INFORMACIÓ I SEGURETAT
7 de juny de 2021

Nom i cognoms (en MAJÚSCULES): _____ NIU: _____ Grup:___

Nota: Cal que **justifiqueu convenientment** totes les respostes.

1. (3.5 punts, 1+0.5+1+1)

   Sigui C un codi del que coneixem una matriu generadora

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

   (a) Doneu els paràmetres n, k, d del codi C.

   (b) Construïu la taula estàndard del codi C.

   (c) Descodifiqueu (**corregint errors i donant la informació associada**) la seqüència 1101110010".

   (d) Doneu la matriu de control del codi estès C^* de C i digueu quina és la distància mínima del codi C^*.

Solució:

(a) La matriu generadora G és sistemàtica en les dues últimes posicions, o sigui que la matriu de control serà:

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

És fàcil veure que el mínim nombre de columnes dependents de H és 3 (per exemple la segona, la tercera i la cinquena columnes són dependents).

Els paràmetres de C són: $n = 5, k = 2, d = 3$.

(b) El codi C és 1-corrector, o sigui que la taula estàndard tindrà com entrades tots els vectors possibles en els quals hi hagi 1 error com a màxim.

Per cada entrada e_i calculem la síndrome $H(e_i)$ i obtenim:

vectors d'error	Síndrome
(00000)	(000)
(10000)	(100)
(01000)	(010)
(00100)	(001)
(00010)	(111)
(00001)	(011)

(c) Per descodificar la seqüencia rebuda 1101110010 la tractarem com dos vectors consecutius, $v_1 = (11011)$ i $v_2 = (10010)$. Primer de tot calcularem la síndrome, $H(v_1) = (010)$, $H(v_2) = (011)$. El primer vector rebut, mirant la taula estàndard observem que l'error corresponent a v_1 és (01000). Corregint l'error podem assegurar que la corresponent paraula-codi és (10011). En quan al segon vector rebut, mirant la taula estàndard observem que l'error corresponent a v_2 és (00001) i, corregint l'error, la corresponent paraula-codi és (10011).

Com que el codi C te la matriu generadora sistemàtica en les dues últimes columnes, podem escriure que la informació associada a v_1 i v_2 com (11) i (11), respectivament.

(d) La matriu de control del codi estès de C té com a matriu de control:

$$H^* = \left(\begin{array}{ccccc|c} 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right)$$

El mínim nombre de columnes linealment dependents a H^* és 4 (per exemple les columnes $2, 3, 5$) o sigui que la distància mínima del codi estès C^* és 4.

2. (1,5 punts) Escriviu una matriu generadora d'un codi lineal tal que les seves paraules-codi (x, y, z, t, u) compleixin:

$$\begin{aligned} x + t &= 0 \\ z + t + u &= 0 \\ x + y + z + t &= 0 \end{aligned}$$

Solució: Les equacions donades ens permeten escriure una matriu de control per aquest codi:

$$H = \left(\begin{array}{ccccc} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{array}\right).$$

A continuació, fent operacions amb les files podem obtenir una matriu sistemàtica:

$$H = \left(\begin{array}{ccccc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right).$$

I, finalment, la matriu generadora que ens demanen:

$$G = \left(\begin{array}{ccccc} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{array}\right).$$

3. (1 punt) L'Anna i en Bernat decideixen utilitzar el protocol quàntic de Bennett-Brassard per a intercanviar-se una clau de sessió.

Quants fotons (aproximadament) ha d'enviar l'Anna a en Bernat per obtenir una clau compartida de 400 bits amb una probabilitat d'un $99,99\%$ de que no hi hagi espies en el canal?

Indicació: $\log(0.75, 0.01) \approx 16$.

Solució: La probabilitat de detectar un espia és d'un 25% en cada fotó enviat en el que els polaritzadors de l'Anna i d'en Bernat coincideixen. En el nostre cas volem que

$$P_d = 1 - (0.75)^k \approx 0.9999,$$

on k són els fotons que hem de desvetllar per assegurar que detectem un espia amb una probabilitat d'aproximadament el $99,99\%$.

Sabem que $(0.75)^{16} \approx 0.01$, o sigui que $(0.75)^{32} \approx 0.0001$ i, per tant, desvetllant 32 fotons dels no desestimats inicialment obtenim una probabilitat de detectar a l'espia de $P_d = 1 - (0.75)^{32} \approx 0,9999$,

Cada fotó enviat per l'Anna a en Bernat té una probabilitat d'un 50% de ser desestimat (és el cas en què l'Anna i en Bernat fan servir polaritzadors diferents). Por obtenir una clau vàlida de 400 bits hauríem de poder obtenir 432 fotons "no desestimats". O sigui que n'hauríem d'enviar aproximadament **864**.

4. (2,5 punts = 1+0,5+1)

   En una PKI basada en el criptosistema RSA és coneguda la clau pública d'en Josep $(n_J, e_J) = (1524212467931, 25)$. La nostra clau pública, en aquest criptosistema, és $(n_U, e_U) = (97546397927339, 3)$ i la nostra clau privada es basa en el coneixement de $n_U = pq = 9876553 \cdot 9876563$.

   (a) Calculeu la nostra clau privada d_U (deixeu indicades les operacions que no sigueu capaços de fer).

   (b) En Josep ens envia $c = 100$, que és el missatge m una vegada l'ha xifrat amb la nostre clau pública. També ens envia la signatura d'aquest missatge m, que val $s = 50$.

      i. Quin és el missatge en clar, m? (deixeu indicades les operacions que no sigueu capaços de fer).

      ii. Com ho hem de fer per validar aquest missatge xifrat c, com a provinent d'en Josep?

   Solució:

   (a) $d_U = 3^{-1} \pmod{\phi(n_U)}$, en què $\phi(n_U) = 9876552 \cdot 9876562$.

   (b) A partir de $c = 100$, $s = 50$ i el valor d_U calculat anteriorment:

      i. $m = 100^{d_U} \pmod{n_U}$.

      ii. Per validar si c prové d'en Josep hem de calcular $s^{(e_J)} \pmod{n_j}$ i comprovar si aquest valor coincideix amb m (calculat a l'apartat anterior).

5. (1,5 punts) Poseu una "F"davant de les funcions que siguin "fàcils"de calcular des d'un punt de vista de la complexitat computacional i una "D"davant de les "difícils".

   Les respostes correctes puntuen 0.15 punts i les incorrectes -0.15 punts. La qualificació mínima serà de zero punts.

   (a) ☐ Multiplicar nombres enters.

   (b) ☐ Multiplicar nombres enters mòdul un nombre primer.

   (c) ☐ Descomposar en factors un nombre enter i trobar tots els seus divisors.

   (d) ☐ Calcular el màxim comú divisor de dos enters.

   (e) ☐ Calcular $a^x \pmod{p}$, en què a, x, p són nombres enters i, a més a més, p és primer.

   (f) ☐ Donat el valor de y, en què $y = a^x \pmod{p}$ i a, x, p (p és primer) són enters coneguts, calcular el valor de x.

   (g) ☐ Calcular l'arrel quadrada d'un enter a mòdul p, en què p és primer.

   (h) ☐ Calcular l'arrel quadrada d'un enter mòdul n, en què n és el producte de dos primers.

   (i) ☐ Calcular el valor de la funció d'Euler.

   (j) ☐ Calcular l'invers d'un element a $\mathbf{Z}_m$.

   Solució: FFDF FDFD DF