INFORMACIÓ I SEGURETAT
17 de juny de 2019

Nom i cognoms: _____ NIU: _____ Grup: _____

1. (4 punts: 1+0.5+1+0.5+1)

   Sigui C un codi del que coneixem una matriu generadora

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

   (a) Doneu una matriu de control H del codi C. **Usant la matriu de control** H, doneu els paràmetres n, k, d del codi C. Justifiqueu els resultats.

   (b) Construïu la taula estàndard del codi C.

   (c) Descodifiqueu (**corregint errors i donant la informació associada al vector rebut**) els vectors rebuts $v_1 = (1,1,1,1,1)$ i $v_2 = (0,1,0,1,1)$.

   (d) Doneu les equacions que han de complir x, y, z, t, u de manera que el vector $v = (x, y, z, t, u)$ sigui del codi C.

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

   Solució:

   (a) La matriu generadora G és sistemàtica, o sigui que la matriu de control serà:

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

   És fàcil veure que el mínim nombre de columnes dependents de H és 3 (per exemple la primera, la tercera i la quarta són dependents). La longitud n és el nombre de columnes de H, $n = 5$, i el nombre de files de H és $n - k$, per tant la dimensió és $k = 2$.

   Així, 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:

Vector d'error	Síndrome
00000	000
10000	110
01000	011
00100	100
00010	010
00001	001

   (c) Per descodificar els vectors rebuts, primer de tot calcularem la síndrome,

$$H(v_1) = H(1,1,1,1,1) = (0,1,0);\ H(v_2) = H(0,1,0,1,1) = (0,0,0).$$

   Mirant la taula estàndard observem que l'error corresponent a v_1 és $(0,0,0,1,0)$ i a v_2 és $(0,0,0)$. O sigui que després de corregir errors en els dos vectors rebuts podem assegurar que les corresponents paraules codi són $(1,1,1,0,1)$ i $(0,1,0,1,1)$.

   Com que el codi C te la matriu generadora sistemàtica podem escriure que la informació associada a v_1 és $(1,1)$ i a v_2 és $(0,1)$.

(d) Les paraules codi $v = (x, y, z, t, u)$ del codi C han de complir que $H(v) = 0$. O sigui:

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

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

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

El mínim nombre de columnes linealment dependents a H^* és 4 (per exemple les columnes $1, 2, 3, 5$) o sigui que la distància mínima del codi estès C^* és 4.

2. (2 punts)

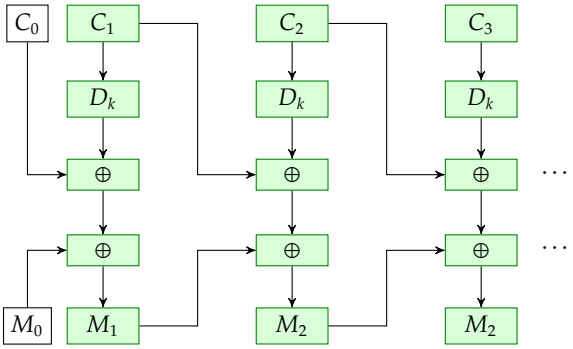
En el mode de xifratge CBC (autenticació) tenim que l'equació per xifrar és $C_i = E_k(M_i \oplus C_{i-1} \oplus M_{i-1})$, on $C_0 = 0$ i $M_0 = 0$.

Escriviu l'equació que ens dona el text en clar M_i en funció del text xifrat i dibuixeu el diagrama del desxifratge.

Solució:

Aïllant M_i de l'equació que ens donen: $M_i = M_{i-1} \oplus C_{i-1} \oplus D_k(C_i)$.

El diagrama del desxifratge és:



3. (1 punts)

De les següents afirmacions digueu quines són certes i quines són falses. En qualsevol cas heu de justificar la resposta.

(a) En la criptografia de clau pública no hi ha confusió ni difusió.

(b) SPN i Feistel són dues tècniques que s'utilitzen dintre de cada round en un xifratge de clau privada. La primera en els xifratges convencionals i la segona en els xifratges lleugers.

(c) Les funcions *unidireccionals* i les *hash unidireccionals* són funciones que no tenen inversa.

(d) La tècnica de la distribució de claus fent servir criptografia quàntica permet tenir una seguretat del 75%, tant a l'emissor com al receptor, que cap espia coneix la clau compartida.

Solució:

(a) Cert. Els conceptes de confusió i difusió només apliquen a la criptografia de clau privada.

(b) Fals. Tant SPN com Feistel són dues tècniques que tant es poden utilitzar en criptografia de clau privada convencional com de clau privada lleugera.

(c) Fals. Les funcions *hash unidireccionals* no tenen inversa, les funcions *unidireccionals* sí que tenen inversa, encara que és "difícil" de calcular.

(d) Fals. La seguretat de que no hi hagi espies que coneguin la clau compartida pot ser tant alta com vulguem.

4. (3 punts: 0.5+1+1+0.5) Definim la funció hash $h_{10} : \mathbb{Z} \longrightarrow \mathbb{Z}_{10}$ que, donat $m \in \mathbb{Z}$ retorna la suma dels dígits de m mòdul 10. Per exemple, $h_{10}(185) = 1 + 8 + 5 \bmod 10 = 4$.

(a) Definiu què és una col·lisió d'una funció hash i doneu una col·lisió de la funció hash h_{10}.

(b) A i B tenen les següents claus públiques en un criptosistema RSA: $PK_A = (n_A, e_A) = (209, 29)$ i $PK_B = (n_B, e_B) = (299, 31)$. L'usuari A sap que $209 = 11 * 19$ i l'usuari B sap que $299 = 13 * 23$.

1) A vol enviar a B els valors (c, s) on c és el missatge $m = 132$ xifrat i s és la signatura de $h_{10}(m)$. Quins valors envia A?

2) Un espia fa un atac *person in the middle* entre A i B. Intercepta els valors (c, s) que A envia a B i els substitueix per $(83, 24)$ fent-se passar per A. Pot verificar B que els valors $(83, 24)$ els ha enviat l'usuari A?

3) Si la resposta a l'apartat anterior és negativa, què hauria d'haver fet l'espia per fer-se passar per l'usuari A. Si la resposta és positiva, justifiqueu què ha fallat en el protocol de signatura digital amb hash?

Solució:

(a) Una col·lisió d'una funció hash és una situació que es dóna quan dos missatges diferents tenen la mateixa imatge després d'aplicar la funció hash. Per exemple, els valors 185 i 220 són una col·lisió ja que $h_{10}(185) = h_{10}(220) = 4$.

(b)

1) Primer A xifra el missatge $m = 132$ per enviar a B. Tenim que

$$c = m^{e_B} \bmod n_B = 132^{31} \bmod 299 = 76.$$

Per signar $h_{10}(132) = 6$, A fa servir la clau privada que és $d_A = e_A^{-1} \bmod \phi(n_A)$. Tenim que $\phi(n_A) = 10 * 18 = 180$ i, per tant, $d_A = 29^{-1} \bmod 180 = 149$. La signatura és

$$s = (h_{10}(m))^{d_A} \bmod n_A = 6^{149} \bmod 209 = 24.$$

A envia $(76, 24)$.

2) Per verificar la signatura, B necessita la seva clau privada que és $d_B = e_B^{-1} \bmod \phi(n_B) = 31^{-1} \bmod 264 = 247$. El missatge m que ha xifrat A és

$$m = 83^{247} \bmod 299 = 268.$$

B, per verificar la signatura, calcula

$$s^{e_A} \bmod n_A = 24^{29} \bmod 209 = 6$$

i comprova que efectivament $h_{10}(268) = 6$. Per tant, la signatura és vàlida.

3) El protocol ha fallat perquè és fàcil trobar col·lisions amb el hash h_{10}.

$29^{-1} \bmod 180 = 149$	$29^{-1} \bmod 209 = 173$	$29^{-1} \bmod 264 = 173$	$29^{-1} \bmod 299 = 165$
$31^{-1} \bmod 180 = 151$	$31^{-1} \bmod 209 = 27$	$31^{-1} \bmod 264 = 247$	$31^{-1} \bmod 299 = 164$
$132^{29} \bmod 180 = 72$	$132^{29} \bmod 209 = 132$	$132^{29} \bmod 264 = 0$	$132^{29} \bmod 299 = 227$
$132^{31} \bmod 180 = 108$	$132^{31} \bmod 209 = 132$	$132^{31} \bmod 264 = 0$	$132^{31} \bmod 299 = 76$
$132^{149} \bmod 180 = 72$	$132^{149} \bmod 209 = 132$	$132^{149} \bmod 264 = 0$	$132^{149} \bmod 299 = 149$
$132^{164} \bmod 180 = 36$	$132^{164} \bmod 209 = 77$	$132^{164} \bmod 264 = 0$	$132^{164} \bmod 299 = 165$
$132^{173} \bmod 180 = 72$	$132^{173} \bmod 209 = 132$	$132^{173} \bmod 264 = 0$	$132^{173} \bmod 299 = 97$
$132^{247} \bmod 180 = 108$	$132^{247} \bmod 209 = 132$	$132^{247} \bmod 264 = 0$	$132^{247} \bmod 299 = 297$
$24^{29} \bmod 180 = 144$	$24^{29} \bmod 209 = 6$	$24^{29} \bmod 264 = 72$	$24^{29} \bmod 299 = 254$
$24^{31} \bmod 180 = 144$	$24^{31} \bmod 209 = 112$	$24^{31} \bmod 264 = 24$	$24^{31} \bmod 299 = 93$
$24^{149} \bmod 180 = 144$	$24^{149} \bmod 209 = 28$	$24^{149} \bmod 264 = 72$	$24^{149} \bmod 299 = 254$
$24^{164} \bmod 180 = 36$	$24^{164} \bmod 209 = 82$	$24^{164} \bmod 264 = 192$	$24^{164} \bmod 299 = 139$
$24^{173} \bmod 180 = 144$	$24^{173} \bmod 209 = 63$	$24^{173} \bmod 264 = 96$	$24^{173} \bmod 299 = 254$
$24^{247} \bmod 180 = 144$	$24^{247} \bmod 209 = 150$	$24^{247} \bmod 264 = 216$	$24^{247} \bmod 299 = 93$
$83^{29} \bmod 180 = 23$	$83^{29} \bmod 209 = 68$	$83^{29} \bmod 264 = 35$	$83^{29} \bmod 299 = 226$
$83^{31} \bmod 180 = 47$	$83^{31} \bmod 209 = 83$	$83^{31} \bmod 264 = 83$	$83^{31} \bmod 299 = 21$
$83^{149} \bmod 180 = 23$	$83^{149} \bmod 209 = 68$	$83^{149} \bmod 264 = 35$	$83^{149} \bmod 299 = 135$
$83^{164} \bmod 180 = 121$	$83^{164} \bmod 209 = 163$	$83^{164} \bmod 264 = 97$	$83^{164} \bmod 299 = 248$
$83^{173} \bmod 180 = 23$	$83^{173} \bmod 209 = 106$	$83^{173} \bmod 264 = 227$	$83^{173} \bmod 299 = 148$
$83^{247} \bmod 180 = 47$	$83^{247} \bmod 209 = 140$	$83^{247} \bmod 264 = 107$	$83^{247} \bmod 299 = 268$