

Códigos y Criptografía

Grado en Ingeniería Informática

Examen escrito 2 (10% nota final)
2021

Fecha: 02 diciembre 2021

Hora: 11:05–11:55

Lugar: Aula 8

Ayuda permitida: cualquier tipo de material impreso: notas, apuntes, libros, ejercicios resueltos, ...

No se permite ninguna ayuda de forma electrónica, salvo una sencilla calculadora y un ordenador portátil o tablet con un lector de ficheros pdf abierto donde se puede consultar un libro electrónico o las pizarras de clase. En particular no debe tenerse abierto un explorador, SageMath o cualquier programa de email/mensajería. El wifi y datos deben estar desactivados.

Preferentemente, se usará una calculadora de bolsillo. En el caso de no tener una calculadora de bolsillo, se podrá usar la calculadora de Windows/Linux.

Cualquier otro tipo de ayuda electrónica no se puede utilizar. Esto incluye calculadoras científicas avanzadas, teléfono móvil, tablets/pdas, smartwatches, reproductores de música, ...

Nota: la resolución de los ejercicios debe **justificarse** de forma **razonada**.

Nota: escribe tu nombre y apellidos y DNI/NIE en todas las hojas que entregues.

Nota: El porcentaje al principio de cada ejercicio indica su valor en el examen.

Ejercicios: pueden encontrarse en las próximas 2 páginas.

Ejercicio 1. (25%) Considera un canal sin ruido que transmite bits (1's y 0's) y considera el alfabeto fuente $\mathcal{A} = \{a, b, c, d, e, f\}$. Después de transmitir muchos símbolos, se ha hecho un estudio y se ha visto que la frecuencia (en tanto por uno) de cada símbolo a transmitir está dada por la siguiente tabla

Símbolo	a	b	c	d	e	f
Frecuencia	0.10	0.20	0.15	0.34	0.12	0.09

- (a) Diseña una codificación trivial de los elementos de \mathcal{A} para este canal. ¿Cuál sería el número medio de bits usados para transmitir un símbolo de \mathcal{A} ?
- (b) Diseña un código compresor óptimo de acuerdo a las frecuencias mencionadas en la tabla (pista: Código de Huffman).
- (c) Usando el código compresor de la pregunta anterior: ¿Cuál es el número medio de bits usados para transmitir un símbolo de \mathcal{A} ?

Ejercicio 2. (15%) Considera un código de transposición cuya clave está dada por la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 4 & 2 & 6 & 7 & 1 \end{pmatrix}$$

y cifra el siguiente mensaje: "MATEMATICASDIVERTIDAS".

Ejercicio 3. (30%) Bob quiere enviar un mensaje a Alice. Dado que comunican a través de un canal inseguro, debe cifrar el mensaje para evitar que un espía lo obtenga. Alice y Bob deciden usar el criptosistema de ElGamal para cifrar el mensaje. Escogen trabajar módulo $p = 11$ con $g = 2$ como elemento generador del grupo multiplicativo (no hace falta demostrar que p es primo o que g es un generador del grupo multiplicativo). El mensaje, que es un entero módulo p , que Bob quiere enviar a Alice es $M = 5$. La clave privada de Alice es 4.

- (a) ¿Cuál es la clave pública de Alice?
- (b) Bob cifra el mensaje M y se lo envía a Alice. Calcula el mensaje cifrado que Bob envía a Alice.
- (c) Alice recibe el mensaje cifrado de Bob y procede a descifrarlo. Calcula como recupera Alice el mensaje M de Bob.

Nota: la respuesta de este ejercicio no es única porque Bob debe escoger un número al azar para el cifrado (que escoges tu).

Ejercicio 4. (30%) Alice quiere firmar un documento M y mostrárselo a Bob. Para ello deciden usar la firma digital basada en RSA con una función hash h . Alice escoge $p = 3$ y $q = 17$ como primos y como clave privada $d = 5$. El hash del documento a firmar tiene valor $h(M) = 3$.

- (a) Muestra como Alice calcula la firma del mensaje M .
- (b) ¿Cuál es la clave pública de Alice?
- (c) Calcula como Bob comprueba la veracidad de la firma del mensaje M calculada en el apartado (a).

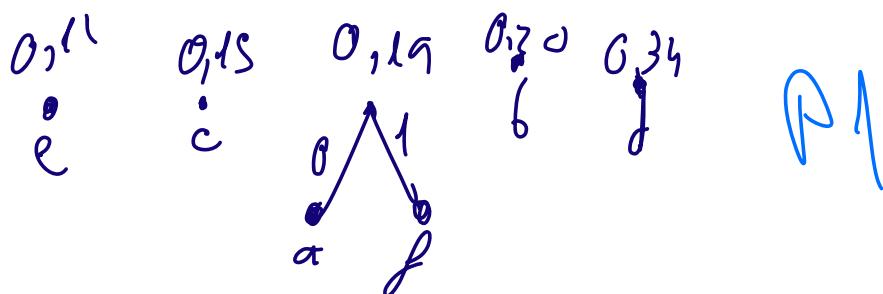
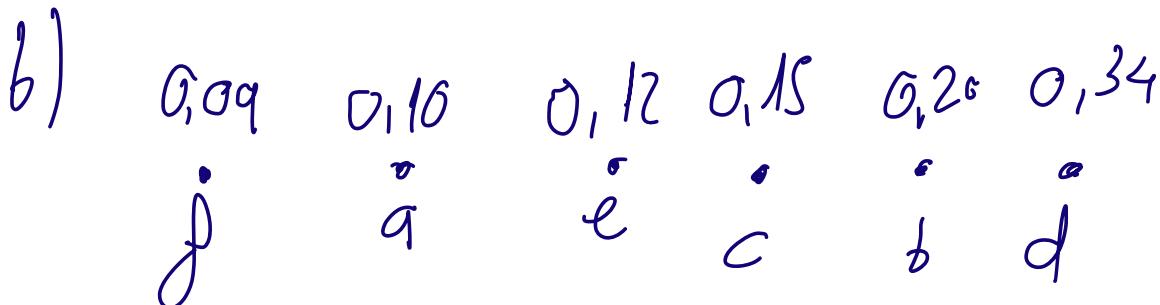
1 -

Ejercicio 1. (25%) Considera un canal sin ruido que transmite bits (1's y 0's) y considera el alfabeto fuente $\mathcal{A} = \{a, b, c, d, e, f\}$. Después de transmitir muchos símbolos, se ha hecho un estudio y se ha visto que la frecuencia (en tanto por uno) de cada símbolo a transmitir está dada por la siguiente tabla

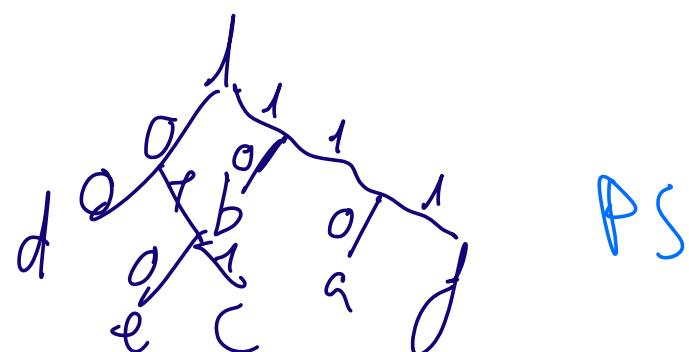
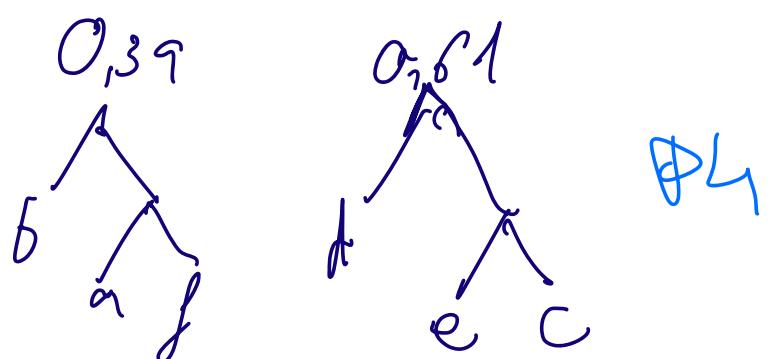
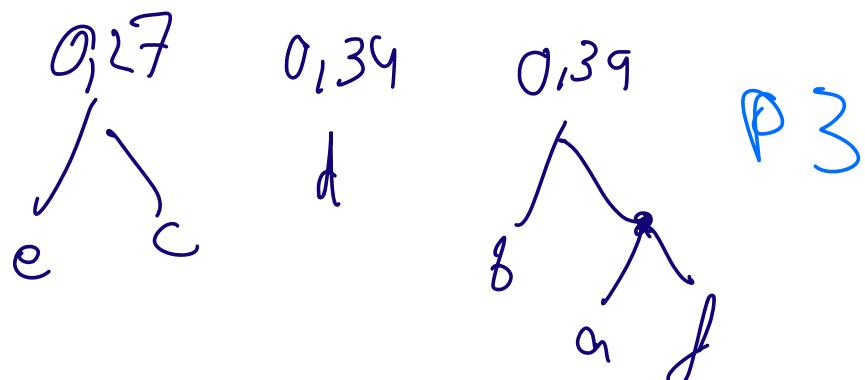
Símbolo	a	b	c	d	e	f
Frecuencia	0.10	0.20	0.15	0.34	0.12	0.09

- Diseña una codificación trivial de los elementos de \mathcal{A} para este canal. ¿Cuál sería el número medio de bits usados para transmitir un símbolo de \mathcal{A} ?
- Diseña un código compresor óptimo de acuerdo a las frecuencias mencionadas en la tabla (pista: Código de Huffman).
- Usando el código compresor de la pregunta anterior: ¿Cuál es el número medio de bits usados para transmitir un símbolo de \mathcal{A} ?

a) $2^2 \leq 6 \leq 2^3 \Rightarrow 4 \leq \text{bits} \leq 8 \Rightarrow 36,75$



0,19	0,20	0,27	0,34	P2
k	b	k	d	



$a = 110$ $c = 011$ $e = 010$ $El de más peso$
 $b = 10$ $d = 00$ $f = 111$ $a la izquierda$

$$\begin{aligned}
 C) & 0,10 \cdot 3 + 0,20 \cdot 2 + 0,15 \cdot 3 + 0,34 \cdot 2 + 0,12 \cdot 3 + \\
 & 20,09 \cdot 3 = 0,3 + 0,4 + 0,45 + 0,68 + 0,36 + 0,18 = \\
 & = 1,15 + 0,68 + 0,36 + 0,18 = 2,37
 \end{aligned}$$

Ejercicio 2. (15%) Considera un código de transposición cuya clave está dada por la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 4 & 2 & 6 & 7 & 1 \end{pmatrix}$$

y cifra el siguiente mensaje: "MATEMATICASDIVERTIDAS".

MATEMATICASDIVERTIDAS
 1 2 3 4 5 6 7 1 2 3 4 5 6 7
 MTEAATM DASCVIVI DTIRASE

MATEMATICASDIVERTIDAS
 1 2 3 4 5 6 7 1 2 3 4 5 6 7
 5 3 4 2 6 7 1 5 3 4 2 6 7 1
 MTEAATM DASCVIVI DTIRASE

MTEAATM DASCVIDTIRASE

Ejercicio 3. (30%) Bob quiere enviar un mensaje a Alice. Dado que comunican a través de un canal inseguro, debe cifrar el mensaje para evitar que un espía lo obtenga. Alice y Bob deciden usar el criptosistema de ElGamal para cifrar el mensaje. Escogen trabajar módulo $p = 11$ con $g = 2$ como elemento generador del grupo multiplicativo (no hace falta demostrar que p es primo o que g es un generador del grupo multiplicativo). El mensaje, que es un entero módulo p , que Bob quiere enviar a Alice es $M = 5$. La clave privada de Alice es 4.

- (a) ¿Cuál es la clave pública de Alice?
- (b) Bob cifra el mensaje M y se lo envía a Alice. Calcula el mensaje cifrado que Bob envía a Alice.
- (c) Alice recibe el mensaje cifrado de Bob y procede a descifrarlo. Calcula como recupera Alice el mensaje M de Bob.

Nota: la respuesta de este ejercicio no es única porque Bob debe escoger un número al azar para el cifrado (que escoges tu).

$$\begin{array}{ccccc}
 p=11 & g=2 & M=5 & a=4 & b=8
 \end{array}$$

a)

$$A = g^a \bmod p = 2^4 \bmod 11 = 16 \bmod 11 = 5$$

b) (B, C)

$$B = g^b \bmod p = 2^8 \bmod 11 = 256 \bmod 11 = 3$$

$$C = A^b M \bmod P = 5^8 \cdot 5 \bmod 11 = 9$$

(3, 9)

c) $k = B^a \bmod P = 3^4 \bmod 11 = 81 \bmod 11 = 4$

$$\begin{aligned} u &= C \cdot k^{-1} \bmod P = 9 \cdot 4^{-1} \bmod P = u = B^{p-1-q} \cdot C \bmod P = \\ &= 3^{11-1-4} \cdot 4 \bmod 11 = 3^6 \cdot 9 \bmod 11 = 6561 \bmod 11 = 5 \end{aligned}$$

$$\boxed{u = 5}$$

Ejercicio 4. (30%) Alice quiere firmar un documento M y mostrárselo a Bob. Para ello deciden usar la firma digital basada en RSA con una función hash h . Alice escoge $p = 3$ y $q = 17$ como primos y como clave privada $d = 5$. El hash del documento a firmar tiene valor $h(M) = 3$.

- Muestra como Alice calcula la firma del mensaje M .
- ¿Cuál es la clave pública de Alice?
- Calcula como Bob comprueba la veracidad de la firma del mensaje M calculada en el apartado (a).

$$p = 3 \quad q = 17 \quad \varphi_a = 5 \quad h(M) = 3 \quad \varphi(n) = (p-1)(q-1) = 32$$

$$n = p \cdot q = 51$$

↓ firma

a) $S = h(m)^d \bmod n = 3^5 \bmod 51 = 39$

b) $3 = 5^e \bmod n \Rightarrow e = \frac{\ln 3}{\ln 5} \bmod 51 =$

~~$h(m) = 5^e \bmod n$~~

~~$3 = 39^e \bmod 51$~~

~~$e = \frac{3}{39} \bmod 51$~~

~~$e = 13^{-1} \bmod 51$~~

CUADRADOS REPETIDOS Clase 1116.

$$39^{13} \bmod 51 = 39^8 \cdot 39^4 \cdot 39 = 39^2 \cdot 39^2 \cdot 39^2 \cdots$$

$$= (33 \cdot 30 \cdot 39) \bmod 51; \boxed{3 = h(m)}$$

$$[39^2] = 39$$

$$[39^2]^2 = [39 \cdot 39] = 1821 \bmod 51 = 42$$

$$[39^2]^3 = [(39^2)^2] = [(39^2) \cdot 39^2] = 42 \cdot 41 \bmod 51 = 30$$

$$[39^2]^4 = [30 \cdot 30] = 900 \bmod 51 = 3$$

$e \circ d^{-1} \bmod \phi(n) \quad 5 \cdot d \equiv 1 \pmod{32}$

c) $h(m) = 39^{13} \bmod 51 =$

\downarrow

$$32 = 6 \cdot 8 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$\rightarrow \sim 2 \cdot 1 + 1$$

$$h(m) = 3 \checkmark$$

$$f = \lambda \cdot 54 \quad \cancel{M \cdot 32 \text{ mod } 32}$$

Códigos y Criptografía Grado en Ingeniería Informática

Examen escrito 2 (10% nota final)

2020

$$\begin{aligned} l &= 522 \\ 5 \cdot 2(32-6r) \end{aligned}$$

$$\begin{aligned} (13) \cdot 5 - 2 \cdot 32 \\ 11 \\ c = 13 \end{aligned}$$

Fecha: 01 diciembre 2020

Hora: 12:05–12:55

Lugar: Aula 101

Ayuda permitida: Cualquier tipo de material impreso: notas, apuntes, libros, ejercicios resueltos, ... No se permite ninguna ayuda de forma electrónica, salvo un ordenador portátil con un lector de ficheros pdf abierto, donde se puede consultar un libro electrónico o las pizarras de clase. En particular no debe tenerse abierto un explorador, SageMath o cualquier programa de email/mensajería. El wifi y datos deben estar desactivados.

Cualquier otro tipo de ayuda electrónica no se puede utilizar. Esto incluye calculadoras, teléfono móvil, tablets/pda, smartwatches, reproductores de música, ...

Nota: Todas las respuestas deben justificarse de forma razonada.

Nota: Escribe tu nombre y apellidos en todas las hojas que entregues.

Nota: El porcentaje al principio de cada ejercicio indica su valor en el examen.

Ejercicios: pueden encontrarse en la próxima página.

Ejercicio 1. (25%) Considera un canal sin ruido que transmite bits (1's y 0's) y considera el alfabeto fuente $\mathcal{A} = \{a, b, c, d, e\}$. Después de transmitir muchos símbolos, se ha hecho un estudio y se ha visto que la frecuencia (en tanto por uno) de cada símbolo a transmitir está dada por la siguiente tabla

Símbolo	a	b	c	d	e
Frecuencia	0.20	0.15	0.05	0.15	0.45

Same

- (a) Diseña una codificación trivial de los elementos de \mathcal{A} para este canal. ¿Cuál sería el número medio de bits usados para transmitir un símbolo de \mathcal{A} ?
- (b) Diseña un código compresor óptimo de acuerdo a las frecuencias mencionadas en la tabla (pista: Código de Huffman).
- (c) Usando el código compresor de la pregunta anterior: ¿Cuál es el número medio de bits usados para transmitir un símbolo de \mathcal{A} ?

Ejercicio 2. (40%) Sean $p = 3$ y $q = 17$. Considera el criptosistema RSA dado por los primos p y q , donde un mensaje es un número entre 0 y $pq - 1$.

- (a) Muestra que $e = 3$ es un exponente de cifrado válido.
- (b) Calcula el exponente de descifrado para $e = 3$.
- (c) ¿Qué datos deben ser públicos y privados en este criptosistema?
- (d) Cifra el mensaje $M = 8$ con la ayuda del exponente $e = 3$.
- (e) Descifra el mensaje que has obtenido en la pregunta anterior.

Nota: p, q, e y M han sido escogidos de forma que no es necesario utilizar una calculadora u ordenador para resolver este ejercicio.

Ejercicio 3. (10%) Considera el cifrado de César (método de sustitución desplazando 3 unidades) y cifra el siguiente mensaje: "EXAMEN FACIL".

Ejercicio 4. (25%) Alice y Bob quieren escoger una clave privada, pero sólo pueden comunicar a través de un canal inseguro. Por tanto, deciden usar el método de intercambio de claves de Diffie-Hellman con el primo $p = 11$ y $g = 2$, como elemento generador del grupo multiplicativo (no hace falta demostrar que p es primo o que g es un generador del grupo multiplicativo). Además, Alice escoge (al azar) el número $a = 4$ y Bob escoge (al azar) el número $b = 3$.

- (a) Dibuja un esquema donde se vea que números se transmiten Alice y Bob para acordar la clave.
- (b) ¿Cuál es la clave que acuerdan Alice y Bob?

Nota: p, g, a y b han sido escogidos de forma que no es necesario utilizar una calculadora u ordenador para resolver este ejercicio.

Ejercicio 1. (25%) Considera un canal sin ruido que transmite bits (1s y 0s) y considera el alfabeto fuente $A = \{a, b, c, d, e\}$. Despues de transmitir muchos simbolos se ha hecho un estudio y se ha visto que la frecuencia (en tanto por uno) de cada simbolo es la siguiente tabla

Símbolo	a	b	c	d	e
Frecuencia	0.20	0.15	0.05	0.15	0.05

Sam

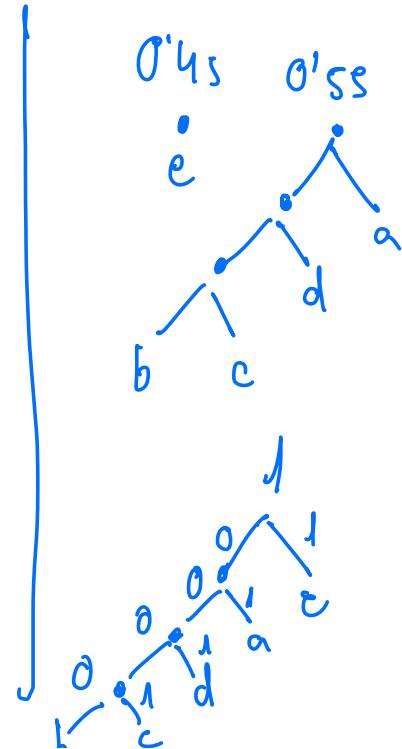
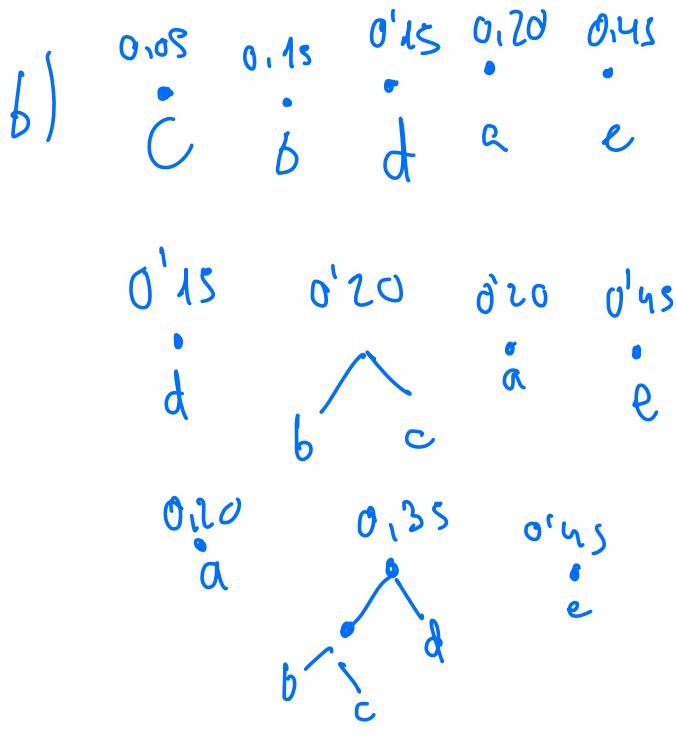
- (a) Diseña una codificación trivial de los elementos de A para este canal. ¿Cuál será el numero medio de bits usados para transmitir un simbolo de A ?
- (b) Diseña un código compresivo óptimo de acuerdo a las frecuencias mencionadas en la tabla (pista: Código de Huffman).
- (c) Usando el código compresivo de la pregunta anterior: ¿Cuál es el numero medio

a) 5 $2^2 < 5 < 2^3 \Rightarrow 3.6$ bits

Símbolo	a	b	c	d	e
Frecuencia	0.20	0.15	0.05	0.15	0.45

codificación trivial de los elementos de A para el

a. 000	01
b 001	0000
c 010	0001
d 011	001
e 100	1



Ejercicio 2. (40%) Sean $p = 3$ y $q = 17$. Considera el criptosistema RSA dado por los primos p y q , donde un mensaje es un número entre 0 y $pq - 1$.

- Muestra que $e = 3$ es un exponente de cifrado válido.
- Calcula el exponente de descifrado para $e = 3$.
- ¿Qué datos deben ser públicos y privados en este criptosistema?
- Cifra el mensaje $M = 8$ con la ayuda del exponente $e = 3$.
- Descifra el mensaje que has obtenido en la pregunta anterior.

a) $0 < e < \varphi(n)$

$$\varphi(n) = (p-1)(q-1) = 2 \cdot 16 = 32$$

$$0 < e < 32$$

$$\begin{array}{c} \parallel \\ 2 \end{array}$$

$$\text{mcd}(3, 32) = 1 \quad \checkmark$$

b) $d \equiv e^{-1} \pmod{\varphi(n)}$
 $\equiv 3^{-1} \pmod{32} = 3$

c) Públicos: n y e
 Privados: $d \Rightarrow p, q, \varphi(n)$

$$n = p \cdot q = 3 \cdot 17 = 51$$

$$d) M = 8 \quad e = 3$$

$$8^3 \bmod 51 = 24$$

$$e) C^d \bmod n \equiv M$$

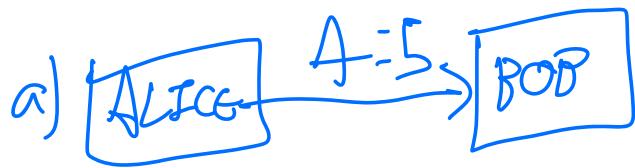
$$2^3 \bmod 51 = 8 \quad \checkmark$$

Ejercicio 3. (10%) Considera el cifrado de César (método de substitución desplazando 3 unidades) y cifra el siguiente mensaje: "EXAMEN FACIL".

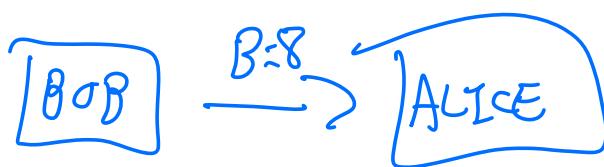
HADPHQ IDFLO

Ejercicio 4. (25%) Alice y Bob quieren escoger una clave privada, pero sólo pueden comunicar a través de un canal inseguro. Por tanto, deciden usar el método de intercambio de claves de Diffie-Hellman con el primo $p = 11$ y $g = 2$, como elemento generador del grupo multiplicativo (no hace falta demostrar que p es primo o que g es un generador del grupo multiplicativo). Además, Alice escoge (al azar) el número $a = 4$ y Bob escoge (al azar) el número $b = 3$.

- Dibuja un esquema donde se vea que números se transmiten Alice y Bob para acordar la clave.
 - ¿Cuál es la clave que acuerdan Alice y Bob?
- Nota: p, g, a y b han sido escogidos de forma que no es necesario utilizar una calculadora u ordenador para resolver este ejercicio.



$$q=4 \quad A = g^q \bmod p = 2^4 \bmod 11 = 5$$



$$b=3 \quad B = g^b \bmod p = 2^3 \bmod 11 = 8$$

b)

$$k = g^{ab} \bmod p = 2^{12} \bmod 11 = 4096 \bmod 11 = 4 //$$

Ej 4 ORD 2020. El GAMAL

$$p=11 \quad g=2 \quad M=7 \quad h(u)=4 \quad a=4 \text{ (Alice private)} \\ b=5 \text{ (Bob private)}$$

a) Alice: $M \xrightarrow[\beta=10]{\text{El GAMAL}} C$

Firma no incluida $k = \text{Aleatoria}$ $A = 2^4 \bmod 11 = 5$ $\alpha \text{ privada}$
 $Alice$ $B = 2^5 \bmod 11 = 10$ $Alice \rightarrow Bob \text{ (mensaje)}$
 $(firm)$

Transparencia: A Pública.
 $B \rightarrow Alice$ (mensaje)
 $Alice$

En el problema
 Alice \rightarrow Bob y Alice firma.
 clave pública = B : clave del receptor.
 clave privada: (b)

En nuestro caso

Alice: $M \rightarrow$

$$(g^k \bmod p, A^k \cdot M \bmod p)$$

aleatoria \downarrow nuestro caso

$$(B, C) \rightarrow (g^k \bmod p, B^k \cdot M \bmod p)$$

$$(g^b \bmod p, A^b \cdot M \bmod p)$$

$$(2^3 = 8, 10^3 \bmod 11 = 4) = (8, 4)$$

b es numero random
 a es = 11

la letra es la def

receptor al mando
 de clave publica

En Diffie-Hellman

$A = g^a \quad B = g^b$

Aquí si es k privada en el Gmail no

$$\begin{array}{ccc} & a & b \\ A = g^a & \xrightarrow{\hspace{2cm}} & B = g^b \\ \cancel{g^a} & & \cancel{g^b} \end{array}$$

$$\begin{array}{cc} B^a & A^b \\ g^{ab} & g^{ab} \end{array}$$

En el Gmail

Alice \rightarrow Bob

$$\begin{array}{cc} A & B^a = g^{ab} \end{array}$$

Cifrar publica receptor $a = \text{clave alice}$
 descifrar privada receptor.

$$g^a \in \{2, \dots, p-2\}$$

$$B = g^b \pmod{p}$$

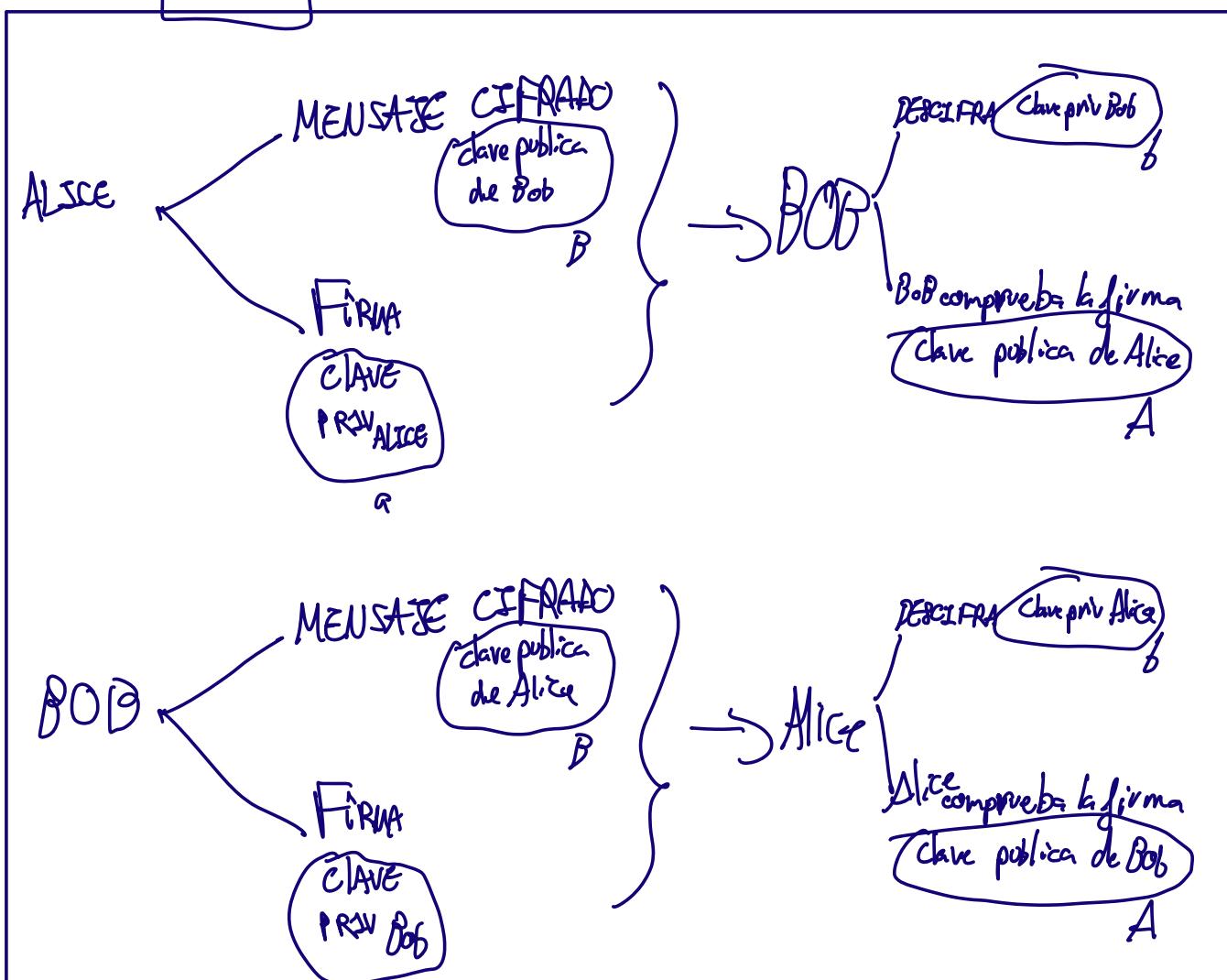
$$r = g^k \mod p$$

$$s = k^{-1} (h(M) - ar) \mod (p-1)$$

$$s = 7^{-1} (4 - 4 \cdot 2) \mod 10 = 8$$

3

$$S = 8$$



- a

$$(8, 4), (2, 8)$$

Mensaje Firma
cifrado

$$M = 4 \cdot (8^S)^{-1} \Rightarrow h(m) \vdash 4$$

Comp Firma
otk
 $1 \leq 7 \leq 10$

$$A^r \cdot r^s \equiv g^{h(u)} \pmod{p}$$

$$5^7 \cdot 7^8 \equiv 2^4 \pmod{11}$$

EL GAMAL

$$p = 11$$

$$g = 2$$

$$M = 7$$

$$\text{hash firmar } h(M) = 4$$

ALICE \rightarrow BOB
Clave priv alice: 4
,, " bob: 5

$$A = 2^5 \bmod 11 = 10$$

$$B = 2^4 \bmod 11 :$$

$$C = 10^4 \cdot 7 \bmod 11 =$$

CIFRADO EN BLOQUE $p=3 \Rightarrow n=51$ $\overbrace{N=2}^{\{0,1\}}$

$$N^k \leq n < N^{k+1}$$

$$32 = 2^5 \leq 51 < 2^6 = 64$$

BLOQUE: $10010 = M$

$m = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 18$

$0 \leq m \leq n$

$0 \leq m \leq 2^5 = 32 \leq 51 = n$

habrá que cambiarlo por los que no usamos de $\{3, 10\}$

$0 \leq m \leq 51$

Como $m \mod n = 18 \mod 51 = 18$

$$18 = 1 \cdot 2^4 + 2^1 = 10010$$

Lo haremos con $m=19$ 10011

$$c \equiv 19^{13} \pmod{51} = 49$$

$$49 = 1 \cdot 2^5 + 1 \cdot 2^4 + 1 = 110001$$

