الملاحق

الملحق (أ): خوارزمية إقليدس

الملحق (ب): تحليل $1 + x^n$

الملحق (ج): مثال على تشفير قرص مدمج

الملحق (د): حلول لتمارين مختارة

الملحق (أ)

خوارزمية إقليدس
The Euclidean Algorithm

القاسم المشترك الأكبر (اختصاراً gcd) لكثيرتي حدود $f(x), g(x) \epsilon K[x]$ هو كثيرة الحدود $d(x) \in K[x]$ التي درجتها أكبر ما يمكن وتحقق $f(x) = q_1(x)d(x)$ و $g(x) = q_2(x)d(x)$ ونكتب عادة $\gcd(f(x), g(x)) = d(x)$.

مثال (١,١)

لنفرض أن:

$$f(x) = 1 + x^2 + x^3 + x^6 + x^7 + x^8 \text{ و } g(x) = 1 + x^3 + x^5 + x^6.$$

بتحليل كل من $f(x)$ و $g(x)$ كحاصل ضرب كثيرات حدود غير قابلة للتحليل نرى أن:

$$f(x) = (1 + x)(1 + x + x^3)(1 + x^4)$$
$$g(x) = (1 + x)(1 + x^2)(1 + x + x^3)$$

كثيرة الحدود ذات الدرجة الأعلى بحيث تقسم كلاً من $f(x)$ و $g(x)$ هي $1 + x + x^3$. إذن،

$$\gcd(f(x), g(x)) = 1 + x + x^3 \quad \blacktriangle$$

إن تحليل $f(x)$ و $g(x)$ إلى عوامل غير قابلة للتحليل لإيجاد القاسم المشترك الأكبر ليس بالطريقة الفعّالة. ولكن الخوارزمية التالية تقدم لنا طريقة فعّالة لإيجاد القاسم المشترك الأعظم لكثيرتي حدود.

خوارزمية إقليدس

لتكن $f(x), g(x) \epsilon K[x]$ حيث $\deg(f(x)) \geq \deg(g(x))$ و $g(x) \neq 0$.

(١) ضع $r_0(x) = f(x)$ ، $r_1(x) = g(x)$ ، $i = 1$.

(٢) إذا كان $r_i(x) > 0$ نقوم بقسمة $r_i(x)$ على $r_{i-1}(x)$ ونفرض أن $r_{i+1}(x)$ هو باقي القسمة. أي أن $r_{i+1}(x) \equiv r_{i-1}(x) (mod\, r_i(x))$.

(٣) إذا كان $r_{i+1}(x) > 0$ نكرّر الخطوة (٢).

(٤) إذا كان $r_i(x) = 0$ نتوقف ويكون $\gcd(f(x), g(x)) = r_{i-1}(x)$.

لاحظ أن هذه الخوارزمية يجب أن تتوقف بعد عدد منته من الخطوات؛ لأنه لكل $i > 1$ تكون درجة الباقي $r_{i+1}(x)$ أصغر من درجة الباقي $r_i(x)$.

من الممكن تحسين هذه الخوارزمية للحصول على $t_i(x), s_i(x) \epsilon K[x]$ تحققان $t_i(x) f(x) + s_i(x) g(x) = r_i(x)$ لكل $i = 0,1,2,\cdots$ على النحو التالي:

بوضع:

$$t_0(x) = 1 \quad t_1(x) = 0$$
$$s_0(x) = 0 \quad s_1(x) = 1$$

وبفرض أن $r_{i-1}(x) = q_i(x) r_i(x) + r_{i+1}(x)$ (باستخدام خوارزمية القسمة) ووضع:

$$t_i(x) = q_{i-1}(x) t_{i-1}(x) + t_{i-2}(x)$$
$$s_i(x) = q_{i-1}(x) s_{i-1}(x) + s_{i-2}(x)$$

لكل $i = 2,3,\cdots$ نجد أن:

$$\begin{aligned} r_j(x) &= (-1)^j[-t_j(x)r_0(x) + s_j(x)r_i(x)] \\ &= t_j(x)r_0(x) + s_j(x)r_1(x) \end{aligned}$$

وبما أن الحقل هو حقل ثنائي فنستطيع تجاهل الاشارة السالبة.

مثال (٢,١)

سنستخدم خوارزمية القسمة لإيجاد القاسم المشترك الأكبر لكثيرتي الحدود:

$$f(x) = x^2 + x^3 + x^6 + x^7$$
$$g(x) = 1 + x^3 + x^4 + x^5$$

ضع $i = 0$ ، $r_0(x) = f(x)$ ، $r_1(x) = g(x)$. بقسمة $r_0(x)$ على $r_1(x)$ نحصل على:

$$x^2 + x^3 + x^6 + x^7 = \left(1 + x^3 + x^4 + x^5\right)\left(1 + x^2\right) + (1 + x^4)$$

إذن، $r_2(x) = 1 + x^4$ و $q_1(x) = 1 + x^2$. بقسمة $r_1(x)$ على $r_2(x)$ نحصل على:

$$1 + x^3 + x^4 + x^5 = \left(1 + x^4\right)(1 + x) + (x + x^3).$$

إذن، $r_3(x) = x + x^3$ و $q_2(x) = 1 + x$. بقسمة $r_2(x)$ على $r_3(x)$ نحصل على:

$$1 + x^4 = \left(x + x^3\right)(x) + \left(1 + x^2\right).$$

إذن، $r_4(x) = 1 + x^2$ و $q_3(x) = x$. بقسمة $r_3(x)$ على $r_4(x)$ نحصل على:

$$x + x^3 = \left(1 + x^2\right)(x) + 0.$$

إذن، $r_5(x) = 0$ ويكون $\gcd(f(x), g(x)) = r_4(x) = 1 + x^2$.

إذا أردنا استخدام خوارج القسمة $q_i(x)$ لحساب $t_i(x)$ و $s_i(x)$ لكل من الخطوات $i = 0,1,2,3,4$ بحيث يكون:

$$r_i(x) = t_i(x) f(x) + s_i(x) g(x).$$

فنرى أن:

$$\begin{aligned} r_2(x) &= r_0(x) + q_1(x) r_1(x) \\ &= (1) f(x) + (1 + x^2) g(x) \end{aligned}$$

$$\begin{aligned} r_3(x) &= x + x^3 \\ &= (1 + x) f(x) + (x + x^2 + x^3) g(x) \end{aligned}$$

$$\begin{aligned} r_4(x) &= 1 + x^2 \\ &= (1 + x + x^2) f(x) + (x + x^3 + x^4) g(x) \end{aligned}$$

والجدول التالي يلخص لنا هذه الخطوات:

i	$t_i(x)$	$s_i(x)$	$r_i(x)$
0	1	0	$f(x)$
1	0	1	$g(x)$
2	1	$1 + x^2$	$1 + x^4$
3	$1 + x$	$x + x^2 + x^3$	$x + x^3$
4	$1 + x + x^2$	$1 + x^3 + x^4$	$1 + x^2$
	—	—	0

باستخدام الاستقراء الرياضي نحصل على المبرهنة التالية:

مبرهنة (١,٣)

إذا كان $\gcd(f(x), g(x)) = d(x)$ فيوجد $t(x), s(x) \epsilon K[x]$ بحيث يكون:

$$t(x) f(x) + s(x) g(x) = d(x).$$

تمارين

(١,٤) جد القاسم المشترك الأكبر لكل زوج من أزواج كثيرات الحدود التالية:

(أ) $g\left(x\right)=1+x+x^3+x^5$,$f\left(x\right)=1+x+x^5+x^6+x^7$.

(ب) $g\left(x\right)=1+x+x^3$,$f\left(x\right)=1+x^2+x^3+x^7$.

(ج) $g\left(x\right)=1+x^2+x^3+x^7$,$f\left(x\right)=1+x+x^4+x^5+x^8+x^9$.

(د) $g\left(x\right)=x+x^3+x^4$,$f\left(x\right)=1+x+x^2+x^3+x^4$.

(١,٥) جد $\gcd(f\left(x\right),g\left(x\right))$ حيث $f\left(x\right)=1+x^9$ و $g(x)$ هي:

(أ) $g\left(x\right)=x+x^2+x^4+x^5+x^7+x^8$.

(ب) $g\left(x\right)=x^3+x^6$.

(ج) $g\left(x\right)=1+x+x^2+x^4+x^5+x^7+x^8$.

(د) $g\left(x\right)=1+x^3+x^6$.

(هـ) $g\left(x\right)=x+x^2+x^3+x^4+x^5+x^6+x^7+x^8$.

(١,٦) جد $\gcd(f\left(x\right),g\left(x\right))$ حيث:

$f\left(x\right)=1+x^{15}$ و $g\left(x\right)=x+x^2+x^4+x^8$.

(١,٧) جد $\gcd(f\left(x\right),g\left(x\right))$ حيث $f\left(x\right)=1+x^{23}$ و

$g\left(x\right)=x+x^2+x^3+x^4+x^6+x^8+x^9+x^{12}+x^{13}+x^{16}+x^{18}$.

الملحق ب

تحليل $1 + x^n$

Factorization of $1 + x^n$

الجدول التالي يُبيّن لنا تحليل $1 + x^n$ إلى حاصل ضرب كثيرات حدود غير قابلة للتحليل لكل عدد فردي n حيث $1 \leq n \leq 31$.

n	التحليل
1	$1 + x$
3	$\big(1 + x\big)\big(1 + x + x^2\big)$
5	$\big(1 + x\big)\big(1 + x + +x^2 + x^3 + x^4\big)$
7	$\big(1 + x\big)\big(1 + x + x^3\big)\big(1 + x^2 + x^3\big)$
9	$\big(1 + x\big)\big(1 + x + x^2\big)\big(1 + x^3 + x^6\big)$
11	$\big(1 + x\big)(1 + x + \cdots + x^{10})$
13	$\big(1 + x\big)(1 + x + \cdots + x^{12})$
15	$\big(1 + x\big)\big(1 + x + x^2\big)\big(1 + x + x^2 + x^3 + x^4\big)\big(1 + x + x^4\big)\big(1 + x^3 + x^4\big)$
17	$\big(1 + x\big)\big(1 + x + x^2 + x^4 + x^6 + x^7 + x^8\big)\big(1 + x^3 + x^4 + x^5 + x^8\big)$
19	$\big(1 + x\big)(1 + x + x^2 + \cdots + x^{18})$
21	$\big(1 + x\big)\big(1 + x + x^2\big)\big(1 + x^2 + x^3\big)\big(1 + x + x^3\big)$ $\big(1 + x^2 + x^4 + x^5 + x^6\big)\big(1 + x + x^2 + x^4 + x^6\big)$

n	التحليل
23	$\big(1+x\big)\big(1+x+x^5+x^6+x^7+x^9+x^{11}\big)$ $\big(1+x^2+x^4+x^5+x^6+x^{10}+x^{11}\big)$
25	$\big(1+x\big)\big(1+x+x^2+x^3+x^4\big)\big(1+x^5+x^{10}+x^{15}+x^{20}\big)$
27	$\big(1+x\big)\big(1+x+x^2\big)\big(1+x^3+x^6\big)\big(1+x^9+x^{18}\big)$
29	$\big(1+x\big)\big(1+x+\cdots+x^{28}\big)$
31	$\big(1+x\big)\big(1+x^2+x^5\big)\big(1+x^3+x^5\big)\big(1+x+x^2+x^3+x^5\big)$ $\big(1+x+x^2+x^4+x^5\big)\big(1+x+x^3+x^4+x^5\big)\big(1+x^2+x^3+x^4+x^5\big)$

الملحق (ج)

مثال على تشفير قرص مدمج
Example of Compact Disc Encoding

يحتاج تقديم مثال لتشفير قرص مدمج إلى كمية كبيرة من الحسابات (انظر البند (٧،٣))، ولذا فسنقدم هنا مثالاً معقولاً بحيث يمكن إجراء الحسابات دون الحاجة إلى وسائل الكترونية. لتكن C شفرة ريد وسولومن على الحقل $GF(2^4)$ بمولّد:

$$\begin{aligned} g(x) &= (1+x)(\beta+x)(\beta^2+x)(\beta^3+x) \\ &= \beta^6 + \beta^0 x + \beta^4 x^2 + \beta^{12} x^3 + x^4 \end{aligned}$$

هذه شفرة من النوع $(15,11,5)$ والتي يمكن قصرها إلى شفرة C_1 من النوع $(8,4,5)$ أو شفرة C_2 من النوع $(12,8,5)$. ويمكن توريقها بعمودين لعمق 8. يمكن تشفير رسالة m إلى كلمة شفرة c في الشفرة C_1 باستخدام مصفوفة مولّدة (انظر الجدول (٣،١)).

الجدول (٣,١). رسالة والتشفير الأول.

$$
m = \begin{matrix}
\beta^4 & 0 & 0 & \beta^3 \\
\beta^1 & \beta^{12} & \beta^3 & 0 \\
0 & 0 & \beta^2 & \beta^4 \\
0 & 0 & 0 & \beta^{13} \\
\beta^1 & 0 & 0 & 0 \\
0 & \beta^3 & \beta^2 & 0 \\
0 & 0 & 0 & 0 \\
\beta^4 & \beta^4 & 0 & \beta^1 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
\beta^1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0
\end{matrix}
\rightarrow c = \begin{matrix}
\beta^{10} & \beta^4 & \beta^8 & \beta^3 & \beta^7 & \beta^7 & \beta^0 & \beta^3 \\
\beta^7 & \beta^9 & \beta^4 & \beta^{10} & \beta^4 & \beta^{11} & \beta^3 & 0 \\
0 & 0 & \beta^8 & \beta^4 & \beta^{12} & \beta^6 & \beta^5 & \beta^4 \\
0 & 0 & 0 & \beta^4 & \beta^{13} & \beta^2 & \beta^{10} & \beta^{13} \\
\beta^7 & \beta^1 & \beta^5 & \beta^{13} & \beta^1 & 0 & 0 & 0 \\
0 & \beta^9 & \beta^{13} & \beta^{12} & \beta^{13} & \beta^0 & \beta^2 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\beta^{10} & \beta^2 & \beta^5 & \beta^6 & \beta^4 & \beta^8 & \beta^{13} & \beta^1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\beta^7 & \beta^1 & \beta^5 & \beta^{13} & \beta^1 & 0 & 0 & 0 \\
0 & 0 & 0 & \beta^6 & \beta^0 & \beta^4 & \beta^{12} & \beta^0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\cdots
\end{matrix}
$$

تظهر هذه الكلمات في الشفرة C_1 للتوريق البيني على النحو التالي:

$$
\begin{matrix}
\beta^{10} & \beta^7 & 0 & 0 & \beta^7 & 0 & 0 & \beta^{10} & 0 & 0 & \beta^7 & 0 & 0 & 0 & 0 & \cdots & & & & \\
 & & \beta^4 & \beta^9 & 0 & 0 & \beta^1 & \beta^9 & 0 & \beta^2 & 0 & 0 & \beta^1 & 0 & 0 & 0 & 0 & \cdots & & \\
 & & & & \beta^8 & \beta^4 & \beta^8 & 0 & \beta^5 & \beta^{13} & 0 & \beta^5 & 0 & 0 & \beta^5 & 0 & 0 & 0 & 0 & 0 \\
 & & & & & & \beta^3 & \beta^{10} & \beta^4 & \beta^4 & \beta^{13} & \beta^{12} & 0 & \beta^6 & 0 & 0 & \beta^{13} & \beta^6 & 0 \\
 & & & & & & & & \beta^7 & \beta^4 & \beta^{12} & \beta^{13} & \beta^1 & \beta^{13} & 0 & \beta^4 & 0 & 0 & \beta^1 \\
 & & & & & & & & & & \beta^7 & \beta^{11} & \beta^6 & \beta^2 & 0 & \beta^0 & 0 & \beta^8 & 0 \\
 & & & & & & & & & & & & \beta^0 & \beta^3 & \beta^5 & \beta^{10} & 0 & \beta^2 & 0 \\
 & & & & & & & & & & & & & & \beta^3 & 0 & \beta^4 & \beta^{13} & 0
\end{matrix}
$$

يمكن اعتبار أعمدة الصفيف أعلاه على أنها رسائل ونقوم بتشفيرها إلى كلمات في الشفرة C_2 حيث كل من صفوف الجدول التالي هو كلمة شفرة:

β^{1}	β^{10}	β^{14}	β^{7}	β^{10}	0	0	0	0	0	0	0
β^{13}	β^{7}	β^{11}	β^{4}	β^{7}	0	0	0	0	0	0	0
0	β^{10}	β^{4}	β^{8}	β^{1}	β^{4}	0	0	0	0	0	0
0	β^{0}	β^{9}	β^{13}	β^{6}	β^{9}	0	0	0	0	0	0
β^{13}	β^{7}	β^{10}	β^{5}	β^{2}	β^{5}	β^{8}	0	0	0	0	0
0	0	β^{10}	β^{4}	β^{8}	β^{1}	β^{4}	0	0	0	0	0
0	β^{7}	β^{7}	β^{14}	β^{9}	β^{12}	β^{2}	β^{3}	0	0	0	0
β^{1}	β^{5}	β^{4}	β^{2}	β^{6}	β^{4}	β^{7}	β^{10}	0	0	0	0
0	0	β^{11}	β^{0}	β^{2}	β^{9}	β^{9}	0	β^{7}	0	0	0
0	β^{8}	β^{10}	β^{5}	β^{14}	β^{8}	β^{9}	β^{0}	β^{4}	0	0	0
β^{13}	β^{7}	β^{11}	0	β^{11}	β^{5}	β^{11}	β^{14}	β^{6}	β^{7}	0	0
0	0	β^{11}	β^{11}	β^{5}	β^{11}	β^{5}	β^{14}	β^{3}	β^{11}	0	0
0	β^{7}	β^{1}	β^{5}	β^{5}	β^{12}	β^{5}	β^{7}	β^{14}	β^{4}	β^{0}	0
0	0	0	β^{12}	β^{12}	β^{12}	β^{1}	β^{12}	β^{12}	β^{8}	β^{3}	0
0	0	β^{11}	β^{5}	β^{9}	β^{2}	β^{3}	β^{6}	β^{1}	β^{12}	β^{10}	β^{3}
0	0	0	0	β^{10}	β^{12}	β^{5}	β^{5}	β^{8}	β^{9}	β^{10}	0
0	0	0	β^{4}	β^{13}	β^{2}	β^{10}	β^{9}	β^{4}	β^{8}	β^{1}	β^{4}
0	0	0	β^{12}	β^{6}	β^{11}	β^{3}	β^{2}	β^{10}	β^{3}	β^{4}	β^{13}
0	0	0	0	β^{7}	β^{1}	β^{5}	β^{13}	β^{1}	0	0	$0\cdots$

وبتحويل كلمات الشفرة هذه إلى النظام الثنائي نحصل على:

0100	1110	1001	1101	1110	0000	0000	0000	0000	0000	0000	0000
1011	1101	0111	1100	1101	0000	0000	0000	0000	0000	0000	0000
0000	1110	1100	1010	0100	1100	0000	0000	0000	0000	0000	0000
0000	1000	0101	1011	0011	0101	0000	0000	0000	0000	0000	0000
1011	1101	1110	0110	0010	0110	1010	0000	0000	0000	0000	0000
0000	0000	1110	1100	1010	0100	1100	0000	0000	0000	0000	0000
0000	1101	1101	1001	0101	1111	0010	0001	0000	0000	0000	0000
0100	0110	1100	0010	0011	1100	1101	1110	0000	0000	0000	0000

0000	0000	0111	1000	0010	0101	0101	0000	1101	0000	0000	0000
0000	1010	1110	0110	1001	1010	0101	1000	1100	0000	0000	0000
1011	1101	0111	0000	0111	0110	0111	1001	0011	1101	0000	0000
0000	0000	0111	0111	0110	0111	0110	1001	0001	0111	0000	0000
0000	1101	0100	0110	0110	1111	0110	1101	1001	1100	1000	0000
0000	0000	1111	1111	1111	0100	1111	1111	1010	0001	0000	0000
0000	0000	0111	0110	0101	0010	0001	0011	0100	1111	1110	0001
0000	0000	0000	0000	1110	1111	0110	0110	1010	0101	1110	0000
0000	0000	0000	1100	1011	0010	1110	0101	1100	1010	0100	1100
0000	0000	0000	1111	0011	0111	0001	0010	1110	0001	1100	1011
0000	0000	0000	0000	1101	0100	0110	1011	0100	0000	0000	0000

من الممكن الآن تحويل هذه الكلمات من كلمات طولها 4 إلى كلمات طولها 6 (على سبيل المثال، يظهر على الأقل صفر وعلى الأكثر أربعة أصفار بين كل ظهورين متتاليين للواحد) باستخدام الجدول التالي:

0000	000100	0001	010001
1000	000101	1001	101000
0100	001010	0101	101001
1100	001001	1101	101010
0010	001000	0011	100100
1010	010100	1011	100101
0110	010101	0111	100010
1110	010010	1111	100001

نضيف الآن إحداثياً بين كل كلمتين من الطول 6 (الإحداثي المضاف هو متمم لكل من الإحداثيين المجاورين). وللحفاظ على هذه الخاصية فستظهر الرسالة الأصلية m (انظر الجدول (٣،١)) على النحو التالي:

001010 1 010010 0 101000 0 101010 1 010010 1 000100 1
000100 1 000100 1 000100 1 000100 1 000100 1 000100 0 −
100101 0 101010 0 100010 1 001001 0 101010 1 000100 1
000100 1 000100 1 000100 1 000100 1 000100 1 000100 1 −
000100 1 010010 1 001001 0 010100 1 001010 1 001001 0
000100 1 000100 1 000100 1 000100 1 000100 1 000100 1 −
000100 1 000101 0 101001 0 100101 0 100100 0 101001 0
000100 1 000100 1 000100 1 000100 1 000100 1 000100 0 −
100101 0 101010 1 010010 1 010101 0 001000 1 010101 0
010100 1 000100 1 000100 1 000100 1 000100 1 000100 1 −
000100 1 000100 1 010010 1 001001 0 010100 1 001010 1
001001 0 000100 1 000100 1 000100 1 000100 1 000100 1 −
000100 0 101010 0 101010 0 101000 0 101001 0 100001 0
001000 0 010001 0 000100 1 000100 1 000100 1 000100 1 −
001010 1 010101 0 001001 0 001000 0 100100 1 001001 0
101010 1 010010 1 000100 1 000100 1 000100 1 000100 1 −
000100 1 000100 0 100010 1 000100 1 000100 0 101001 0
101001 0 000100 0 101010 1 000100 1 000100 1 000100 1 −
000100 1 010100 1 010010 1 010101 0 101000 1 010100 0
101001 0 000101 0 001001 0 000100 1 000100 1 000100 0 −
100101 0 101010 0 100010 1 000100 0 100010 1 010101 0
000100 0 101000 0 100100 0 101010 1 000100 1 000100 1 −
000100 1 000100 0 100010 0 100010 1 010101 0 100010 0
010101 0 101000 1 010001 0 100010 1 000100 1 000100 1 −
000100 0 101010 1 001010 1 010101 0 010101 0 100001 0
010101 0 101010 0 101000 1 001001 0 000101 0 000100 1 −
000100 1 000100 0 100001 0 100001 0 100001 0 001010 0
100001 0 100001 0 010100 1 010001 0 000100 1 000100 1 −
000100 1 000100 0 100010 1 010101 0 101001 0 001000 1
010001 0 100100 1 001010 0 100001 0 010010 1 010001 0 −
000100 1 000100 1 000100 1 000100 1 010010 0 100001 0

010101 0 010101 0 010100 0 101001 0 010010 1 000100 1 –
000100 1 000100 1 000100 1 001001 0 100101 0 001000 1
010010 0 101001 0 001001 0 010100 1 001010 1 001001 0 –
000100 1 000100 1 000100 0 100001 0 100100 0 100010 1
010001 0 001000 1 010010 1 010001 0 001001 0 100101 0 –
000100 1 000100 1 000100 1 000100 0 101010 1 001010 1
010101 0 100101 0 001010 1 000100 1 000100 1 000100 ?–

الملحق (د)

حلول لتمارين مختارة
Solutions to Selected Exercises

الفصل الأول: مقدمة في نظرية التشفير

(١,٢,١) (أ) $000, 010, 100, 110, 001, 011, 101, 111$.

(ب) $0000, 0100, 1000, 1100, 0001, 0101, 1001, 1101, 0010, 0110,$
$1010, 1110, 0011, 0111, 1011, 1111$

(١,٢,٢) 2^n.

(١,٢,٤) يمكن تحويل القناة إلى قناة تامة باستبدال كل إحداثي 1 بالإحداثي 0 وكل إحداثي 0 بالإحداثي 1.

(١,٢,٥) استبدل كل إحداثي 0 بالإحداثي 1 وكل إحداثي 1 بالإحداثي 0.

(١,٢,٦) لا نستطيع استنتاج أي شيء عن كلمة الشفرة المرسلة من الكلمة المستقبلة.

(١,٣,٤) 001.

(١,٣,٥) $C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$.

(أ) نعم

(ب) $0101, 1001, 1100, 1111$.

(ج) لا. يوجد لكل كلمة من الكلمات ذات الطول 4 التي لا تنتمي إلى الشفرة C أربع كلمات مختلفة هي الأقرب إليها.

(١,٣,٧) 8.

(١,٣,٨) 16 ، 32 ، 2^{n-1}.

(١,٤,١) 1 ، $\frac{3}{4}$ ، $\frac{1}{3}$.

(١,٦,٢) (أ) $p^3(1-p)^5 = 2 \cdot 2 \times 10^{-8}$

(ب) $p^7 = 0 \cdot 81$

(ج) $(1-p)^5 = 2 \cdot 4 \times 10^{-8}$

(د) $p^5 = 0 \cdot 86$

(هـ) $p^4(1-p)^3 = 2 \cdot 4 \times 10^{-5}$

(و) $(1-p)^5 = 2 \cdot 4 \times 10^{-8}$

(ز) $(1-p)^6 = 7 \cdot 3 \times 10^{-10}$.

(١,٦,٥) 0001110.

(١,٦,٦) 101101101.

(١,٦,٧) 00011.

(١,٦,٨) 100110.

(١,٦,٩) 110101 أو 101000.

(١,٦,١٠) (أ) $\varphi_p(v_1, w) \leq \varphi_p(v_2, w)$ إذا وفقط إذا كان $d_1 \leq d_2$.

(ب) $\varphi_p(v_1, w) = (\frac{1}{2})^n$ لكل w و v.

(١,٩,٥) إذا كانت أي من الكلمات 000 أو 001 أو 010 أو 011 هي المستقبلة فتستنتج طريقة IMLD أن الكلمة المرسلة هي 001. أما في الحالات المتبقية فتستنتج طريقة IMLD بصورة غير صائبة أن الكلمة المرسلة هي 101.

(١,٩,٦) فك تشفير 000 هو 000. فك تشفير كل من 001 و 011 و 101 هو 001. وفك تشفير 110 و 111 هو 110. أما بالنسبة للكلمتين 010 و 100 فيطلب إعادة إرسال.

(١,٩,٧) علامة * في الجدول التالي تعني طلب إعادة إرسال.

(أ)

فك التشفير	الكلمة المستقبلة
*	000
*	001
011	010
011	011
101	100
101	101
111	110
111	111

(ب)

فك التشفير	الكلمة المستقبلة
000	000
001	001
010	010
011	011
000	100
001	101
010	110
011	111

▲

(١,١٠,٢) (أ) $L(001) = \{000\,,001\,,010\,,011\}$.

وبهذا نجد أن:

$$\Theta_p(C,001) = p^3 + 2p^2(1-p) + p(1-p)^2.$$

(ب) $L(001) = \{100\,,101\,,110\,,111\}$.

وبهذا يكون:

$$\Theta_p(C,001) = p^3 + 2p^2(1-p) + p(1-p)^2.$$

(١,١٠,٤) (أ) $\Theta_p(C,001) = p^3 + p^2(1-p)$.

(ب) لفك تشفير 000 تكون الكلمة المرسلة هي فقط 000، وبهذا نجد أن

$$\Theta_p(110{,}000) = p(1-p)^2.$$

(١,١٠,٥) (أ) $\Theta_p(C,101) = p^3 + p^2(1-p)$.

(ب) $\Theta_p(C,v) = p^3 + p^2(1-p)$ لكل $v\epsilon C$.

(ج) $\Theta_p(C,0000) = p^4 + 3p^3(1-p)$

$$\Theta_p(C,0001) = p^4 + 3p^3(1-p)$$

$$\Theta_p(C,1110) = p^4 + 4p^3(1-p).$$

(هـ) $\Theta_p(C,00000) = \Theta_p(C,11111)$

$$= p^5 + 5p^4(1-p) + 10p^3(1-p)^2$$

(ز) $\Theta_p(C,v) = p^5 + 3p^4(1-p)$ لكل $v \epsilon C$.

(ح) $\Theta_p(C,v) = p^6 + 6p^5(1-p) + 9p^4(1-p)^2$ لكل $v \epsilon C$.

(١,١١,٢) (أ) لا (ب) نعم (ج) لا.

(١,١١,٣) (أ) (i) لا (ii) نعم (iii) لا.

(ب) (i) نعم (ii) نعم (iii) لا.

(١,١١,٤) لا يوجد.

(١,١١,٧) (أ) 001,011,101,111 .

(ج) $K^4 \backslash \{0000,0001,1110,1111\}$.

(هـ) $K^5 \backslash \{00000,111111\}$.

(ح) $K^6 \backslash \{000000,101010,010101,111111\}$.

(١,١١,١٢) (أ) 1 (ب) 1 (ج) 1

(د) 2 (هـ) 5 (و) 3

(ز) 2 (ح) 3.

(١,١١,١٣) 2.

(١,١١,١٨) $K^3 \backslash \{000,011,101,110\}$.

(١,١١,١٩) (أ) لا يوجد.

(د) {1000,0100,0010,0001}.

(هـ) جميع أنماط الأخطاء من الأوزان 1 ، 2 ، 3 ، 4.

(ح) جميع أنماط الأخطاء من الأوزان 1 أو 2.

(١,١٢,١٢) (أ) (i) 000,001 (ii) 000

(ج) (i) 0000,0010,0100,1000 (ii) 0000

(و) (i) 00000,10000,01000,00100,00010,00001

(ii) 00000,10000,01000,00100,00010,00001

(ز) (i) 00000,01000,00100,00010

(ii) 00000.

الفصل الثاني: الشفرات الخطية

(٢,١,١) الشفرتان (أ) و (ج) غير خطيّتين وباقي الشفرات هي شفرات خطيّة.

(٢,٢,٣) (أ) $\langle S\rangle = \{000\,,010\,,011\,,111\,,001\,,101\,,100\,,110\}$.

(ب) $\langle S\rangle = \{0000\,,1010\,,0101\,,111{,}1111\}$.

(د) $\langle S\rangle = K^4$.

(٢,٢,٧) (أ) $C^{\perp} = \{000\}$.

(ب) $C^{\perp} = \{0000\,,1010\,,0101\,,1111\}$.

(ج) $C^{\perp} = \{0000\,,1111\}$.

(٢,٣,٤) (أ) مُستقلة خطيّاً.

(ب) $\{101\,,011\,,010\}$.

(هـ) مُستقلة خطياً.

(ح) $\{1100\,,1010\,,1001\}$.

(ط) $\{10101010\,,01010101\}$.

(٢,٣,٧) (أ) $B = \{100\,,010\,,001\}$ ، $B^{\perp} = \phi$.

(ب) $B = \{1010\,,0101\}$ ، $B^{\perp} = B$.

(ج) $B = \{1010\,,0101\,,1100\}$ ، $B^{\perp} = \{1111\}$.

(هـ) $B = \{11000\,,01111\,,11110\,,01010\}$ ، $B^{\perp} = \{11111\}$.

(٢,٣,٨) (أ) $\dim C = 3$ ، $\dim C^{\perp} = 0$.

(ب) $\dim C = 2$ ، $\dim C^{\perp} = 2$.

(ج) $\dim C = 3$ ، $\dim C^{\perp} = 1$.

(هـ) $\dim C = 4$ ، $\dim C^{\perp} = 1$.

(و) $\dim C = 3$ ، $\dim C^{\perp} = 2$.

(٢,٣,١٦) (أ) $\dim C = 4$ (ب) $|C| = 16$.

(٢,٣,١٧) $|C| = 32$.

(٢,٤,١) $DC = \begin{bmatrix}101011\\110000\\011011\\000110\end{bmatrix}$ $BD = \begin{bmatrix}1000\\0010\\1010\end{bmatrix}$ $BC = \begin{bmatrix}110000\\011101\\101101\end{bmatrix}$.

(٢,٤,٦) $D \leftrightarrow \begin{bmatrix}1000\\0101\\0010\\0000\end{bmatrix}$ $C \leftrightarrow \begin{bmatrix}101011\\011011\\000110\\000000\end{bmatrix}$ $B \leftrightarrow \begin{bmatrix}1001\\0101\\0000\end{bmatrix}$ $A \leftrightarrow \begin{bmatrix}11011\\00101\\00000\end{bmatrix}$

(٢,٥,٣) (أ) $\{100, 010, 001\}$

(ج) $\{1001, 0101, 0011\}$

(هـ) $\{100001, 01001, 00101, 00011\}$

(ز) $\{1011, 0101, 0011\}$.

(٢,٥,٦) (أ) $\{010, 011, 111\}$

(ج) $\{0101, 1010, 1100\}$

(هـ) $\{11000, 01111, 11110, 01010\}$

(ز) $\{0110, 1010, 0011\}$.

(٢,٥,١٠) (أ) ϕ

(ب) $\{1010, 0101\}$

(ج) $\{11111\}$

(د) $\{101000, 110110, 000101\}$.

(٢,٥,١٢) (أ) $B = \{111000, 000111\}$

(ب) $B = \{1000110, 0100011, 0010111, 0001101\}$

(ج) $B = \{1000001, 0100001, 0010001, 0001001, 0000101, 0000011\}$

(و) $B = \{001000, 000100, 000010, 000001\}$.

(٢,٦,٤) (i) نعم (ii) لا.

(٢,٦,٥) (أ) $\begin{bmatrix}010\\001\end{bmatrix}$ (ب) $\begin{bmatrix}1001\\0110\end{bmatrix}$ (د) $\begin{bmatrix}11011\\00111\end{bmatrix}$.

(٢,٦,٦) (أ) $dim\, C = 3, \begin{bmatrix}100110\\010101\\001011\end{bmatrix}$.

(٢,٦,٧) (أ) $(8,4,4), \begin{bmatrix}10010110\\01010101\\00110011\\00001111\end{bmatrix}$ (ج) $(9,3,3), \begin{bmatrix}100100100\\010010010\\001001001\end{bmatrix}$

(و) $(6,3,2), \begin{bmatrix}101010\\011010\\000111\end{bmatrix}$ (ز) $(7,4,3), \begin{bmatrix}1001011\\0101010\\0011001\\0000111\end{bmatrix}$

(٢,٦,١٠) (أ) (i) 10011 (ii) 01010 (iii) 11100.

(٢,٦,١١) 01011, 10011, 01011, 00101, 01110, 01011, 10110.

(٢,٦,١٢) (أ) 1111111, 1110100, 0001011, 1001100

(ب) 1111001, 1110101, 0001011, 0001100.

(٢,٦,١٣) للتمرين (٢,٦,٦) (أ) $|C| = 8, R = 1/2$

(ب) $|C| = 8, R = 1/3$

(ج) $|C| = 4, R = 1/5$.

وللتمرين (٢,٦,٧) (أ) $|C| = 16, R = 1/2$

(ب) $|C| = 16, R = 1/2$

(ج) $|C| = 8, R = 1/3$

(د) $|C| = 8, R = 3/5$

(و) $|C| = 8, R = 1/3$

(ز) $|C| = 16, R = 4/7$.

(٢,٧,٤) (أ) $\begin{bmatrix}1\\0\\0\end{bmatrix}$ (ب) $\begin{bmatrix}01\\10\\10\\01\end{bmatrix}$ (ج) $\begin{bmatrix}001\\111\\100\\010\\001\end{bmatrix}$

(٢,٧,٥) (أ) $\begin{bmatrix}110\\101\\011\\100\\010\\001\end{bmatrix}$ (ب) $\begin{bmatrix}10010\\01010\\00101\\10000\\01000\\00100\\00010\ \ 00001\end{bmatrix}$ (ج) $\begin{bmatrix}1000\\1000\\0010\\0010\\0100\\0100\\0001\\0001\end{bmatrix}$

(ز) $\begin{bmatrix}11\\01\\10\\01\\01\end{bmatrix}$ (ي) $\begin{bmatrix}111\\110\\101\\100\\011\\010\\001\end{bmatrix}$.

(٢,٧,٩) (أ) $G(C^{\perp}) = G(C) = \begin{bmatrix}110000\\001010\\000101\end{bmatrix}$.

(٢,٧,١٠) تحتوي $C^{\perp}$ على 16 كلمة طول كل منها عدد زوجي في الحقل K^5.

(٢,٧,١١) (أ) $dim\, C = t\,, dim\, C^{\perp} = 2^t - t - 1\,, |C| = 2^t\,,$

$|C^{\perp}| = 2^{2^t - t - 1}\,, R = t/(2^t - 1)$

(ب) $dim\, C = 11\,, dim\, C^{\perp} = 12\,, |C| = 2^{11} = 2048\,,$

$|C^{\perp}| = 2^{12} = 4096\,, R = 11/23$

(ج) $dim\, C = 8\,, dim\, C^{\perp} = 7\,, |C| = 2^8 = 256\,,$

$|C^{\perp}| = 2^7 = 128\,, R = 8/15$.

(٢,٨,٤) (أ) 1111100 (ب) 1011000.

(٢,٨,١٠) (أ) $C' = \{00000\,, 11100\,, 10101\,, 01001\}$.

(٢,٨,١١) (أ) $G' = \begin{bmatrix} 100011 \\ 010010 \\ 001001 \\ 000100 \end{bmatrix}$.

(٢,٨,١٢) (أ) $G' = \begin{bmatrix} 10110 \\ 01011 \end{bmatrix}$.

(٢,٨,١٤) (أ) نعم (ب) نعم (ج) لا.

(٢,٩,٤) (أ) 4 (ب) 4 (ج) 4.

(٢,١٠,٦) (أ) $C, C + 1000, C + 0010, C + 0011$

(ب) $C, C + 1000, C + 0100, C + 0001$.

(٢,١٠,٧) (أ) $C, C + 100000, C + 010000, C + 001000, C + 000100,$
$C + 000010, C + 000001, C + 001001$

(د) $C, C + 100000$

(و) $C, C + 1000, C + 0100, C + 0010, C + 0001,$
$C + 1100, C + 1010, C + 1001$.

(٢,١٠,٨) (أ) $C, C + 1000, C + 0100, C + 0001$

(ب) $C, C + 1000000, C + 0100000, C + 0010000, C + 0001000,$
$C + 0000100, C + 0000010, C + 0000001$

(ج) $C, C + 000100, C + 010000, C + 001100, C + 100000,$
$C + 100100, C + 110000, C + 110100$

(٢,١١,٢) (أ) 010011 (ب) 101001 (ج) 001111

(د) 010011 (هـ) 110101 (و) 001111.

(٢,١١,٨)

(أ)

التناذر	نمط الخطأ
11	*
00	0000
01	*
10	0010

، $H = \begin{bmatrix} 01 \\ 01 \\ 10 \\ 01 \end{bmatrix}$.

(٢,١١,٩) (أ)

التناذر	نمط الخطأ
000	000000
001	000001
010	000010
011	100000
100	000100
101	010000
110	001000
111	*

، $H = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}$.

(٢,١١,١٠)

(ب)

التناذر	نمط الخطأ
000	0000000
001	0000001
010	0000010
011	0001000
100	0000100
101	0010000
110	0100000
111	1000000

(٢,١١,١٩) (أ) (i) 1100 (ii) 1001 (iii) 0101

(ج) (i) 001110 (ii) 001110 (iii) .011011

(٢,١١,٢١) (أ)

التناذر	نمط الخطأ
000	0000000
001	0000001
010	0000010
011	0001000
100	0000100
101	0010000
110	0100000
111	1000000

(٢,١٢,٢) للتمرين **(٢,١٠,٦)** (أ) $\theta_p(C) = p^4 + p^3(1-p)$.

(ج) $\theta_p(C) = p^5 + 3p^4(1-p)$.

وللتمرين **(٢,١٠,٧)** (أ) $\theta_p(C) = p^6 + 6p^5(1-p)$.

(ب) $\theta_p(C) = p^6 + 6p^5(1-p) + 9p^4(1-p)^2$.

وللتمرين (٢,١٠,٨) (أ) $\theta_p(C) = p^4 + 2p^3(1-p)$.

(ب) $\theta_p(C) = p^7 + 7p^6(1-p)$.

الفصل الثالث: الشفرات التامة والشفرات ذات الصلة بها

(٣,١,٥) (أ) 2^4 (ب) 2^4 (ج) 2^4

(هـ) 2^8 (و) 4096.

(٣,١,١٨) (أ) (8,6,3)، لا، $16 \le |C| \le 16$

(د) (15,6,3)، نعم، 2048.

(٣,١,١٩) (أ) $64 \le |C| \le 256$ (ب) $2048 \le |C| \le 2048$

(ج) $128 \le |C| \le 128$ (د) $256 \le |C| \le 256$

(هـ) $32 \le |C| \le 256$ (و) $16 \le |C| \le 32$.

(٣,١,٢٠) لا.

(٣,٣,٤)

التناذر	نمط الخطأ
000	0000000
111	1000000
110	0100000
101	0010000
011	0001000
100	0000100
010	0000010
001	0000001

$H = \begin{bmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$ (أ) 0101011 (ج) 0011110.

(٣,٤,٧) (أ) 696 (ب) 17 (ج) 17.

(٣,٦,٥) (أ) 100000001001, 000000000000

(ب) 000000100000, 001000010000

(ج) 000000100000 , 000000010000

(د) اطلب إعادة ارسال.

(هـ) 011000000000 , 00000000100

(ز) 001010000000 , 000000000000.

(٣,٦,٦) (أ) 010010000000 , 000000000000

(ب) 000000000000 , 001000110000

(ج) 001000000000 , 100000000000

(د) 000000000101, 000000000001

(هـ) 000100000000 , 000110000000

(و) 000000001000 , 000001000000.

(٣,٧,٣) (أ) 111111100000 , 10101111011

(ب) 100000000000 , 11011100010

(ج) 000101011001 , 11100000000

(د) 011000001001 , 011011011011.

(٣,٧,٧) 253.

(٣,٨,٥)
$$\begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0001 & 0001 \\ 0000 & 1111 \\ 0000 & 0101 \\ 0000 & 0011 \end{bmatrix}$$

(٣,٨,١٠) (أ) 0101 1010 (ب) 0110 0110

(ج) اطلب إعادة ارسال. (د) 1100 1100

(٣,٩,٦) (أ) $m = (0101)$ $w_3 = (2,-2,2,-2,-2,-6,-2,2)$.

(ب) $m = (0110)$ $w_3 = (2,-2,-2,-6,-2,2,2,2)$.

(ج) $m =?$ $w_3 = (-4,-4,0,0,0,0,-4,4)$.

(د) $m = (1010)$ $w_3 = (2,2,6,-2,-2,-2,2,2)$.

الفصل الرابع: الشفرات الخطية الدورية

(٤,١,١٠) (أ) $q(x) = x^3, r(x) = x^3$.

(٤,١,١٣) (أ) $\{0 + x^2, x, x + x^2\}$ (ج) $\{0, x^3, 1 + x + x^2\}$.

(٤,٢,٢٢) (أ) $g(x) = 1$ (هـ) $g(x) = 1 + x$.

(٤,٣,٥) (أ) $\begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix}$.

(٤,٣,٦) (ب) $\begin{bmatrix} 101010 \\ 010101 \end{bmatrix}$ $g(x) = 1 + x^2 + x^4$.

الفصل الخامس: شفرات BCH

(٥,١,١٥)

(أ) $\begin{bmatrix} 00 & 0 \\ 10 & \beta^0 \\ 01 & \beta \\ 11 & \beta^2 \end{bmatrix}$ (ب) $\begin{bmatrix} 000 & 0 \\ 100 & \beta^0 \\ 010 & \beta \\ 001 & \beta^2 \\ 101 & \beta^3 \\ 111 & \beta^4 \\ 110 & \beta^5 \\ 011 & \beta^6 \end{bmatrix}$.

(٥,١,١٧) $\beta, \beta^2, \beta^4, \beta^7, \beta^8, \beta^{11}, \beta^{13}, \beta^{14}$.

(٥,٢,٧)

كثيرة الحدود الأصغرية	العنصر
x	0
$1 + x$	1
$1 + x + x^3$	β, β^2, β^4
$1 + x^2 + x^3$	β, β^6, β^5

(٥,٢,٨)

كثيرة الحدود الأصغرية	العنصر
x	0
$1 + x$	1
$1 + x + x^2$	β^5, β^{10}
$1 + x + x^4$	$\beta^7, \beta^{14}, \beta^{13}, \beta^{11}$
$1 + x^3 + x^4$	$\beta, \beta^2, \beta^4, \beta^8$
$1 + x + x^2 + x^3 + x^4$	$\beta^3, \beta^6, \beta^9, \beta^{12}$

(٥,٢,٩) (أ) اطلب إعادة ارسال. (ب) 10.

(ج) 5 و 8. (د) 6 و 11.

(هـ) اطلب إعادة ارسال. (و) اطلب إعادة ارسال.

(ز) 0 و 13. (ح) كلمة شفرة.

الفصل السادس: شفرات ريد وسولومن

(٦,١,٦) (أ) 2^{15}.

(ب) $g(x) = \beta + \beta^3 x + x^2$.

(ج) (i) $\beta\beta\beta^6\beta^6 000$.

(د) $g_k(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^4+x)$.

(٦,١,٧) (أ) 2^{44}.

(ب) $g(x) = \beta^{10} + \beta^3 x + \beta^6 x^2 + \beta^{13} x^3 + x^4$.

(ج) (i) $\beta^{10}\beta^3\beta^6\beta^{13}100000\beta^2\beta^{10}\beta^{13}\beta^5\beta^7$.

(د) $g_k(x) = (\beta^8+x)(\beta^6+x)(\beta^{12}+x)(\beta^9+x)g(x)$.

(٦,٢,٣) (أ) β^2 (ب) β^5 (ج) β^4.

(٦,٢,٧) (أ) $n = 3, k = 1, d = 3$ و $|C| = 4$

(ب) $G = [\beta\beta^2 1]$

(ج)

كلمة الشفرة c	الرسالة	$f(c)$
0 0 0	0	000000
$\beta\ \beta^2\ 1$	1	011110
$\beta^2\ 1\ \beta$	β	111001
$1\ \beta\ \beta^2$	β^2	1001111

(٦,٢,٨) (أ) $n = 7, k = 3, d = 5$ و $|C| = 8^3 = 512$.

(ب) $g(x) = \beta^6 + \beta^5 x + \beta^5 x^2 + \beta^2 x^3 + x^4$.

(٦,٢,٩) (أ) $\beta + \beta^2 x + x^2 = (\beta^3 + x)(\beta^4 + x) = (1 + x)(\beta + x)$.

(ب) $1 + \beta^6 x + x^2 = (\beta^3 + x)(\beta^4 + x)$.

(ج) $\beta^3 + \beta x + x^2 + \beta^3 x^3 + x^4 = (\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x)$

(د)
$$\begin{aligned}\beta^{10} + \beta^3 x + \beta^6 x^2 + \beta^3 x^3 + x^4 \\ = (\beta + x)(\beta^2 + x) + (\beta^3 + x)(\beta^4 + x)\end{aligned}$$

(ج)
$$\begin{aligned}\beta^{21} + \beta^{24} x + \beta^{16} x^2 + \beta^{24} x^3 + \beta^9 x^4 + \beta^{10} x^5 + x^6 \\ = (\beta + x)(\beta^2 + x) \cdots (\beta^6 + x)\end{aligned}$$

(٦,٣,٥) (أ) $00\beta\beta^5\beta^3\beta^2\beta^{13}\beta^{10}\beta 000000$

(ب) $1\beta^4\beta^2\beta\beta^{12}\beta^9 10\beta\beta^5\beta^3\beta^2\beta^{13}\beta^{10}\beta$

(ج) $\beta\beta^{10}\beta^7 0\beta^{12}\beta^3\beta^3 10000000$.

(٦,٣,٦) (أ) $001\beta^8\beta^{11}\beta^3\beta^5 00000000$

(ب) $0\beta^{10}\beta^3\beta^6\beta^{13}0\beta^8\beta^{11}\beta^3\beta^5 00000$

(ج) $\beta^4\beta^{12}1\beta^7 0\beta^2\beta^5\beta^{12}\beta^{14}000000$.

(٦,٣,٨) (أ) $0\beta^2 0000000000000$

(ب) $00\beta 00\beta^3 000000000$

(ج) 100000000000000

(د) $\beta^5 11100000000000$

(هـ) $\beta^{10}\beta^3 0001000010000$

(و) $\beta^2 0000\beta^2 0000\beta^2 0000$.

(٦,٥,٤) (أ) $(\beta + x)$

(ب) $(\beta^2 + x)(\beta^3 + x)$

(ج) $(\beta^5 + x) + (\beta^{10} + x)$

(د) $(1+x)(\beta+x)(\beta^2+x)(\beta^3+x)$

(هـ) $(1+x)(\beta+x)(\beta^5+x)(\beta^{10}+x)$

(و) $(1+x)(\beta^5+x)(\beta^{10}+x)$

في الجدول التالي، لكل p_i و q_i يمثل الرمز * عنصر الحقل الصفري والرمز i يمثل العنصر β^i.

(أ)

-1	0	2	3	4	5	6	7	8	9				0	-1	$-\infty$
0	2	3	4	5	6	7	8	9				0	*	0	-1
1	7	8	9	10	11	12	13				0	2	*	1	0
2	*	*	*	*	*	*				0	1	*	*	2	1
3	*	*	*	*	*				0	1	*	*	*	4	1
4	*	*	*	*				0	1	*	*	*		6	1
5	*	*	*				0	1	*	*	*			8	1
6	*	*				0	1	*	*	*				10	1
7	*				0	1	*	*	*					12	1
8				0	1	*	*	*						(14)	(1)

$$\sigma(x) = x + \beta^1$$

(ب)

-1	0	9	13	7	4	12	4	8	2				0	-1	$-\infty$
0	9	13	7	4	12	4	8	2				0	*	0	-1
1	8	*	0	1	12	3	*				0	9	*	1	0
2	12	13	9	0	*	7				0	4	*	*	2	1
3	13	14	10	1	*				0	*	13	*	*	3	2
4	*	*	*	*				0	1	7	*	*		4	3
5	*	*	*				0	1	7	*	*			6	3
6	*	*				0	1	7	*	*				8	3
7	*				0	1	7	*	*					10	3
8				0	1	7	*	*						(12)	(3)

$$\sigma(x) = x^2 + \beta^1 x + \beta^7 = (x+\beta^2)(x+\beta^5)$$

(ج)

-1	0	0	0	0	0	0	0	0	0				0	-1	$-\infty$
0	0	0	0	0	0	0	0	0				0	*	0	-1
1	*	*	*	*	*	*	*				0	0	*	1	0
2	*	*	*	*	*	*				0	0	*	*	3	0
3	*	*	*	*	*				0	0	*	*	*	5	0
4	*	*	*	*				0	0	*	*	*		7	0
5	*	*	*				0	0	*	*	*			9	0
6	*	*				0	0	*	*	*				11	0
7	*				0	0	*	*	*					13	0
8				0	0	*	*	*						(15)	(0)

$$\sigma(x) = x + \beta^0$$

(د)

-1	0	10	3	13	3	12	5	13	3				0	-1	$-\infty$
0	10	3	13	3	12	5	13	3				0	*	0	-1
1	11	*	13	1	13	6	13				0	10	*	1	0
2	4	2	0	*	*	2				0	8	*	*	2	1
3	2	13	9	6	13				0	*	3	*	*	3	2
4	6	10	6	13				0	13	2	*	*		4	3
5	4	0	9				0	11	2	7	*			5	4
6	2	14				0	4	9	9	*				6	5
7	2				0	11	*	7	5					7	6
8				0	12	4	0	6						(8)	(7)

$$\sigma(x) = x^4 + \beta^{12}x^3 + \beta^4x^2 + \beta^0x + \beta^6$$
$$= (x + \beta^0)(x + \beta^1)(x + \beta^2)(x + \beta^3)$$

(هـ)

-1	0	12	8	*	7	13	4	13	0				0	-1	$-\infty$
0	12	8	*	7	13	4	13	0				0	*	0	-1
1	12	5	7	11	2	12	5				0	12	*	1	0
2	4	7	8	14	6	7				0	11	*	*	2	1
3	2	6	0	5	3				0	8	4	*	*	3	2
4	9	13	14	7				0	3	14	*	*		4	3
5	*	1	2				0	4	3	11	*			5	4
6	1	2				0	4	3	11	*				7	4
7	1				0	4	4	14	6					6	6
8				0	1	*	0	1						(8)	(7)

$$\sigma(x) = x^4 + \beta^1x^3 + \beta^0x + \beta^1$$
$$= (x + \beta^1)(x + \beta^0)(x + \beta^5)(x + \beta^{10})$$

(و)

-1	0	2	$*$	$*$	2	$*$	$*$	2	$*$					0	-1	$-\infty$
0	2	$*$	$*$	2	$*$	$*$	2	$*$					0	$*$	0	-1
1	4	$*$	2	4	$*$	2	4					0	2	$*$	1	0
2	$*$	2	$*$	$*$	2	$*$					0	$*$	$*$	$*$	2	1
3	2	$*$	$*$	2	$*$					0	$*$	$*$	$*$	$*$	4	1
4	$*$	0	$*$	$*$					0	$*$	13	0	$*$		3	3
5	0	$*$	$*$					0	$*$	13	0	$*$			5	3
6	$*$	$*$					0	$*$	$*$	0	$*$				6	3
7	$*$					0	$*$	$*$	0	$*$					8	3
8					0	$*$	$*$	0	$*$						(10)	(3)

$$.\sigma(x) = x^3 + 1 = (x + \beta^0)(x + \beta^5)(x + \beta^{10})$$

(٦,٦,٩) (أ) 1010 1111 1111 0011 1001 0000 0000

(ب) 1001 1010 0000 0011 1010 0011 1001

(ج) 0101 1001 0000 1100 1001 1100 0101

(د) 0000 1010 1111 1111 0011 1001 0000.

(٦,٦,١٠) فك تشفير $f(w)$ ليكون $f(c)$ حيث c هي:

(أ) $\beta^{10}\beta^{12}\beta^{7}\beta^{3}\beta^{12}\beta^{8}\beta^{8}\beta^{2}0000000$

(ب) $\beta^{10}0\beta\beta^{7}\beta^{7}0\beta^{0}\beta^{2}0000000$

(ج) $0\beta^{12}\beta^{14}\beta^{4}\beta^{2}\beta^{8}\beta^{2}00000000$.

(٦,٦,١١) فك تشفير $\bar{f}(w)$ ليكون $\bar{f}(c)$ حيث $c = \beta^{7}\beta^{7}1\beta^{9}\beta\beta^{10}\beta^{8}10000000$.

الفصل السابع: شفرات تصويب الأخطاء الاندفاعية

(٧,١,٥) C ليست شفرة تصويب خطأين؛ لأن عدد مجموعاتها المشاركة يساوي 32.

(٧,١,٦) C ليست شفرة تصويب ثلاثة أخطاء؛ لأن عدد مجموعاتها المشاركة يساوي 64.

(٧,١,١٣) (أ) 101100000001000

(ج) 100000101010011

(هـ) 00000111100100 .

(٧,١,١٤) (أ) 010100000010010

(ج) 001110000000100

(هـ) 000000011111010 .

(٧,٢,٤) (أ) 1000110 0110110 1110000 0011100 0110110 0001111

(ب) 10 01 01 00 11 11 00 10 10 11 01 01 00 00 00 10 10 01 11 11 01

(ج) 101 011 011 000 110 110 000 000 010 110 101 111 011 001.

(٧,٢,٨) (أ) 1 ****** 00 ***** 110 **** 0110 *** 00101 ** 011011 *

(ب) 1 ****** 0 ****** 10 ***** 01 ***** 010 **** 001 ****.

(٧,٢,٩) يتم ارسال كلمات الشفرة بالترتيب دون توريق.

(٧,٢,١٢) (أ) 01 10 11 11 10 01 10 11 11 01 01 00 01 00 11 01

10 11 10 10 11 00 01 01

(ب) 011 101 111 110 100 010 001 100 111 101 110 011.

(٧,٢,١٣) (أ) $m_1 = 0000, m_2 = 0011, m_3 = 0000$

(ب) $m_1 = 1000, m_2 = 0110, m_3 = 0011$.

الفصل الثامن: شفرات التلاف

(٨,١,٧) (أ) 11101001 ⋯ (ب) 0010111 ⋯ .

(٨,١,١٢) (أ) 000 , 0010000 (ب) 001 , 1110000.

(٨,١,١٤) (أ) 000 , 0010000 (ب) 000 , 100 .

(٨,٢,٢) (أ) $c(x) = (1 + x + x^4 + x^6, 1 + x + x^2 + x^4 + x^5 + x^6, 1 + x^2 + x^5 + x^6)$

(ب) $c(x) = (1 + x^2 + x^6, 1 + x^3 + x^5 + x^6, 1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$

(ج) $c(x) = (1 + \sum_{i=3}^{\infty} x^i, 1 + x^2, 1 + x + \sum_{i=3}^{\infty} x^i)$.

(٨,٢,٣) (أ) $c(x) = (1 + x + x^2 + x^3 + x^6, 1 + x^2 + x^5 + x^6)$

(ب) $c(x) = (1 + x + x^5 + x^6 + x^7, 1 + x^7)$

(ج) $c(x) = (1 + x^2 + \sum_{i=1}^{\infty} x^{2i+1}, 1 + x + \sum_{i=3}^{\infty} x^i)$.

(٨,٢,٦) صيغة التوريق لكلمات الشفرة هي :

للتمرين (٨,٢,٢) (أ) 111 110 011 000 110 011 111 ...

(ب) 111 001 101 011 001 011 111 ...

(ج) 111 001 010 101 101 101 101 ... .111

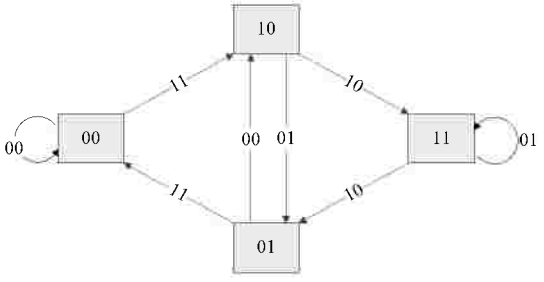
وللتمرين (٨,٢,٣) (أ) 11 10 11 10 00 01 11 ...

(ب) 11 10 00 00 00 10 10 11 ...

(ج) . 11 01 10 11 01 11 01 11 01 ...

(٨,٢,١١)

(أ)

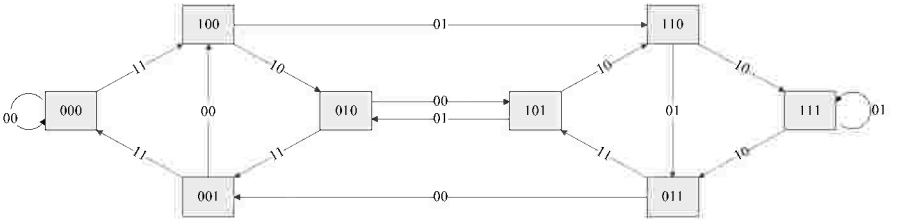


(ب) (i) 11 01 00 01 11 00 00 ... (ii) 11 10 01 10 11 00 00 ...

(ج) (i) 1 0 1 0 0 0 ... (ii) .0 1 1 1 1 0 1 ...

(٨,٢,١٢)

(أ)



(ب) (i) ⋯ 11 10 11 00 10 11 11 00 00

(ii) ⋯ 11 01 01 11 01 11 11 00 00

(iii) ⋯ 11 01 10 01 01 01

(ج) (i) ⋯ 1 0 1 0 1 1 1

(ii) ⋯ 0 1 1 1 1 0 0.

(٨,٣,١) (أ) $m = 1010101\cdots = \sum_{i=1}^{\infty} x^{2i}$

(ب) ⋯ $1 * 1 * 1 *$

(ج) ⋯ $000 *$

(٨,٣,٢) (أ) $gcd = 1 + x$ والعروة على المرحلة 111 هي دورة وزنها صفر.

(ب) $gcd = 1$ وهي ليست شفرة اخفاق تام.

(ج) $gcd = 1 + x + x^2$ ، (0110,1011,1101) دورة وزنها صفر.

(٨,٣,٣) (أ) 5 (ب) 6 (ج) 7.

(٨,٣,٦) (أ) $\tau(a) = 2, \tau(2) = 6$

(ب) $\tau(1) = 2, \tau(2) = 6$

(ج) $\tau(1) = 2, \tau(2) = 9, \tau(3) = 13$.

(٨,٤,٤)

المرحلة s	$t=8$	$t=9$	$t=10$	$t=11$	$t=12$
000	3,00000 **	3,000000 *	3,0000000	3,0000000	3,0000000
100	5,100 ****	3,1001001	5,100 ****	3,1001110	5,100 ****
010	4,0100100	4,0101001	4,0100100	4,0101110	4,0100111
110	4,1100100	4,1101001	4,1100100	4,1101110	4,1100111
001	3,0010011	5,001 ****	3,0011100	5,001 *** 0	5,001 * 1 * 1
101	3,1010011	5,101 ****	3,1011100	5,101 *** 0	5,101 * 1 * 1
011	4,011 * 0 **	2,0111001	4,0111 * 0 *	4,0111010	5,0111001
111	2,1110011	4,111 * 0 **	4,1110100	4,1110010	4,1110111
فك التشفير	1	1	0	0	0

(٨,٤,٥) (أ) $m = 0\,0\,0$ (ب) $m = 1\,0\,0$.

(٨,٤,١٤) (ب)

المرحلة s	المخرج $X_3=0$	المخرج $X_3=1$	$t=1$	2	3	4	5	6	7	8
000	00	11	∞	∞	∞	7	6	6	6	6
100	11	00	2	∞	∞	5	4	5	5	6
010	10	01	∞	3	∞	4	6	5	6	6
110	01	10	∞	3	∞	4	6	5	6	6
001	11	00	∞	∞	5	4	5	5	6	6
101	00	11	∞	∞	3	6	4	6	5	6
011	01	10	∞	∞	4	5	5	6	6	7
111	10	01	∞	∞	4	5	5	6	6	7

$d = 6, \tau(1) = 2, \tau(2) = 6$

الفصل التاسع: شفرات ريد ومولر وبريبراتا

(٩,١,٣) (أ) $f_I(x) = (x_0 + 1)(x_3 + 1)$

(ب) $v_I = 1000100000000000, f_I(x) = (x_0 + 1)(x_1 + 1)(x_3 + 1)$

(ج) $f_I(x) = (x_1 + 1)$

(د) $v_I = 1111000000000000, f_I(x) = (x_2 + 1)(x_3 + 1)$

(هـ) $v_I = 1, f_I(x) = 1$

(و) $.100\cdots 0, f_I(x) = \prod_{i=0}^{3}(x_i + 1)$

(٩,١,٤) (أ) $f_I(x) = (x_0 + 1)(x_4 + 1)$

(ج) $f_I(x) = (x_1 + 1)$

(د) $f_I(x) = (x_1 + 1)(x_2 + 1)(x_4 + 1)$

(هـ) $v_I = 11\cdots 1, f_I(x) = 1$

(و) $.v_I = 100\cdots 0, f_I(x) = \prod_{i=1}^{4}(x_i + 1)$

(٩,١,٥) يوجد عدد $|I|$ من الإحداثيات الصفرية وخياران لكل من الإحداثيات الأخرى التي عددها $m - |I|$ في H_I.

(٩,١,٦) بما أن أوزان جميع v_I (عدا v_{I_m}) زوجية فنرى أن وزن v زوجي إذا وفقط إذا كان $.v\epsilon\langle v_{I_m}\rangle^{\perp}$

(٩,١,٩) (أ)

$$\begin{bmatrix} 11111111 \\ 11110000 \\ 11001100 \\ 10101010 \\ 11000000 \\ 10100000 \\ 10001000 \end{bmatrix} \begin{matrix} v_\emptyset \\ v_2 \\ v_1 \\ v_0 \\ v_{1,2} \\ v_{0,2} \\ v_{0,1} \end{matrix}$$

(٩,١,١٢) (أ) $c = v_2 + v_0 = 0101\ 1010\ 1010\ 1010$

(ب) $c = v_{0,1} = 1000\ 1000\ 1000\ 1000$

(ج) $.c = v_2 + v_{0,3} = 0101\ 1010\ 1111\ 0000$

(٩,٢,٧) (أ) 0 1000 000001 0 (ب) 0 0000 0 11000 0

(ج) 1 1001 100000 1 (د) 1 1111 111111 1

(هـ) 0 0100 000100 0 (و) 0 0101 010000 0

(ز) 0 0000 000010 0 (ح) 0 0110 00000 0

(ط) 1 0001 000101.

(٩,٢,٨) (أ) 0 00000 0000000100 0 (ب) 0 00100 1000100001 0

(ج) 1 00000 0000010000 (د) 1 00100 1100000000 1

(هـ) 0 01001 0000000100 0 (و) 0 10010 0000000000 0

(ز) اطلب اعادة ارسال.

(٩,٣,١٠) (أ) (ii) 1001 1010 11110011 (iii) 01100101 11110011

(ج) (ii) 11000110 10101111 (iii) 11001001 11100111.

(٩,٣,١١) (أ) إذا كان $\alpha = 0$ فنرى أن $\alpha U = \{0\}$ ومن ثم $|\alpha U|$ عدد فردي. من ذلك نرى أن $[\chi(U), \chi(V)]$ لا تحقق الشرط (i) من التعريف (٩,٣,٣).

(٩,٣,١٧) (أ) 01000001 01110100 (ب) 00001001 01001110

(ج) 00000011 11010010.

(٩,٤,٦) (أ) 10101001 11011011 (ب) 10101001 00100100

(ج) 11111111 11111111 (د) 11111111 00000000

(هـ) 00000000 11111111.

(٩,٤,٧) (أ) $10100 \cdots 0$ 00000100010 $\cdots 0$ (ب) $10100 \cdots 00 \cdots 0$.

(٩,٤,٨) (أ) 31 (ب) 21.

(٩,٥,٣) (أ) 1000001 11101000 (ب) 00011110 01000010

(ج) 00000101 10100110 (د) 01000010 00011110

(هـ) 11101000 10000001 (و) 10011011 01111101

(ز) اطلب إعادة إرسال (ح) 10100101 10010000

(ط) 11101101 01010101 (ي) 10111011 01101010

(ك) 01010101 11101101 (ل) 01101010 10111011

(م) 10100101 10010000.

(٩,٥,٤) (أ) 11000 11000 10000 00000 00000 10000 11 00011 11000
00000 01000 00011 00100 00

(ب) 10100 00000 00000 00000 00000 00000 00 00000 10001
00000 00000 01010 10111 00

(٩,٥,٥) لا.

الفصل العاشر: التعمية التقليدية

(١٠,٢,٥) تقترح الكلمة "VHV" بأن طول المفتاح يقسم 16. وبما أن النص المعمى للنص الواضح 'an' هو 'AE' فنرى أن جزءاً من كلمة المفتاح هو 'AR'. بعد إثبات أن طول المفتاح يجب أن يكون أكبر من 2 ، أدرس الحالة التي تفترض أن طول المفتاح يساوي 4. المعلومات التي تحصل عليها من الجزء 'AE' تؤدي إلى أن المفتاح يجب أن يكون '?AR' حيث علامة الاستفهام تعني حرف غير معلوم. الآن استخدم المعلومات التي تتعلق أزواج من كلمات مكررة مكونة من ثلاثة حروف لتخمين كلمة المفتاح.

(١٠,٢,٨) توجد سيناريوات تدعى أن الضغط المتبوع بتعمية يساعد على كسر النظام (على سبيل المثال، إذا استخدم الضغط على رأس مقدمة مخرجات معلوم فمن الممكن كسر النظام باستخدام معرفة النص الواضح ويعتمد ذلك على نظام التعمية المستخدم). والاقتراح العام هو إجراء عملية الضغط أولاً. يمكن أن يكون الضغط أكثر فاعلية على النص الواضح منه على النص المعمى. إذا كانت عملية التعمية أو ارسال المعلومات مكلفة فإن اجراء

الضغط أولاً قد يؤدي إلى تحسين العملية. كما أن عملية الضغط قبل التعمية يمكن أن تخلق صعوبات لمحاولة الكسر المبنية على تذيل المصدر. انظر بويد (Boyd [16]) والمصادر الأخرى المذكورة فيه.

(١٠,٣,١) $m = (m_0, m_1) = (1110, 0000)$

(١٠,٣,٣) $m_1 = m_3 \oplus f_{k_2}(m_2) = 1010 \oplus f_1(1010) = 0000$
$m = (m_0, m_1) = (1110, 0000)$

(١٠,٣,٤) (أ) كشف المعمى في CBC هو $m_i = \mathrm{DES}_k^{-1}(c_i) \oplus c_{i-1}$ فقط m_j و m_{j+1} يعتمدان على c_j.

(١٠,٣,٥) (أ) لاحظ أن $k_2 = \mathrm{DES}_{k_1}(m) \oplus E_k(m)$ لكل $0 \le i < 2^{56}$ ضع $j = \mathrm{DES}_i(m_1) \oplus c_1$. إذا كان $\mathrm{DES}_i(m_2) \oplus j = c_2$ فمن المرجح أن يكون $(i, j) = (k_1, k_2)$. نحتاج على الأكثر إلى 2^{57} عملية DES لإيجاد مرشحاً.

(١٠,٣,٧) ليس معلوماً أن خاصية أخذ المتمم تحسن من استنفاذ المفاتيح لكسر النظام بطريقة معرفة النص الواضح فقط. أما في حالة استخدام طريقة اختيار النص الواضح، احصل على زوجين (m, c_1) و $(\overline{m}, c_2)$ واستخدم خاصية أخذ المتمم لحذف مفتاحين مرشحين مع كل عملية DES.

الفصل الحادي عشر: مواضيع في الجبر ونظرية الأعداد

(١١,١,١٤) باستخدام الخوارزمية **(١١,١,٧)** حيث $n = 576$ نجد أن:

i	0	1	2	...	8
k_i	0	0	1	...	1
A	47	$47^2 \bmod n = 481$	$481^2 \bmod n = 385$	...	$193^2 \bmod n = 385$
b	1	1	$1 \cdot 385 \bmod n = 385$	...	$385 \cdot 385 \bmod n = 193$

ومن ثم يكون $47^{332} \equiv 193 (\mathrm{mod}\, 576)$.

(١١,١,١٦) يمكن إيجاد مجموعة المولدات $\{2,6,7,8\}$ بحسابات مباشرة، على سبيل المثال:

$$2^2 \equiv 4 \text{ ، } 2^4 \equiv 4 \cdot 4 \equiv 5 \text{ ، } 2^5 \not\equiv 1 .$$

ومن ثم فإن رتبة 2 تساوي 10 ؛ لأن رتبة العنصر يجب أن تقسم $\varphi(11) = 10$. إذا كان α مولّداً للزمرة $\mathbb{Z}_n^*$ فمن الممكن أثبات أن α^i مولّداً إذا وفقط إذا كان $(i, \varphi(n)) = 1$. من ذلك نرى أنه إذا كانت $\mathbb{Z}_n^*$ دورية فإن عدد المولدات يساوي $\varphi(\varphi(n))$. في هذا التمرين عدد المولّدات هو $\varphi(\varphi(11)) = \varphi(10) = 4$ وهي 2^i حيث $i \in \{1,3,7,9\}$.

(١١,١,٢١) (أ) استخدم خوارزمية القسمة لكتابة:

$$x = q \cdot ord(a) + r \text{ حيث } 0 \le r < ord(a) .$$

لنفرض أن $a^x \equiv 1 (\mathrm{mod}\, n)$. عندئذ،

$$1 \equiv a^{q \cdot ord(a) + r} \equiv a^r (\mathrm{mod}\, n)$$

وبما أن $r < ord(a)$ فنرى استناداً إلى تعريف الرتبة أن $r = 0$. وبهذا يكون $ord(a) \mid x$.

(١١,١,٢٢) استخدم وجود مولّداً للزمرة $\mathbb{Z}_p^*$ و التمرين **(١١,١,٢٠)**.

(١١,٢,٧) احسب قيمة $x^2 (\mathrm{mod}\, 30)$ لكل $x \in \mathbb{Z}_{30}^* = \{1,7,11,13,17,19,23,29\}$ لتحصل على $Q_{30} = \{1,19\}$. يكفي أن تجري الحسابات حيث $x < \frac{30}{2}$ ؛ لأن $n - x \equiv -x (\mathrm{mod}\, n)$.

(١١,٢,٨) $\left(\frac{156}{235}\right) = -1$ و

$$\left(\frac{1833}{587}\right) = \left(\frac{72}{587}\right) = \left(\frac{2^3 \cdot 3^2}{587}\right) = \left(\frac{2}{587}\right)^3 \left(\frac{3}{587}\right)^2 = -1 .$$

(**١١,٢,١٣**) استخدم معيار أويلر.

(**١١,٣,٥**) إذا لم يكن a شاهداً لأويلر فإن:

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\, n) \text{ وأن } (a,n) = 1 .$$

احسب مربع كل من مقادير التطابق.

من الممكن تصميم لاختبار أن العدد مؤلف باستخدام شاهد فيرما ولكن توجد أعداد مؤلفة n (تسمى أعداد كارمايكل) بحيث لا يكون لها أي شاهد فيرما في المجموعة $\mathbb{Z}_n^*$.

(**١١,٤,٥**) $m = \lfloor \sqrt{n} \rfloor = 32$ و $q(z) = (z+32)^2 - 1081$.

أساس التحليل هو $B = \{-1,2,3,5,11\}$ لأن $\left(\frac{n}{7}\right) = -1$. الجدول التالي يقدم بعض قيم z بحيث يتحلل $q(z)$ على B.

z	$a = z + m$	$b = q(z)$	التحليل
-1	31	-120	$-2^3 \cdot 3 \cdot 5$
1	33	8	2^3
2	34	75	$3 \cdot 5^2$
-3	29	-240	$-2^4 \cdot 3 \cdot 5$

العلاقات للقيم تؤدي إلى $x^2 \equiv y^2 (\mathrm{mod}\, n)$ حيث $x = 31 \cdot 33 \cdot 29$ و $y = 2^5 \cdot 3 \cdot 5$. ولسوء الحظ $x \equiv 480 \equiv y (\mathrm{mod}\, n)$. ولا توجد تركيبات أخرى تؤدي إلى مربع كامل، ولهذا نحتاج لتوليد قيم أخرى.

(**١١,٤,٦**) ظهرت هذه المسألة في [63]. وجدت قيم x و y التي تحقق تقابل $z \in \{0,1,-2\}$ و $z \in \{-1,4,-6\}$. القيم الأولى منها تؤدي إلى أن $x \equiv -y$.

(**١١,٤,٨**) لاحظ أن $179 \equiv 3 (\mathrm{mod}\, 11)$ وأن $179 \equiv 9 (\mathrm{mod}\, 17)$. وبما أن $11 \equiv 3 (\mathrm{mod}\, 4)$ فالتطابق $x^2 \equiv 3 (\mathrm{mod}\, 11)$ له الحلان $x = \pm 3^{(11+1)/4}$.

وعلى الرغم من عدم تقديمنا خوارزمية لحل التطابق $x^2 \equiv 9 (\mathrm{mod}\, 17)$ إلا أنه يمكن وبسهولة إيجاد الحلين بالتجريب وهما $x \equiv \pm 3 (\mathrm{mod}\, 17)$. باستخدام خوارزمية جاوس نجد أن 71 هو أحد الجذور التربيعية للعدد 179.

(١١,٤,١٠) يمكن حساب قيمة $p+q$ بمعرفة n و φ. الآن، ادرس المعادلة $(x-p)(x-q) = 0$.

(١١,٥,٣) الجدول التالي يبين قيم الأزواج (j, α^j) :

j	0	1	2	3	4	5	6	7	8	9
$\alpha^j \bmod p$	1	5	25	28	43	21	8	40	6	30

وبحساب $\beta\alpha^{-im} \bmod p$ حتى الحصول على تقابل نجد أن :

$$\begin{aligned}
i = o: &\quad \beta(\alpha - m)^0 \equiv \beta \equiv 4 \\
i = 1: &\quad \beta(\alpha - m)^1 \equiv 4 \cdot 11 \equiv 44 \\
i = 2: &\quad \beta(\alpha - m)^2 \equiv 44 \cdot 11 \equiv 96 \\
i = 3: &\quad \beta(\alpha - m)^3 \equiv 96 \cdot 11 \equiv 86 \\
i = 4: &\quad \beta(\alpha - m)^4 \equiv 86 \cdot 11 \equiv 73 \\
i = 5: &\quad \beta(\alpha - m)^5 \equiv 73 \cdot 11 \equiv 27 \\
i = 6: &\quad \beta(\alpha - m)^6 \equiv 27 \cdot 11 \equiv 6
\end{aligned}$$

إذن $\beta\alpha^{-im} \equiv \alpha^j$ حيث $i = 6$ و $j = 8$ ولهذا يكون $\log_5 4 = 68 \in \mathbb{Z}_{97}$.

(١١,٥,٦) (أ) بوضع $\lambda = 2^i\lambda'$ حيث λ' فردي نستطيع افتراض أن $2^i \mid \varphi(p)$ دون المساس بالعمومية. اعتبر الآن عنصراً $a \in \mathbb{Z}_n^*$ من الرتبة $\varphi(p)$ كعنصر ينتمي إلى $\mathbb{Z}_p^*$ ومن الرتبة $\dfrac{\varphi(q)}{2}$ كعنصر ينتمي إلى $\mathbb{Z}_q^*$.

(ب) أثبت أن $\lambda = ord(a)\lambda'$ وأن $x = 2^i ord(a)x'$ لأعداد $i \geq 0$ ، λ' ، x' حيث λ' فردي. عندئذ يكون :

$$a^{\lambda/2} \equiv a^{ord(a)\lambda'/2} \equiv a^{ord(a)/2} \equiv a^{x/2^{i+1}} (\mathrm{mod}\, n).$$

الفصل الثاني عشر: أنظمة التعمية ذوات المفتاح المعلن

(١٢,١,٧) يمكن أن يقوم العدو بحساب $h(kxy) = f(M, y)$ لكل قالب y.

(١٢,١,٨) لاحظ أن $2pq \mid (x_i - x_j)$. إذا كان على سبيل المثال، $d = (x_1 - x_2, x_1 - x_3) < n$ فنكون قد وجدنا $2pq$ أو $4pq$. وبما أن $n = (2p + 1)(2q + 1)$ فمن الممكن أن نجد الآن بطريقة فعالة على p و q بمعرفة n و d.

(١٢,٢,٢) (أ) استخدم خوارزمية إقليدس لإيجاد $d = 233$.

(ب) استخدم الخوارزمية **(١١,١,٧)** لإثبات أن:

$$c \equiv m^e (\mathrm{mod}\, pq) \equiv 921 (\mathrm{mod}\, pq).$$

(١٢,٢,٣) من الممكن الإجابة على هذا التمرين مباشرة باستخدام الصيغة التي تحسب عدد الرسائل ذاتية التعمية. بصورة عامة لأي عدد قياس $n = pq$ لنظام ESA من السهل الاثبات على وجود قوة e بحيث تحقق $1 < e < \varphi(n)$، $(e, \varphi(n)) = 1$، $m^e \equiv m (\mathrm{mod}\, n)$ لكل m.

ضع $e = 1 + j\varphi(n) \,/\, (p - 1, q - 1)$ حيث $1 \le j < (p - 1, q - 1)$.

التمرين هو الحالة $j = (p - 1, q - 1) \,/\, 2$.

(١٢,٢,٤) لنظام التطابقات $x \equiv c_i (\mathrm{mod}\, n_i)$ الحل $x < n_1 n_2 n_3$. بما أن $m < n_i$ فنجد أن $x = m^3$. من الممكن إيجاد الجذر التكعيبي للعدد x بطريقة فعالة لنحصل على m (في الحالة النادرة التي تكون فيها القياسات ليست أولية نسبياً مثنى مثنى نقوم بتحليل القياسات أولاً).

(١٢,٢,٦) (أ) إذا كان $k < 1$ فإن $ed - k\varphi(n) \ge ed - 1$ ومن ثم نحصل على تناقض. بما أن $d < \varphi(n)$ فنجد أن $ed - k\varphi(n) < (e - k)\varphi(n)$ وأن $k < e$.

(ب) $ed - k\varphi(n) = ed - k(n - p - q + 1)$.

وبهذا يكون:

$$\frac{kn+1}{e} - d = \frac{k}{e}(p+q-1) < p+q.$$

(١٢,٢,٧) (أ) $n - \varphi(n) = n - (n-p-q+1) < p+q < 3\sqrt{n}$.

(ب)
$$\left|\frac{e}{n} - \frac{k}{d}\right| = \left|\frac{ed-kn}{dn}\right| < \frac{k(n-\varphi(n))}{dn} < \frac{3k}{d\sqrt{n}} < \frac{1}{3d^2}$$

(ج) احسب أقرب تقريب للعدد $\frac{k'}{d'}$ إلى $\frac{e}{n}$. من التحقق من العدد d' بإيجاد φ' من $ed' - k'\varphi' = 1$ ومن ثم (بحالة $\varphi' \in \mathbb{Z}$) حاول تحليل العدد n باستخدام التمرين **(١١,٤,١٠)**.

(١٢,٢,١٠) إذا كان $ed \equiv 1 (\mathrm{mod}\, \lambda)$ فإن $ed \equiv 1 (\mathrm{mod}\, p-1)$ وأن $m^{ed} \equiv m (\mathrm{mod}\, p)$. وبالمثل، $m^{ed} \equiv m (\mathrm{mod}\, q)$. وبهذا يكون $m^{ed} \equiv m (\mathrm{mod}\, n)$. لاحظ أن $\lambda \mid \varphi(n)$. وبهذا فإن استخدام λ يمكن أن يؤدي إلى عدد d أصغر. وإذا اخترنا p و q عشوائياً فمن المتوقع أن يكون $(p-1, q-1)$ صغيراً.

(١٢,٢,١١) (أ) مماثل تقريباً للتمرين **(١٢,٢,١٠)**.

(ب) $\lambda = 12$ ، $\varphi(n) = 48$ ، $\varphi(p,q) = 84$ ، $\lambda \mid \varphi(p,q)$.

(١٢,٢,١٣) اختار رسالة $m > p$ ثم احسب $c \equiv m^e (\mathrm{mod}\, n)$ ليكون النص المعمى المختار.

(١٢,٤,٢) (أ) $x = 9$ و $(r,s) = (7,13)$.

(١٢,٥,٣) (ب) إذا كان من التوقع هو $e = 1$ فإن الخيارين $X = S$ و $y = 1$ سيحققان شرط التحقيق المقابل على الغم من أن الشهادة من هذه الجلسة ستظهر أنها غير حقيقية. وبدلاً من ذلك خذ الخيار $X = S^x$.

المراجع
Bibliography

[1] Derek Atkins, Michael Graff, Arjen K. Lenstra, and Paul C. Leyland. The magic words are squeamish ossifrage. In Josef Pieprzyk and Reihanah Safavi-Naini, editors, *Advances in Cryptology –ASIACRYPT '94*volume 917 of *Lecture Notes in Computer Science*, pages 263-277. Springer-Verlag, 1995.

[2] Eric Bach. Discrete logarithms and factoring. Technical Report UCB/CSD 84/186, University of California Berkeley, Computer Science Division, June 1984.

[3] Henry Beker and Fred Piper, *Cipher Systems: The Protection of Communication*. J. Wiley & Sons, New York, 1982.

[4] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In Alfredo De Santis, editor, *Advances in Cryptology –EUROCRYPT '94*volume 950 of *Lecture Notes in Computer Science*, pages 92-111. Springer-Verlag, 1995. A revised version is available via http://www.cse.ucsd.edu/users/mihir/.

[5] E.R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill, 1968.

[6] R.E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.

[7] I. F. Blake and R. C. Mullin. *An Introduction to Algebraic and Combinational Coding Theory*. Academic Press, 1976.

[8] Ian F. Blake, G. Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1999.

[9] Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener. Minimal key lengths for symmetric ciphers to provide adequate commercial security: A report by an ad

hoc group of cryptographers and computer scientists. Available through http://www.bsa.org/, January 1996.

[10] Daniel Bleichenbacher. Generating ElGamal signatures without knowing the secret key. In Maurer [59], pages 10-18. A revised version correcting Corollary 2 is available from the Information Security and Cryptology Research Group, ETH-Zurich, ftp://ftp.inf.ethz.ch.

[11] M. Blum. Coin flipping by telephone: a protocol for solving impossible problems. In *Proceedings of the 24th IEEE Computer Conference (CompCon)*, pages 133-137, 1982.

[12] Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203-213, February 1999. Available via http://theory.stanford.edu/~dabo/.

[13] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults. In Fumy [35], pages 37-51. The extended abstract is expanded in "On the importance of eliminating errors in cryptographic computations", available via http://thory.stanford.edu/~dabo/.

[14] Dan Boneh and Glenn Durfee. New results on the cryptanalysis of low exponent RSA. In J. Stern, editor, *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1-11. Springer-Verlag, 1999. Available via http://theory.stanford.edu/~dabo/.

[15] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may be easier the factoring. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT ' 98* volume 1403 of *Lecture Notes in Computer Science*, pages 59-71. Springer-Verlag, 1998. Available via http://theory.stanford.edu/~dabo/.

[16] Colin Boyd. Enhancing security by data compression: theoretical and practical aspects. In D. W. Davies, editor, *Advances in Cryptology – EUROCRYPT '91* pages 267-280. Springer-Verlag, 1991.

[17] Gilles Brassard, editor. *Advances in Cryptology – CRYPTO '89*volume 435 of *Lecture Notes in Computer Science*. Springer-Verlag, 1989.

[18] Gilles Brassard, and Claude Crépeau. Sorting out zero- knowledge. In J. J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology – UROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 181-191. Springer-Verlag, 1990.

[19] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf. An improved protocol for demonstrating possession of discrete logarithms and some generalizations. In David Chaum and Wyn L. Price, editors, *Advances in Cryptology – EUROCRYPT '87* volume 304 of *Lecture Notes in Computer Science*, pages 127-141. Springer-Verlag, 1988.

[20] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf, and René Peralta. Demonstrating possession of a discrete logarithm without revealing it. In

Andrew M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86* volume 263 of *Lecture Notes in Computer Science*, pages 200-212. Springer-Verlag, 1987.

[21] Clifford C. Cocks. A note on 'non-secret encryption'. Technical report, Communication Electronics Security Group (CESG), November 1973. Available via http://www.cesg.gov.uk.

[22] Don Coppersmith. Cheating at mental poker. In Williams [98], pages 104-107.

[23] Don Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 38(3):243-250, May 1994.

[24] Don Coppersmith, Mathew Franklin, Jacques Patarin, and Michael Reiter. Low-exponent RSA with related messages. In Maurer [59], pages 1-9.

[25] Richard A. DeMillo, Georgie I. Davida, David P. Dobkin, Michael A. Harrison, and Richard J. Lipton. *Applied Cryptology, Cryptographic Protocols, and Computer Security Models.* Proceedings of Symposia in Applied Mathematics. American Mathematical Society, Providence, 1983. Lecture notes for the AMS short course. *Cryptology in Revolution: Mathematics and Models*, San Francisco, 1981.

[26] Whitfield Diffie, The first ten year of public key cryptography. In Simmons [81], chapter 3, pages 135-175.

[27] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644-654, 1976.

[28] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard. *Computer*, 10(6): 74-84, June 977.

[29] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions of Information Theory*, 31(4):469-472, July 1985.

[30] J. H. Ellis. The possibility of secure non-secret digital encryption. Technical report, Communications Electronics Security Group (CESG), January 1970. Available via http://www.cesg.gov.uk.

[31] J. H. Ellis. The history of non-secret encryption. Technical report, Communications Electronics Security Group (CESG), December 1997. Available via http://www.cesg.gov.uk.

[32] David C. Feldmeier and Philip R. Karn. Unix password security – ten years later. In Brassard [17], pages 44-63.

[33] Steven Fortune and Michael Merritt. Poker protocols. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO '84* volume 196 of *Lecture Notes in Computer Science*, pages 454-464. Springer-Verlag, 1985.

[34] Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*. Distributed by O'Reilly and Associates, 1998.

[35] Walter Fumy, editor. *Advances in Cryptology – EUROCRYPT '97* volume 1233 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.

[36] R.G. Gallager, *Information Theory and Reliable Communication*. John Wiley and Sons, 1968.

[37] Simon Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly & Associates, 1995.

[38] W. J. Gilbert. *Modern Algebra with Applications*. Wiley, 1976.

[39] Ian Goldberg and David Wagner. Randomness and the Netscape Browser. *Dr. Dobb's Journal*, pages 66-70, January 1996.

[40] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM journal on Computing* 18(1):186-208, February 1989.

[41] Martin Handford. *Where's Waldo?* Little, Brown, Boston, 1987.

[42] G.H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford Clarendon Press, second edition, 1945.

[43] R. Hill. *A First Course in Coding Theory*. Oxford University Press, 1986.

[44] Don Johnson and Alfred Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). CORR 99-134, University of Waterloo, Canada, August 1999. Available from http://cacr.math.uwaterloo.ca.

[45] D. S. Jones. *Elementary Information Theory*. Oxford University Press, 1979.

[46] Antoine Joux and Reynald Lercier. State-of-the-art in implementing algorithms for the (ordinary) discrete logarithm problem. The 3rd workshop on Elliptic Curve Cryptography (ECC '99), University of Waterloo, http://www.cacr.math.uwaterloo.ca, November 1-3 1999.

[47] Marc Joye, Arjen K. Lenstra, and Jean-Jacques Quisquater. Chinese remaindering based cryptosystems in the presence of faults. *Journal of Cryptology*, 12(4):241-245, Autumn 1999.

[48] David Khan. *The Codebreakers: The Story of Secret Writing*. Scribner, New York, revised edition, 1996.

[49] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In Koblitz [51], pages 252-267. Available via http://www.cs.ucdavis.edu/~rogaway/; a summary appears in [73].

[50] Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer, second edition, 1994.

[51] Neal Koblitz, editor. *Advances in Cryptology – CRYPTO '96* volume 1109 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.

[52] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology – CRYPTO '99* volume 1666 of *Lecture Notes in Computer Science*, pages 388-397. Springer-Verlag, 1999.

[53] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DES and other systems. In Koblitz [51], pages 105-113.

[54] B. A. LaMacchia and A. M. Odlyzko. Computation of discrete logarithms in prime fields. *Designs, Codes and Cryptography*. 1(1):47-62. May 1991.

[55] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. The 3rd workshop on Elliptic Curve Cryptography (ECC '99), University of Waterloo, http://www.cacr.math.uwaterloo.ca, November 1-3 1999.

[56] R. Lidl and H. Neiderreiter. *Finite Fields*. Cambridge University Press, 1984.

[57] S. Lin and D. J. Costello, Jr. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.

[58] F. J. MacWilliams and J. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[59] Ueli Maurer, editor. *Advances in Cryptology EUROCRYPT '96* volume 1070 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.

[60] R. J. McEliece. *The Theory of Information and Coding*. Addison-Wesley, 1977.

[61] R. J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.

[62] Alfred J. Menezes. *Elliptic Curve Public Key Cryptosystems*, volume 234 of *Kluwer international series in engineering and computer science*. Kluwer Academic Publishers, 1993.

[63] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996. Errata and a complete on-line copy of the book are available on http://www.cacr.math.uwaterloo.ca/hac/.

[64] J. H. Moore. Protocol failures in cryptosystems. In Simmons [81], chapter 11, pages 541-558.

[65] Moni Naor, Yael Naor, and Omer Reingold. Applied kid cryptography, or how to convince your children that you are not cheating. CRYPTO '98 rump session, August 1998.

[66] W. W. Peterson and E. J. Weldon, Jr. *Error-Correcting Codes*. MIT Press, 1972.

[67] V. Pless. *Introduction to the Theory of Error-Correcting Codes*, Wiley, 1982.

[68] Jean-Jacques Quisquater, Louis Guillou, and Tom Berson. How to explain zero-knowledge protocols to your children. In Brassard [17], pages 628-631.

[69] M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report 212, MIT Laboratory for Computer Scientists, 1979.

[70] Rick Ramsey. *All About Administering NIS+* SunSoft, second edition, 1994.

[71] Ronald L. Rivest. Cryptography. In van Leeuwen [91], pages 719-755.

[72] Ronald L. Rivest, and Adi Shamir. How to expose an eavesdropper. *Communications of the ACM*, 27(4):393-395, April 1984.

[73] Phillip Rogaway. The security of DESX. *CryptoBytes*, 2(2):8-11, Summer 1996. RSA Laboratories newsletter, http://www.rsa.com. The article is a summary of [49].

[74] Kenneth H. Rosen. *Elementary number Theory and its Applications.* Addison-Wesley, third edition, 1993.

[75] Arto Salomaa. *Public-Key Cryptography.* Texts in theoretical computer science. Springer-Verlag, second edition, 1996.

[76] Bruce Schneier. *Applied Cryptography: protocols, algorithms, and source code in C.* John Wiley & Sons, Inc., second edition, 1996.

[77] Jennifer Seberry and Josef Pieprzyk. *Cryptography: an introduction to computer security.* Prentice Hall, 1989.

[78] Adi Shamir. RSA for paranoids. *CryptoBytes*, 1(3):1-4, Autumn 1995. RSA Laboratories newsletter, http://www.rsa.com.

[79] Adi Shamir, Ronald L. Rivest, and Leonard M. Adelman. Mental poker. In David A. Klarner, editor, *The Mathematical Gardner*, pages 37-43. Prindle, Weber, and Schmidt, Boston, 1981.

[80] C. E. Shannon. A mathematical theory of communications. *Bell System Technical Journal*, 27:379-423 and 623-56, 1948.

[81] G. J. Simmons, editor. *Contemporary Cryptology: the science of information integrity.* IEEE Press, 1992.

[82] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. In David Chaum, editor *Advances in Cryptology – CRYPTO '83* pages 51-67, New York, 1984. Plenum Press.

[83] Gustavus J. Simmons. The subliminal channel and digital signatures. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology – EUROCRYPT '84* volume 209 of *Lecture Notes in Computer Science*, pages 364-378.Springer-Verlag, 1985.

[84] Gustavus J. Simmons. Subliminal channels; past and present. *European Transactions on Telecommunications*, 5(4):459-473, July – August 1994.

[85] Gustavus J. Simmons. Subliminal communication is easy using DSA. In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 218-232. Springer-Verlag, 1994.

[86] Douglas R. Stinson. *Cryptography: Theory and Practice* . CRC Press, Boca Raton, Florida, 1995.

[87] Robert Sugarman. On foiling computer crime. *IEEE Spectrum*, 16(7):31-32, July 1979. This is the first of a series of articles: Martin E. Hellman, DES will be total insecure within ten years, 32-39; Security Agency denies tampering with DES, National Security Agency, 39; George I. Davida, Hellman's scheme breaks DES in its basic form, National Science Foundation, 39; Walter Tuchman, Hellman presents no shortcut solution to the DES, 40-41; Dennis Branstad, Hellman's data does not support his conclusion, National Bureau of Standards, 41.

[88] Bradley Taylor and David Goldberg. Secure networking in the Sun environment. Technical Report 905, Sun Microsystems, January 1991.

[89] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. SIAM *Journal on Applied Mathematics*, 24:88-96,1973.

[90] Malcolm Turnbull. *The Spycatcher Trial: the scandal behind the #1 best seller.* Salem house Publishers, 1989. See [101].

[91] J. van Leeuwen, editor. *Handbook of Theoretical Computer Science.* Elsevier Science Publishers, 1990.

[92] J. H. van Lint. *Introduction to Coding Theory.* Springer- Verlag, 1982.

[93] Michael Wiener. Efficient DES key search. In W. Stallings, editor, *Practical Cryptography for Data Internetworks*, pages 31-79. IEEE Computer Society Press, 1996. Reprinted from Crypto 93 rump session.

[94] Michael Wiener. Efficient DES key search – an update. In *Cracking DES* [34], chapter 11, pages 1-4.

[95] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553-558, May 1990.

[96] H. C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, 26(6):726-729, November 1980.

[97] H. C. Williams. An M^3 public-key encryption scheme. In Williams [98], pages 358-368.

[98] Hugh C. Williams, editor, *Advances in Cryptology – CRYPTO '85* volume 218 of *Lecture Notes in Computer Science.* Springer-Verlag, 1985.

[99] Malcolm J. Williamson. Non-secret encryption using a finite field. Technical report, Communications Electronics Security Group (CESG), January 1974. Available via http://www.cesg.gov.uk.

[100] Malcolm J. Williamson. Thoughts on cheaper non-secret encryption. Technical report, Communication Electronics Security Society (CESG), August 1976. Available via http://www.cesg.gov.uk.

[101] Peter Wright. *Spycatcher: the candid autobiography of a senior intelligence officer.* Viking, New York, 1987. See also [90].

[102] Adam Young and Moti Yung. The dark side of "black-box" cryptography, or: should we trust Capstone. In Koblitz [51], pages 89-103.

[103] Adam Young and Moti Yung. Kleptography: using cryptography against cryptography. In Fumy [35], pages 62-74.

[104] Philip R. Zimmermann. *The Official PGP User's Guide.* MIT Press, Cambridge, Massachusetts, 1995.

[105] V. Zinoviev and V. Leontiev. The nonexistence of perfect codes over Galois fields. *Problems of Control and Information Theory*, 2(2):16-24, 1973.

ثبت المصطلحات
Glossary

أولاً: عربي – إنجليزي

أ

اختبار الأوليات	Primality testing
اختبار سولوفي وستراسن	Solovay-Strassen test
اختبار كاسيكي	Kasiski test
اختبار ميلر ورابن	Miller-Rabin test
اختيار عشوائي	Random choice
اختيار نص معمى	Chosen-ciphertext
اختيار نص واضح	Chosen-plaintext
استنفاد فضاء المفاتيح	Axhaustive keyspace
أشباه المربعات	Pseudosquares
أشكال العمليات	Modes of operations
الأعداد الصحيحة	The integers
الأعداد الصحيحة قياس n	The integers odulo n

الأمن القابل للبرهان	Provable security
التعمية المتكررة	Multiple encryption
التعمية ذات المفتاح المتماثل	Symmetric-key encryption
الخطوة الصغيرة	Baby-step
الخطوة الكبيرة	Giant-step
الخوارزميات	Algorithms
الرواسب التربيعية	Quadratic residues
الرواسب غير التربيعية	Quadratic nonresidues
العدو (حواء)	Adversary (Eve)
القاسم المشترك الأكبر	Greatest common divisor
اللوغاريتمات المنفصلة	Discrete logarithms
المحافظة على السر	Confidentiality
المرسل (أليس)	Sender (Alice)
المرشح التربيعي	Quadratic sieve
المستقبل (بوب)	Receiver (Bob)
المضاعف المشترك الأصغر	Least common multiple
النشر	Diffusion
النص المعمى	Ciphertext
النص الواضح	Plaintext
آمن برهاناً	Provably secure
آمن تماماً	Unconditionally secure

آمن حسابياً	Computationally secure
انتحال الشخصية	Impersonation
انتروبيا	Entropy
أنظمة السيل	Stream ciphers
أنظمة المرحلة	State ciphers
أنظمة تعمية قالبية	Block ciphers
أوليان نسبياً	Relatively prime

ب

بذرة بدائية	Initial seed
برتوكول الثلاث خطوات لشامير	Shamir's 3-pass protocol
برتوكولات تعموية	Cryptographic protocols
بطاقة ذكية	Smartcard

ت

تحليل الأعداد	Factoring of numbers
تحليل التردد	Frequency analysis
تحليل التعمية	Cryptanalysis
تذيل (تمليح) الرسالة	Salting the message
تركيب خطي	Linear combination
تزوير الرسالة	Forgery
تزوير وجودي	Existential forgery
تشويش	Confusion

تعقد الحسابات	Complexity
تعمية تقليدية	Classical cryptography
تعمية سلسلة قوالب	Cipher-block chaning
تعمية فينونا	VENONA
توقيع الجمل	ELGamal signature
توقيع إلكتروني	Digital signature
توقيع إلكتروني مع ملحق	Digital signature with appendix
توليد مفتاح	Key generating

ج

جذور تربيعية	Square roots

ح

حساب التطابقات	Moduler arithmetic
حساب الدليل	Index calculus
حلقة	Ring
حواشي	Notes

خ

خصوصية جيدة وبارعة	Pretty good privacy (PGP)
خصوصية سيئة جداً	Pretty awful privacy
خطة توقيع نظام RSA	RSA Signature scheme
خطط التعمية	Encryption schemes
خطط المفتاح المتماثل	Symmetric-key schemes

خوارزمية إقليدس	Euclidean algorithm
خوارزمية إقليدس الموسعة	Extended Euclidean algorithm
خوارزمية التربيع والضرب	Square and multiply algorithm
خوارزمية التموية الآمنة	Secure hash
خوارزمية القسمة	Division algorithm
خوارزمية جاوس	Gauss algorithm
خوارزمية حدودية	Polynomial time algorithm
خوارزمية فعالة	Efficient algorithm

د

دالة التعمية	Encryption function
دالة أويلر	Euler function
دالة تمويه	Hash function
دالة تمويه تعموية	Cryptographic hash function
دالة ذات اتجاه واحد	One-way function
دالة ذات باب سري	Trapdoor function
دالة كشف المعمى	Decryption function

ر

رتبة عدد صحيح	Order of integer
رسالة ملخصة	Message digest
رمز O الكبيرة	Big-oh notation
رمز جاكوبي	Jacobi symbol
رمز ليجندر	Legendre symbol

ز

زمرة	Group

س

سلامة البيانات	Date integrity
سلطة الشهادات	Certification authority
سلم فيستل ملتو	Feistel twisted ladder

ش

شاهد أويلر	Euler witness
شاهد فيرما	Fermat witness
شاهد قوي	Strong witness
شفرة اكتشاف معدلة	Modification detection code
شفرة توثيق الرسالة	Message authentication code
شفرة مطابقة هوية الرسالة	Message authentication code
شكل رو	Rho-diagram
شهادة	Certificate

ض

ضغط البيانات	Data compression
ضم (تسلسل)	Concatenation

ط

طريقة الالتقاء بالمنتصف	Meet-in-the-middle attack
طريقة رو لبولارد	Pollard's rho method
طول القالب	Block length

ع

عدد أولي	Prime number
عدد مؤلف	Composite number
عدم الإنكار (التنصل)	Nonrepudiation
عدم المعرفة مطلقاً	Zero-knowledge
عدو غير فعال	Passive adversary
عدو فعال (نشط)	Active adversary
علم التعمية	Cryptology
عملية الفصل المتنافية (XOR)	Exclusive or (XOR)

ف

فصل تطابق	Congruence class
فصل تكافؤ	Equivalence class
فضاء الرسائل	Message space
فضاء المفاتيح	Key space

ق

قابل للعكس	Invertible
قانون المقلوب التربيعي	Low of quadratic reciprocity
قناة اتصال	Communication channel
قناة آمنة	Secure channel
قناة غير آمنة	Nonsecure channel
قناة مخفية	Subliminal channel

قوة شاملة	Universal exponent
قيمة عشوائية	Random value

ك

كتاب التعمية الإلكتروني	Electronic cod book
كلمة سر	Password
كلمة سر (مفتاح)	Secret word (key)

ل

لفافة لمرة واحدة	One-time pad

م

مبرهنة الأعداد الأولية	Prime number theorem
مبرهنة الباقي الصينية	Chinese remainder theorem
مبرهنة أويلر	Euler's theorem
مبرهنة فيرما الصغرى	Fermat's little theorem
مثنى مثنى	In pairs
محاولات بيرنولي	Bernoulli trials
مربعات عشوائية	Random squares
مرشح الحقل العددي	Number field sieve
مسألة الجذور التربيعية	SQROOT
مسألة الجمل	ELGAMAL
مسألة الرواسب التربيعية	QRP
مسألة اللوغاريتم المنفصل	DLP

مسألة تحليل الأعداد الصحيحة	FACTOR
مسألة حساب Φ	COMPUTE Φ
مسألة ديفي وهيلمان	DHP
مسألة رابن	RABIN
مطابقة الهوية الشخصية	Identification
مطابقة هوية الرسالة	Message authentication
معامل الصدفة	Index of coincidence
معرفة النص المعمى فقط	Cipher text-only
معرفة النص الواضح	Known-plaintext
معكوس (نظير) ضربي	Multiplicative inverse
معيار أويلر	Euler's criterion
منع التزوير	Non-repudiation
موثوقية (تطابق الهوية)	Authentication
مولِّد	Generator

ن

نظام RSA	RSA cipher
نظام أحادي	Monoalphabetic cipher
نظام الازاحة	Shift cipher
نظام البيانات الجديد المحكم	New data seal (NDS)
نظام التعمية القياسي المتقدم	Advanced encryption standard (AES)
نظام الجمل	ELGamal
نظام القيصر	Ceasar cipher

نظام تطابقات	Congruence system
نظام تعددي	Polyalphabetic cipher
نظام تعمية البيانات القياسي	Date encryption standard (DES)
نظام تعمية ذو مفتاح معلن	Public-key cryptography
نظام تعمية فيرنام	Vernam cipher
نظام تعمية فيستل	Feistel cipher
نظام تعويض بسيط	Simple substitution cipher
نظام رابن	Rabin cipher
نظام رواسب تام	Complete residue system
نظام فيجينير	Vigenere cipher

هـ

هجائية	Alphabet
هجوم تكيفي	Adaptive attack

و

وكالة الأمن القومي	National security agency (NSA)

ي

يقسم	Divide

ثانياً: إنجليزي – عربي

A

Active adversary	عدو فعال (نشط)
Adaptive attack	هجوم تكيفي
Advanced encryption standard (AES)	نظام التعمية القياسي المتقدم
Adversary (Eve)	العدو (حواء)
Algorithms	الخوارزميات
Alphabet	هجائية
Authentication	موثوقية (تطابق الهوية)
Axhaustive keyspace	استنفاد فضاء المفاتيح

B

Baby-step	الخطوة الصغيرة
Bernoulli trials	محاولات بيرنولي
Big-oh notation	رمز O الكبيرة
Block ciphers	أنظمة تعمية قالبية
Block length	طول القالب

C

Ceasar cipher	نظام القيصر
Certificate	شهادة
Certification authority	سلطة الشهادات
Chinese remainder theorem	مبرهنة الباقي الصينية
Chosen-ciphertext	اختيار نص معمى

Chosen-plaintext	اختيار نص واضح
Cipher text-only	معرفة النص المعمى فقط
Cipher-block chaning	تعمية سلسلة قوالب
Ciphertext	النص المعمى
Classical cryptography	تعمية تقليدية
Communication channel	قناة اتصال
Complete residue system	نظام رواسب تام
Complexity	تعقد الحسابات
Composite number	عدد مؤلف
Computationally secure	آمن حسابياً
COMPUTE Φ	مسألة حساب Φ
Concatenation	ضم (تسلسل)
Confidentiality	المحافظة على السر
Confusion	تشويش
Congruence class	فصل تطابق
Congruence system	نظام تطابقات
Cryptanalysis	تحليل التعمية
Cryptographic hash function	دالة تمويه تعموية
Cryptographic protocols	برتوكولات تعموية
Cryptology	علم التعمية

D

Data compression	ضغط البيانات

Date encryption standard (DES)	نظام تعمية البيانات القياسي
Date integrity	سلامة البيانات
Decryption function	دالة كشف المعمى
DHP	مسألة ديفي وهيلمان
Diffusion	النشر
Digital signature	توقيع إلكتروني
Digital signature with appendix	توقيع إلكتروني مع ملحق
Discrete logarithms	اللوغاريتمات المنفصلة
Divide	يقسم
Division algorithm	خوارزمية القسمة
DLP	مسألة اللوغاريتم المنفصل

E

Efficient algorithm	خوارزمية فعالة
Electronic cod book	كتاب التعمية الإلكتروني
ELGAMAL	مسألة الجمل
ELGamal	نظام الجمل
ELGamal signature	توقيع الجمل
Encryption function	دالة التعمية
Encryption schemes	خطط التعمية
Entropy	انتروبيا
Equivalence class	فصل تكافؤ
Euclidean algorithm	خوارزمية إقليدس

Euler function	دالة أويلر
Euler witness	شاهد أويلر
Euler's criterion	معيار أويلر
Euler's theorem	مبرهنة أويلر
Exclusive or (XOR)	عملية الفصل المتنافية (XOR)
Existential forgery	تزوير وجودي
Extended Euclidean algorithm	خوارزمية إقليدس الموسعة

F

FACTOR	مسألة تحليل الأعداد الصحيحة
Factoring of numbers	تحليل الأعداد
Feistel cipher	نظام تعمية فيستل
Feistel twisted ladder	سلم فيستل ملتو
Fermat witness	شاهد فيرما
Fermat's little theorem	مبرهنة فيرما الصغرى
Forgery	تزوير الرسالة
Frequency analysis	تحليل التردد

G

Gauss algorithm	خوارزمية جاوس
Generator	مولِّد
Giant-step	الخطوة الكبيرة
Greatest common divisor	القاسم المشترك الأكبر
Group	زمرة

H

Hash function	دالة تمويه

I

Identification	مطابقة الهوية الشخصية
Impersonation	انتحال الشخصية
In pairs	مثنى مثنى
Index calculus	حساب الدليل
Index of coincidence	معامل الصدفة
Initial seed	بذرة بدائية
Invertible	قابل للعكس

J

Jacobi symbol	رمز جاكوبي

K

Kasiski test	اختبار كاسيكي
Key generating	توليد مفتاح
Key space	فضاء المفاتيح
Known-plaintext	معرفة النص الواضح

L

Least common multiple	المضاعف المشترك الأصغر
Legendre symbol	رمز ليجندر
Linear combination	تركيب خطي
Low of quadratic reciprocity	قانون المقلوب التربيعي

M

Meet-in-the-middle attack	طريقة الالتقاء بالمنتصف
Message authentication	مطابقة هوية الرسالة
Message authentication code	شفرة توثيق الرسالة
Message authentication code	شفرة مطابقة هوية الرسالة
Message digest	رسالة ملخصة
Message space	فضاء الرسائل
Miller-Rabin test	اختبار ميلر ورابن
Modes of operations	أشكال العمليات
Modification detection code	شفرة اكتشاف معدلة
Moduler arithmetic	حساب التطابقات
Monoalphabetic cipher	نظام أحادي
Multiple encryption	التعمية المتكررة
Multiplicative inverse	معكوس (نظير) ضربي

N

National security agency (NSA)	وكالة الأمن القومي
New data seal (NDS)	نظام البيانات الجديد المحكم
Nonrepudiation	عدم الإنكار (التنصل)
Non-repudiation	منع التزوير
Nonsecure channel	قناة غير آمنة
Notes	حواشي
Number field sieve	مرشح الحقل العددي

O

One-time pad	لفافة لمرة واحدة
One-way function	دالة ذات اتجاه واحد
Order of integer	رتبة عدد صحيح

P

Passive adversary	عدو غير فعال
Password	كلمة سر
Plaintext	النص الواضح
Pollard's rho method	طريقة رو لبولارد
Polyalphabetic cipher	نظام تعددي
Polynomial time algorithm	خوارزمية حدودية
Pretty awful privacy	خصوصية سيئة جداً
Pretty good privacy (PGP)	خصوصية جيدة وبارعة
Primality testing	اختبار الأوليات
Prime number	عدد أولي
Prime number theorem	مبرهنة الأعداد الأولية
Provable security	الأمن القابل للبرهان
Provably secure	آمن برهاناً
Pseudosquares	أشباه المربعات
Public-key cryptography	نظام تعمية ذو مفتاح معلن

Q

QRP	مسألة الرواسب التربيعية

Quadratic nonresidues	الرواسب غير التربيعية
Quadratic residues	الرواسب التربيعية
Quadratic sieve	المرشح التربيعي

R

RABIN	مسألة رابن
Rabin cipher	نظام رابن
Random choice	اختيار عشوائي
Random squares	مربعات عشوائية
Random value	قيمة عشوائية
Receiver (Bob)	المستقبل (بوب)
Relatively prime	أوليان نسبياً
Rho-diagram	شكل رو
Ring	حلقة
RSA cipher	نظام RSA
RSA Signature scheme	خطة توقيع نظام RSA

S

Salting the message	تذيل (تمليح) الرسالة
Secret word (key)	كلمة سر (مفتاح)
Secure channel	قناة آمنة
Secure hash	خوارزمية التموية الآمنة
Sender (Alice)	المرسل (أليس)
Shamir's 3-pass protocol	برتوكول الثلاث خطوات لشامير

Shift cipher	نظام الازاحة
Simple substitution cipher	نظام تعويض بسيط
Smartcard	بطاقة ذكية
Solovay-Strassen test	اختبار سولوفي وستراسن
SQROOT	مسألة الجذور التربيعية
Square and multiply algorithm	خوارزمية التربيع والضرب
Square roots	جذور تربيعية
State ciphers	أنظمة المرحلة
Stream ciphers	أنظمة السيل
Strong witness	شاهد قوي
Subliminal channel	قناة مخفية
Symmetric-key encryption	التعمية ذات المفتاح المتماثل
Symmetric-key schemes	خطط المفتاح المتماثل

T

The integers	الأعداد الصحيحة
The integers odulo n	الأعداد الصحيحة قياس n
Trapdoor function	دالة ذات باب سري

U

Unconditionally secure	آمن تماماً
Universal exponent	قوة شاملة

V

VENONA	تعمية فينونا

نظام تعمية فيرنام	Vernam cipher
نظام فيجينير	Vigenere cipher

Z

عدم المعرفة مطلقاً	Zero-knowledge

كشاف الموضوعات
index

ص

ض

ط

ن

هـ

و