PrimerParcial2023.pdf

alucero

Criptografia i Seguretat

3º Grado en Ingeniería de Datos

Escuela de Ingeniería
Universidad Autónoma de Barcelona

Criptografia i Seguretat **19 d'abril 2023**
Curs 2023 **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 tindran cap impacte en l'avaluació.

1. Donat el següent text **xifrat amb Vigenère**:

```
VOPVC FRTCU MBGHG KGSCT YKTNJ MPKIB VGYQE YSSRK YYEEJ GWGVQ
RGPST LNDIF VIOMM TGGYU SLGZN CZCJE YGGSJ VGJIJ DSLRV ARWCY
ECOTP VWYUS CEIQL SQLIP DMLGW RJEQJ IAZFG JIJRO RRILV OFGWÑ
ZXYCY QHWYE NNKIB VPYUV GUHNE HCVWR RFYZQ EJIQR HNLVY KWSWV
GJYLR GAZHC EXCUY PRQRV YLNMY AIBVG YTIPZ ECEFN LWSRQ YIYCC
IÑJST GGNMQ YWVYT XSJEC EOYTE BVVY ...
```

Observem dues cadenes de **4 lletres** repetides una vegada, KIBV i GJIJ. A més, hi ha quatre cadenes més de **3 lletres** repetides també una vegada, TGG, YUS, VGJ i ECE. Les distàncies que separen aquestes cadenes són:

KIBV = 135; GJIJ = 48; TGG = 189; YUS = 39; VGJ = 114; ECE = 33

(a) Quina pot ser la **mida de la clau** que s'ha fet servir i perquè?

(b) Quina avantatge té aquest criptosistema respecte el del Cèsar (c=m+k mod 27)?

2. Considerant els **LFSR** analitzats en criptografia simètrica:

(a) **Explica quina és la seva finalitat** relacionant-los amb el sistema de xifra **Vernam** (aquell que està basat en xor).

3. Donades les següents **funcions hash** H1 i H2, amb el següent comportament:

   - **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 multiplica l'últim dígit per 5 i aplica mòdul 20. Per exemple: H2(7) = 15, H2(46) = 10, H2(7029) = 5.

   Trobeu una segona preimatge (o una col·lisió feble) pel missatge "2027" i la funció H2.

4. Raona quines col·lisions són **més complicades** de trobar les fortes o les febles. Posa un exemple referenciant la funció H1.

5. Donat un sistema de xifra **simètric** $E_k()$, proposa un algorisme perquè dos entitats A i B que comparteixen una clau k puguin enviar-se missatges **de manera autèntica però no confidencial**. Descriu les operacions que han de fer tant A com a B.

6. Als sistemes de xifra simètrics, en el mode ***Electronic Code Book*** (ECB) on per qualsevol bloc i, $c_i = E_k(m_i)$, digueu un punt **positiu** i un **negatiu** d'aquest mode de xifrar la informació.

7. (a) Quin **conjunt** es mesura amb la funció $\Phi(n)$ d'Euler? Dona una utilitat a aquesta funció.

   (b) Quin és el valor de $\Phi(59)$, essent 59 un nombre primer?

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** de l'exercici 3, raona si el NIU 23131 està inclòs al filtre de bloom o no.

9. Proposem un **sistema de xifra** que per cada element m ($m \in [0..26]$) es xifra de la següent manera:

   ```
   c = (4 * m + 4) mod 27
   ```

   (a) Com faríem per **desxifrar** c?

   (a) I si ara xifrem de la següent manera?

   ```
   c = (9 * m + 4) mod 27
   ```

10. Una blockchain per emmagatzemar números primers té els següents camps als blocs:

    - **Hash anterior:** hash del bloc precedent (2 xifres decimals).
    - **Nombre primer:** Nombre primer que es vol emmagatzemar.
    - **Nonce:** valor que fan servir els miners per tancar un bloc (2 xifres decimals).

    Els blocs es representen com a nombres decimals. Per exemple, el bloc amb el camp **Hash anterior** amb valor 91 que vol emmagatzemar el **nombre primer** 29 i fa servir el **Nonce** 16 dona la xifra decimal 912916.

    (a) Fent servir la **funció hash H1 de l'exercici 3**, **proposa una condició dinàmica** per acceptar un bloc com a vàlid en aquesta blockchain per afavorir que es mini més durant el cap de setmana que els dies entre setmana.

    (b) Posa un **exemple de bloc** vàlid.