# PrimerParcialCriptografia.pdf


alucero

Criptografia i Seguretat

3º Grado en Ingeniería de Datos

Escuela de Ingeniería
Universidad Autónoma de Barcelona



# Primer parcial

● Graded

**Student**

**Total Points**

**Question 1**

## Cèsar

1 / 1 pt

✔ **– 0 pts** Correct

**– 1 pt** No fa servir suma o bé està en blanc.

**Question 2**

## AES 2

0.5 / 1 pt

**– 0 pts** Correct

**– 0.5 pts** Polinomi malament

✔ **– 0.5 pts** Operació malament

**– 1 pt** Tot malament

**Question 3**

## Contrasenyes 2

0.5 / 1 pt

**– 0 pts** Correct

**– 1 pt** Incorrecte

✔ **– 0.5 pts** Click here to replace this description.

**Question 4**

## Hash

0.25 / 1 pt

**– 0 pts** Correcte!

✔ **– 0.75 pts** Falta justificar perquè no és possible (o bé la justificació és totalment errònia).

**– 0.5 pts** La justificació no és del tot correcta.

**– 0.25 pts** El raonament és correcte, però no hauríem de poder limitar la mida de l'entrada.

**– 1 pt** Resposta incorrecta.

**– 1 pt** Resposta en blanc.

**Question 5**

**LFSR** **0** / 1 pt

– **0 pts** Correcte!

– **0.5 pts** Falta la justificació (o la justificació és errònia).

– **0.5 pts** Falta indicar quin és el període.

– **1 pt** Resposta incorrecta.

✔ – **1 pt** Resposta en blanc (o no es respon a la pregunta).

**Question 6**

**CBC** **0** / 1 pt

– **0 pts** Correcte!

– **0.5 pts** L'error no es propagarà més enllà del bloc $m_{j+1}$.

– **0.75 pts** L'error també afecta al següent bloc ($m_{j+1}$).

✔ – **1 pt** Resposta incorrecta.

– **1 pt** Resposta en blanc.

**Question 7**

Invers **0.15** / 1 pt

7.1 **Càlcul** **0.15** / 0.5 pts

– **0 pts** Correcte!

✔ – **0.1 pts** Falta indicar el mètode utilitzat per calcular l'invers (o el mètode indicat és erroni).

✔ – **0.25 pts** Falta acabar de desenvolupar els càlculs per trobar el resultat.

– **0.25 pts** Càlculs erronis (plantejament correcte).

– **0.5 pts** Resposta errònia. Resultat i plantejament incorrectes.

– **0.5 pts** Resposta en blanc.

7.2 **Comprovació** **0** / 0.5 pts

– **0 pts** Correcte!

– **0.25 pts** Resposta parcialment correcta.

– **0.5 pts** Resposta incorrecta.

✔ – **0.5 pts** Resposta en blanc (o falta demostrar que el resultat és correcte).

Question 8

## Filtre Bloom

1 / 1 pt

✔ – 0 pts Correcte!

– 0.5 pts Resposta incorrecta, però ben encaminada. Amb 5 elements com a molt hi haurà 10 bits fixats a 1.

– 0.75 pts Resposta incorrecta. El mínim nombre d'elements es dona quan les dues funcions hash retornen valors diferents per als elements afegits.

– 1 pt Resposta incorrecta.

– 1 pt Resposta en blanc.

Question 9

## A5

1 / 1 pt

✔ – 0 pts Correct

– 1 pt Resposta incorrecte

– 0.5 pts La resposta no és del tot correcte. Hi ha errors de concepte.

Question 10

## Blockchain

1 / 1 pt

✔ – 0 pts Correcte

– 1 pt No s'explica com s'aconsegueix la dificultat de tancar un bloc i com aquesta és dinàmica.

**Criptografia i Seguretat** **15 d'abril 2024**
**Curs 2023/2024** **Primer 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 ti... ...n cap impacte en l'avaluació.

1. Donat el següent t **xifrat amb Cèsar** (algorisme de substitució monoalfabétic monogràmic):

```
Þḿ ol ohk hufaopun jvumpkluaphs av zhf, ol dyval pa
pu jpwoly, aoha pz, if zv johunpun aol vykly vm aol
slaalyz vm aol hswohila, aoha uva h dvyk jvbsk il thkl vba.
```

Si sabem que la clau $k$ és 7. Indica com podem desxifrar cadascun dels elements fent servir una expressió que no faci servir la resta sinó la suma.

2. A l'algorisme **AES** el primer byte de la matriu d'estats d'entrada és "11".

   a) Quin polinomi representa?

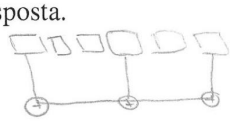
   b) Quin és el resultat de l'operació "11" $\otimes$ "02" mod $x^8 + x^4 + x^3 + x + 1$?

3. Considerem un **sistema de contrasenyes** que fa servir contrasenyes de 10 caràcters on cada caràcter pot tenir 32 possibles valors i, addicionalment, una salt de 16 caràcters. Volem trencar la contrasenya d'un usuari en concret. Indica el nombre màxim d'operacions que haurem de fer. Descriu bé cadascuna de les operacions $n = 10$, $a = 32$ $s = 16$

4. És possible dissenyar una **funció hash criptogràfica** que no presenti col·lisions? Raona la teva resposta.

5. Donat un **LFSR** (*Linear Feedback Shift Register* o Registre de Desplaçament Realimentat Linealment) amb polinomi de connexions $C(x) = x^5 + x^2 + 1$. Si aquest polinomi és **primitiu**, quin serà el període de la seqüència que generarà? Justifica la resposta.

El període de la seqüència serà finit ja que en algun moment es tornarà a repetir la seqüència. Aquest concret serà que el polinomi entri en un bucle, tot i que potser no es iniciat al temps 0.



6. Als sistemes de xifra simètrics, el mode ***Cipher Block Chaining*** (CBC) xifra qualsevol bloc $i$ de manera que $c_i = E_k(m_i \oplus c_{i-1})$. Si es produeix un error d'un bit al bloc xifrat $c_j$, descriviu com afectarà aquest error al text en clar resultant de desxifrar. Quins blocs de text en clar es veuran afectats per aquest error?

hopii

# Productos de Apple a precios que no parecen de Apple. ¿Suena bien, no?

**Escanea y consigue hasta un 25% de descuento**

Una iniciativa de
Mutualidad

**electronica.hopii.es**

7. (a) Calculeu $2^{-1} \mod 39$ (és a dir, l'**invers de 2 mòdul 39** per l'operació **multiplicació**). Quin mètode heu fet servir per trobar l'invers?

(b) Demostreu que el resultat trobat és correcte.

8. Un **filtre de bloom** F gestiona la pertinença d'un NIU a un grup d'aquesta assignatura. En un moment donat el filtre F té el valor 01111111000100100101 ($f_0, f_1, f_2, ..., f_{19}$). Si aquest filtre de bloom fa servir les dues funcions hash H1 i H2 definides a continuació, quin és el nombre mínim d'elements que conté el filtre en aquest moment?

   - **La funció H1** d'un nombre suma el primer dígit i l'últim i aplica mòdul 15. Si el nombre només té un dígit el segon dígit és 0. Per exemple: H1(7) = 7, H1(46) = 10, H1(7029) = 1.
   - **La funció H2** d'un nombre suma tots els dígits del nombre i aplica mòdul 20. Per exemple: H2(7) = 7, H2(46) = 10, H2(7029) = 18.

9. A l'algorisme A5, **què són i què aporten** els *clocking bits*?

10. A una **blockchain**, com es pot assegurar que es creïn els blocs a una velocitat més o menys constant?