

# Sistemas-de-clave-publica.pdf



**BeaSalga**



**Criptografia i Seguretat**



**3º Grado en Ingeniería de Datos**



**Escuela de Ingeniería  
Universidad Autónoma de Barcelona**

antes



**Descarga sin publi  
con 1 coin**



Después

**WUOLAH**



Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato  
→ Planes pro: más coins

perdo  
espacio



Necesito  
concentración

ali ali ooh  
esto con 1 coin me  
lo quito yo...

WUOLAH

## Sistemas de clave pública

### 1. PROBLEMA CON LA ENCRIPCIÓN SIMÉTRICA:

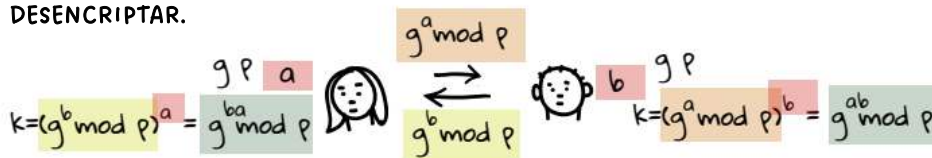
VALE, LA ENCRIPCIÓN CON LLAVE SIMÉTRICA FUNCIONA, PERO ¿CÓMO PODEMOS ENTREGAR UNA KEY A MI COMPAÑERO SABIENDO QUE EL MEDIO DE COMPARTICIÓN ES HOSTIL?

CIFRADO SIMÉTRICO: LOS DATOS CIFRADOS CON UNA CLAVE SIMETRICA NO SE PUEDEN DESCIFRAR CON NINGUNA OTRA CLAVE, POR LO TANTO, SIEMPRE LAS DOS PARTES QUE LA UTILICEN LA MANTENGAN EN SECRETO, CADA UNA DE LAS PARTES PUEDE ESTAR SEGURA DE QUE SE ESTÁ COMUNICANDO CON LA OTRA SIEMPRE QUE LOS MENSAJES DESCIFRADOS SIGAN TENIENDO SENTIDO.

SI ALGUIEN ENCUENTRA LA CLAVE, AFECTARÁ TANTO A LA CONFIDENCIALIDAD COMO A LA AUTENTICACIÓN. UNA PERSONA CON UNA CLAVE SIMÉTRICA NO AUTORIZADA, NO SOLO PUEDE DESCIFRAR LOS MENSAJES ENVIADOS CON ESA CLAVE, SINO QUE, TAMBIÉN PUEDE CIFRAR LOS MENSAJES NUEVOS Y ENVIARLOS COMO SI PROCEDIERAN DE UNA DE LAS DOS PARTES QUE ORIGINALMENTE USABAN LA CLAVE.

### 2. DIFFIE HELLMAN

- ALICE ESCOGE ALEATORIAMENTE UNA  $a$  Y COMPUTA  $A = g^a$
- BOB ESCOGE ALEATORIAMENTE UNA  $b$  Y COMPUTA  $B = g^b$
- ALICE ENVIA  $A$  A BOB. BOB ENVIA  $B$  A ALICE.
- ALICE COMPUTA  $k = B^a = (G^b)^a = G^{ab}$
- BOB COMPUTA  $k = A^b = (G^a)^b = G^{ab}$
- AHORA ALICE Y BOB PUEDEN USAR  $k$  COMO SU SECRETO PARA ENCRIPITAR Y DESENCRIPTAR.



LA IMPLEMENTACIÓN MÁS SIMPLE Y ORIGINAL DEL PROTOCOLO UTILIZA EL GRUPO MULTIPLICATIVO DE INTEGERS MODULO  $p$ , DONDE  $p$  ES PRIMO Y  $G$  ES UNA RAÍZ PRIMITIVA MODULO  $p$ .

EN LA ARITMÉTICA MODULAR UN NÚMERO  $G$  ES UNA RAÍZ PRIMITIVA MODULO  $N$  SI CDA NÚMERO  $A$  COPRIMOS CON  $N$  ES CONGRUENTE CON UNA POTENCIA DE  $G$  MÓDULO  $N$ .

2 is a primitive root mod 5, because for every number  $a$  relatively prime to 5, there is an integer  $z$  such that  $2^z \equiv a$ .  
All the numbers relatively prime to 5 are 1, 2, 3, 4, and each of these (mod 5) is itself (for instance  $2 \pmod{5} = 2$ ):

- $2^0 = 1$ ,  $1 \pmod{5} = 1$ , so  $2^0 \equiv 1$
- $2^1 = 2$ ,  $2 \pmod{5} = 2$ , so  $2^1 \equiv 2$
- $2^3 = 8$ ,  $8 \pmod{5} = 3$ , so  $2^3 \equiv 3$
- $2^2 = 4$ ,  $4 \pmod{5} = 4$ , so  $2^2 \equiv 4$ .

For every integer relatively prime to 5, there is a power of 2 that is congruent.

4 is not a primitive root mod 5, because for every number relatively prime to 5 (again, 1, 2, 3, 4) there is not a power of 4 that is congruent. Powers of 4 (mod 5) are only congruent to 1 or 4. There is no power of 4 that is congruent to 2 or 3:

- $4^0 = 1$ ,  $1 \pmod{5} = 1$
- $4^1 = 4$ ,  $4 \pmod{5} = 4$
- $4^2 = 16$ ,  $16 \pmod{5} = 1$
- $4^3 = 64$ ,  $64 \pmod{5} = 4$

and the pattern continues...

WUOLAH

### EJEMPLO (DEFFIE HELLMAN)

- ALICE Y BOB ACEPTAN PÚBLICAMENTE USAR UN MÓDULO  $P = 23$  Y BASE  $G = 5$
- ALICE ESCOGE UN SECRETO INTEGER  $a = 4$ , DESPUÉS ENVIA A BOB  $A = g^a \mod p$   
 $A = 5^4 \mod 23 = 4$
- BOB ESCOGE UN SECRETO INTEGER  $b = 3$ , DESPUÉS ENVIA A ALICE  $B = g^b \mod p$   
 $B = 5^3 \mod 23 = 10$
- ALICE COMPUTES  $k = B^a \mod p$   
 $K = 10^4 \mod 23 = 18$
- BOB COMPUTES  $k = A^b \mod p$   
 $K = 4^3 \mod 23 = 18$
- ALICE Y BOB AHORA COMPARTEN UN SECRETO (EL NÚMERO 18)

### 3. ESQUEMA DE CLAVE ASIMÉTRICA:

CLAVE ASIMÉTRICA: TAMBIÉN CONOCIDA COMO CRIPTOGRAFÍA DE CLAVE PÚBLICA. ES UN PROCESO QUE UTILIZA UN PAR DE CLAVES RELACIONADAS, UNA CLAVE PÚBLICA Y OTRA PRIVADA PARA CIFRA Y DESCIFRAR UN MENSAJE Y PROTEGERLO DE ACCESOS O USOS NO AUTORIZADOS. UNA CLAVE PÚBLICA ES UNA CLAVE CRIPTOGRÁFICA QUE PUEDE SER UTILIZADA POR CUALQUIER PERSONA PARA CIFRAR UN MENSAJE DE MANERA QUE SOLO PUEDA SER DESCIFRADO POR EL DESTINATARIO CON SU CLAVE PRIVADA. UNA CLAVE PRIVADA (CLAVE SECRETA) SOLO SE COMPARTIÓ CON EL INICIADOR DE LA CLAVE.

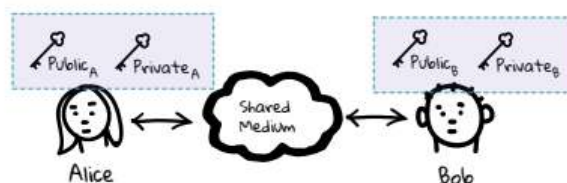
CUANDO ALGUIEN QUIERE ENVIAR UN MENSAJE CIFRADO, PUEDE OBTENER LA CLAVE PÚBLICA DEL DESTINATARIO DE UN DIRECTORIO PÚBLICO Y UTILIZARLA PARA CIFRAR EL MENSAJE ANTES DE ENVIARLO. EL DESTINATARIO DEL MENSAJE PUEDE ENTONCES DESCIFRARLO UTILIZANDO SU CLAVE PRIVADA CORRESPONDIENTE.

SI EL REMITENTE ENCRIPTA EL MENSAJE CON SU CLAVE PRIVADA, SOLO PODRÁ DESENCRIPTARLO CON LA CLAVE PÚBLICA DEL REMITENTE, LO QUE PERMITIRÁ AUTENTICARLO. ESTOS PROCESOS DE DESCIFRADO Y CIFRADO SE PRODUCEN AUTOMÁTICAMENTE PUES LOS USUARIOS NO NECESITAN BLOQUEAR Y DESBLOQUEAR FÍSICAMENTE EL MENSAJE.

EL PRINCIPAL BENEFICIO DE LA CRIPTOGRAFÍA ASIMÉTRICA ES EL AUMENTO DE LA SEGURIDAD DE LOS DATOS. ES EL PROCESO DE CIFRADO MÁS SEGURO PORQUE LOS USUARIOS NUNCA TIENEN QUE REVELAR O COMPARTIR SUS CLAVES PRIVADAS, LO QUE DISMINUYE LAS POSIBILIDADES DE QUE UN CIBERDELINCUENTE DESCUBRA LA CLAVE PRIVADA DE UN USUARIO DUANTE LA TRANSMISIÓN.

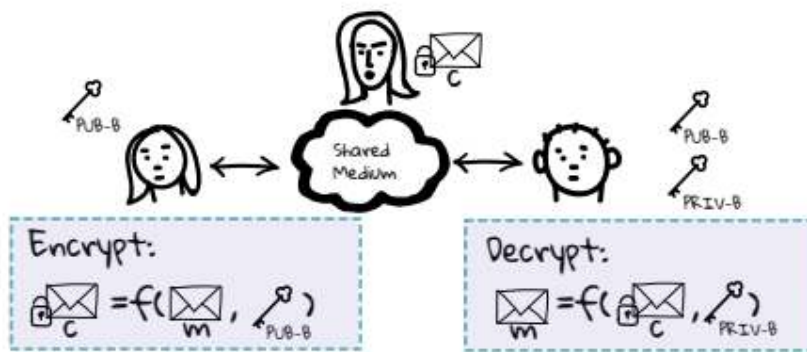
LOS ESQUEMAS DE CIFRADO ASIMÉTRICO SE BASAN EN DOS CLAVES PARA CADA USUARIO.

ESAS CLAVES TIENEN LA PROPIEDAD DE QUE LO QUE SE ENCRIPTA CON UNA DE ELLAS SERÁ DESCIFRADO CON LA OTRA.



- **CONFIDENCIALIDAD**

LA CRIPTOGRAFÍA DE CLAVE PÚBLICA O CRIPTOGRAFÍA ASIMÉTRICA, ES UN SISTEMA CRIPTOGRÁFICO QUE UTILIZA PARES DE CLAVES : CLAVES PÚBLICAS QUE PUEDEN DIFUNDIRSE AMPLIAMENTE Y CLAVES PRIVADAS, QUE SOLO CONOCE EL PROPIETARIO

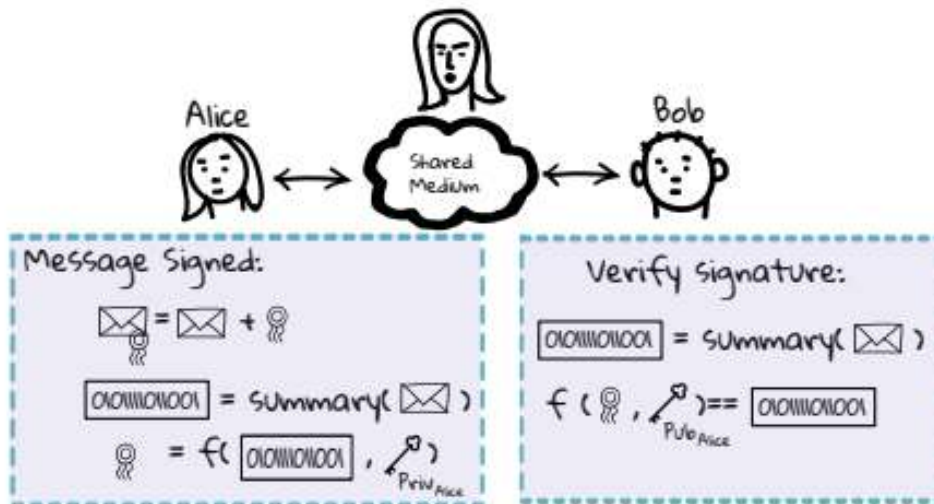


EN DICHO SISTEMA, CUALQUIER PERSONA PUEDE ENCRIPtar UN MENSAJE UTILIZANDO LA CLAVE PÚBLICA DEL RECEPTOR, PERO ESE MENSAJE CIFRADO SOLO SE PUEDE DESCIFRAR CON LA CLAVE PRIVADA DEL RECEPTOR.

- AUTENTICACIÓN / INTEGRIDAD**

UN MENSAJE SE FORMA RESUMIENDO EL MENSAJE MEDIANTE UNA FUNCIÓN HASH, POR EJEMPLO.

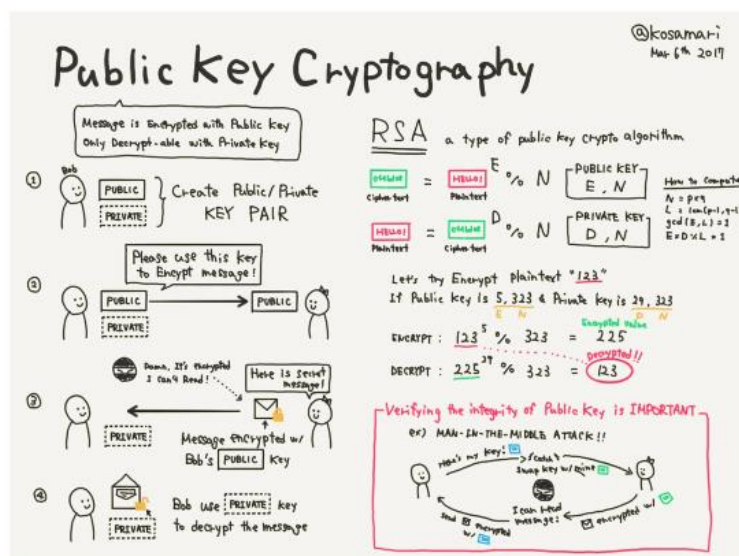
LUEGO, EL RESUMEN SE CIFRA UTILIZANDO LA CLAVE PRIVADA DEL REMITENTE.



EL DESTINATARIO DEL MENSAJE PUEDE VERIFICAR LA INTEGRIDAD DEL MENSAJE CALCULANDO EL RESUMEN DEL MENSAJE RECIBIDO Y COMPARARLO CON EL RESULTADO DE DESCIFRAR CON LA CLAVE PÚBLICA DEL REMITENTE LA FIRMA.

#### 4. RSA (VISUAL)

LAS SIGLAS VIENEN DE LOS NOMBRES DE SUS CREADORES





Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins?

Plan Turbo: barato

Planes pro: más coins

perdo  
espacio



Necesito  
concentración

ali ali ooh  
esto con 1 coin me  
lo quito yo...

WUOLAH

### RSA (RECETA)

EL ALGORITMO RSA BASA SU FORTALEZA EN LA DIFICULTAD COMPUTACIONAL DE FACTORIZAR UN NÚMERO COMPLEJISTO MUY GRANDE PRODUCTO DE DOS NÚMEROS PRIMOS MUY GRANDES, UN PROBLEMA INABORDABLE PARA LA CAPACIDAD MUNDIAL DE COMPUTO EN 2016 CON MAGNITUDES POR ENCIMA DE 1000 BITS.

LA SEGURIDAD DEL ALGORITMO ESTÁ BASADA EN LO DIFÍCIL QUE ES LA FACTORIZACIÓN DADO  $N = P * Q$ , SIN SABER UN ALGORITMO EFICIENTE PARA RECUPERAR P Y Q.

**ALGORITMO PARA LA GENERACIÓN DE CLAVES RSA:** GENERACIÓN DE LA CLAVE POR RSA CON ENCRIPCIÓN DE CLAVE PÚBLICA

RESUMEN: CADA ENTIDAD CREA UNA CLAVE RSA PÚBLICA Y UNA CORRESPONDIENTE LLAVE PRIVADA.

CADA ENTIDAD A DEBERÍA HACER LO SIGUIENTE:

- GENERA DOS RANDOMS LARGOS (Y DISTINTOS) PRIMOS P Y Q, CON EL MISMO TAMAÑO
- COMPUTAR  $N = P * Q$  Y  $\phi = (P-1) * (Q-1)$
- SELECCIONAR UN INTEGER RANDOM E,  $1 < E < \phi$  TAL QUE  $GCD(e, \phi) = 1$
- USAR EL ALGORITMO EXTENDIDO DE EUCLIDES PARA COMPUTAR EL UNICO INTEGER D TAL QUE  $1 < D < \phi$  TAL QUE  $e * d = 1 \mod \phi$
- UNA CLAVE PÚBLICA DE CADA ENTIDAD ES (N,E). UNA CLAVE PRIVADA DE CADA ENTIDAD ES D

ALICIA Y BERNARDO ESCOGEN UN MÓDULO DE CIFRA EN  $N = P * Q$  SIENDO P Y Q PRIMOS DE UN TAMAÑO SUPERIOR A 512 BITS. HOY EN DÍA ES RECOMENDABLE QUE SEA DE 1024 BITS. ESTE MÓDULO ES UN SECRETO SOLO CONOCIDO POR AMBOS.

EN EL CASO DE ALICIA :  $N_a = P_a * Q_a$

EN EL CASO DE BERNARDO:  $N_b = P_b * Q_b$

SE CALCULA EL MÓDULO Y EL INDICADOR DE EULER PHI DE ESE MÓDULO N. EN EL CASO DE DOS PRIMOS, RECORDAMOS QUE EL EULER =  $(P-1)*(Q-1)$

EN EL CASO DE ALICIA:

$$N_a = 839 * 947 = 794533 \mid \phi(N_a) = (P_a - 1) * (Q_a - 1) = 838 * 946 = 792.748$$

EN EL CASO DE BERNARDO

$$N_b = 761 * 1019 = 775456 \mid \phi(N_b) = (P_b - 1) * (Q_b - 1) = 760 * 1018 = 773.680$$

Estos valores phi serán números grandes, conocidos como TRAMPA.

CADA USUARIO ELIGIRÁ UN VALOR DE CLAVE PÚBLICA ENTRE 1 Y phi ( $1 < e < \phi$ ).

HAY QUE ASEGURARSE DE QUE EXISTA EL INVERSO MULTIPLICATIVO DEBE CUMPLIRSE QUE

$$MCD [e, \phi] = 1$$

EN EL CASO DE ALICIA:

$$E_a = 41 \mid N_a = 794533 \text{ Y CALCULA } D_a = \text{inv}(E_a, \phi(N_a)) = \text{inv}(41, 792748) = 425377 \mod N_a$$

EN EL CASO DE BERNARDO:

$$E_b = 53 \mid N_b = 775456 \text{ CALCULA } D_b = \text{inv}(E_b, \phi(N_b)) = \text{inv}(53, 773680) = 277357 \mod N_b$$

ALICIA Y BERNARDO HACEN PÚBLICO EL CUERPO  $N_{a/b}$  Y SU CLAVE PÚBLICA  $E_{a/b}$  Y GUARDAN EN SECRETO LA CLAVE PRIVADA  $D_{a/b}$  Y LOS PRIMOS  $P$  Y  $Q$  QUE LES SERVIRÁN PARA ACELERAR LA OPERACIÓN DE DESCIFRADO MEDIANTE EL TEOREMA CHINO DE LOS RESTOS.

### CIFRADO Y DESCIFRADO

IMAGINEMOS QUE ALICIA QUIERE ENVIAR EL NÚMERO SECRETO  $N = 1234$  A BERNARDO:

ALICIA  $\rightarrow D_a = 23131 \mid N_a = 42593, e_A = 31 \rightarrow (\text{ENCR}) C = B^{e_b} \bmod N_b = 1234^{31} \bmod 46031 = 15017$

BERNARDO  $\rightarrow D_b = 37553 \mid N_b = 46031, e_B = 17 \rightarrow (\text{DEC}) C^{D_b} \bmod n_B = 15017^{37553} \bmod 46031 = 1234$

#### 1. ENCRIPCIÓN:

- CONSEGUIR LA CLAVE PÚBLICA DE A ( $N, E$ )
- REPRESENTAR EL MENSAJE COMO UN INTEGER  $M$  EN EL INTERVALO  $[0, N-1]$
- COMPUTAR  $C = M^E \bmod N$
- ENVIAR EL TEXTO CIFRADO  $C$  A A.

#### 2. DESENCRIPTACIÓN

- USAR LA CLAVE PRIVADA  $D$  PARA RECUPERAR  $M = C^D \bmod N$

#### RSA (EJEMPLO)

- ESCOGEMOS DOS NÚMEROS PRIMOS,  $P = 5, Q = 11$
- CALCULAMOS  $N = P \cdot Q = 55$
- CALCULAMOS  $\phi = (P-1) \cdot (Q-1) = 40$
- ESCOGEMOS UNA  $E$  TAL QUE SEA COPRIMO CON  $\phi$ , POR EJEMPLO  $E = 7$   
 $1 < 7 < 40$  Y  $\text{MCD}[7, 40] = 1$
- ESCOGEMOS  $D$  COMO EL INVERSO DEL MÓDULO  $\phi$ , QUE ES  $E \cdot D = 1 \pmod{\phi}$ .  
 $D = \text{inv}(e, \phi(N)) = \text{inv}(7, 40) = 23$  ( $7 \cdot 23 \bmod 40 = 1$ )
- PUBLIC KEY = ( $E, N$ )
- PRIVATE KEY = ( $D, N$ )




























CREACIÓN DEL MENSAJE: ESCOGE UN MENSAJE, POR EJEMPLO "HELLO". EMPEZAMOS CON H (8)  
 $M = 8$

ENCRIPCIÓN:  $C = M^E \bmod N = 8^7 \bmod 55 = 2$

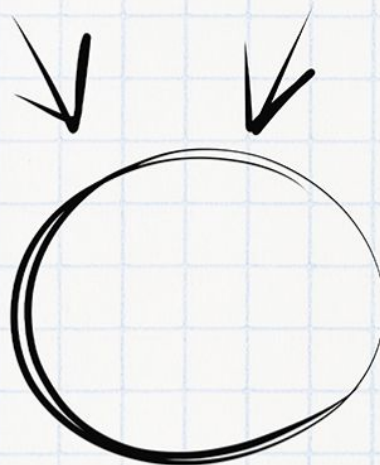
DESENCRIPTACIÓN:  $M = C^D \bmod N = 2^{23} \bmod 55 = 8$

# Imagínate aprobando el examen

## Necesitas tiempo y concentración

Planes	 PLAN TURBO	 PLAN PRO	 PLAN PRO+
 Descargas sin publi al mes	10 	40 	80 
 Elimina el video entre descargas			
 Descarga carpetas			
 Descarga archivos grandes			
 Visualiza apuntes online sin publi			
 Elimina toda la publi web			
 Precios <span>Anual <input type="checkbox"/></span>	0,99 € / mes	3,99 € / mes	7,99 € / mes

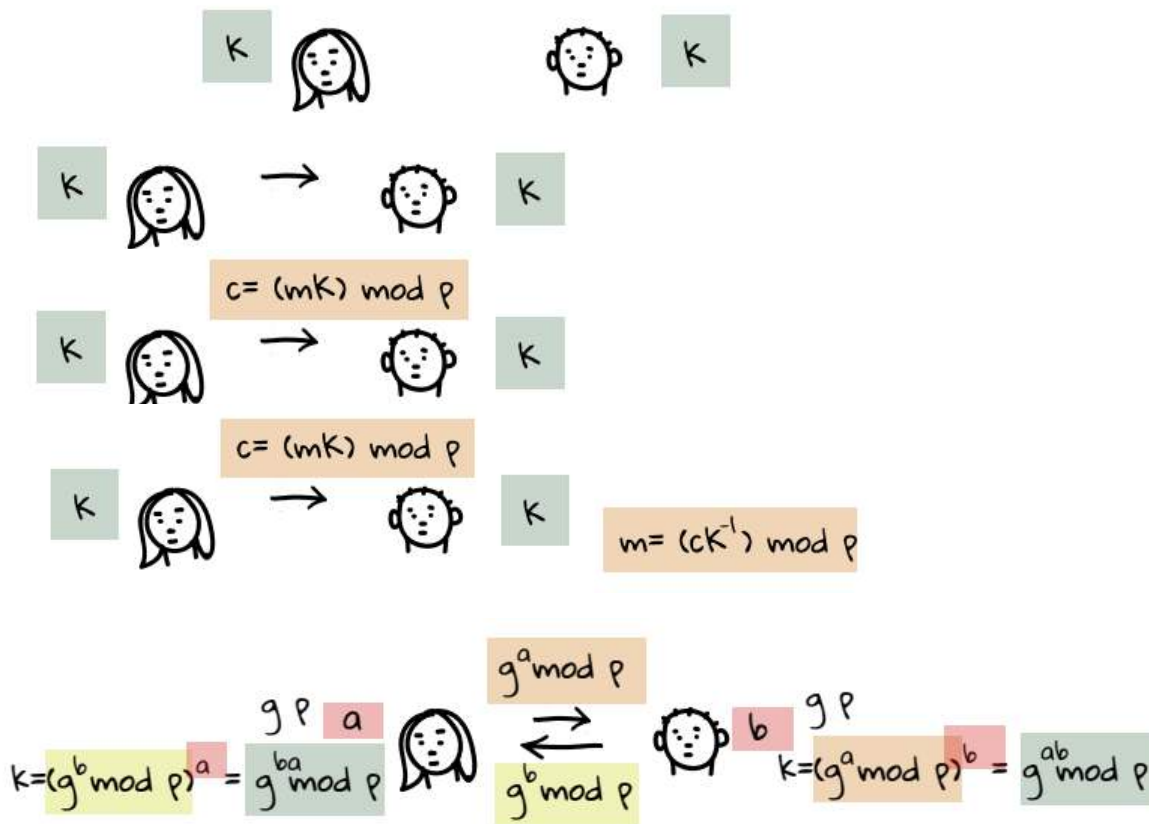
Ahora que puedes conseguirlo,  
¿Qué nota vas a sacar?



# WUOLAH

## 5. EL GAMMAL (ALGORITMO DISCRETO)

ELGAMAL ES UN CRIPTOSISTEMA DE CLAVE PÚBLICA BASADO EN DEFFIE- HELLMAN Y EL PROBLEMA DEL LOGARITMO DISCRETO.



ALICE ESCOGE ALEATORIAMENTE UNA  $a$  Y COMPUTA  $A = g^a$

- BOB ESCOGE ALEATORIAMENTE UNA  $b$  Y COMPUTA  $B = g^b$
- ALICE ENVIA A A BOB. BOB ENVIA B A ALICE.
- ALICE COMPUTA  $k = B^a = (G^b)^a = G^{ab}$
- BOB COMPUTA  $k = A^b = (G^a)^b = G^{ab}$
- AHORA ALICE Y BOB PUEDEN USAR  $k$  COMO SU SECRETO PARA ENCRIPtar Y DESENCRIPTAR.



Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins? → Plan Turbo: barato  
→ Planes pro: más coins

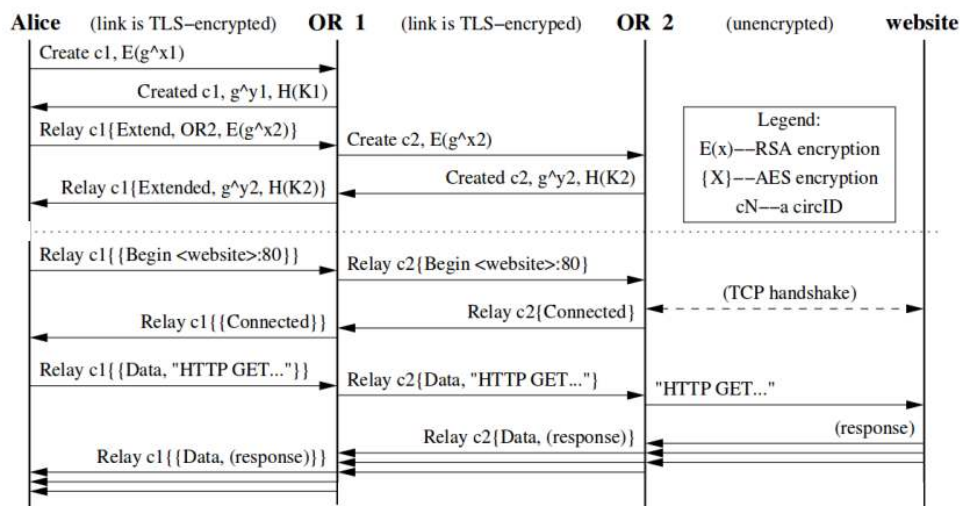
perdo  
espacio



Necesito  
concentración

ali ali ooh  
esto con 1 coin me  
lo quito yo...

WUOLAH



WUOLAH