ملحوظة: رتب إجابتك في الدفتر حسب ترتيب ورود الأسئلة.

1. في النظام التآلفي ذو المفتاح (a,b) قياس 26 ، حيث $a>1$ ، أثبت أن هناك حرفين يحققان $e_{(a,b)}(x)=x$ إذا و فقط إذا كان b زوجياً. جد هذين الحرفين عندما $(a,b)=(9,4)$.

2. إذا كان p أولياً، فأثبت أن عدد مفاتيح نظام هيل من الدرجة m قياس p هو
$$(p^m-1)(p^m-p)\cdots(p^m-p^{m-1})$$

3. بيّن مفصلاً كيف يمكن إنشاء مفتاح سري مشترك في شبكة تحوي n من النقط، حيث $n\geq 2$.

4. لتكن C شفرة خطية من نوع (n,k,d) . أثبت أن $k\leq n-d+1$. أعطِ مثالاً على شفرة تحدث فيها المساواة.

5. إذا كانت C شفرة طول كلماتها n و مسافتها d ، فأثبت أن
$$|C|\leq \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{t}}$$ ، حيث $t=\left\lfloor \frac{d-1}{2} \right\rfloor$.

6. لتكن $C=\langle S\rangle$ ، حيث $S=\{1010,0011,1001\}$. جد المصفوفة H و الصفيف SDA . اذا تم استلام الكلمة $w=0111$ ، فهل يمكن حساب الكلمة المُرسلة؟ و ما هي؟

لا يكتب في هذا الهامش

السؤال الاول :- ~~[illegible]~~

إن دالة التشفير في النظام التآلفي هي

$$e_{(a,b)}(x) = ax+b \mod 26$$

لكن $e_{(a,b)}(x) = x$

وعليه فإن

~~$x = ax+b \mod 26$~~

$$ax+b = x \mod 26$$

$$\Rightarrow ax - x = -b \mod 26$$

$$\Rightarrow x(a-1) = 25b \mod 26$$

لكن $a>1 \Leftarrow a-1>0$ وعليه

6

$a-1$ ليس له مقلوب في 26

~~$\Rightarrow x = \frac{25}{(a-1)} b \mod 26$~~

لكن إن $(a,26)=1 \Leftarrow a$ عدد فردي $\Leftarrow a-1$ زوجي

وبالتالي لابد أن يكون b عدد زوجيا حتى يكون $\frac{25}{a-1}$ عدد صحيح

الاتجاه الاخر

إذا كان b زوجيا بحيث $b=2k, k\in Z$ وبالتالي

$$e_{(a,b)}(x) = ax+2k \mod 26$$

~~[illegible]~~

$$\Rightarrow e_{(a,b)}(x) = ax+2k+26t \quad , t\in Z$$

$$= ax + 2(k+13t)$$

$$= ax+2L \quad , L = k+13t$$

$$\Rightarrow ax+2L \equiv ax+2k \mod 26$$

$$\Rightarrow 2L \equiv 2k \mod 26$$

$$\Rightarrow L = k \mod 26$$

يكتب في
هذا الهامش

إن دالة التعمية هي

$$E_{(9,4)}(x) = 9x + 4 \bmod 26$$

الحرف الاول هو G

الحرف الثاني هو T

كيف توصلت
الى هذا الحل ؟!

لا يكتب
هذا الهامش

السؤال الثاني :- نبدأ بالمصفوفات من النوع $m \times m$ القابلة للانقلاب قياس p حيث p عدد أولي لأن Z_p حقل ((A معكوسة على الحقل $Z_p \Leftrightarrow$ كانت صفوف A مستقلة خطياً)) إذاً

في الصف الأول الامكانيات هي $p^m - 1$ — لماذا؟

في الصف الثاني الامكانيات هي $p^m - p$ — لماذا؟

في الصف الثالث الامكانيات هي $p^m - p^2$

((لأننا استبعدنا أي تركيب خطي في الصف الأول والثاني))

وهكذا لو استمرينا على الصف m الامكانيات هي $p^m - p^{m-1}$

((لأننا استبعدنا أي تركيب خطي من الـ $m-1$ من الصفوف السابقة))

وبالتالي فإن عدد المصفوفات القابلة للانقلاب هي

$$(p^m - 1)(p^m - p)(p^m - p^2)\cdots(p^m - p^{m-1})$$

7

السؤال الثالث /

لنثبت بالاستقراء الرياضي

4

الخطوة الأولى عندما $n=2$ يعني ليس أحمد وبدر داخل الشبكة

① يتم اختيار عدد أولي p كبير لا يقل عن ٢٠٠ مرتبة عشرية وأن يعرف تحليل العدد $p-1$

② يتم اختيار مولد للزمرة الدورية Z_p^* وليكن α

③ يقوم أحمد باختيار عدد عشوائي $1 < k_1 < p-1$ ويحسب $\alpha^{k_1} \bmod p$ ويرسله إلى بدر

④ يقوم بدر باختيار عدد عشوائي $1 < k_2 < p-1$ ويحسب $\alpha^{k_2} \bmod p$ ويرسله إلى أحمد

⑤ يقوم أحمد بحساب $\alpha^{k_1 k_2} \equiv (\alpha^{k_2})^{k_1} \bmod p$ ويقوم بدر بحساب $\equiv (\alpha^{k_1})^{k_2}$

خطوة الاستقراء

لنفرض أنه يوجد في الشبكة $n-1$ ومفتاحهم السري $\alpha^{k_1 k_2 \cdots k_{n-1}}$

ونريد إثباتها لـ n

الآن يقوم الشخص رقم $n-1$ بإرسال العدد $\alpha^{k_1 k_2 \cdots k_{n-1}}$ إلى الشخص رقم n عندئذ يقوم الشخص رقم n بحساب

$$\alpha^{k_1 \cdots k_{n-1} k_n} = (\alpha^{k_1 \cdots k_{n-1}})^{k_n} \bmod p$$

ماذا؟ على ...

لا يكتب

هذا الهـ

السؤال الرابع: لنعتبر مصفوفة تحديد التوقيع H ، نعلم أن أعمدة H مستقلة خطياً وتولد الفضاء $C^{\perp}$

: البعد العمودي هو $n-k$

: البعد الصفري هو $n-k$ أيضاً

من تعريف المسافة هي أقل أصغر وزن لكلمة من كلمات الشفرة

ويكون لدينا $v \in C \iff vH = 0$

$$(x_1 x_2 x_3 \dots x_n) H = x_1 W_1 + x_2 W_2 + \dots + x_n W_n$$

حيث W_i هي صفوف H نستنتج من ذلك أن كل $d-1$ من صفوف H مستقلة خطياً ويكون البعد الصفري هو $n-k$

وعليه فإن

$$d-1 \le n-k$$

$$\Rightarrow d \le n-k+1$$

$$\Rightarrow k \le n-d+1$$

المثال هو $= \{000, 101, 011, 110\}$

$d=2$ ، $n=3$ ، $k=2$

$k = n-d+1 = 3-2+1 = 2$

حدثت المساواة

السؤال الخامس: إن $\bigcup_{v \in C} B(v,t) \subset \mathbb{Z}_2^n$

وعليه فإن

$$\left|\bigcup_{v \in C} B(v,t)\right| \le |\mathbb{Z}_2^n| = 2^n$$

لكن الكرات لا تتقاطع لأن لو كان

$v_1, v_2 \in C$ ، $w \in B(v_1,t) \cap B(v_2,t)$

$$\Rightarrow w \in B(v_1,t) \wedge w \in B(v_2,t)$$

وبالتالي فإن

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

$$\le t + t = 2t$$

$$\le 2\left(\frac{d-1}{2}\right) = d-1$$

وهذا تناقض مع تعريف المسافة d إذاً $B(v_1,t) \cap B(v_2,t) = \phi$

وعليه فإن

$$\sum_{v \in C} |B(v,t)| \le 2^n$$

$$\Rightarrow |C|\left(\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{t}\right) \le 2^n$$

لا يكتب في
هذا الهامش

السؤال السادس:

لتكن A هي

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

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

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

حولنا المصفوفة A الى الصيغة الدرجية المختزلة

الان نحذف الصفوف الصفرية فنحصل على المصفوفة G

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

الان نبدل الاعمدة الرئيسية ونجعلها متتالية فنحصل على G'

$$G' = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

الان نعين المصفوفة H' وهي

$$H' = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{matrix} 1 \\ 3 \\ 2 \\ 4 \end{matrix}$$

الان نحصل على المصفوفة H وهي

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

[illegible] [illegible] [illegible] العناصر لنحسب المجموعات المشاركة

$$2^{n-k} = 2^{4-2} = 2^2 = 4$$

اذن C={0000, 1010, 0011, 1001} وبالتالي فان [illegible]

0000	1000	0100	1100
1010	0010	1110	0110
0011	1011	0111	1111
1001	0001	[illegible]	[illegible]

لا يكتب في
هذا الهامش

وبالتالي فإن التصنيف هو

u	uH
0000	00
1000	*
0100	10
1100	*

ملاحظة / * تعني طلب إعادة الإرسال

ثم نحسب الآن متلازمة w

$$0111 \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} = 10$$

نبحث في جدول التصنيف فنجد أن $u=0100$

وبالتالي فإن

$u+w = 0011$

وهي موجودة في C