A_C
www.wuolah.com/student/A_C

1633

Criptografía Asimétrica.pdf

Apuntes Pesonales: Criptografía Asimétrica

2° Criptografía y Seguridad Informática

Grado en Ingeniería Informática

Escuela Politécnica Superior
UC3M - Universidad Carlos III de Madrid

SECRET KEY DISTRIBUTION USING SYMMETRIC CRYPTOGRAPHY

* Symmetric encryption scheme requires that both sender and receiver share a SECRET KEY
* How to distribute it in a secure way?
* Often system fails because of the key distribution, not because of the weakness of the encryption algorithm.

POSIBILIDADES: distribuir la clave físicamente; si los interlocutores se han comunicado anteriormente, pueden usar la misma clave que usaron para cifrar / crear una nueva clave, etc.

TAMBIÉN... LA UTILIZACIÓN DE:

SESSION KEYS:

- They are temporary keys
- Used for encryption of data between users.
- Used for a single session and then discarded.

MASTER KEYS:

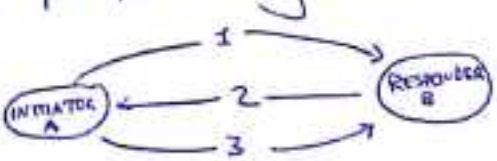
- Used to encrypt the session keys (automatically).
- Shared by user and key distribution center.

* OBJETIVE: two entities share the same secret key.
* PRINCIPLE: change keys frequently.
* HOW TO EXCHANGE A SECRET KEY?

a) Decentralized Key Distribution: manual distribution of master keys between all entities, automatic distribution of session keys.

b) Key Distribution Center (KDC): manual distribution of master keys with KDC, automatic distribution of session keys.

Ver video: https://www.youtube.com/watch?v=lha91MHKKzU



NEWS

WUOLAH

LUN 22 JUL

Noticias para el mundo universitario.

nº 46. Semana del 22 al 28

Viajes y experiencias, los recuerdos más felices.

¿Qué proporciona más felicidad? ¿Un teléfono móvil o una escapada?

Las vacaciones de verano son época de viajes y hoy en día estamos muy concienciados de la gran importancia de vivir las experiencias. Un estudio de los investigadores Paulina Pchelin & Ryan T. Howel del departamento de psicología de la Universidad Estatal de San Francisco (publicado en 2014) concluyó que aquellas personas que emplean su dinero en experiencias en lugar de objetos sienten mayor bienestar. Lo que sentimos positivamente después de comprar un objeto deseado se desvanece rápidamente y, sin embargo, una experiencia nos deja un poso mucho más positivo y duradero: los recuerdos.

Muchas veces no relacionamos que, el tener un móvil de última generación nos puede privar de cualquier otra cosa, como un viaje. El móvil es un aparato que va cambiando y no dura eternamente, pero los momentos vividos con tus amigos estarán ahí para siempre. Lo mismo sucede con la ropa u otros caprichos. Sin duda, los viajes nos dejan experiencias marcadas.

Los recuerdos nos ayudan a revivir experiencias.

Una investigación de las universidades de Birmingham y Bonn en la revista Nature Communications., por B. Staresina y F. Mormann (2019), concluyó que cuando queremos guardar en la memoria las experiencias, las dividimos previamente dependiendo de qué ocurrió, dónde fue, y qué sentimos en ese momento. El cerebro reúne todos estos elementos y archiva la experiencia en nuestra memoria con una determinada coherencia. Incluso incorpora algunos elementos de otros recuerdos similares para darle más precisión al recuerdo guardado. Por ejemplo, si vemos una foto de un fin de semana en la playa, podremos sentir el olor y la brisa del mar.

"Si quieres recordar las experiencias especiales de tu vida, vívelas intensamente y minimiza el hacer fotos y videos para las redes sociales" - Miguel Ángel Rizaldos, psicólogo clínico.

De esta forma de proceder no somos conscientes. Nuestra mente añade elementos informativos para autocompletar, al igual que sucede con los procesadores de texto, que nos ayudan a completar la frase cuando escribimos. Estos elementos añadidos nos facilitan revivir el recuerdo de una experiencia vivida. A nivel neurológico Staresina y Mormann constataron que las neuronas del hipocampo se activan intensamente al recordar una experiencia, al igual que en la corteza entorrinal, cuya función es formar una red amplia tanto para la memoria como para la orientación. Dicho procedimiento se intensifica aún más en ambas regiones del cerebro cuando, además, hay que vincular un elemento físico con el acontecimiento recordado.

En pocas palabras, esto quiere decir que recordar activa las neuronas de un modo muy similar a su activación durante la experiencia real.

¿Las RRSS mejoran o empeoran el recuerdo de lo vivido?

Una investigación de Q. Wang, de la Universidad de Cornell (EEUU) publicada en 2016 concluye que recordamos mejor lo que publicamos online. Si en Facebook, Instagram o en nuestro blog plasmamos nuestras experiencias, será más fácil que posteriormente lo recordemos. Wang argumenta que sería el mismo efecto de llevar un diario o relatar a un amigo lo que hemos experimentado. Los datos mostraron que, después de una o dos semanas, compartir la experiencia en redes sociales tenía una probabilidad mayor de ser recordada pasado el tiempo.

En contraposición a este estudio, encontramos una investigación de la Universidad de Princeton publicada en mayo 2018 en el Journal of Experimental Social Psychology. Esta concluye que el uso de las redes sociales está afectando a nuestra memoria de una manera negativa. El aporte principal de esta investigación es que aquellas personas que comparten sus experiencias en Facebook, Instagram, Twitter y otras redes sociales construyen recuerdos menos precisos de las experiencias vividas.

Durante el estudio, los datos corroboraban que compartir notas, fotos y videos en las redes sociales disminuye un 10% los recuerdos de las experiencias vividas. Algunos investigadores consideran que el problema no se encuentra en las redes sociales, sino en el hecho de enviar la experiencia a las redes sociales en forma de nota, foto o vídeo. De este modo hace que se reste parte de la experiencia original y que la recordemos de manera menos precisa.

Exercise: If we have a network of 1000 users, how many master keys will we need?

NETWORK → 1000

MASTER KEYS → $\frac{1000 * 999}{2}$ = 499.500 master keys we will need. (manually).

SESSION KEYS (at any time) → same nº as master keys 499500 (automatic way) ∴ easy to change.

→ PROBLEM: Too many master keys to distribute manually

SOLUTION: Use a Key Distribution Center (KDC).

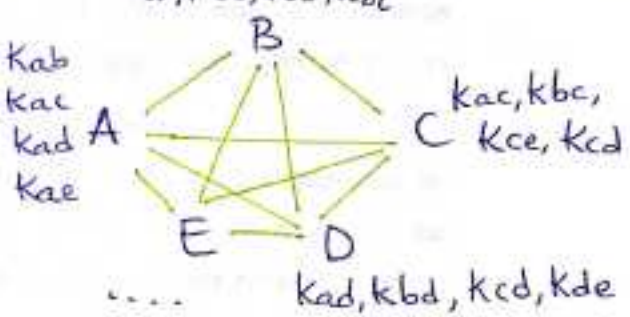
Ver Video ° https://www.youtube.com/watch?v=z42uJ05_Itℓ0 (Q so zero)

→ DEMOSTRATION OF THE SOLUTION:

5 Users DECENTRALISED KD

network → 5 users

master keys → $\frac{5 * 4}{2}$ = 10



5 Users CENTRALISED KD

network → 5 users

master keys → 5

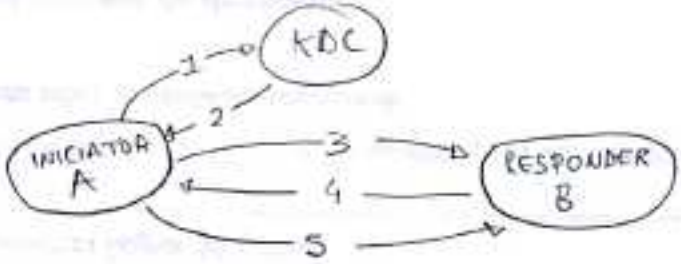
Ka, Kb, Kc, Kd, Ke

Generates the Session key ← KDC

A Ka | B Kb | C Kc | D Kd | E Ke

ADVANTAGE: Far fewer master keys that have to be manually exchanged.

en el video:



Para poder meternos en lo que es la criptografía asimétrica, 1ero tendremos que recordar... ARITMÉTICA MODULAR

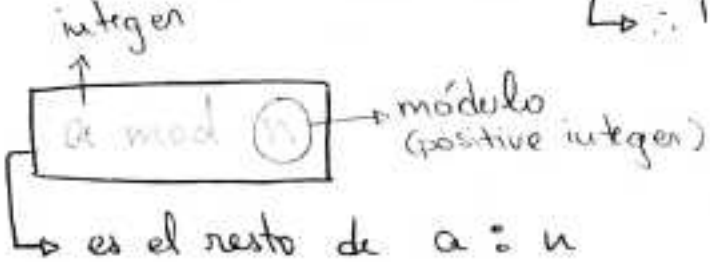
* 2 numbers are relatively prime if its gcd = 1

16	2
8	2
4	2
2	2
1	1
0	

24	2
12	2
6	2
3	3
1	1
0	

15	3
5	5
1	1
0	

$16: 2^4 \cdot 1$
$24: 2^3 \cdot 3 \cdot 1$
$15: 3 \cdot 5 \cdot 1$
$\gcd(16,24) = 2^3 = 8$
$\gcd(16,15) = 1$
$\therefore$ 16 and 15 are relatively primes.



* Two integers a and b are congruent modulo n if $(a \bmod n) = (b \bmod n)$, which is written as $a \equiv b \pmod n$

(12 mod 10, 2 mod 10 & 22 mod 10 are congruent on mod 10 (todos tienen resto 2))

* Modular arithmetic ~~maps~~ performs arithmetic operations within confines of set

$$Z_n = \{0, 1, \dots, (n-1)\}$$

e.g: $X \bmod 10 \Rightarrow Z_{10} = \{0, \dots, 9\}$ → cuando hacemos mod 10, el resultado va a estar siempre entre 0 y 9.

e.g: $13 \bmod 10 = 3$
$13 \equiv 3 \pmod{10}$
$Z_{10} = \{0, \dots, 9\}$

MULTIPLICATIVE INVERSE

Z_8

a	0	1	2	3	4	5	6	7
MI(a)	x	1	x	3	x	5	x	7
		$1 \bmod 8 = 1$		$9 \bmod 8 = 1$		$25 \bmod 8 = 1$		$49 \bmod 8 = 1$

$9, 25 \equiv 49 \bmod 8$

Z_{10}

a	0	1	2	3	4	5	6	7	8	9
MI(a)	x	1	x	7	x	x	x	3	x	9
		$1 \bmod 10 = 1$		$21 \bmod 10 = 1$				$21 \bmod 10 = 1$		$81 \bmod 10 = 1$

ADITIVE INVERSE

Z_{10} $\quad AI_{10}(3) = 7$

$4 + 3 \equiv 7 \bmod 10 = 7$

$4 - 7 \equiv [4 + AI(7)] \bmod 10$

$\equiv [4 + 3] \bmod 10 = 7 \bmod 10 = 7.$

PROPERTIES:

$$[(a \bmod n) \pm (b \bmod n)] \bmod n = (a \pm b) \bmod n$$
$$*$$

cumplen las propiedades ...

- Conmutativa => $w + x = x + w$
- Distributiva => $w \cdot (x + y) = (w \cdot x) + (w \cdot y)$
- Asociativa => $w + (x + y) = (w + x) + y$
- Identidades => $0 + w = w$
- Aditive Inverse

Ejercicios de repaso...

Z_8 $\quad 132 \bmod 8 = [12 \bmod 8 \cdot 11 \bmod 8] \bmod 8 =$

$= [4 \cdot 3] \bmod 8 =$

$= 12 \bmod 8 = 4$

132	2	} 12
66	2	
33	3	
11	11	} 11
1	1	
0		

Z_{13} $\quad 11^7 \bmod 13 = [11^4 \bmod 13 \cdot 11^3 \bmod 13] \bmod 13 =$

$= [((11^2)^2 \bmod 13 \cdot 11^2 \bmod 13 \cdot 11 \bmod 13] \bmod 13 =$

$= [4^2 \bmod 13 \cdot 4 \cdot 11] \bmod 13 =$

$= [3 \cdot 4 \cdot 11] \bmod 13 = 132 \bmod 13 =$

$= 2$

$4^2 = 16$

$16 \mid 13$

$3 \quad 1$

$11 \times 11 + 11 + 11 = 121$

$121 \mid 13$

$04 \quad 9$

$12 \times 11 = 12 + 12 = 132$

$132 \mid 13$

$02 \quad 1$

Relatively prime ...: Euler's totient

Relatively prime with 4 $\Rightarrow \Phi_4 = ?$

$Z_4 = \{0, 1, 2, 3\}$

» $\gcd(4,1) = 1$
$\gcd(4,2) = 2$
» $\gcd(4,3) = 1$

} 2 $\therefore \Phi_4 = 2$

$\Phi_8 = ?$ $Z_8 = \{0, 1, 2, \dots, 7\}$

» $\gcd(8,1) = 1$
$\gcd(8,2) = 2$
» $\gcd(8,3) = 1$
$\gcd(8,4) = 4$
» $\gcd(8,5) = 1$
$\gcd(8,6) = 2$
» $\gcd(8,7) = 1$

} $\Phi_8 = 4$

$\Phi_{35} = \Phi_7 \cdot \Phi_5 = 6 \cdot 4 = 24$

$\Phi_7 = 7 - 1 = 6$

$\Phi_5 = 5 - 1 = 4$

FERMAT'S THEOREM

If "p" is a prime number and "a" is a positive integer, then ... $a^p \equiv a \pmod p = a$

e.g: $3^{\textcircled{5}} \bmod \textcircled{5} = 3$

$3^5 = 243 \;\big|\; 5$
$\quad\;\; 43 \quad 48$
$\quad\;\; 3$

✓

e.g. $3^3 \bmod 3 = 0$

EULER'S THEOREM

for positive integers "a" and "n" ...

$a^{\Phi(n)+1} \equiv a \pmod n = a$

$97^{121} \bmod 143 = 97$ ✓

143	11
13	13
1	1
0	

$\Phi_{143} = \Phi_{11} \cdot \Phi_{13} = 10 \cdot 12 = 120$

$\Phi_{143} + 1 = 121$

Primitive Roots:

$a^i \bmod 7$

$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$

$\varphi = 6$ ($7-1$)

a	a^1	a^2	a^3	a^4	a^5	a^6	
1	1	1	1	1	1	1	
2	2	4	1	2	4	1	
3	3	2	6	4	5	1	«
4	4	2	1	4	2	1	
5	5	4	6	2	3	1	«
6	6	1	6	1	6	1	

} There are the bases of "a" that will give us unique answers

$a^i \bmod 7 = x$

$\text{dlog}_{a,7}(x) = i$

$\therefore$ 3 and 5 are the primitive roots of 7.

Ejercicios:

$\Phi(23) = 23 - 1 = 22$

$149^{133} \bmod 161$ = applying Euler's theorem =

$= 149$

161 | 17
21 | 23
0

161 | 7
23 | 23
1 | 1
0 |

$$\begin{array}{r} 22 \\ \times\ 6 \\ \hline 132 \end{array}$$

$\Phi_{161} = 132$

$d\log_{2,19}(3)$ = discrete logarithm = 8

b	1	2	3	4	5	6	7	8	9	...	18
$\log_{2,19}(b)$	18	1	13	2	16	14	6	3	8		9

Public Key Cryptography: Asymmetric Encryption

* In Public Key Cryptography there are 2 keys: you encrypt with one key and decrypt with a different key.

RSA: Ron Rivest, Adi Shamir & Len Adleman

(1) Generate a key

PRIVATE

a) Chose primes p and q, and calculate $n = p \cdot q$

b) Select "e": $\gcd(\Phi n, e) = 1$ tal que $1 < e < \Phi n$

c) Find $d \equiv e^{-1} \bmod \Phi n$ (*) $d \cdot e \bmod \Phi n = 1$

* In RSA we generate 2 keys from some parameters (one public and another private.)

∴ Every user generates a key-pair:

$PU = \{e, n\}$, $PR\{d, n\}$ p and q are also private.

Public Key — Private Key.

(2) Encryption

Encryption of plaintext "M", where $M < n$:

$C = M^e \bmod n$

* M is going to be an integer *
* e from the receiver *

(3) Decryption

Decryption of ciphertext "C". * d from the receiver *

$M = C^d \bmod n$

Ver Video: https://www.youtube.com/watch?v=t4E-dYLBfsM

RSA SIGNATURE

SIGN: $F(M) = M^{d_{SIGNER}} \bmod n_{SIGNER}$

VERIFY: $M = F^{e_{SIGNER}} \bmod n_{SIGNER}$

⊛ RSA Key Generation EXAMPLE

USER A: $p_A = 13$, $q_A = 23$

① $n_A = p_A q_A = 13 \cdot 23 = 299$

② Calculate $\Phi n_A = \Phi_{13} \cdot \Phi_{23} = 12 \cdot 22 = 264$

③ Select 'e' such as $\gcd(\Phi_{299}, e) = 1$ ∴ they have to be relatively prime; and $1 < e < \Phi n$

Empezamos de menor a mayor

264	2] 4
132	2] 6
66	2
33	3
11	11
1	

1 is relatively prime? Yes, pero ~~1 < 1~~ $1 < \Phi_{299}$

2 is relatively prime? NO

3 is relatively prime? NO

4 is relatively prime? NO

>> 5 is relatively prime? YES ←

∴ $\boxed{e_A = 5}$

$\gcd(\Phi_{299}, 5) = \gcd(264, 5) = 1$

④ Find "d"

$$\begin{cases} d \equiv e^{-1} \bmod (\Phi_{299}) \\ d \equiv 5^{-1} \bmod 264 \end{cases}$$

$e \cdot d \bmod \Phi n = 1$

$5 \cdot d \bmod 264 = 1 \longrightarrow 5 \cdot d = 265 \longrightarrow$

$\longrightarrow d = \frac{265}{5} \longrightarrow$

$\longrightarrow \boxed{d_A = 53}$

$5 \cdot 53 \bmod 264 = 265 \bmod 264 = 1$ ✓

⑤ $PU_A = \{e_A, n_A\}$, $PR_A = \{d_A, n_A\}$

∴ $PU = \{5, 299\}$, $PR_A = \{53, 299\}$

USER B: $p_B = 17$, $q_B = 11$

① $n_B = p_B \cdot q_B = 17 \cdot 11 = 187$

② $\Phi_{187} = \Phi_{17} \cdot \Phi_{11} = 16 \cdot 10 = 160$

③ Select "e"

$$\begin{bmatrix} \gcd(\Phi_{187}, e) = 1 \\ 1 < e < \Phi_{187} \end{bmatrix} \rightarrow \gcd(160, e) = 1$$

160	2
80	2
40	2
20	2
10	2
5	5
1	1
0	

divisores (160) = {1, 2, 4, 5, 8, 16, 32, 10, 20, 40, 80, 160, 32*5 ?}

$\boxed{e_B = 3}$

④ Select "d"

$$\begin{bmatrix} d = e^{-1} \bmod \Phi_{187} = e^{-1} \bmod 160 \\ d \cdot e \bmod \Phi_{187} = 1 \end{bmatrix}$$

$d \cdot 3 \bmod 160 = 1$

$d \cdot 3 = \square$ Necesitamos un entero, por lo que si la división $\frac{\square}{3}$ no da un número entero, le sumamos 160 al $\square$.

$d = \frac{161}{3}$ ×

$d = \frac{321}{3} = 107$ ✓ ∴ $\boxed{d_B = 107}$

⑤ $PU_B = \{3, 187\}$, $PR = \{107, 187\}$

⊛ RSA EXAMPLE: Alice sends a message to Bob

ALICE (A)	BOB (B)
$PU_A = \{e_A = 5, n_A = 299\}$	$PU_B = \{e_B = 7, n_B = 187\}$
$PR_A = \{d_A = 53, n_A = 299\}$	$PR_B = \{d_B = 23, n_B = 187\}$

$M = 8$, $A \rightarrow B$

*ALICE CIFRA CON LAS CLAVES PÚBLICAS DE BOB:

$$C_{AB} = M^{e_B} \bmod n_B$$

$$C_{AB} = 8^7 \bmod 187 = [8^3 \cdot 8^3 \cdot 8] \bmod 187 =$$

$$= [8^3 \bmod 187 \cdot 8^3 \bmod 187 \cdot 8 \bmod 187] \bmod 187 =$$

$$= [138 \cdot 138 \cdot 8] \bmod 187 =$$

$$= 152352 \bmod 187 = 134$$

$$\boxed{C_{AB} = 134}$$

$8 \cdot 8 = 64$

$64 \times 8 = 512$

$512 \div 187 = 2$ (resto 138)

$138 \times 138 = 19044$

$19044 \div 187 = 101$ (resto 134)

*BOB DESCIFRA CON SUS CLAVES PRIVADAS:

$$M = C_{AB}^{d_B} \bmod n_B = 134^{23} \bmod 187 = 8$$

$$\boxed{M = 8}$$

DIFFIE - HELLMAN KEY EXCHANGE ⇒ Sirve para generar claves.

(*) PUBLIC ELEMENTS: q (prime number), α $\forall \alpha < q$ and α is primitive root of q.

(*) USER A KEY GENERATION:

PRIVATE: X_A (a), $\forall X_A < q$ (RANDOM)

PUBLIC: Y_A (A), $Y_A = \alpha^{X_A} \bmod q$, $A = g^a \bmod p$

(*) USER B KEY GENERATION:

PRIVATE: X_B (b), $\forall X_B < q$ (RANDOM)

PUBLIC: Y_B (B), $Y_B = \alpha^{X_B} \bmod q$, $B = g^b \bmod p$

(*) CALCULATION OF SECRET KEY USER A:

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

$$B^a \bmod p$$

(*) CALCULATION OF SECRET KEY USER B:

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

$$A^b \bmod p$$

Both sides have the same K

$K = K_A = K_B$

PARA CIFRAR UN MENSAJE...

Calculate the ciphertext using some encryption algorithm that will need that key.

e.g. $C_1 = E_{AES}(K, M_1)$

PARA DESCIFRAR...

e.g. $M_1 = D_{AES}(K, C_1)$

(*) Diffie-Hellman EXAMPLE.

PUBLIC: $\begin{cases} q = 353 \\ \alpha = 3 \end{cases}$

	A	B
PRIVATE:	① $X_A = 97$	④ $X_B = 233$

PUBLIC: ② $Y_A = \alpha^{X_A} \bmod q$

$Y_A = 3^{97} \bmod 353$

$Y_A = 40$

③ SEND IT TO B

$Y_A = 40,\ q = 353,\ \alpha = 3$

⑤ $Y_B = \alpha^{X_B} \bmod q$

$Y_B = 3^{233} \bmod 353$

$Y_B = 248$

⑥ SEND IT BACK TO A

$Y_B = 248$

$K_A = Y_B^{X_A} \bmod q$

$K_A = 248^{97} \bmod 353$

$K_A = 160$

$K_B = Y_A^{X_B} \bmod q$

$K_B = 40^{233} \bmod 353$

$K_B = 160$

$K_A = K_B = K$

* A and B have shared a secret ($K = 160$)

How to break it?

ATTACKER KNOWS: $q = 353,\ \alpha = 3,\ Y_A = 40,\ Y_B = 248$

$K_A = Y_B^{X_A} \bmod q = 248^{X_A} \bmod 353$

∴ Attacker needs to figure out X_A.

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

$40 = 3^{X_A} \bmod 353$

$X_A = d\log_{3,353}(40)$ ⇒ Problema del logaritmo discreto.

SOLUCIÓN: El Gamal

How to ~~break~~ ATTACK it?

A — public: $\begin{bmatrix} q = 19 \\ \alpha = 3 \end{bmatrix}$ — B

$X_A = 10$

$Y_A = 3^{10} \bmod 19 = 16$

MAN IN THE MIDDLE

$Y_A = 16$ → Attacker → $Y_A = 9$ → $X_B = 11$

$Y_B = 3^{11} \bmod 19 = 10$

Attacker: $X_{ATT_B} = 2$ (RANDOM)

$Y_{ATT_B} = 9$

A

$K_A = Y_B^{X_A} \bmod q$

$K_A = 2^{10} \bmod 19 = 17$

$Y_B = 2$ ← Attacker ← $Y_B = 10$

B

$K_B = Y_A^{X_B} \bmod q$

$K_B = 9^{11} \bmod 19 = 5$

Attacker: $K_B = Y_B^{X_{ATT_B}} \bmod 19 = 5$

$X_{ATT_A} = 7$ (RANDOM)

$Y_{ATT_B} = 2$

$K_A = Y_A^{X_{ATT_A}} \bmod 7 = 17$

A

$C_1 = E_{AES}(17, M_1)$

C_1 → Attacker → C_2 → B

Attacker: $M_1 = D(17, C_1)$

$C_2 = E(5, M_1)$

$M_1 = D(5, C_2)$

EL GAMAL :

(*) Based on the discrete logarithm problem.

(*) PUBLIC ELEMENTS:

p ⟶ VEEEERY large prime number (mayor que 1000 bits / 300 dígitos) so that it is computationally impossible to break it within a lifetime of a person.

α (generator) ⟶ primitive root of p

(*) USER A KEY GENERATOR:

PRIVATE: X_A, $\forall X_A < p \Rightarrow 1 < X_A < p-1$

PUBLIC: Y_A, $Y_A = \alpha^{X_A} \bmod p$

(*) USER B KEY GENERATOR:

PRIVATE: X_B, $\forall X_B < p \Rightarrow 1 < X_B < p-1$

PUBLIC: Y_B, $Y_B = \alpha^{X_B} \bmod p$

(*) MESSAGE / PLAINTEXT TO ENCRYPT: $M < p$

PROCESS OF ENCRYPTION: (FROM A TO B)

1. Choose lowercase k (randomly); $1 \leq k \leq p-1$
2. Calculate "C_1"
$$C_1 = \alpha^k \bmod p$$
3. Calculate uppercase $\bar{K} = Y_B^k \bmod p$
4. Calculate "C_2".
$$C_2 = \bar{K} \cdot M \bmod p$$

$$\bar{K} = Y_B^k \bmod p \qquad \bar{K}^{-1} = C_1^{p-1-X_B}$$

PROCESS OF DECRYPTION:

1. Calculate $\bar{K} = C_1^{X_B} \bmod p$
2. Calculate $M = C_2 \bar{K}^{-1} \bmod p$

$C(M, r, s)$

EL GAMAL SIGNATURE

TO SIGN: $M = H(M) = [X_{A\,\text{SIGNER}} \cdot r \cdot k \cdot s] \bmod p-1$

$C_1 = r = g^k \bmod p$

TO VERIFY: $V_1 = Y^r \cdot r^s \bmod p$ } $V_1 = V_2$

$V_2 = g^{M_{\text{SIGNER}}} \bmod p$

DIFFIE-HELLMAN EXERCISES:

1.

$$\left[\begin{array}{l} p = 17 \\ g = \alpha = 2 \end{array}\right] \text{ PUBLIC} \qquad K = K_A = K_B = ?$$

$$A \left[\begin{array}{ll} \text{PRIVATE:} & X_A = 2 \\ \text{PUBLIC:} & Y_A = \alpha^{X_A} \bmod p \end{array}\right] \quad K_A = (Y_B)^{X_A} \bmod p$$

$$B \left[\begin{array}{ll} \text{PRIVATE:} & X_B = 5 \\ \text{PUBLIC:} & Y_B = \alpha^{X_B} \bmod p \end{array}\right] \quad K_B = (Y_A)^{X_B} \bmod p$$

① $Y_A = 2^2 \bmod 17 = 4 \bmod 17 = 4$

② $Y_B = 2^5 \bmod 17 = 32 \bmod 17 = 15$

$$\begin{array}{r} 32 \\ -17 \\ \hline 15 \end{array} \quad \begin{array}{|l} 17 \\ \hline 1 \end{array}$$

③ $K_A = 15^2 \bmod 17 = 4$

$$\begin{array}{r} 15 \\ \times 15 \\ \hline 75 \\ + \quad 15 \\ \hline 255 \end{array} \qquad \begin{array}{r} 255 \\ -17 \\ \hline 055 \\ -04 \end{array} \quad \begin{array}{|l} 17 \\ \hline 13 \end{array}$$

④ $K_B = 4^5 \bmod 17 = (2^5 \cdot 2^5) \bmod 17 = (15 \cdot 15) \bmod 17 =$
$= 255 \bmod 17 = 4$

⑤ $\boxed{K = K_A = K_B = 4}$

$$\left[\begin{array}{l} p = 17 \\ g = \alpha = 7 \text{ in } \mathbb{Z}_{17} \end{array}\right\} \text{PUBLIC}$$

ALICE $\left\{\begin{array}{ll} \text{PRIVATE:} & X_A = 7 \\ \text{PUBLIC:} & Y_A = \alpha^{X_A} \bmod p \end{array}\right]$ $K_A = Y_B^{X_A} \bmod p$

BOB $\left\{\begin{array}{ll} \text{PRIVATE:} & X_A = 8 \\ \text{PUBLIC:} & Y_B = \alpha^{X_A} \bmod p \end{array}\right]$ $K_B = Y_A^{X_B} \bmod p$

a) $K = K_A = K_B = ?$

① $Y_A = 7^7 \bmod 17 = [7^2 \cdot 7^2 \cdot 7^2 \cdot 7] \bmod 17 =$

$7^2 = 49 \;|\; 17$ → 15, 2

$= [15 \cdot 15 \cdot 15 \cdot 7] \bmod 17 =$

$= [255 \cdot 15 \cdot 7] \bmod 17 =$

$= [4 \cdot 15 \cdot 7] \bmod 17 =$

$= 420 \bmod 17 = \boxed{12 = Y_A}$

15 × 15 = 225 → 225 | 17 → 4, 13

15 × 4 = 60

60 × 7 = 420 → 420 | 17 → 080, 24 → 12

② $Y_B = 7^8 \bmod 17 = [12 \cdot 7] \bmod 17 = 16$

12 × 7 = 84 → 84 | 17 → 16, 4

③ $K_A = 16^7 \bmod 17 = 16$

④ $K_B = 12^8 \bmod 17 = 16$

⑤ $K = K_A = K_B = 16$

2. $\left[\begin{array}{l} p=13 \\ g=\alpha=7 \quad \text{in } Z_{13} \end{array}\right]$ PUBLIC

ALICE $\left[\begin{array}{l} \text{PRIVATE: } X_A = 7 \\ \text{PUBLIC: } Y_A = \alpha^{X_A} \bmod p \end{array}\right]$ $K_A = Y_B^{X_A} \bmod p$

BOB $\left[\begin{array}{l} \text{PRIVATE: } X_B = 8 \\ \text{PUBLIC: } Y_B = \alpha^{X_B} \bmod p \end{array}\right]$ $K_B = Y_A^{X_B} \bmod p$

a) K?

① $Y_A = 7^7 \bmod 13 = 6$
② $Y_B = 7^8 \bmod 13 = 3$
③ $K_A = 3^7 \bmod 13 = 3$
④ $K_B = 6^8 \bmod 13 = 3$
⑤ $\boxed{K = K_A = K_B = 3}$

b) Man in the middle attack.

C = ATTACKER $\left[\begin{array}{l} \text{PRIVATE: } X_C = 10 \\ \text{PUBLIC: } Y_C = \alpha^{X_C} \bmod p \end{array}\right]$

① $Y_A = 7^7 \bmod 13 = 6$
② $Y_B = 7^8 \bmod 13 = 3$
③ $Y_C = 7^{10} \bmod 13 = 4$

A knows...	C knows...	B knows...
$X_A = 7$	$X_C = 10$	$X_B = 8$
$Y_A = 6$	$Y_A = 6$	$Y_B = 3$
$Y_C = 4$	$Y_B = 3$	$Y_C = 4$
$p = 13$	$Y_C = 4$ $p = 13$	$p = 13$

④ $K_{AC} = Y_C^{X_A} \bmod p = 4^7 \bmod 13 = 4$
⑤ $K_{BC} = Y_C^{X_B} \bmod p = 4^8 \bmod 13 = 3$
⑥ $K_{CA} = Y_A^{X_C} \bmod p = 6^{10} \bmod 13 = 4$
$K_{CB} = Y_B^{X_C} \bmod p = 3^{10} \bmod 13 = 3$

$\therefore$ $K_{ALICIA} = 4$
$K_{BOB} = 3$

c) What can they do to avoid this attack?

The problem is that BOB and ALICE are not authenticated, so they could avoid this problem by using digital certificates (public key)

3.

$$\left[\begin{array}{l} p = 47 \\ g = \alpha = 23 \end{array}\right\} \text{PUBLIC}$$

$$A\left\{\begin{array}{l} \text{PRIVATE: } X_A = 12 \\ \text{PUBLIC: } Y_A = \alpha^{X_A} \bmod p \end{array}\right] \quad K_A = Y_B^{X_A} \bmod p$$

$$B\left\{\begin{array}{l} \text{PRIVATE: } X_B = 33 \\ \text{PUBLIC: } Y_B = \alpha^{X_B} \bmod p \end{array}\right] \quad K_B = Y_A^{X_B} \bmod p$$

a) k?

① $Y_A = 23^{12} \bmod 47 = 27$

② $Y_B = 23^{33} \bmod 47 = 33$

③ $K_A = 33^{12} \bmod 47 = 25$

④ $K_B = 27^{33} \bmod 47 = 25$

$\Big\} \boxed{k = K_A = K_B = 25}$

b) To encrypt $\longrightarrow C = H^K \bmod n$

To decrypt $\longrightarrow H = C^J \bmod n$

$\Big\}$ ¿J? THEORETICALLY

$C = H^K \bmod n \longrightarrow H^K = C \bmod n \longrightarrow C = H^K$

$H = C^J \bmod n \longrightarrow$

$\longrightarrow H = (H^K)^J \bmod n = H^{K \cdot J} \bmod n$

$$\boxed{K \cdot J \bmod \Phi n = 1}$$

c) $M=16$, $K=25$, $p=47=n$
get J to decrypt and prove that M is obtained from C.

$K \cdot J \bmod \Phi n = 1$

$C = M^K \bmod n = 16^{25} \bmod 47 = 21$

$\therefore \boxed{C = 21}$

$\Phi_{47} = 46$

$\rightarrow 25 \cdot J \bmod 46 = 1$

APLICAMOS ALGORITMO DE EUCLIDES

$46 = \underline{25} \cdot 1 + \underline{21}$
$25 = 21 \cdot 1 + 4$
$21 = 4 \cdot 5 + 1$
$4 = 1 \cdot 4 + 0$

$1 = 21 - 4 \cdot 5 =$
$= 21 - [25 - 21] \cdot 5 =$
$= 21 - [25 - (46 - 25)] \cdot 5 =$
$= 21 - [2 \cdot 25 - 46] \cdot 5 =$
$= 21 - 10 \cdot 25 + 5 \cdot 46 =$
$= 46 - 25 - 10 \cdot 25 + 5 \cdot 46 =$
$= \underbrace{-11}_{\alpha} \cdot (25) + \underbrace{6}_{\beta} \cdot (46)$

$\therefore \boxed{\text{inverso} = J = -11}$

$1 = 25\alpha + 46\beta$

$25 \cdot \underbrace{(-11) \bmod 46}_{J} = 1$

$J = -11 \bmod 46 = (46-11) \bmod 46 =$
$= 35 \bmod 46 = 35$

$\boxed{J = 35}$

$\boxed{M = C^J \bmod n = 21^{35} \bmod 47 = 16}$ ✓

1. RSA

a) $p_B = 5$, $q_B = 7$, $d_B = 11$. Encrypt $M = 2$ & decrypt the result.

¿Qué necesito tener yo para encriptar el mensaje? → me falta e_B

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

$n_B = p_B \cdot q_B = 35$

$\varphi n_B = \varphi_{35} = \varphi_7 \cdot \varphi_5 = 6 \cdot 4 = 24$

$\gcd(\varphi n, e) = 1$

$[d_B \cdot e] \bmod \varphi n = 1$

$11 \cdot e \bmod 24 = 1$

$24 = 11 \cdot 2 + 2$
$11 = 2 \cdot 5 + 1$
$2 = 1 \cdot 2 + 0$

$1 = 11 - 2 \cdot 5$
$1 = 11 - [24 - 11 \cdot 2] \cdot 5$
$1 = 11 - 24 \cdot 5 + 11 \cdot 2 \cdot 5$
$1 = -24 \cdot 5 + 11 \cdot \underline{11}$

inverso. $\therefore e$

$\boxed{e_B = 11}$

Cifrar:

$C = 2^{11} \bmod 35 = 2^6 \cdot 2^5 \bmod 35 =$
$= [64 \bmod 35 \cdot 32 \bmod 35] \bmod 35 =$
$= [29 \cdot 32] \bmod 35 = 18$

$32 \times 29 = 288 + 64 = 928$

$928 \mid 35$
$228 \quad 26$
18

Descifrar:

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

$M = 18^{11} \bmod 35 = 2$ ✓

b) $p_B = 3$, $q_B = 11$, $e_B = 7$. Encript $M = 5$ a Bob:

$n_B = p_B \cdot q_B = 3 \cdot 11 = 33$

$d_B \equiv e_B^{-1} \bmod \Phi n_B$

$[d_B \cdot e_B] \bmod \Phi n_B = 1$

$\Phi n_B = \Phi_{33} = \Phi_3 \cdot \Phi_{11} = 2 \cdot 10 = 20$.

$d_B \cdot 7 \bmod 20 = 1$

APLICAMOS EL ALGORITMO DE EUCLIDES

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

$20 = 7 \cdot 2 + 6$
$7 = 6 \cdot 1 + 1$
$6 = 1 \cdot 6 + 0$

$1 = 7 - 6 \cdot 1$
$1 = 7 - [20 - 7 \cdot 2]$
$1 = 7 - 20 + 7 \cdot 2$
$1 = -20 + 7 \cdot 3$
$d_B = 3$

CIFRAMOS:

$C = M^{e_B} \bmod n_B$
$C = 5^7 \bmod 33 = [5^5 \cdot 5^3 \cdot 5] \bmod 33 =$
$= [26 \cdot 26 \cdot 5] \bmod 33 =$
$= [16 \cdot 5] \bmod 33 = 14$

125 | 33
26 | 3

26 × 26 = 156 + 52 = 676

676 | 33
016 | 20

16 × 5 = 80

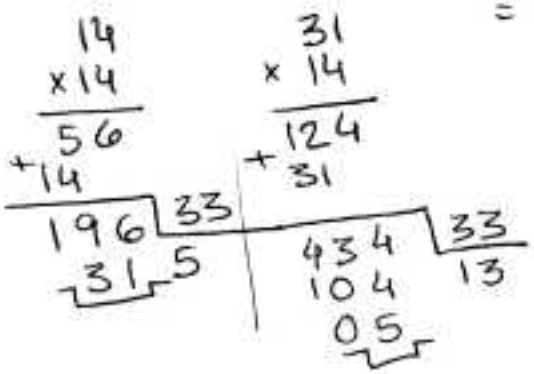
80 | 33
14 | 2

DESCIFRAMOS:

$$M = C^{d_B} \bmod n_B = 14^3 \bmod 33 = [14^2 \cdot 14] \bmod 33 =$$

$$= [31 \cdot 4] \bmod 33 = 434 \bmod 33 =$$

$$= 5$$



✓