INFORMACIÓ I SEGURETAT
2 de juliol de 2019

Nom i cognoms: _____ NIU: _____ Grup: _____

- Cal que **justifiqueu convenientment** totes les respostes.
- $\log 3 = 1.58$, $\log 5 = 2.32$, $\log 7 = 2.80$, $\log 23 = 4.52$.

1. (1.5 punt 1+0.5) Considereu la font $S = \{a_1, a_2, a_3, a_4, a_5\}$ amb distribució de probabilitats $\{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}\}$.
   (a) Doneu un codi binari òptim C per a la font S. Quina és la longitud mitjana del codi C? Quina és la seva eficiència?
   (b) Si fem servir un codi binari de longitud fixa, pot ser òptim?

   Solució:

   (a) Aplicant l'algorisme de Huffman, obtenim el següent codi binari òptim: $C = \{10, 00, 01, 110, 111\}$. La longitud mitjana del codi és $\bar{L} = \frac{18}{8} = 2.25$. Com que totes les probabilitats són potències de 2, l'eficiència del codi òptim és 1. Tot i així, anem a calcular-la explícitament. La fórmula de l'eficiència és

   $$\eta = \frac{H(S)}{\bar{L} \log 2}.$$

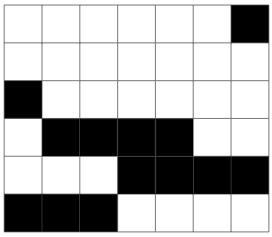
   L'entropia de S és

   $$H(S) = 3\frac{1}{4}\log 4 + 2\frac{1}{8}\log 8 = \frac{6}{4} + \frac{2}{8} = \frac{9}{4} = 2.25 \text{ bits}.$$

   Per tant, $\eta = \frac{2.25}{2.25} = 1$.

   (b) Un codi binari de longitud fixa ha de tenir la mínima longitud L que satisfà $2^L \geq 5$; per tant, $L = 3$. Com que la longitud del codi és més gran que la longitud mitjana d'un codi òptim, que és 2.25, aleshores el codi no pot ser òptim.

2. (1 punt) Codifiqueu el següent mapa de bits fent servir la codificació RLE i doneu la taxa i el percentatge de compressió (doneu les fórmules que feu servir i el resultat final).



   Solució: La codificació RLE del mapa de bits és

Fila	*Codificació*
1	6 1
2	7
3	0 1 6
4	1 4 2
5	3 4
6	0 3 4

La mida del fitxer original és $|M| = 7 \cdot 6 + 3 = 45$ i la mida del fitxer comprimit és $|C| = 14 \cdot 3 + 3 = 45$. Per tant, la taxa de compressió és $R = \frac{45}{45} = 1$ bpb. i el percentatge de compressió és $(1-1) \cdot 100 = 0\%$.

3. (2.5 punts 0.5+0.5+1+0.5) Considereu el canal amb conjunt de valors d'entrada $A = \{a_1, a_2, a_3, a_4\}$ i de sortida $B = \{b_1, b_2, b_3\}$. La matriu del canal és la següent:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

   (a) Digueu de quin tipus de canal es tracta i quina és la seva capacitat.

   (b) Per a quina distribució de probabilitats inicials s'assoleix la capacitat del canal?

   (c) Considereu ara que la distribució inicial és $(\frac{1}{8}, \frac{1}{2}, \frac{1}{8}, \frac{1}{4})$.

      i. Doneu la informació mútua de l'entrada i la sortida.

      ii. Doneu la probabilitat mitjana d'error descodificant a mínima probabilitat d'error (MPE) i doneu també la funció de descodificació a MPE.

Solució:

   (a) Cada fila té un únic element diferent de zero, per tant es tracta d'un canal determinista. Tenim que $H(B|A) = 0$ i la capacitat del canal és $C = \log 3 = 1.58$.

   (b) La capacitat del canal s'assoleix quan la distribució final és equiprobable. Considerem $p_i = p(a_i)$, per $i = 1, \ldots, 4$. Les probabilitats de la sortida són $p(B_1) = p_1$, $p(B_2) = p_3 + p_4$ i $p(B_3) = p_2$. Per tal que la distribució final sigui equiprobable s'ha de complir $p_1 = p_3 + p_4 = p_2 = \frac{1}{3}$. Per tant, una distribució d'entrada que faci que la distribució final sigui equiprobable és $(\frac{1}{3}, \frac{1}{3}, \frac{1}{6}, \frac{1}{6})$.

   (c) Com que $H(B|A) = 0$, tenim que $I(A,B) = H(B)$. Partint de la matriu del canal i considerant la distribució inicial $(\frac{1}{8}, \frac{1}{2}, \frac{1}{8}, \frac{1}{4})$, tenim la següent taula

$p(A_i, B_j)$	b_1	b_2	b_3
A_1	$\frac{1}{8}$	0	0
A_2	0	0	$\frac{1}{2}$
A_3	0	$\frac{1}{8}$	0
A_4	0	$\frac{1}{4}$	0
$p(B_j)$	$\frac{1}{8}$	$\frac{3}{8}$	$\frac{1}{2}$

   Per tant, $I(A,B) = H(B) = H(\frac{1}{8}, \frac{3}{8}, \frac{4}{8}) = \frac{1}{8}\log 8 + \frac{3}{8}\log\frac{8}{3} + \frac{4}{8}\log\frac{8}{4} = \frac{1}{8}\log 8 + \frac{3}{8}(\log 8 - \log 3) + \frac{4}{8}(\log 8 - \log 4) = \log 8 - \frac{3}{8}\log 3 - \frac{4}{8}\log 4 = 3 - \frac{3}{8} \cdot 1.58 - 1 = 2 - 0.59 = 1.41$.

   (d) La probabilitat mitjana d'error descodificant a MPE és $\bar{p}_e = 1 - \frac{1}{8} - \frac{1}{4} - \frac{1}{2} = 1 - \frac{7}{8} = \frac{1}{8} = 0.125$. La regla de descodificació és

$$\begin{aligned} B_1 &\longrightarrow A_1, \\ B_2 &\longrightarrow A_4, \\ B_3 &\longrightarrow A_2. \end{aligned}$$

4. (1.5 punt 0.5+1) Sigui C un codi lineal binari i G, H una matriu generadora i una matriu de control, respectivament.

   (a) Digueu com es pot obtenir la distància mínima del codi C a partir de la matriu de control H.

   (b) Doneu una matriu de control d'un codi binari lineal $C[10, 6, 3]$.

Solució:

(a) La distància mínima de C és el mínim nombre de files de H linealment dependents.

(b) Hem de construir una matriu de deu columnes i quatre files que tingui rang 4 i que el mínim nombre de columnes dependents sigui tres.
Un exemple seria:

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

5. (1.5 punts 0.5+0.5+0.5) Considereu el codi binari lineal C_1 que és 2-corrector i té com a paràmetres $[11, 4, d]$. (**Responeu i justifiqueu les respostes**)

(a) Quina és la distància mínima del codi C_1? I del seu codi estés C_1'?

(b) Quantes files no nul·les hi ha a la taula de síndromes del codi C_1?

(c) Ompliu la taula següent:

	longitud	dimensió
C_1		
C_1'		
$C_1^\perp$		
$(C_1')^\perp$		

Solució:

(a) Com que $t = 2$, aleshores $d = 5$ o $d = 6$. En qualsevol cas, la distància mínima del codi estès és 6.

(b) La taula de síndrome del codi C_1 conté els vectors no nuls de longitud 11 i pes menor o igual a 2

- pes 1: 11 vectors,
- pes 2: $\binom{11}{2} = \frac{11 \cdot 10}{2} = 55$ vectors.

Per tant, en total té 66 files.

(c)

	longitud	dimensió
C_1	11	4
C_1'	12	4
$C_1^\perp$	11	7
$(C_1')^\perp$	12	8

6. (2 punts)

(a) Signeu digitalment amb RSA el missatge $m = 121$ sabent que les dades del firmant són $p = 19$; $q = 31$, $d = 149$.

(b) Calculeu la clau pública del signant.

(c) Com ho ha de fer qualsevol membre de la mateixa PKI que el signant per a validar la signatura s si rep la tupla (m, s)? Valideu la signatura que heu calculat a l'apartat a).

Per a resoldre l'exercici, podeu fer servir els resultats que es troben a la taula següent. **Si no trobeu algun dels valors a la taula, deduïu el resultat**.

$121^{-1} \bmod 540 = 241$	$149^{-1} \bmod 589 = 253$	$19^{149} \bmod 588 = 31$	$31^{31} \bmod 540 = 391$
$121^{-1} \bmod 588 = 277$	$149^{121} \bmod 540 = 329$	$19^{149} \bmod 589 = 266$	$31^{31} \bmod 588 = 31$
$121^{-1} \bmod 589 = 258$	$149^{121} \bmod 588 = 317$	$19^{19} \bmod 540 = 19$	$31^{31} \bmod 589 = 31$
$121^{121} \bmod 540 = 481$	$149^{121} \bmod 589 = 366$	$19^{19} \bmod 588 = 19$	$31^{29} \bmod 540 = 151$
$121^{121} \bmod 588 = 457$	$149^{149} \bmod 540 = 389$	$19^{19} \bmod 589 = 152$	$31^{29} \bmod 588 = 19$
$121^{121} \bmod 589 = 121$	$149^{149} \bmod 588 = 53$	$19^{31} \bmod 540 = 19$	$31^{29} \bmod 589 = 217$
$121^{149} \bmod 540 = 421$	$149^{149} \bmod 589 = 346$	$19^{31} \bmod 588 = 19$	$258^{121} \bmod 540 = 108$
$121^{149} \bmod 588 = 529$	$149^{19} \bmod 540 = 149$	$19^{31} \bmod 589 = 19$	$258^{121} \bmod 588 = 468$
$121^{149} \bmod 589 = 258$	$149^{19} \bmod 588 = 233$	$19^{29} \bmod 540 = 199$	$258^{121} \bmod 589 = 258$
$121^{19} \bmod 540 = 121$	$149^{19} \bmod 589 = 149$	$19^{29} \bmod 588 = 31$	$258^{149} \bmod 540 = 108$
$121^{19} \bmod 588 = 289$	$149^{31} \bmod 540 = 329$	$19^{29} \bmod 589 = 266$	$258^{149} \bmod 588 = 468$
$121^{19} \bmod 589 = 577$	$149^{31} \bmod 588 = 485$	$31^{121} \bmod 540 = 391$	$258^{149} \bmod 589 = 121$
$121^{31} \bmod 540 = 481$	$149^{31} \bmod 589 = 366$	$31^{121} \bmod 588 = 31$	$258^{19} \bmod 540 = 432$
$121^{31} \bmod 588 = 205$	$149^{29} \bmod 540 = 209$	$31^{121} \bmod 589 = 31$	$258^{19} \bmod 588 = 216$
$121^{31} \bmod 589 = 121$	$149^{29} \bmod 588 = 305$	$31^{149} \bmod 540 = 511$	$258^{19} \bmod 589 = 49$
$121^{29} \bmod 540 = 61$	$149^{29} \bmod 589 = 408$	$31^{149} \bmod 588 = 19$	$258^{31} \bmod 540 = 432$
$121^{29} \bmod 588 = 445$	$19^{121} \bmod 540 = 19$	$31^{149} \bmod 589 = 217$	$258^{31} \bmod 588 = 384$
$121^{29} \bmod 589 = 258$	$19^{121} \bmod 588 = 19$	$31^{19} \bmod 540 = 31$	$258^{31} \bmod 589 = 258$
$149^{-1} \bmod 540 = 29$	$19^{121} \bmod 589 = 19$	$31^{19} \bmod 588 = 31$	$258^{29} \bmod 540 = 108$
$149^{-1} \bmod 588 = 221$	$19^{149} \bmod 540 = 199$	$31^{19} \bmod 589 = 31$	$258^{29} \bmod 588 = 552$
			$258^{29} \bmod 589 = 121$

Solució:

(a) Només cal calcular $s = 121^d \bmod n$, on $n = 19{\cdot}31 = 589$. Resulta $s = 258$.

(b) La clau pública és (n, e), en què e és l'invers de d mòdul $\phi(n) = (30{\cdot}18) = 540$. Resulta $e = d^{-1} \bmod 540 = 29$.

(c) Per a validar la signatura hem de comprovar que $s^e \bmod 589 = m$. Efectivament $258^{29} \bmod 589 = 121$.