المحاضرة السادسة

أنظمة التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أنظمة التشفير

- أنظمة التشفير التعويضية تحتاج إلي إحلال حرف محل حرف أخر أو تعويض كل حرف في النص الصريح بأي حرف أخر
- من الطبيعي أن يحتوي النص الصريح علي لأحرف الهجائية
- مواقع هذه الأحرف لا تتغير وإنما الأحرف نفسها هي التي تتغير
- يمكن القيام بالتعويض باستخدام أحرف أخري أو أرقام أو رموز

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

رموز مورس بمثابة شفرة

- نظام مورس هو أحد أنظمة الترميز التي تستخدم رموزا أخري لتحل محل الأحرف الهجائية
- نظام الترميز يظهر في الشكل التالي
- A.- B-… C-.-. D-.. E. F..-. G--. H-…
- I-- J.--- K-.- L.-.. M-. N- O---
- P.--. Q--.- R.-. S… T- U..- V…- W.- X-..- Y-.- Z--..

د عثمان محمد دفع الله
أستاذ مشارك جامعة كردي

رموز مورس

- كل حرف من الحروف الهجائية له بديل مكون من نقاط وشرطات
- من السهل انجاز الترميز بواسطة مورس مثال علي ذلك شفر الرسالة التالية بواسطة شفرة مورس
- CHANGE CIPHER KEY
- -.- -..- .-.- --. -.- -. .-. ---- .-.
- عند استخدام شفرة مورس يجب وضع فراغ بين رموز النص المشفر

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرة الرقمية

- تتضمن طريقة التشفير التعويضي البسيط والمباشر بتعين المواقع العددية للأحرف الهجائية الستة والعشرون
- أي أن حرف Aهو الحرف الأول والحرف B هو الحرف الثاني وهكذا كما موضح أدناه
- A 1 B 2 C 3 D 4 E 5 F 6 G 7 H 8 I 9 J 10 K 11 L 12 M 13 N 14 O 15 P 16 Q 17 R 18 S 19 T 20 U 21 V 22 W 23 X 24 Y 25 Z 26

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرة الرقمية

- لغرض تشفير رسالة واضحة يتطلب أن يحل محل كل حرف الرقم المقابل له مثال علي ذلك شفر الرسالة
- THINK SECURITY
- الشفرة الرقمية هي
- T H I N K S E C U R I T Y
- 20 8 9 14 11 19 5 3 21 18 9 20 25

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أنظمة تشفير الأسكى

- نظام تشفير أخر نأخذه بنظر الاعتبار وهو استخدام رموز اسكي للتشفير والذي تم شرحه من قبل
- هذا النظام يقوم بتحديد قيمة للحرف A مقدارها 65 وللحرف B = 65 وهكذا
- مثل هذه الرموز ذات الأعداد الصحيحة لها فائدة في بناء أنظمة التشفير
- في حالة الشفرة التعويضية كل حرف من الرسالة الواضحة يحل محله قيمة اسكي المكافئة له

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أنظمة تشفير الأسكى

- مثال :-
- شفر الرسالة الآتية باستخدام أسكي
- SECRET COMMUNICATION
- النص المشفر هو
- 83 69 82 69 84 67 79 77 77 85 78 73 67 65 84 73 79 78
- يمكن عمل برنامج لعملية التشفير و فك التشفير باستخدام أسكي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أنظمة تشفير الأسكى

- مثال :-
- فك الرسالة الاتية
- 65 84 65 68 82 69 72 80 73 67 78 69 الرسالة الصريحة هي
- ENCIPHER DATA

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرة العكسية

- من الممكن تشفير رسالة بواسطة عكس الحروف الهجائية للنص الصريح لغرض توليد النص المشفر
- هذا النوع من التعويض هو عكسي بحيث يحل الحرف Z موقع الحرف A والحرف Y موقع الحرف B وهكذا
- هذه الشفرة تكون كالأتي
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ZYXWVUTSRQPONMLKJIHGFEDCBA

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرة العكسية

- مثال:-
- شفر الرسالة الآتية
- SEND GUNS SOON
- النص المشفر هو
- HVMW TFMH HLLM

- لأجل حل النص المشفر نحتاج إلي نفس أسلوب عملية التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرة العكسية

- باستخدام خوارزمية بديلة يتم تحويل قيمة لكل حرف من النص الصريح إلي قيمة أسكي جديدة مكافئة ومن ثم إلي الحرف الهجائي المعكوس وهي
- C(I)=(90 – B(I))+65
- حيث B(I) قيمة أسكي للنص الصريح
- C(I) هي قيمة أسكي الجديدة
- مثلا الحرف K قيمة أسكي له هو 75 إذ أن القيمة المعكوسة له هي
- C(I)= (90 - 75)+65=80
- C(I)=P

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرات القيصرية

- الشفرات القيصرية هي طريقة تشفير تعويضية هجائية تتضمن إزاحة الهجائية الاعتيادية
- سميت كذلك علي اسم يوليس قيصر باعتباره أول شخص استخدمها
- هذه الشفرة تستبدل حرف النص الصريح بحرف أخر يقع موقعه ثلاث أحرف أبعد في الهجائية مثال علي ذلك
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- DEFGHIJKLMNOPQRSTUVWXYZABC

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرات القيصرية

- مثال:-
- شفر الرسالة الآتية باستخدام قيصر
- SECURE ALL MESSAGES
- النص المشفر هو
- VHFXUH DOO PHVVDJHV
- مثال
- فك شفرة الرسالة باستخدام قيصر
- XVH FRGHV DQG FLSKHUV
- الرسالة الأصلية هي USE CODES AND CIPHERS

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الشفرة الهجائية العشرية

- هجائية الشفرة القيصرية تحتوي علي إزاحة ثابتة تعتمد علي مفتاح وتكون الحروف فيها ذات تسلسل متتابع
- لضمان توفير أمنية عالية ينبغي إيجاد هجائية تستخدم مفتاحا يقوم بتوفير الإزاحة ولكن بشرط أن تكون الأحرف فيها ذات تسلسل غير متتابع
- مثل هذه الهجائية يمكن توفيرها بواسطة الهجائية العشرية

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خطوات توليد الهجائية العشرية

١) خذ كل من أحروف الأبجدية الإعيادية واستبدله بقيمة الرقم المقابل له مثلا A=1 B=2 .....Z=26

٢) خذ كل قيمة عددية وأضربها في رقم المفتاح (k) من الممكن أن يكون المفتاح وتري ليس العدد 13أو مضاعفاتها

٣) قسم نتيجة الخطوة الثانية علي الرقم 26.1

٤) خذ الجزء الصحيح من الخطوة الثالثة (2,1,0) ثم أضربه بالرقم (26)

٥) أطرح القيمة المشتقة السابقة من الخطوة الثانية

٦) أشتق هجائية النص المشفر باستخدام مكافئات الأحرف للأرقام التي تم الحصول عليها في الخطوة الخامسة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خطوات توليد الهجائية العشرية

- لأجل توضيح عملية الحصول علي هجائية الشفرة العشرية أفرض ما يلي :-

a = القيمة العددية لأحرف الهجائية الاعتيادية

k = قيمة المفتاح

b = ka/26.1

c= القيمة العددية لأحرف الهجائية العشرية

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نص صريح	a	ka	b=ka/26.1	c=ka-b. (26)	حرف الهجائية العشرية
A	1	3	0.115	3=3-0x26	C
B	2	6	0.23	6=6-0x26	F
C	3	9	0.346	9=9-0x26	I
M	13	39	1.464	13=39-26x1	M
N	14	42	1.669	16=42-1x16	P
X	24	72	2.759	20=72-2x26	J
Y	25	75	2.874	23=75-2x26	W
Z	26	78	2.989	26=78-2x26	Z

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خطوات توليد الهجائية العشرية

- حيث أن

$$c=ka-b.(26)$$

b. هي الجزء الصحيح من القيمة b

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خطوات توليد الهجائية العشرية

- عند إعطاء المفتاح k يجب إيجاد الجدول الخاص بذلك المفتاح ثم بعد ذلك نأخذ كل حرف ونجري الخطوات الستة السابقة وتتم عملية التشفير
- لإيجاد النص الصريح إذا أعطينا الرسالة المشفرة يجب عمل الخطوات الآتية

I. وضع الحروف بالترتيب الهجائي وما يعادلها من أرقام
II. تشفير الحروف الهجائية من A إلي Z باستخدام المفتاح المعطي
III. يجب أخذ كل من الحروف المشفرة وإيجاد ما يقابلها من حروف النص الصريح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري