المحاضرة الثامنة

الحساب المعياري

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الحساب المعياري

- أغلب لوغرزمات التشفير التماثلي والغير متماثل تعتمد علي علي الحساب المعياري ضمن مجموعة محددة من العناصر
- أفرض أن لدينا مجموعة من تسعة عناصر من الأعداد يمكن إجراء عدد من العمليات الحسابية بشرط أن تكون النتيجة ضمن هذه المجموعة وتكون أصغر من 9
- {0,1,2,3,4,5,6,7,8}
- 3X2=6
- 4+4=8
- 2+5=7 وهكذا

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الحساب المعياري

- ولكن إذا أخذنا الأعداد

$$8+4=12>9$$

وإذا قسمنا هذه النتيجة علي 9

$$12/9=1$$ والباقي 3

وفي هذه الحالة نأخذ الباقي لأنه ضمن المجموعة أعلاه ويمكن كتابتها كالتالي

$$8+4\equiv \mod 9$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العملية المعيارية

- أفرض أن لدينا

m,z,r,a حيث أن المجموعة z عبارة عن أعداد صحيحة

$$m>0$$

$$a\equiv r \bmod m$$

- m: المعياري أو المعامل
- r:الباقي

$$a,r,m\epsilon Z$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

مثال

- إذا كان لدينا

$$a=42$$

$$m=9$$

$$42=4x9+6$$

$$42\equiv 6 \bmod 9$$

- دائما r يجب أن تحقق

$$0\le r\le m-1$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تعريف الحلقة Ring

- أفرض أن لدينا الحلقة الصحيحة

$$Z_m = \{0,1,2, \ldots \ldots, m-1\}$$

- تجري عمليتي الجمع والضرب لكل

$$a, b \in Z_m$$

- حيث

$$1.\ a + b \equiv c\ mod m \qquad (c \in Z_m)$$

$$2.\ a \times b \equiv d\ mod\ m \qquad (d \in Z_m)$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كردي

تعريف الحلقة Ring

- إذا كان لدينا Z_9 حيث

$$Z_9 = \{1,2,3,4,5,6,7,8\}$$

$$\therefore \quad 6 + 8 = 14 \equiv 5 \; mod \; 9$$

$$6 \times 8 = 48 \equiv 3 \; mod \; 9$$

- أفرض أن لدينا

$$a \in Z_m$$

- معكوس a هو a^{-1} حيث

$$a.\, a^{-1} \equiv 1 \bmod m$$

تعريف الحلقة Ring

- إذا كان للعنصر a معكوس فإنه يمكن كتابة

$$b/a \equiv b.a^{-1} \, mod \, m$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خصائص الحلقة

١. يمكن جمع أو ضرب أي عددين في المجموعة والنتيجة تكون ضمن المجموعة وفي هذه الحالة فإن المجموعة تكون مغلقة

٢. إذا كان لدينا $a, b, c \in Z_m$ فإن

$$a + (b + c) = (a + b) + c$$
$$a.(b.c) = (a.b).c$$

٣. $a \in Z_m$ فإن

$$a + 0 \equiv a \ mod \ m$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خصائص الحلقة

٤. لأي عنصر في الحلقة a يوجد عنصر a– سالب حيث

$$a + (-a) \equiv 0 \; mod \; m$$

٥. بالنسبة لعمليات الضرب فإن العنصر المحايد هو ١ ومن ذلك فإن

$$a \in Z_m \rightarrow a \times 1 \equiv a \; mod \; m$$

٦. إذا كان $a \in Z_m$ فإن معكوس a يعرف كالأتي

$$a.a^{-1} \equiv 1 \; mod \; m$$

مثلا $a = 3 \; , m = 26$ فإن $\mathrm{a}^{-1} = 9$

$$3 \times 9 \equiv mod \; 26$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كردي

شفرة قيصر

- هذه الشفرة تعتمد علي الإزاحة وتمثل الحرف بالأرقام التي تبدأ من الصفر وحتي الرقم 25 وهي تعتبر حالة خاصة من التشفير التعويضي
- هذه الشفرة تعمل علي إزاحة عناصر النص الصريح بعدد ثابت من الخانات وتسمي الشفرة أيضا بشفرة الإزاحة
- الجدول التالي يوضح الحروف وما يقابلها من المواقع

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

شفرة قيصر

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تعريف شفرة الإزاحة

- أفرض أن لدينا

$$x, u, k \in Z_{26}$$

- عملية التشفير $e_k(x)$

$$e_k(x) \equiv x + k \ mod \ 26$$

- فك الشفرة

$$d_k(y) \equiv y - k \ mod 26$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

مثال

- إذا كان المفتاح k يساوى 17
- النص الصريح عبارة عن

$$x_1, x_2, \dots\dots\dots, x_6 = 0,19,19,0,2,10$$

- النص المشفر عبارة عن

$$y_1, y_2, \dots\dots\dots\dots, y_6 = 17,10,10,17,19,1$$

$$rkkrtb$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

شفرة قيصر

- شفرة قيصر ليست أمنة إطلاقا لأن هنالك فقط 26 مفتاح يمكن الحصول منها علي النص المشفر باستخدام هجوم بروت أو تحليل التردد لأحرف الرسالة المشفرة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

شفرة أفين Affine

- هذه الشفرة تعتمد علي ضرب النص الصريح بجزء من المفتاح وإضافة الجزء الثاني
- أفرض أن لدينا

$$x, y, a, b \in Z_{26}$$

- تشفير الرسالة

$$e_k(x) = y \equiv a.x + b \; mod26$$

- حل الشفرة

$$\mathrm{d_k}(y) = x \equiv a^{-1}.(y - b) mod26$$

- بشرط أن

$$k = (a, b)$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

شفرة أفين Affine

- حيث

$$\gcd(a, 26) = 1$$

- عملية فك الشفرة بسيطة حيث أن

$$a.x + b \equiv y \; mod 26$$
$$a.x \equiv (y - b) mod 26$$
$$x \equiv a^{-1}(y - b) mod 26$$

- A يجب أن ينتمي إلي المجموعة

$$a \in [1,3,5,7,9,11,15,19,21,23,25]$$
$$a.a^{-1} \equiv 1 \; mod 26$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

شفرة أفين Affine

- إذا كان $a = 3$ فإن $a^{-1} = 9$ حيث

$$3 \times 9 = 27 \equiv 1 \; mod \; 26$$

- مثال

شفر الرسالة التالية باستخدام شفرة أفين attack المفتاح

يصبح النص المشفر كالأتي

$$k = (a, b) = (9,13)$$

$$y_1, y_2 \ldots\ldots y_6 = 13,2,2,13,5,25 \equiv nccnfz$$

حقل المفتاح بالنسبة لشفرة أفين هو 12X26=312

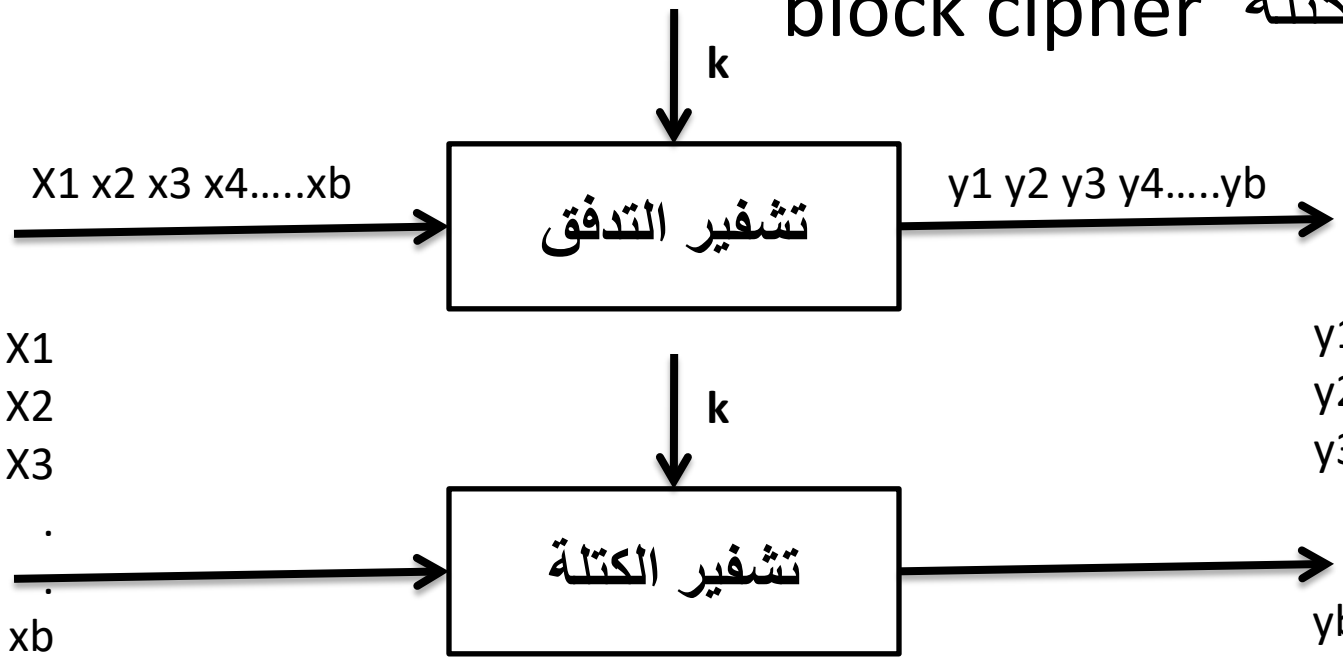
د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تشفير التدفق Stream Ciphers

- يمكن تقسيم التشفير المتماثل إلي

a) تشفير التدفق stream cipher

b) تشفير الكتلة block cipher



د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تشفير التدفق Stream Ciphers

- بالنسبة لتشفير التدفق فإنه يقوم بتشفير كل بت من البيانات علي أي بت تكون منفردة وهذا يتم بإضافة بت من المفتاح الي بت من النص الصريح
- بالنسبة لتشفير الكتلة فإنه يتم بتشفير كتلة من البيانات باستخدام نفس المفتاح
- أغلب مشفرات الكتلة فإن طول الكتلة عبارة عن 128بت
- عمليا فإن مشفرات الكتلة أكثر استخداما بالنسبة للانترنت

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تشفير التدفق Stream Ciphers

- مشفرات التدفق سريعة ولا تحتاج إلي معدات كثيرة فإنها تستخدم للاتصالات المتنقلة cell phone وبعض المعدات المدمجة embedded أيضا هو جزء من منظومة GSM

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تشفير التدفق Stream Ciphers

- التشفير وفك التشفير بالنسبة لتشفير التدفق كالأتي
- إذا كان لدينا

$$x_i, y_i, s_i \in \{0,1\}$$

- فإن التشفير يكون لكل بت من النص الصريح علي حده
- التشفير $y_i = e_{s_i}(x_i) \equiv x_i + s_i \ mod\ 2$
- فك التشفير $x_i = d_{s_i}(y_i) \equiv y_i + s_i \ mod\ 2$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تشفير التدفق Stream Ciphers

- نلاحظ أن عملية التشفير وفك التشفير تستخدم نفس الدالة

$$\begin{aligned} d_{s_i}(y_i) &\equiv y_i + s_i \ mod\ 2 \\ &\equiv (x_i + s_i) + s_i \ mod\ 2 \\ &\equiv x_i + 2s_i mod\ 2 \\ &\equiv x_i + 0 \ mod\ 2 \\ &\equiv x_i mod 2 \end{aligned}$$

- من هنا نلاحظ أن $2s_i mod\ 2$ دائما تساوي صفرا وذلك كالأتي

$$2 \equiv 0\ mod 2$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تشفير التدفق Stream Ciphers

- أيضا إذا كانت s_i تساوي صفرا فإن

$$2s_i = 2.0 \equiv 0 \; mod \; 2$$

- أو s_i تساوي واحد فإن

$$2s_i = 2.1 = 2 \equiv 0 \bmod 2$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري