ملحوظة: رتب إجابتك في الدفتر حسب ترتيب ورود الأسئلة

١- لتكن $C=\{101,110,111\}$. أحسب الأخطاء التي تكتشفها و التي تصوبها الشفرة C .

٢- لتكن C شفرة خطية من نوع (n,k,d_C) . أثبت أن $2^k \le \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}}$ ، حيث $r=\left\lfloor \frac{d_C-1}{2} \right\rfloor$.

٣- إذا كانت $C=\langle 0101,0111,0010 \rangle$ ، فأحسب المصفوفتين G و H ثم أحسب الصفيف SDA . إذا تم استلام الكلمة $w=1110$ ، فهل يمكن معرفة الكلمة المرسلة؟

٤- عرِّف المسافة $d(v_1,v_2)$ بين كلمتين في $\mathbb{Z}_2^n$ ، ثم أثبت أن $d(v_1,v_2) \le d(v_1,w)+d(w,v_2)$ مع بيان و برهان الشرط الضروري و الكافي للمساواة.

٥- لنعتبر النظام الأفيني (التآلفي) قياس 26 . جد جميع الحروف x التي تحقق $e(x)=x$ ، إذا كان مفتاح التعمية هو (5,8) .

٦- ما هو المقصود بالنظام التبادلي في التعمية ؟ أثبت أن هذا النظام هو حالة خاصة من نظام هيل.

٧- عرِّف مدلول الرموز (P,C,K,L,F,E,D) في نظام المفتاح الذاتي قياس 26 ، ثم جد تعمية النص malik عندما $k=7$.

لا يكتب في هذا الهامش

$C = \{101, 110, 111\}$ ①

الأخطاء التي تكتشفها الشفرة
$\{000, 011, 010, 001\}$
الأخطاء لا تكتشفها الشفرة

العناصر التي تكتشفها الشفرة هي
$\{100, 110, 101, 111\}$ #

الجدول القياسي

w	w+101	w+110	w+111
000	101	110	111
011	110	101	100*
010	111	100*	101
001	100*	111	110

3

ثم الذي يصحح $n = 100$ *

~~سؤال ② لقد ذكر ...~~

حلة سؤال ② / ... شفرة خطية من نوع (n, k, d)

فإن $|C| = 2^k$

$$2^k \leq \frac{2^n}{\binom{n}{0} + \cdots + \binom{n}{r}}$$ لأن

تم البرهان

ج) أثبت أنه إذا كانت C شفرة خطية من نوع (n,k,d_c) فإن $2^k \le \frac{2^n}{\binom{n}{0}+\cdots+\binom{n}{r}}$

حيث $r=\left\lfloor \frac{d_c-1}{2} \right\rfloor$

البداية سنبدأ من تمهيديتين للاستفادة منها في برهان المطلوب

تمهيدية 1

$$|B(v,r)| = \binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}$$

الإثبات: $|B(v,r)|$ هو عدد النقاط التي تبعد مسافتها صفر عن المركز + عدد النقاط التي تبعد مسافة 1 عن المركز + ... + عدد النقاط التي تبعد مسافة r عن المركز

$$B(v,r) = 1+\binom{n}{1}+\cdots+\binom{n}{r}$$
$$= \binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}$$

تمهيدية 2 إذا كانت C شفرة مسافتها d_c فإن الكرات $B(v,r)$ حيث $r=\left\lfloor \frac{d_c-1}{2} \right\rfloor$

و لكل $v \in C$ فإن $B(v_1,r)\cap B(v_2,r)=\phi$ لكل $v_1 \ne v_2 \in C$

البرهان بالتناقض:

$$B(v_1,r)\cap B(v_2,r) \ne \phi \quad , \quad v_1 \ne v_2 \in C$$

$\Leftarrow$ يوجد $w \in \mathbb{Z}_2^n$ بحيث

$$w \in B(v_1,r) \ , \ w \in B(v_2,r)$$

$$d(v_1,v_2) \le d(v_1,w)+d(w,v_2)$$
$$\le r+r = 2r = 2\left\lfloor \frac{d_c-1}{2} \right\rfloor$$
$$\le (d_c-1) \le d_c$$

تناقض مع تعريف مسافة الشفرة

7

الآن نعود لإثبات أن

$$2^K \le \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}}$$

نعتبر الكرات $B(v,r)$ حيث $v \in C$ و $r=\left\lfloor \frac{d_c-1}{2} \right\rfloor$ حسب التمهيدية الثانية

فإن هذه الكرات لا تتقاطع

$$\left|\bigcup_{v\in C} B(v,r)\right| = \sum_{v\in C} |B(v,r)|$$

من التمهيدية الأولى فإن: $|B(v,r)| = \binom{n}{0}+\cdots+\binom{n}{r}$

$$\left|\bigcup B(v,r)\right| = \sum \binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}$$
$$= |C|\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}\right) \quad (*)$$

وكذلك $\mathbb{Z}_2^n \supseteq \bigcup B(v,r)$

إذاً

$$\left|\bigcup_{v\in C} B(v,r)\right| \le 2^n$$

إذاً من $(*)$ نستنتج أن

$$K\left(\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{r}\right) \le 2^n$$

لا يكتب في هذا الهامش

$$A = \begin{bmatrix} 0&1&0&1 \\ 0&1&1&1 \\ 0&0&1&0 \end{bmatrix} \rightarrow \begin{bmatrix} 0&1&0&1 \\ 0&0&1&0 \\ 0&0&1&0 \end{bmatrix} \rightarrow \begin{bmatrix} 0&1&0&1 \\ 0&0&1&0 \\ 0&0&0&0 \end{bmatrix}$$

$G = \begin{bmatrix} 0&1&0&1 \\ 0&0&1&0 \end{bmatrix}$ $k \times n = 2 \times 4$, $k = 2$

$G' = \begin{bmatrix} 1&0&0&1 \\ 0&1&0&0 \end{bmatrix}$ (I | X), $H' = \begin{bmatrix} 0&1 \\ 0&0 \\ 1&0 \\ 0&1 \end{bmatrix} \rightarrow H = \begin{bmatrix} 1&0 \\ 0&1 \\ 0&0 \\ 0&1 \end{bmatrix}$ #

١) لا يوجد مجاميع مشاركة

$|Z_2^{n-k}| = |Z_2^{4-2}| = |Z_2^2| = 2^2 = 4 \rightarrow$ عدد المجاميع

نوجد عناصر الشفرة عددها $4 = 2^2$ $C = \{0000, 0101, 0111, 0010\}$

1	2	3	4
0000*	0001	1000*	1100
0101	0100	1101	1001
0111	0110	1111	1011
0010	0011	1010	1110

٢) العنصر الرئيس في المجموعة المشاركة

$u = \begin{bmatrix} 0000 \\ 0001 \\ 1000 \\ 1100 \end{bmatrix}$

(العنصر الأصغر) SDA

u	uH	
0000	00	
0001	*	(الوزن ١ مكرر)
1000	10	
1100	*	(الوزن ٢ مكرر)

استقبلنا $w = 1110$

$wH = 11$

لا يمكن تصحيحها

8

Eight

لا يكتب في هذا الهامش

~~$d(v_1,v_2) \le d(v_1,w)+d(w,v_2)$~~

المسافة بين كلمتين هي عدد مواقع الاختلاف في قيمة أحد الثنائي.

$$d(v_1,v_2) \le d(v_1,w)+d(w,v_2)$$

$d(v_1,v_2) = wt(v_1+v_2)$
$= wt(v_1+w+w+v_2)$
$= wt((v_1+w)+w+(w+v_2))$
كيف؟ $\le wt(v_1+w)+wt(w+v_2)$
$= d(v_1+w)+d(w+v_2)$

خذ ثم البرهان

الشرط الضروري والكافي للمساواة (برهان)

$$wt(v_1+v_2) = wt(\underbrace{v_1+w}_{c_1}) + wt(\underbrace{w+v_2}_{c_2})$$

لاحظ أنه $c_1+c_2 = v_1+v_2$ المطلوب إيجاد شرط ضروري وكافي لكي يكون

$wt(c_1+c_2) = wt(c_1)+wt(c_2)$

فإن الشرط الضروري والكافي هو عدم ظهور 1 في نفس الخانة في كلا الحدين، نستنتج أن الشرط الضروري

الكافي كي نحصل على المساواة هو التالي

$v_1 = x_1 \cdots x_n$
$v_2 = y_1 \cdots y_n$
$w = z_1 \cdots z_n$

في حالة $x_i = y_i \Leftarrow x_i = z_i$

في حالة $x_i \ne y_i$ ولا قيود على z_i ✗

(4)

لا يكتب في
هذا الهامش

(5)

$e_{(5,8)}(a) = 5(a) + 8 = 8(i)$

$e_{(5,8)}(b) = 5 + 8 = 13(m)$ $e_{(5,8)}(c) = 10 + 8 = 18(s)$, $e_{(5,8)}(d) = 15 + 8 = 23(x)$

$e(e) = 20 + 8 = 2(c)$, $e(f) = 25 + 8 = 7(H)$, $e(g) = 30 + 8 = 12$

$(H) = 17(r)$, $e(i) = 22(w)$, $e(j) = 27(b)$

$(k) = 6(g)$, $e(L) = 11(L)$, $e(m) = 16(Q)$

$(N) = 21(v)$, $e(\Phi) = 0(a)$, $e(p) = 5(f)$

$(Q) = 10(k)$, $e(r) = 15(P)$, $e(s) = 20(w)$

$(t) = 25(z)$, $e(u) = 4(e)$, $e(v) = 9(j)$

$(w) = 14(o)$, $e(x) = 19(t)$, $e(y) = (24) = Y$

$e(z) = 3(d)$

(7)

(6) لتبديل

(i) $P = C = \mathbb{Z}_{26}^{n}$

(ii) $K = S_m$

$\sigma = k$ بالعكس

$e_\sigma(x_1 - - - x_m) = (x_{\sigma(1)}, - - - - x_{\sigma(m)})$

$d_\sigma(y_1 - - - y_m) = (y_{\sigma^{-1}(1)} - - - - y_{\sigma^{-1}(m)})$

$|K| = S_m = m!$

\# ——— \# ——— \# ——— \#

نظام التباديل حالة خاصة من نظام هيل

نوضح بمثال:

$e_\sigma(x_1, x_2, x_3) = (x_3, x_1, x_2)$

$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ $\sigma = (132)$

$e_\sigma(x_1, x_2, x_3)$ نعطينا $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_2 \\ x_1 \end{pmatrix}$

لا يكتب في
هذا الهامش

الحل

عرف الرموز لنظام الاتي:

(P, C, K, L, F, E, D)

كتابياً

① $P = C = K = L = \mathbb{Z}_{26}$

② $z_1 = f_1(k) = k$

$z_2 = f_2(k, x_1) = x_1$

⋮

$z_i = f_i(k, x_1 \ldots x_{i-1}) = x_{i-1}$

③ $y_i = e_{z_i}(x_i) = z_i + x_i \mod 26$

$x_i = d_{z_i}(y_i) = y_i - z_i \mod 26$

\# ——— # ——— #

7

النص الواضح Malik.

$K = 7$

المكافئات العددية 12 0 11 8 10

7 12 0 11 8

19 12 11 19 18

النص المشفر **TMLTS**