Criptografia i Seguretat **10 de Juny 2024**
Curs 2024 **Segon Parcial**

Nom i Cognoms: _____

NIU: _____

Puntuació: Exercicis 1-10: 1 punt
Duració: 110 minuts.

Assistència a classe en percentatge: %
Hores estudiades per aquest examen: hores
Gràcies per contestar aquestes preguntes que no tindran cap impacte en l'avaluació.

1. En un sistema de comunicacions basat en **criptografia de clau pública**, tres usuaris disposen dels següents parells de claus:

Usuari	Parell de claus (pública, privada)
Alícia	(PK_A, sk_A)
Bernat	(PK_B, sk_B)
Carlota	(PK_C, sk_C)

(1) En Bernat vol enviar a l'Alícia un missatge **confidencial**. Quina clau farà servir per aconseguir-ho?

(2) L'Alícia ha rebut un missatge **autenticat** de la Carlota. Quina clau farà servir per validar-lo?

2. En George Lucas acaba de finalitzar la producció de l'última pel·lícula d'Indiana Jones i està molt satisfet amb el resultat final. Per assegurar que ningú canvia cap escena de la pel·lícula i deixar constància del seu vist-i-plau d'aquesta versió, decideix fer una **signatura digital** fent servir **RSA** del fitxer de vídeo que conté la pel·lícula.

   Vosaltres, com a experts en criptografia, li recomaneu que abans de fer la signatura, calculi el **hash** del fitxer de vídeo, i que després signi aquest hash. Per què li heu fet aquesta recomanació?

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 detalleu tres.

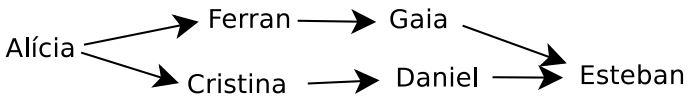
4. Al paper "*An improved protocol for demonstrating possession of discrete logarithms and some generalizations*" (Chaum, D., Evertse, J.H. and Graaf, J.V.D., 1987) s'explica un **protocol de coneixement nul** per demostrar el coneixement de logaritmes discrets sense realment revelar-los. En aquest protocol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

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.

6. Al següent diagrama es veuen diferents certificats d'un **sistema distribuït** de signatura de claus. La notació A->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.



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**.

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

8. L'Alícia 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'Alícia ha trobat el següent missatge ($c1$):

   - $c1 = Encrypt\_Paillier_{pub1}(23)$

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

   - $c2 = Encrypt\_Paillier_{pub1}(2) * c1$

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

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 $E_k(m) = k \oplus m$.

10. Per establir una clau **simètrica** l'Alícia 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'Alícia retorna sempre el valor 3 i el d'en Bernardo el valor 5. Quina **clau compartida** acabaran derivant l'Alícia 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.

Taula de potències modulars:

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

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