

Question 5

Compromís

1 / 1 pt

✓ - 0 pts Correct

- 0.3 pts Incomplet o no proposa protocol
- 1 pt Incorrecte. Protocol no funciona
- 1 pt En blanc
- 1 pt El protocol no és de compromís. No és correcte el protocol.

Question 6

PGP

1 / 1 pt

✓ - 0 pts Correct

- 0.1 pts Falta el raonament o raonament incorrecte
- 0.5 pts Falta G i D com a marginal
- 0.3 pts Esteban no és vàlida perquè G i D no són vàlids.
- 1 pt Tot malament
- 0.2 pts Falta F i C com a vàlides
- 0.3 pts Confusió entre confiança i validesa

Question 7

RSA

0 / 1 pt

- 0 pts Correct

- 1 pt No volem una demostració sinó un raonament perquè és segur. És segur factoritzar és computacionalment costós.

✓ - 1 pt Raonament incorrecte.

Question 8

Xifrat homomòrfic

0 / 1 pt

- 0 pts Correct

✓ - 1 pt El resultat O el raonament és incorrecte

- 1 pt En blanc

Question 9

3 passos de Shamir

1 / 1 pt

✓ - 0 pts Correct

- 1 pt Incorrecte
- 0 pts Resposta en blanc
- 0 pts Solució incompleta

Question 10

Diffie-Hellman

1 / 1 pt

✓ - 0 pts Correcte

- 0.5 pts Plantejament correcte, càlculs incorrectes.

3. Com a part d'un protocol criptogràfic que esteu executant, acabeu de rebre un **certificat digital** X.509 i necessiteu comprovar-ne la seva validesa. Expliqueu **tres comprovacions** que hauríeu de fer per validar-lo.

Nota: hi ha més de tres comprovacions que s'haurien de fer per validar el certificat, però només cal que en detal·leu tres.

- comprovar la data d'autenticitat del missatge
- comprovar l'usuari que ho ha enviat (el seu ID)
- comprovar la validesa mitjançant el destinatari del certificat digital.

4. Al paper "An improved protocol for demonstrating possession of discrete logarithms and some generalizations" (Chaum, D., Evertse, J.H. and Graaf, J.V.D., 1987) s'explica un **protocol de coneixement nul** per demostrar el coneixement de logaritmes discrets sense realment revelar-los. En aquest protocol es proposa el següent intercanvi de missatges:

Pas	Provador (P)	Verificador (V)
1.	Tria $r \in_R \mathbb{Z}_p \setminus \{0, 1\}$ Calcula $c = g^r \pmod{p}$	$\xrightarrow{c}$
2.		$\xleftarrow{b}$ Tria un bit aleatori $b \in_R \{0, 1\}$
3.	Calcula $h = r + b \cdot x \pmod{p-1}$	$\xrightarrow{h}$
4.		Verifica que $c \cdot y^b = g^h \pmod{p}$

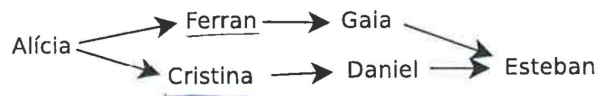
El Verificador ha instal·lat una llibreria insegura per a generar valors aleatoris i el bit que tria al Pas 2 és sempre 0. **Raona** quines implicacions té aquest fet per a la seguretat de l'esquema.

Que el bit triat al pas 2 sempre sigui 0, implica que el provador no necessita saber el missatge real  $x$  que s'ha enviat al verificador que ni que el coneix. Ja que si sempre es 0, quan el provador calcula  $h$ , el valor de  $h$  ja no dependrà del càlcul de  $b \cdot x$  con  $x$  es el missatge ja que aquest terme sempre resultaria 0, i per tant,  $h = r + 0$

5. L'Alícia i el Bernardo **volen jugar a cara i creu per telèfon**. Per aquest motiu, en Bernardo ha proposat que L'Alícia triarà un nombre molt gran ( $a$ ) i el Bernardo triarà un altre nombre molt gran ( $b$ ). Després s'intercanviaran els nombres triats per telèfon, de tal manera que si  $a + b$  **es parell**, guanyarà Alícia i en cas contrari, guanyarà el Bernardo. L'Alícia sap molt de criptografia i li diu al Bernardo que aquest protocol no és segur ja que el primer en enviar el nombre per telèfon jugaria en desavantatge. **Completa aquest protocol** que proposa en Bernardo fent servir un **compromís** de tal manera que cap jugador jugui en desavantatge.

S'hauran de comprometre per tant a afegir un prefix als dos nombres  $a$  i  $b$ , perquè així es pugui verificar que el nombre no ha estat modificat al rebre el nombre del contrari.

6. Al següent diagrama es veuen diferents certificats d'un **sistema distribuït** de signatura de claus. La notació  $A \rightarrow B$  vol dir que **A ha signat el certificat** de B. En aquest sistema una **clau és vàlida** si s'ha signat personalment, si s'ha signat amb una clau de **total confiança**, o bé, si ha estat signat per **dues claus** de confiança marginal.



Valid :  
- personalment  
- 1 full  
- 2 marginals

Si sabem que l'Alícia té una **confiança marginal** en el Ferran i la Cristina, raona quines claus considerarà l'Alícia com a vàlides **especificant el tipus de validesa**.

Alícia

Tipus	
Marginal	Full
Ferran	
Cristina	

→

Valid	
Marginal	Full
Gaia	Ferran
Daniel	Cristina

= Degut a que  
està signat  
personalment per  
l'Alícia (F i C)  
i la G i D  
estàn signats per  
un full

7. Raona per què l'algoritme criptogràfic de clau pública RSA és segur.

El algoritme criptogràfic de clau pública RSA és segur perquè assegura que un missatge signat només pot ser desxifrat per la persona destinatària. Així doncs, tot i que el missatge sigui interceptat, no es podria desxifrar sense la clau privada de destinari (destinataria). És a dir, només la persona que coneixi la clau privada  $(d, n)$ .



# ARCADE LAND



Medusa  
FESTIVAL



7 A 11 AGOSTO 2025

PLAYA DE CULLERA

ACT OF RAGE -  
AFROJACK -  
- ALESSO -  
- AMBER BROOS  
- ARMIN VAN BUUREN -  
- ART OF FIGHTERS  
- BEN SIMS  
- BRENDA SERNA -  
- CARL CRAIG -  
- CHARLOTT E DE WITTE  
- CRISTIAN VARELA -  
- D-BLOCK & STEFAN -  
- DENNIS CRUZ  
- DEXPHASE  
- DJ PEPO -  
- DUAL DAMAGE -  
- DYEN  
- EDU IMBERNON  
- ENDYMION  
- FATIMA HAJJI  
- FEDDE LE GRAND -  
- HARDWELL  
- HÉCTOR OAKS  
- JAMIE JONES -  
- KLANGKUE  
- NSTLER -  
- KREWELLA  
- LA LUNA LIVE -  
- LAIDBACK  
- LUKE -  
- LEE ANN ROBERTS  
- LILLY PALMER -  
- LUCIANO -  
- MANDY

Anaia Lucila Abad  
1608667

8. L'Àlícia ha trobat **una clau pública**  $pub1$ . La clau pertany al Bernardo que té la seva clau privada corresponent. La clau  $pub1$  és una clau del sistema de xifra Paillier (sistema de clau asimètrica homomòrfic). A més a més, l'Àlícia ha trobat el següent missatge ( $c1$ ):

$$c1 = \text{Encrypt\_Paillier}_{pub1}(23)$$

Fent servir la clau  $pub1$ ,  $c1$  i l'operació de multiplicació (\*), l'Àlícia crea el **següent missatge** ( $c2$ ):

$$c2 = \text{Encrypt\_Paillier}_{pub1}(2) * c1$$

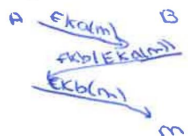
**Raona** quina informació obtindrà en Bernardo **desencriptant**, fent servir la seva clau privada, el missatge  $c2$ :

Com la clau pública es tenen dos missatges del Bernardo, significaria que podria desencriptar-ho tot. Sabent per tant que la informació rebuda seria la multiplicació dels dos missatges encriptats 23 i 2.

9. El **protocol de Shamir** entre dos nodes, A i B, funciona en tres etapes. **Primer**, A xifra un missatge amb la seva clau i envia el missatge xifrat a B ( $E_{ka}(m)$ ). En la **següent etapa**, B xifra aquest missatge amb la seva clau i el torna a enviar a A ( $E_{kb}(E_{ka}(m))$ ). En l'etapa **final**, A desxifra el segon missatge amb la seva clau i envia el resultat a B ( $E_{kb}(m)$ ). D'aquesta manera, B pot desxifrar aquest últim missatge per obtenir el missatge original. **Raona** les implicacions que té que l'algoritme de xifra en aquest context sigui  $E_k(m) = k \oplus m$ .

Si l'algoritme de xifra es  $\oplus$  tindrà implicacions negatives, degut a que si es intercepta per algú, no molt fàcil adivinar el missatge en clau. Això es perquè s'encrpta igual que es desencripta, es a dir, amb la mateixa operació i valor  $k$ .

$$ka \oplus m \oplus kb \oplus m \oplus ka \oplus m \oplus kb \oplus m$$



10. Per establir una clau **simètrica** l'Àlícia i el Bernardo utilitzen el protocol **Diffie-Hellman** (DH) amb els següents valors públics: el primer  $p = 1291$  i el generador  $g = 44$ . A més, el generador pseudoaleatori que fa servir l'Àlícia retorna sempre el valor 3 i el d'en Bernardo el valor 5. Quina **clau compartida** acabaran derivant l'Àlícia i el Bernardo amb l'execució del protocol?

Nota: Podeu fer servir els valors de la taula de l'última pàgina d'aquest examen per tal de calcular la clau compartida.  $p = 1291$ ,  $g = 44$ ,  $a = 3$ ,  $b = 5$

Àlícia		Bernardo
$a = 3$		$b = 5$
$g^a \mod p = 44^3 \mod 1291 = 1269$	$\longrightarrow$	$A = 1269$
$B = 11$	$\longleftarrow$	$g^b \mod p = 44^5 \mod 1291 = 11$
$B^a \mod p = 11^3 \mod 1291 = 40$		$A^b \mod p = 1269^5 \mod 1291 = 40$

Per tant ara comparteixen la clau 40.



Taula de potències modulars:

$44^2 \bmod 1291 = 645$	$1291^2 \bmod 44 = 5$	$3^2 \bmod 1291 = 9$
$44^3 \bmod 1291 = 1269$	$1291^3 \bmod 44 = 31$	$3^3 \bmod 1291 = 27$
$44^4 \bmod 1291 = 323$	$1291^4 \bmod 44 = 25$	$3^4 \bmod 1291 = 81$
$44^5 \bmod 1291 = 11$	$1291^5 \bmod 44 = 23$	$3^5 \bmod 1291 = 243$
$44^6 \bmod 1291 = 484$	$1291^6 \bmod 44 = 37$	$3^6 \bmod 1291 = 729$
$44^7 \bmod 1291 = 640$	$1291^7 \bmod 44 = 27$	$3^7 \bmod 1291 = 896$
$44^8 \bmod 1291 = 1049$	$1291^8 \bmod 44 = 9$	$3^8 \bmod 1291 = 106$
$44^9 \bmod 1291 = 971$	$1291^9 \bmod 44 = 3$	$3^9 \bmod 1291 = 318$
$44^{10} \bmod 1291 = 121$	$1291^{10} \bmod 44 = 1$	$3^{10} \bmod 1291 = 954$
$44^{11} \bmod 1291 = 160$	$1291^{11} \bmod 44 = 15$	$3^{11} \bmod 1291 = 280$
$44^{12} \bmod 1291 = 585$	$1291^{12} \bmod 44 = 5$	$3^{12} \bmod 1291 = 840$
$44^{13} \bmod 1291 = 1211$	$1291^{13} \bmod 44 = 31$	$3^{13} \bmod 1291 = 1229$
$44^{14} \bmod 1291 = 353$	$1291^{14} \bmod 44 = 25$	$3^{14} \bmod 1291 = 1105$
$44^{15} \bmod 1291 = 40$	$1291^{15} \bmod 44 = 23$	$3^{15} \bmod 1291 = 733$
$44^{16} \bmod 1291 = 469$	$1291^{16} \bmod 44 = 37$	$3^{16} \bmod 1291 = 908$
$44^{17} \bmod 1291 = 1271$	$1291^{17} \bmod 44 = 27$	$3^{17} \bmod 1291 = 142$
$44^{18} \bmod 1291 = 411$	$1291^{18} \bmod 44 = 9$	$3^{18} \bmod 1291 = 426$
$44^{19} \bmod 1291 = 10$	$1291^{19} \bmod 44 = 3$	$3^{19} \bmod 1291 = 1278$
$44^{20} \bmod 1291 = 440$	$1291^{20} \bmod 44 = 1$	$3^{20} \bmod 1291 = 1252$
...	...	...
$44^{43} \bmod 1291 = 1100$	$1291^{43} \bmod 44 = 31$	$3^{43} \bmod 1291 = 1046$
$44^{44} \bmod 1291 = 633$	$1291^{44} \bmod 44 = 25$	$3^{44} \bmod 1291 = 556$
$44^{45} \bmod 1291 = 741$	$1291^{45} \bmod 44 = 23$	$3^{45} \bmod 1291 = 377$

$5^2 \bmod 1291 = 25$	$1269^2 \bmod 1291 = 484$	$11^2 \bmod 1291 = 121$
$5^3 \bmod 1291 = 125$	$1269^3 \bmod 1291 = 971$	$11^3 \bmod 1291 = 40$
$5^4 \bmod 1291 = 625$	$1269^4 \bmod 1291 = 585$	$11^4 \bmod 1291 = 440$
$5^5 \bmod 1291 = 543$	$1269^5 \bmod 1291 = 40$	$11^5 \bmod 1291 = 967$
$5^6 \bmod 1291 = 133$	$1269^6 \bmod 1291 = 411$	$11^6 \bmod 1291 = 309$
$5^7 \bmod 1291 = 665$	$1269^7 \bmod 1291 = 1286$	$11^7 \bmod 1291 = 817$
$5^8 \bmod 1291 = 743$	$1269^8 \bmod 1291 = 110$	$11^8 \bmod 1291 = 1241$
$5^9 \bmod 1291 = 1133$	$1269^9 \bmod 1291 = 162$	$11^9 \bmod 1291 = 741$
$5^{10} \bmod 1291 = 501$	$1269^{10} \bmod 1291 = 309$	$11^{10} \bmod 1291 = 405$
$5^{11} \bmod 1291 = 1214$	$1269^{11} \bmod 1291 = 948$	$11^{11} \bmod 1291 = 582$
$5^{12} \bmod 1291 = 906$	$1269^{12} \bmod 1291 = 1091$	$11^{12} \bmod 1291 = 1238$
$5^{13} \bmod 1291 = 657$	$1269^{13} \bmod 1291 = 527$	$11^{13} \bmod 1291 = 708$
$5^{14} \bmod 1291 = 703$	$1269^{14} \bmod 1291 = 25$	$11^{14} \bmod 1291 = 42$
$5^{15} \bmod 1291 = 933$	$1269^{15} \bmod 1291 = 741$	$11^{15} \bmod 1291 = 462$
$5^{16} \bmod 1291 = 792$	$1269^{16} \bmod 1291 = 481$	$11^{16} \bmod 1291 = 1209$
$5^{17} \bmod 1291 = 87$	$1269^{17} \bmod 1291 = 1037$	$11^{17} \bmod 1291 = 389$
$5^{18} \bmod 1291 = 435$	$1269^{18} \bmod 1291 = 424$	$11^{18} \bmod 1291 = 406$
$5^{19} \bmod 1291 = 884$	$1269^{19} \bmod 1291 = 1000$	$11^{19} \bmod 1291 = 593$
$5^{20} \bmod 1291 = 547$	$1269^{20} \bmod 1291 = 1238$	$11^{20} \bmod 1291 = 68$
...	...	...
$5^{43} \bmod 1291 = 855$	$1269^{43} \bmod 1291 = 947$	$11^{43} \bmod 1291 = 347$
$5^{44} \bmod 1291 = 402$	$1269^{44} \bmod 1291 = 1113$	$11^{44} \bmod 1291 = 1235$
$5^{45} \bmod 1291 = 719$	$1269^{45} \bmod 1291 = 43$	$11^{45} \bmod 1291 = 675$

