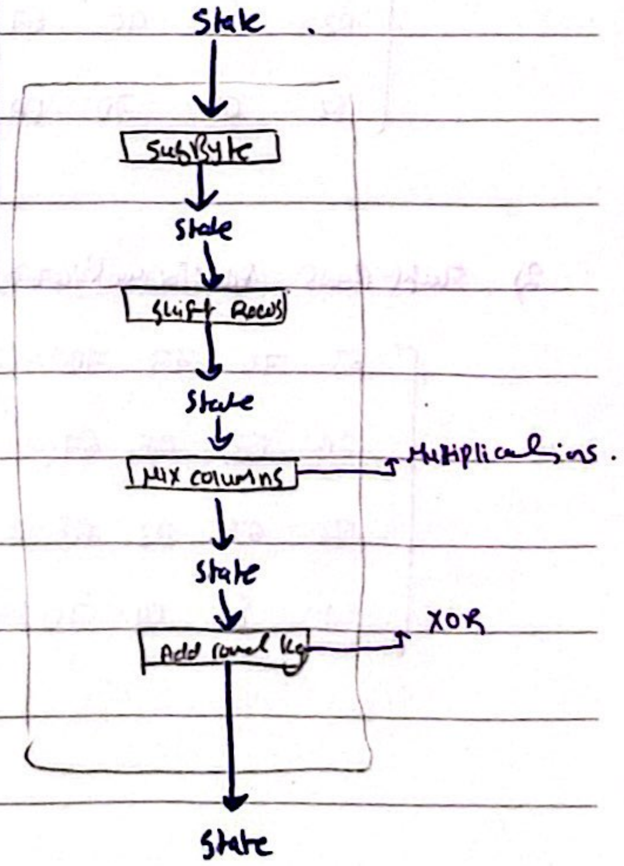
there are 3 versions:-

10 rounds . 128 bit for key

12 rounds 192 bit for key

14 rounds . 256 bit for key

- each word has 4 byte when the byte is 8 bit.
- 128 bit it's 16 byte.
  4 words.
- block ≡ state .
  so it's 16 byte too.



* SubBox ⇒ Diffusion.

* AES ⇒ confusion.

Example:-

$$\begin{bmatrix} 00 & 01 & 02 & 03 \\ 0A & 0B & 0C & 1B \\ 1A & 1B & 1C & 0A \\ 11 & 12 & 13 & 14 \end{bmatrix}$$

1) SubBox transformation:

$$\begin{bmatrix} 63 & 7C & 77 & 7B \\ 67 & 2B & FE & AF \\ A2 & AF & 9C & 67 \\ 82 & C9 & 7D & FA \end{bmatrix}$$

2) Shift Rows transformation:-

$$\begin{bmatrix} 63 & 7C & 77 & 7B \\ 2B & FE & AF & 67 \\ 9C & 67 & A2 & AF \\ FA & 82 & C9 & 7D \end{bmatrix}$$

**Mix columns:**

$$\begin{bmatrix} D4 & 01 & 03 & A0 \\ BF & A0 & 01 & A1 \\ 5D & B1 & 21 & B1 \\ 30 & B2 & 23 & B3 \end{bmatrix} \times \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

the state after shift rows.

constant matrix.

$$= \begin{bmatrix} \underline{\underline{r_0}} & r_4 & r_8 & r_{12} \\ r_1 & r_5 & r_9 & r_{13} \\ r_2 & r_6 & r_{10} & r_{14} \\ r_3 & r_7 & r_{11} & r_{15} \end{bmatrix}$$

$\Rightarrow \boxed{r_0} = (02 \times D4) + (03 \times BF) + (0.1 \times 5D) + (01 \times 30)$

$r_1 = (01 . D4) + (02 . BF) + (03 . 5D) + (01 \times 30)$

$r_2 = (01 . D4) + (01 . BF) + (02 . 5D) + (0.3 . 30)$

$r_3 = (03 . D4) + (01 . BF) + (01 . 5D) + (02 . 30)$ .

$r_4 = (02 \times D1) + (03 . A0) + (01 \times B1) + (01 \times B2)$

and so on...

$$\Rightarrow r_0 = (02 \cdot d4) + (03 \cdot bf) + (01 \cdot \overset{5d}{5d}) + (01 \cdot \overset{30}{30}) = 6d \oplus 64 = 4$$

$\oplus$ $\oplus$ 01011101 $\oplus$ 00110000

- $02 \cdot \underline{\underline{d4}}$

$\boxed{02}$ . ①1010100 . = 10101000 xor 1B .

xor

00010011

10110011 .

- ③·bf

⇐ عند الضرب بـ 02 نزيل آخر منزلة من الشمال، وإذا كانت 1 نعمل shift ونضع 0 من اليمين بدل الواحد . بعدين نعمل xor مع 1B . وعندما يكون 0 نعمل الshift بدون xor مع 1B .

01 xor 10 = (01 · bf) xor ($\overset{02}{\boxed{10}}$ bf)

① $\boxed{bf}$

bf ⇒ ①0111111

0111110 xor 1B

xor

00011011

② $\boxed{= 01100101}$

now XOR 1 and 2 .

01100101

xor

10111111

11011010

$\Rightarrow r_1 = (01.d4) \oplus (02.bf) \oplus (03.5d) \oplus (01.30) = 0x\ A6$

$11010100 \quad \oplus \quad\quad \oplus \quad\quad \oplus \; 00110000$

$\Rightarrow 02.\underline{bf}.$

$\downarrow$

$\textcircled{1}0111111 \Rightarrow 10111110 \text{ xor } 1B.$

xor

$\underline{00011011}$

$\Rightarrow 10100101$

$\Rightarrow 03.5d = (01.5d) \oplus (10.5d).$

$5d \oplus \overset{x}{(10.5d)}$

$\hookrightarrow 02.\underline{5d}$

$\downarrow$

$\textcircled{0}1011101 \Rightarrow 10111010.$

o now $x \oplus 5d.$

$1011\ 1010$

xor

$0101\ 1101$

$\Rightarrow 1110\ 0111$

$\Rightarrow (63 \cdot 02) \oplus (F2 \cdot 03) \oplus (7D \cdot 01) \oplus (D4 \cdot 01) \cdot = 0x62$

$\oplus \qquad \oplus\ 01111101 \oplus 11010100$

$\Rightarrow 02 \cdot \underline{63}$

↓

0110 0011 ⇒ 1100 0110 "C6"

$\Rightarrow 03 \cdot F2 = (01 \cdot F2) \oplus (10 \cdot F2)$

$F2 \oplus (10 \cdot F2)$

↳ $02 \cdot F2$

↓

1111 0010 = 1110 0100 xor 1B

xor 0001 1011

1111 1111

o now $F2 \oplus FF$

1111 1111

xor

1111 0010

0000 1101 "0D"

$$\begin{bmatrix} B4 \\ 52 \\ E0 \\ AE \end{bmatrix} \cdot [0D, 09, 0E, 0B]$$

$\Rightarrow (B4.0D) \cdot (52.09) \cdot (E0, 0E) + (AE, 0B)$

1) B4. 0D

1011 0100 0000 1101

$(x^7 + x^5 + x^4 + x^2) \cdot (x^3 + x^2 + 1)$

$x^{10} + x^9 + \cancel{x^7} + x^8 + \cancel{x^7} + \cancel{x^5} + \cancel{x^7} + x^6 + \cancel{x^4} + \cancel{x^7} + \cancel{x^5} + \cancel{x^4} + x^2.$

---

$x^{10} + x^9 + \cancel{x^7} + x^8 + \cancel{x^7} + \cancel{x^5} + x^7 + x^6 + \cancel{x^4} + \cancel{x^5} + \cancel{x^4} + x^2.$

$(x^8 \cdot x^2) + (x^8 \cdot x) + x^8 + x^7 + x^6 + x^2.$

$(x^4 + x^3 + x + 1).x^2 + (x^4 + x^3 + x + 1).x + x^8 + x^7 + x^6 + x^2$

$\cancel{x^6} + \cancel{x^5} + x^3 + \cancel{x^2} + \cancel{x^5} + \cancel{x^4} + \cancel{x^2} + \cancel{x} + \boxed{x^8} + x^7 + x^6 + x^2$

$\cancel{x^4} + \cancel{x^3} + \cancel{x} + 1$

$= \boxed{1000\ 0101}$

2) 52 . 09

0101 0010 0000 1001

$(x^6+x^4+x).(x^3+1)$

$x^9+x^6+x^7+\cancel{x^4}+\cancel{x^4}+x$

$\downarrow$

$(x^8.x) = (x^4+x^3+x+1)x = x^5+x^4+x^2+\cancel{x}$

$= \boxed{1111\ 0100}$

3) E0 . 0E

1110 0000 0000 1110

$(x^7+x^6+y^5).(x^3+x^2+x)$

$x^{10}+\cancel{x^9}+x^8+\cancel{x^9}+\cancel{x^8}+\cancel{x^7}+\cancel{x^8}+\cancel{x^7}+\cancel{x^6}$

$\downarrow \qquad \downarrow$

$x^8.x^2 \qquad x^4+\cancel{x^3}+x+1$

$\downarrow$

$(x^4+x3+x+1).x^2 = \cancel{x^6}+x^5+\cancel{x^3}+x^2$

$= \boxed{0011\ 0111}$

4) AE . 0B

1010 1110 0000 1011

$(x^7+x^5+x^3+x^2+x).(x^3+x+1)$

$x^{10}+\cancel{x^6}+x^7+\cancel{x^8}+\cancel{x^6}+\cancel{x^5}+\cancel{x^6}+\cancel{x^4}+\cancel{x^3}+\cancel{x^5}+\cancel{x^3}+\cancel{x^2}+\cancel{x^4}+\cancel{x^2}+x$

$\downarrow$

$(x8.x^2) = (x^4+x3+x+1).x^2 = x^6+x^5+x^3+x^2$

$= \boxed{1110\ 1110}$

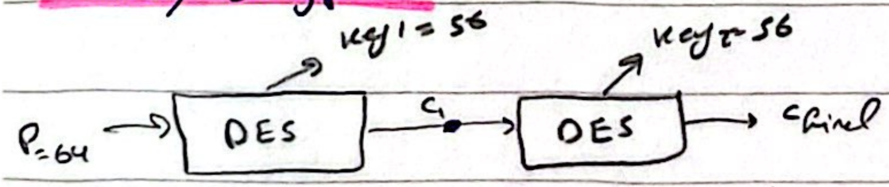
Q: the largest version of AES 256 bit key, How many keys whould have to be searched per second in order for brute for ue attake to break AES in a year?

- total num of keys: $2^{256}$
- number of second per year: $365 \times 24 \times 60 \times 60 = 31536000$ sec.
- number of searched per second to finish the task in a year:

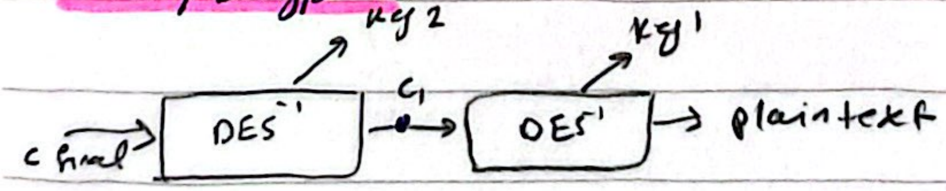
$$\frac{2^{256}}{3136000} = 3.67 \times 10^{69}.$$

← صعب على ال attaker ان يجرّب النص ك brut fors att- ، بيكون من الممكن
ان يحصل عليه عن طريق الاحتمالات .

2DES / Encryption:



2DES / Decryption:

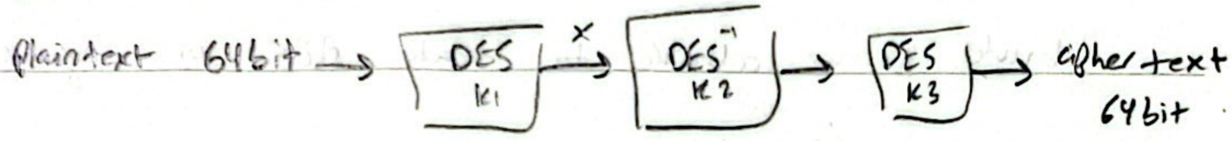


- Man in the Meddle.

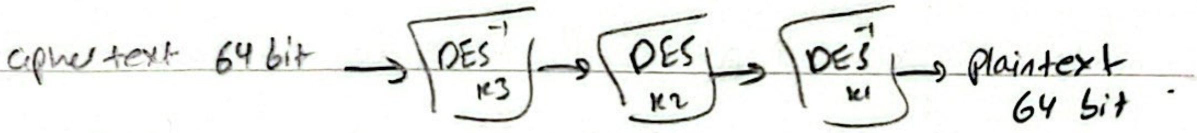
key space = $2^{56} \times 2 = 2^{57}$.

## 3 DES:-

Sender:



Receiver:-



⇐ بطيء .

key space $2^{168}$.

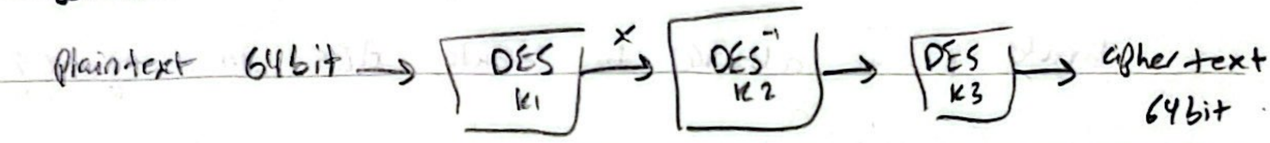
**Security:-**

2DES: its vulnerable to attakes as the effective key length is only 56 bits, which is insufficient for modern security needs.

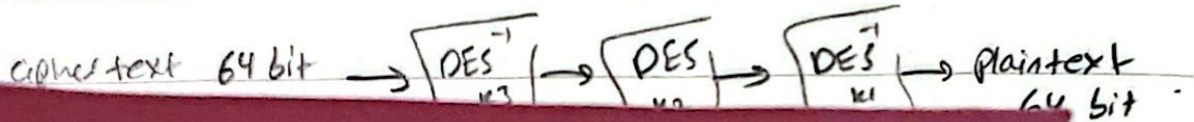
3DES: its more secure than 2DES but it's slower ↓ coz it applies the DES 3 times with three diffent key.

## 3 DES:-

Sender:



Receiver:-



. ⇐

ey space $2^{168}$.

**Implementation:-**

the implementation of 2DES is simpler compared to 3DES cuz its require two roundss of DES. 3DES use three rounds with 3 different keys thats mean its More secure but its more computational resources and slower than 2DES.

## why we use IV in CBC:

In summary, the IV in CBC mode plays a crucial role in introducing randomness and preventing error propagation, thereby enhancing the security and reliability of the encryption process.

## collision and one-wayness:

In summary, collision resistance implies one-wayness because finding a pre-image efficiently whould allow an attacker to find collisions efficiently, which contradicts the definition of collision resistance. However, one-wayness alone does not guarantee

CBC is secure if we used with a secure encryption algorithm like AES, and each IV should be unique for each encryption operation with the same key.

collision resistance because it only focuses on the difficulty of finding specific pre-images and does not directly address the possibility of finding collisions.

# Diffie Hellman (D-H) key exchange.

| Alice (S) | Public change. | Bob (R). |
|---|---|---|
| key: a=4 | Alice and Bob agree on | key: b=3 |
| "secret key" | public parameters. | "secret key". |
| Alice cobines her | p=23 "prime num" | "Same as Alice" |
| secret key (a) with | g=5 "generator" | $5^3$ mod 23 = 10 |
| the paramete | "clear info for attaker" | |
| and send this result | 10<br>. the prime num and | |
| "public key" to bob. | the generator should | |
| $A = 5^4$ mod 23 = 4 | be very large. 4 | bob |
| $p.k = g^a$ mod p. | | |
| $10^4$ mod 23 = $\boxed{18}$ | | $4^3$ mod 23 = $\boxed{18}$ |
| share key. | | |

=> the secret key "a or b in this example" should be less than (p-1) and greater than 1. $1 \leq secret.k \leq p-1$

في حال دمجوا " public key معا، attacker لا يستطيع معرفة

" secret key لانها ليست عملية خطية، من الصعب ارجاع

الناتج.

note: the prime number should be very large P> 1024 bit, which will be very hard to analizig by the attaker.

## Generator:-

$\textcircled{2}$ is generator of mod $\textcircled{13}^{n}$.

$2^1 = 2$ mod $13 = 2$

$2^2 = 4$ mod $13 = 4$

$2^3 = 8$ mod $13 = 8$

$2^4 = 16$ mod $13 = 3$

$2^5 = 32$ mod $13 = 6$

$2^6 = 64$ mod $13 = 12$

$2^7 = 128$ mod $13 = 11$

$2^8 = 256$ mod $13 = 9$

$2^9 = 512$ mod $13 = 5$

$2^{10} = 1024$ mod $13 = 10$

$2^{11} = 2048$ mod $13 = 7$

$2^{12} = 4096$ mod $13 = 1$

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ Yes, it's a generator of 13.

ال set تكون عبارة عن أرقام متسلسلة

من 1-(n-1) ، غير ذلك يكون not generator.

Summary :-

Step 1 : Alice and bob get public parameters

$p = 23$ and $g = 9$

g should be generator of p.

Step 2: Alice selected private key $a = 4$

and bob " " " $b = 3$

Step 3: Alice and bob compute public values .

Alice : $x = g^{\overset{a}{4}} \bmod p = 6$

Bob : $y = g^{\overset{b}{3}} \bmod p = 16$

Step 4: Alice and Bob exchange public numbers.

Step 5: Alice resive 16, bob resive 6 .

Step 6: Alice and Bob compute shared key = 9

$\boxed{y^a \bmod p = x^b \bmod p = 9}$

## RSA:

1) choose two large prime numbers p and q.

2) compute $n = p * q$

3) compute $\phi = (p-1) * (q-1)$

4) choose large number $\underline{\underline{e}}$ : $GCD(\overset{\text{co-prime}}{e}, \phi) = 1$

public-key.

5) compute $\underline{\underline{d}}$. privite key.

$e.d = 1 \bmod \phi$

$\boxed{d = e^{-1}} \Rightarrow d = e^{-1} \bmod \phi$

- (e,n) public
- (d,n) privire.

⇒ Encryption = $m^e \bmod n$

Decryption = $c^d \bmod n$

---

Alice

- $p = 5,\ q = 11$
- $n = 55$
- $\phi = 40$
- choose e ⇒ $GCD(e, 40) = 1$ ↓ 17

public key = (17,55) →

Bob

$M = 37$

↓

$C = 37^e \bmod n$

$C = 37^{17} \bmod 55$

$= \boxed{27}$

the ciper text

- $d = e^{-1} \bmod \phi$

$= 17^{-1} \bmod 40$

$= 33$

$DEC = 27^d \bmod n$

$= 27^{33} \bmod 55$

$= 37$

$\Rightarrow 17^{-1} \bmod 40$

$GCD(40, 17) \Rightarrow$

$40 = 2(17) + 6$

$17 = 2(6) + 5$

$6 = 5 + 1 \quad \Longrightarrow \quad 1 = 6 + 5(-1)$

$1 = 6 + \big(17 - 6(2)\big)(-1)$

$1 = 6 + 17(-1) + 6(+2)$

$1 = 6(3) + 17(-1)$

$1 = [40 - 17(2)](3) + 17(-1)$

$1 = 40(3) + 17(-6) + 17(-1)$

$1 = 40(3) + 17(-7)$

$\downarrow$

$40(3) \bmod 40 = 0$

$1 = 17(-7) \Rightarrow \frac{1}{17} \bmod 40 = -7 \bmod 40$

$\therefore 17^{-1} \bmod 40 = 33$

# RSA, digital signature.

| Sender | Receiver. |
|---|---|
| $p, q$ | $p \cdot q$ |
| $n = p \cdot q$ | $n = p \cdot q$ |
| $\phi = (p-1)(q-1)$ | $\phi = (p-1)(q-1)$ |
| $GCD(e, \phi) = 1$ | $GCD(e, \phi) = 1$ |
| $(e_s, n_s)$ public key | $\boxed{(e_R, n_R)}$ public key. |
| $(d_s, n_s)$ privite key | $d = e_R^{-1} \bmod \phi$ |
| $C = M^{e_R} \bmod n_R$ | $\boxed{(d_K, n_k)}$ privite key. |
| $S = M^{d_s} \bmod n_s$ | |
| $(C, S)$ → | $M = C^{d_R} \bmod n_R$ |

$$\begin{tikzcd} (C,S) \arrow[r] & M = C^{d_R} \bmod n_R \\ (C,S) \arrow[u] \arrow[d] & \\ M` = S^{e_s} \bmod n_s & \end{tikzcd}$$

$\Rightarrow$ M and M` should be the same.

in short:-

Directory.

$(Pu_A, Pu_B)$

Alice $(Pu_A, Pr_A)$ Bob $(Pu_B, Pr_B)$

$Pu_B = (e_B, n_B)$

so, $C = M^{e_B} \bmod n_B$ "non-repudation".

$S = M^{Pr_A} \bmod n_A$.

$\{c, s\} \longrightarrow$ DES

$c$

$M' = S^{e_A} \bmod n_A$

$=$

$M = C^{d_B} \bmod n_B$

Example: $p = 47$, $q = 59$. find $d$.

$n = (47.59) = 2773$.

$\phi = (46.58) = 2668$

$e \Rightarrow GCD(e, \phi) = 1$ "it's can be 17".

$\Rightarrow GCD(2666, 17)$

$2666 = 17(156) + 16$ $\Rightarrow$ $1 = 17 + 16(-1)$

$17 = 16 + 1$

$1 = 17 + [2668 + 17(-156)](-1)$

$1 = 17 + 2668(-1) + 17(156)$

$1 = 2668(-1) + 17(157)$.

$\Rightarrow 2668(-1) \bmod 2668 = 0$

$\Rightarrow \frac{1}{17} \bmod 2268 = 157 \bmod 2268 = \underbrace{\boxed{157}}_{d}$

Example!- Alice uses RSA signalure with $p=13$, $q=23$

and the verifecation expont $e = 53$

what is Alice private signing key?

Alice sign digise documat $D = 100$ .

what is the signalure?

$\phi = 12 \cdot 22 = 264$ , $n = 299$

$53^{-1} \bmod 264 \Rightarrow$

o GCD (264, 53)

$264 = 53(4) + 52$

$53 = 52(1) + 1$

$\Rightarrow$ $1 = 53 + 52(-1)$

$1 = 53 + [264 + 53(-4)](-1)$

$1 = 264(-1) + 53(5)$

$264(-1) \bmod 264 = 0$

$\frac{1}{53} = 5 \bmod 264 = \underline{\underline{5}}$

$\Rightarrow$ $100^5 \bmod 299$

Q: Alice and Bob use the Diffie-Hellman algoritum to exchange a secret key. Eve intercepts the following values $q = 283$, $g = 12$, $Y_A = 77$ and $Y_B = 196$. where g is a primitive root of the prime number q. $Y_A$ is Alice's public key and $Y_B$ is Bob's public key. compute shared secret key (k).

Alice privite key is $x_A$ $1 \leq X_A < 282$.

and her public key is $g^{x_A} \bmod q = Y_A$

$12^{x_A} \bmod 283 = 77$

$\Rightarrow 12^1 \bmod 283 = 12$ ✗

$12^2 \bmod 283 = 144$ ✗

$12^3 \bmod 283 = 30$ ✗

$12^4 \bmod 283 = 77$ ✓

so, Alice's privite key is 77 ...

therefore, sherd key is $(Y_B)^{X_A} \bmod q$

$(196)^4 \bmod 283 = \boxed{90}$

## Elgamal - Encryption:

1) obtain public key $(\overset{B.K}{\beta}, \overset{p}{p}, \overset{g}{\alpha})$ from receiver.

2) choose an Integer $i$, $i \in [2, \dots, p-2]$ private key

3) compute $K_E = \alpha^{i} \bmod p$ , $K_E$ public key.

4) compute $K_M = \beta^{i} \bmod p$ shared key.

5) Represent plain text as an integer $x$.

6) compute cipher text $Y = X \times \underset{\text{shared key}}{K_M} (\bmod p)$.

7) send $(Y, \underset{\text{public key}}{K_E})$ to BOB.

i ⇒ the private key should be different each $\underset{\text{plain text}}{\underline{\text{encryption}}}$.

## Decryption:

1) obtain ciphertext and EK $(Y, K_E)$ from sender.

2) compute $K_M = K_E^{d} \bmod p$. shared key.

3) Recover plain text $X = Y \cdot K_M^{-1} \bmod p$.

$X = Y \cdot K_E^{p-1-d} \bmod p$.

⇒ public key set : $(\underset{\text{public key}}{\beta}, \underset{\text{prime}}{p}, \overset{gen}{\alpha})$

Q: Alice and Bob use the Elgamal algoritum. Alice chooses a prime number $q=107$ and $\alpha=2$ as primitive root of q. she select her private key $X_A = 67$.

i) what is Alice's public key.

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

$= 2^{67} \bmod 107$

$= 94$

∴ Alice public key is (107, 2, 94)

ii) Bob wants to encrept a message $M=66$ and sends it to Alice. He chooses a random integer $k=45$. which is the encrepted message.

Shared key ⇒ $94^{45} \bmod 5 = 5$.

$C1 \Rightarrow 2^{45} \bmod 107 = 28$

$C2 \Rightarrow KM \bmod q = 5 \cdot 66 \bmod 107$

$= 9$

∴ the encrepted message is $(C1, C2) = (28, 9)$

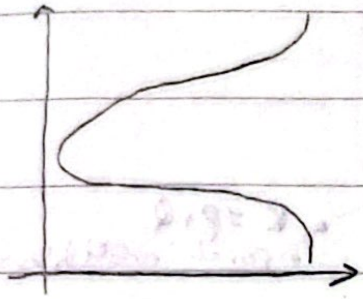
Q: Suppose Alice and Bob wish to do Diffie-Hellman Key excharge. Alice and Bob have agreed upon a prime p=15, and generator g=2. Alice has chosen her private exponent to be a=5. while Bob has chosen his private exponent to be b=4. unknown to Alice and Bob, Eve is listening and is able to intercept their messages as will as inject her own messages. Suppose Eve chooses an exponent e=7. Explain how Eve can use e to perform the Intruder-in-the-middle attack on the Alice-Bob Diffie-Hellman key exchage.

| Alice | Eve | Bob. |
|---|---|---|
| $a=5$ | $e=7$ | $b=4$ |
| $Y_A = g^a \bmod q$ | $Y_E = 2^7 \bmod 13$ | $Y_B = 2^4 \bmod 13$ |
| $= 2^5 \bmod 13 = 6$ | $= 11$ | $= 3$ |
| $K_{AE} = 11^5 \bmod 13$ | $K_{EA} = 6^7 \bmod 13 = 7$ | $K_{BE} = 11^4 \bmod 13$ |
| $= 7$ | $K_{EB} = 3^7 \bmod 13 = 3$ | $= 3$ |

⇒ what is the difficulty of computing discrete logarithms?

The Discrete logarithm problem is considered to be computationally intractable. that is, no efficient classical algorithm is known for computing discrete logarithms in general. A general algorithm for computing " $\log_b a$ " in finite groups G is to raise b to larger and larger powers k until the desired a is found.

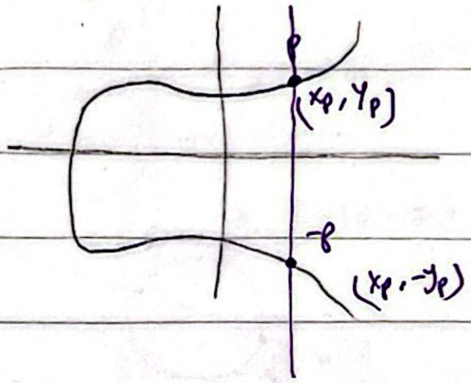
# Elliptic curve crypto ECC.



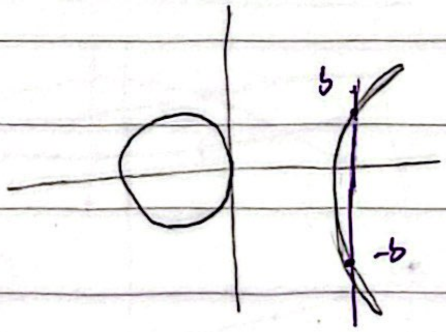
elliptc. "كيرف متقابل".

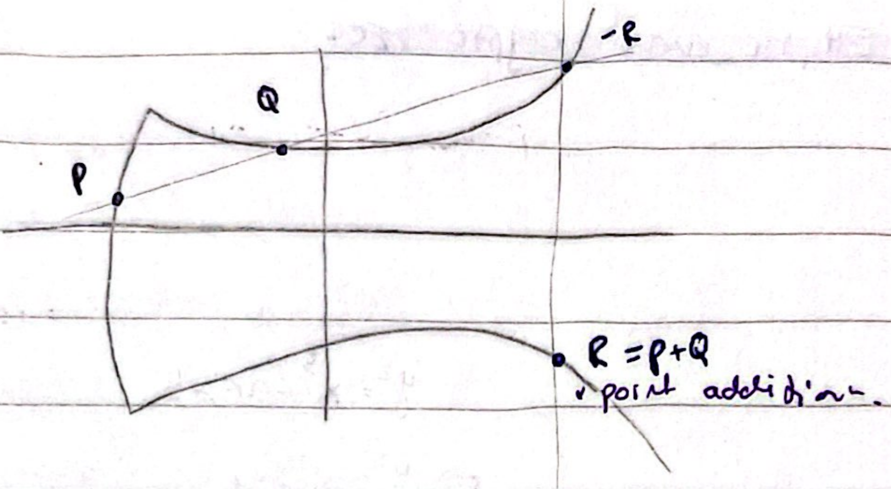
$y^2 = x^3 + ax + b$ (#of curve ∞)

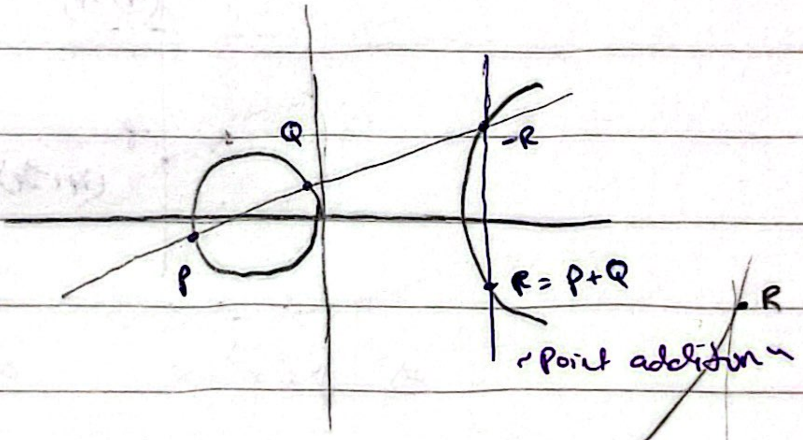
$\Rightarrow y^2 = x^3 - x + 1$ "$a=-1, b=1$".



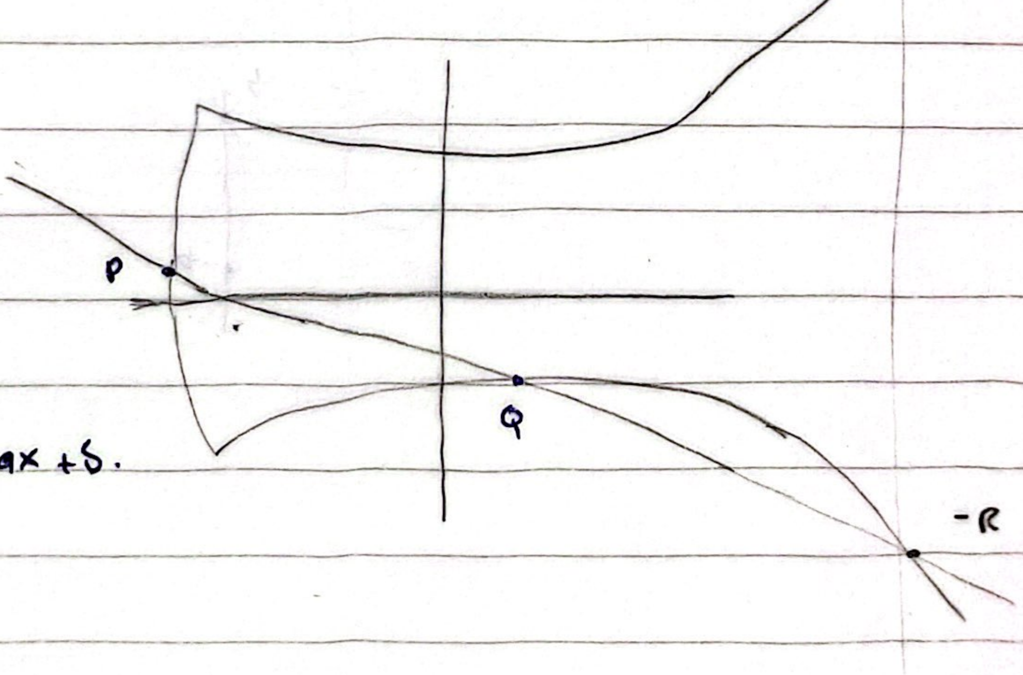
$\Rightarrow y^2 = x^3 - x$ "$a=-1, b=0$"



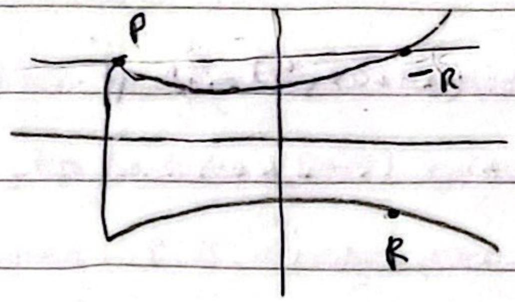




P+Q

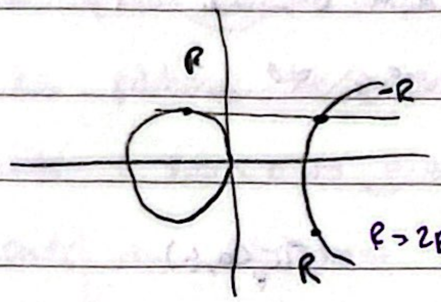


$y^2 = x^3 + ax + b.$



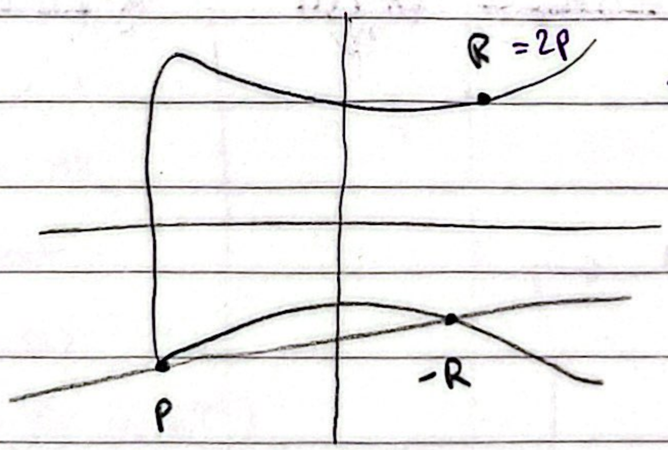
$\boxed{R = 2P}$

point multiplication



R = 2P = P+P

"point mult."



"point mult."

$y^2 = x^3 + \textcircled{a}x \textcircled{+b}.$

we just change this var.

$y^2 \bmod p = (x^3 + ax + b) \bmod p$.

$y^2 \bmod 23 = (x^3 + x + 1) \bmod 23$

$p = 23$ , $a = 1$ , $b = 1$

$ECC_{23}(1,1)$ . $ECC_p(a,b)$ .

Y and x from $0 - \boxed{22}$ $p-1$

# of curves $\Rightarrow \infty$

| Sender | $ECC_p(a,b)$ . | Receiver . |
|---|---|---|
| $y^2 \bmod 23 = (x^3 + x + 1) \bmod 23$ | $ECC_{23}(1,1)$ . | $y^2 \bmod 23 = (x^3 + x + 1) \bmod 23$ |

Q: Alice wants to send two messages M-1 and M-2 to Bob, but they do not share symmetric key.

Assume that p is a large prime and that g is a generator mod p. Assume that all computations are done modulo p in scheme A.

Scheme A: Bob publishes his public key $B = g^b$. Alice randomly selects r from 0 to (p-2).

Alice then sends the ciphertext (R, S1, S2)

$(g^r, M\text{-}1 \times B^r, M\text{-}2 \times B^{r+1})$.

Alice

M1 and M2

↓

cipher text.

(R, S1, S2)

$(g^r, M1 \cdot B^r, M2 \cdot B^{r+1})$

Bob

$B = g^b$.

1) Decryption for $\boxed{M1}$ →

$M_1 = S1 \cdot B^{-r}$

$= S1 \cdot (g^b)^{-r}$

$= S1 \cdot (g^r)^{-b}$

$\boxed{= S1 \cdot R^{-b}}$

2) decryption for $\boxed{M2}$ → $S2 = M_2 \times B^{r+1}$

$M2 = S2 \cdot (B^{r+1})^{-1}$

$M2 = S^2 \cdot B^{-r} \cdot B^{-1}$

$\Rightarrow B^{-r} = R^{-b}$

$\Rightarrow B^{-1} = \frac{1}{B}$

so, $M2 = S2 \cdot R^{-b} \cdot \frac{1}{B}$

Q: $(n,e) = (1255, 3)$ . Find private key $d$.

$n = p.q$

$= 251 . 5$

$\phi = 250 . 4 = 1000$ .

$d = e^{-1} \bmod \phi$

$= 3^{-1} \bmod 1000$

$= 667.$

$1000 = 3(333) + 1$

$1 = 1000 + 3(-333)$

$\frac{1}{3} = -333 \bmod 1000.$

$\therefore 3^{-1} \bmod 1000 = 667.$

## ECC cont.:-

$y^2 \bmod 5 = x^3 + x + 1 \bmod 5$

$P = (4,2)$ $(x_P, y_P)$

$Q = (2,4)$ $(x_Q, y_Q)$

$R = (P + Q)$ $(x_R, y_R)$

$x_R = (\lambda^2 - x_P - x_Q) \bmod \boxed{p}$ → 5 in this example.

$y_R = (\lambda(x_P - x_R) - y_P) \bmod \boxed{p}$

where

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} \bmod p & P \neq Q \\[2ex] \dfrac{3x_P^2 + a}{2y_P} \bmod p & P = Q \end{cases}$$

$P = (4,2)$ $Q = (4,2)$

$\boxed{P = Q}$

- $\lambda = \dfrac{3 \cdot 16 + 1}{2 \cdot 2} \bmod 5 = 1$

- $x_R = ((1)^2 - 4 - 4) \bmod 5 = -7 \bmod 5 = 2$
- $y_R = (1(4-3) - 2) \bmod 5 = -1 \bmod 5 = 4$

$\therefore R$ or $2P = (2,4)$

**Ex:**

$Ecc_{29}(-2, 15)$

$y^2 \bmod 29 = (x^3 - 2x + 15) \bmod 29.$

| | public. | |
|---|---|---|
| Alice | $y^2 \bmod 29 = (x^3 - 2x + 15) \bmod 29$ | Bob. |
| pr $a = \textcircled{3}$ | $P = (4, 5)$ | pr $b = \textcircled{7}$ |
| $\textcircled{3}P = 2P + P$ | | $\textcircled{7}P = 2P + 2P + 2P + P$ |
| $3P = (13, 22)$ | | $7P = (17, 8)$ |
| $(17, 8)$ | | $(13, 22)$ |
| $a \times (17, 8)$ | | $b \times (13, 22)$ |
| $3 \times (17, 8)$ | | $7 \times (13, 22)$ |
| $= (15, 5)$ | | $= (15, 5).$ |

**EX:** when using the RSA algorithm to form a digital signature the output $s = [h[m]]^d$ mod n for suitable hash function h. the message m and s are send to receiver

1) How does the receiver cheack the signature?

$s^e$ mod n = hash..

compute h(m)

2) suppose now that the hash function is not used so the signature simply $m^d$ mod n. show how attaker can constract valid signature.

$s = m^d$ mod n

Attaker choose random signature and compute

$m = s^e$ mod n

$\underline{\underline{s}}$ with random message m existered forgery