التشفير الحسابي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير الحسابي

- بتطبيق الرياضيات والحاسوب في تغنيان التشفير فإنه من الممكن التوسع إلي أبعد من تغنيان التشفير القياسية التي تمت مناقشتها سابقا
- ان الحسابات التي يمكن تطبيقها علي التقنيات التي شرحت سابقا تتضمن العمليات الحسابية كالجمع والطرح والضرب والقسمة بالإضافة إلي ذلك فإن العمليات الجبرية وعمليات المصفوفة يمكن أن تضم إلي عمليات التشفير التقليدية

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات الحسابية

- إن رسالة النص الصريح يمكن تشفيرها بسهولة باستخدام العمليات الحسابية بصفتها مفتاحا ولأجل التوضيح نستخدم الرسالة الآتية

CHANGE KEYS TODAY

- فإذا أبدل كل من هذه الحروف بقيمة أسكي المكافئة فإن النص الصريح سيصبح شفرة تعويضية بصورة متوالية من أعداد ذوات رقمين كالأتي :-
-

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات الحسابية

- CHANGE 67 72 65 78 71 69
- KEYS 75 69 89 83
- TODAY 84 79 68 65 89
- فإذا ميزت هذه الأعداد بصفتها قيم أسكي فإن هذا سيقدم لنا الرسالة المشفرة وبتطبيق واحد أو أكثر من العمليات الحسابية عليها نتمكن من تمويه هذه الأعداد وبطرح العدد 50 من كل قيمة من قيم أسكي نحصل علي الأتي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات الحسابية

CHANGE	17	22	15	28	21	29
KEYS	25	19	39	33		
TODAY	34	29	18	15	39	

- وإذا ضربنا بالقيمة 20 فإننا نحصل علي متوالية من القيم

CHANGE	1340	1440	1300	1650	1420	1380
KEYS	1500	1380	1780	1660		
TODAY	1680	1580	1360	1300	1780	

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات الحسابية

- مما ذكر أنفا يمكن تشفير النص الصريح باستخدام واحد من المفاتيح الأربعة المعتمدة علي قيم أسكي هذه المفاتيح هي

١. قيمة أسكي + قيمة ثابتة تعطي حرف مشفر
٢. قيمة أسكي – قيمة ثابتة تعطي حرف مشفر
٣. قيمة أسكي X قيمة ثابتة تعطي حرف مشفر
٤. قيمة أسكي علي قيمة ثابتة تعطي حرف مشفر

- وتتم هذه العمليات بواسطة الحاسوب
- إن النص المشفر بهذه العمليات الحسابية لا تكون ذات أمنية عالية ضد فعالية فك الشفرة بمعرفة المفتاح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات الحسابية

- لذلك فإن أفضل طريقة حسابية ستشمل مفتاحا لا يكون ثابتا بل متغيرو أن هذه الطريقة تكون شاملة لكل العمليات الحسابية الأربع في عملية التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- إن التعبير الجبري الشائع هو معادلة الخط المستقيم

$$y = a + bx$$

- حيث a هو قيمة y عندما x تساوي صفر أو قطع y وb هو الميل و x هي قيمة وال y هو الناتج
- إن أي قيمة تعطي ل x تؤدي إلي y تعطينا نقطة (y,x)علي المخطط البياني
- والأن كيف يمكن لهذا التعبير الجبري أن يستخدم في التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- المطلوب هو تمويه نتيجة النص المشفر بحيث يكون من الصعب للأفراد غير المخولين أن يفكوا هذا النص المشفر
- المطلوب عملية بسيطة بسيطة للتشفير وفك التشفير
- إن التعبير الجبري السابق يمكن أن يساعد للوصول إلي طريقة بسيطة وذلك بإيجاد الثابتين a و b
- إن هذين الثابتين هما المفتاح المطلوب في عمليتي التشفير وفك التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

Linear Equations المعادلات الخطية

- أفرض أن المفتاح هو 2, 0.5 وعندئذ تكون المعادلة كالأتي

$$y = 2 + \frac{1}{2}x$$

- ال x هو مكافئ أسكي العددي إذا أخذنا الرسالة السابقة
- CHANGE KEYS TODAY بعد تحويله إلي قيم اسكي يصبح
- CHANGE 67 72 65 78 71 69
- KEYS 75 69 89 83
- TODAY 84 79 68 65 89

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- إن قيم اسكي سوف تحول إلي مجموعة جديدة من القيم المشفرة بواسطة العملية الآتية

$$\text{قيمة جديدة} = 2 + \frac{1}{2}(\text{قيمة اسكي})$$

- وللمثال فإن الحرف C يساوي 67 في الاسكي لذا فإن العملية تعطي القيم الجديدة الآتية

$$2 + \frac{1}{2}(67) = 2 + 33.5 = 35.5$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- وتصبح الرسالة المشفرة كالأتي

CHANGE 35.5 38 34.5 41 37.5 36.5

KEYS 39.5 36.5 46.5 43.5

TODAY 44 41 36 34.5 46.5

- إن النص المشفر الناتج يملك كلا من الأعداد الكاملة والقيم الكسرية
- إن القيم مثل 35.5 تدل علي أن بعض عمليات التشفير الجبري قد أستخدمت

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- لذلك لا بدا من مفتاح ينتج عنه أعداد صحيحة فقط
- إن كلا من a و b أو كليهما يمكن أن يكونا أعداد صحيحة سالبه أو موجبة فإذا أستخدم المفتاح 15- و2 مع النص الصريح فإن الناتج سيكون كالأتي

CHANGE 119 129 115 141 127 123

KEYS 135 123 163 151

TODAY 153 143 121 115 163

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- لفك الشفرة لا بدأ من عكس العملية
- بما أن الإعادة للنص المشفر يمكن أن توفر لمحلل الشفرة الدليل لكسر الشفرة لذلك لا بدأ من تمويه النتائج بحيث يمنع التكرار
- إن إحدي الطرائق الممكنة لإنجاز هذا التمويه هو بإضافة قيمة مختلفة لكل قيمة من قيم النص المشفر ولكن بطريقة تجعل فك شفرة النص المشفر النهائي أمرا سهلا

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- لذلك تكتب المعادلة الخطية كالأتي

$$y = a + bx(i) + i \qquad \text{حيث } i \text{ من } 0 \text{ ويزداد } 1+$$

- بعد ذلك يصبح النص المشفر كالأتي

CHANGE	119	131	118	145	132	129
KEYS	142	131	172	161		
TODAY	164	155	134	129	178	

نلاحظ أن حرف ال E أخذ قيما تعويضية مختلفة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات الخطية Linear Equations

- إن الطريقة البديلة هي طرح قيمة متغيرة إلي دالة التشفير كالأتي

$$y = a + bx(i) - i$$

- والنتيجة لذلك هو النص المشفر الاتي

CHANGE 118 127 112 137 122 117

KEYS 128 115 154 141

TODAY 142 131 108 101 148

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات اللاخطية Non linear equation

- الدالة الأخرى التي يمكن استخدامها هي المعادلة اللاخطية
- هذه الدالة تمتلك حدودا مرفوعة إلي بعض القوي بقيم تختلف عن الواحد وللمثال علي ذلك

$$y = a + bx^2$$

- هي دالة لاخطية بحيث يكون x مرفوعا إلي اثنين
- شفر كلمة CHANGE مستخدما المفتاح a=-15 , b=2

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

Non linear equation المعادلات اللاخطية

- المثال

نص صريح	C	H	A	N	G	E
قيمة اسكي	67	72	65	78	71	69
x^2	4489	5184	4225	6084	5041	4761
bx^2	8978	10368	8450	12168	10082	9522
$a - bx^2$	8963	10353	8435	12153	10067	9507

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات اللاخطية Non linear equation

- إن فك النص المشفر بالاعتماد علي الدالة اللاخطية استخدام المعادلة اللاخطية لفك الشفرة
- في هذه الحالة عندما تكون دالة التشفير هي

$$y = a + bx^2$$

- لذا يجب أن نحل هذه المعادلة لإيجاد قيم x

$$y - a = bx^2 \quad \rightarrow x^2 = \frac{y-a}{b} \rightarrow x = \sqrt{\frac{y-a}{b}}$$

- أو

$$x = \left(\frac{y-a}{b}\right)^{\frac{1}{2}}$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كردي

المعادلات اللاخطية Non linear equation

- عند استخدام الدوال اللاخطية يكون من الأفضل عمليا الابتداء بتعبير تشفيري يملك حدود مرفوعة إلي قيم صحيحة مثل x^3 x^2 وهكذا
- إن فك التشفير يتطلب الحصول علي جزر هذه التعابير
- أما إذا كانت دالة التشفير المستخدمة في الصورة التالية

$$y = a + b\sqrt{x} \quad \rightarrow \quad y = a + bx^{\frac{1}{2}}$$

- فعندئذ سنتمكن من تحويل النص الصريح إلي نص مشفر بسهولة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كردي

المعادلات اللاخطية Non linear equation

- لكن إرجاع النص المشفر إلي النص الصريح مشكلة خصوصا عند استخدام عمليات الحاسوب ولإيضاح ذلك يمكننا إستخدام

$$y = a + b\sqrt{x} \quad = a + bx^{\frac{1}{2}}$$

- المفتاح هو a=0 , b=1 وكلمة النص هي QUEST عندئذ سنحصل علي مايلي

النص الصريح	Q	U	E	S	T
قيمة اسكي	81	85	69	83	84
$y = \sqrt{x}$	9.00000	9.21954	8.30662	9,11043	9.16515

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات اللاخطية Non linear equation

- إن النص الصريح QUEST قد شفر إلي متوالية بدقة خمس منازل عشرية
- عند فك التشفير نقوم بتربيع قيمة y لإرجاعها إلي قيم اسكي صحيحة وبعد ذلك إلي حروف هجائية
- ينتج عن ذلك بعض الصعوبات كمايلي

نص مشفر		9.00000	9.21954	8.30662	9,11043	9.16515
y^2	81	84.9999	68.9999	82.9999	83.9999	

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المعادلات اللاخطية Non linear equation

- نلاحظ عدا القيمة 81 فإن كل النتائج الأخرى لم تنعكس بصورة تامة الي القيم الصحيحة من الأسكي الأصلية
- إن القيم الناتجة تكون متقاربة ولكنها ليست متساوية إلي القيم الأصلية
- لا يتمكن الحاسوب تلقائيا من تقريب ال 84.9999 إلي 85 أو 68.9999 إلي 69 وهكذا
- للتغلب علي هذه المشكلة في البرمجة تضاف قيمة صغيرة مثل 0.5 مثلا إلي الجانب الأيمن للدالة ثم نأخذ الجزء الصحيح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات المصفوفة Matrix operations

- عندما يكون الحاسوب قادرا علي العمل مع حروف هجائية أو متسلسلة في جدول أو مصفوفة فإن عمليات التشفير وفك الشفرة يمكن أن يتطور باستخدام فكرة جبر المصفوفة
- في المصفوفة يتغير النص الصريح إلي قيم عددية من الاسكي ثم بعد ذلك يمكن إنجاز مختلف التحويلات علي المصفوفة
- إذا أخذنا كلمة DATA وأجرينا عليها كل العمليات لتحويلها إلي نص مشفر

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات المصفوفة Matrix operations

- نص صريح

$$\begin{bmatrix} D & A \\ T & A \end{bmatrix} \rightarrow \begin{bmatrix} 68 & 65 \\ 84 & 65 \end{bmatrix}$$

- إذا كانت مصفوفة قيم اسكي يرمز لها بالرمز V لذا عند ضربها بقيمة ثابتة أو بالمفتاح K فإن الناتج هو مصفوفة نص مشفر جديدة C أي أن
- C=(K)XV
- فإذا كان المفتاح هو K=2 فالناتج هو

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

العمليات المصفوفة Matrix operations

- الناتج هو

$$C = 2 \times \begin{bmatrix} 68 & 65 \\ 84 & 65 \end{bmatrix} \rightarrow \begin{bmatrix} 136 & 130 \\ 168 & 130 \end{bmatrix}$$

- إن النص المشفر النهائي إذا أخذ من ال C بصورة أفقية يصبح متوالية من الأعداد هي

136 130 168 130 تمثل كلمة النص الصريح DATA

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير بالإبدال المصفوفي

- إن عملية عكس المصفوفة هي عملية مناظرة لإيجاد معكوس القيمة
- لذا فإذا كان x=4 فإن المعكوس $\frac{1}{4}$ او $\frac{1}{x} = x^{-1}$
- لإنتاج نص مشفر باستخدام معكوس المصفوفة لقيم اسكي فإن معادلة المعكوس هي

$$C = V^{-1} = \begin{bmatrix} -0.625 & 0.625 \\ 0.808 & -0.654 \end{bmatrix}$$

- إذا أخذت القيم أفقيا تصبح كالأتي
- -0.654 0.808 0.625 -625 كلمة النص الصريح DATA

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري