

SegonParcialCriptografia.pdf



alucero



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



Segon parcial

● Graded

Student

Total Points

Question 1

Claus cripto asimètrica

0.5 / 1 pt

– 0 pts Correcte

– 0.5 pts Apartat (1) incorrecte.

✓ – 0.5 pts Apartat (2) incorrecte.

Question 2

Hash per signar

■ 0 / 1 pt

– 0 pts Correcte!

– 0.25 pts Falta contextualitzar la resposta en relació a l'algorisme de signatura RSA.

✓ – 1 pt Resposta incorrecta.

💬 Però aquesta garantia ja l'aconseguim sense introduir el hash (només amb la signatura del missatge).

Question 3

Validació certificat

0 / 1 pt

– 0 pts Correcte!

– 0.3 pts Falta una comprovació o comprovació incorrecta (o bé comprovacions majoritàriament correctes).

– 0.6 pts Falten dues comprovacions o són incorrectes (o bé comprovacions parcialment correctes).

✓ – 1 pt Resposta incorrecta.

– 1 pt Resposta en blanc.

Question 4

ZK logaritme discret

0.9 / 1 pt

– 0 pts Correcte!

✓ – 0.1 pts Falta comentar que es compromet la solvència (*soundness*) del protocol.

– 0.5 pts Resposta parcialment correcta, ben encaminada.

– 1 pt Resposta incorrecta.

– 1 pt Resposta en blanc.

Necesito
concentración

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

WUOLAH

WUOLAH

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.

Importante

Puedo eliminar la publi de este documento con 1 coin

¿Cómo consigo coins?

Plan Turbo: barato

Planes pro: más coins

perdo
espacio



Criptografia i Seguretat Curs 2024

10 de Juny 2024
Segon Parcial

Nom i Cognoms: _____

NIU: _____

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

Assistència a classe en percentatge: 50 %
Hores estudiades per aquest examen: 5 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)
Àlícia	(PK_A, sk_A)
Bernat	(PK_B, sk_B)
Carlota	(PK_C, sk_C)

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

- (2) L'Àlícia ha rebut un missatge **autènticat** 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 $c \cdot y^h = g^h \pmod{p}$

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 revelar el seu secret x perquè el verificador
pot verificar la prova sense necessitat de conèixer x .

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 Anual <input type="checkbox"/>	0,99 € / mes	3,99 € / mes	7,99 € / mes

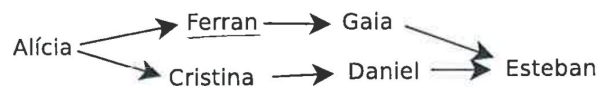
Ahora que puedes conseguirlo,
¿Qué nota vas a sacar?



WUOLAH

5. L'Àlícia i el Bernardo **volen jugar a cara i creu per telèfon**. Per aquest motiu, en Bernardo ha proposat que L'Àlícia 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 Àlícia i en cas contrari, guanyarà el Bernardo. L'Àlícia 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 $A \rightarrow B$ 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.



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

Alicia

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

un munt de coses

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

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** ($c2$):

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

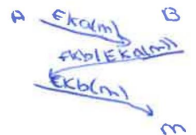
Raona quina informació obtindrà en Bernardo **desencriptant**, fent servir la seva clau privada, el missatge $c2$:

Com la clau pública es les dos muntades del Bernardo significarà
... mació
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 averiguar el missatge en clau. Això es vegeu n'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

$$a = 3$$

$$\text{mod } p = 44^3 = 1269$$

Bernardo

$$b = 5$$

$$A = 1269$$
$$b \text{ mod } a = 44^5 \text{ mod } 1291 = 11$$
$$269^5 \text{ mod } 1291$$
$$= 40$$

WUOLAH

Taula de potències modulars:

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

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

