المحاضرة الخامسة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

قيم أسكي كمفتاح

- مختصر أسكي يرمز إلي نظام الترميز القياسي الأمريكي لتبادل المعلومات
- هذا النظام مبني علي البيانات في الحاسوب تمثل بوجود أو عدم وجود إشارة كهربية داخل دائرة الحاسوب
- هذا المختصر يستخدم النظام الثنائي Binary digit
- النظام الثنائي يستخدم الأرقام صفر وواحد في تركيبات مختلفة لتمثيل الحروف الهجائية والأعداد والرموز

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

قيم أسكي كمفتاح

- بتطور أنظمة الحاسوب وتغير المطلوبات ظهرت مجموعة من الرموز الثنائية العشرية Binary Coded Decimal BCD لغرض تمثيل الحروف مثال علي ذلك الحرف A يكن تمثيله علي شكل 6 بتات BCD أو ثمانية بتات
- 6 Bit BCD 110001
- 7 Bit BCD 1000001
- 8 Bit BCD 11000001

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

قيم أسكي كمفتاح

- تعرف رموز البتات السبعة BCD ASCII-7 أو نظام ترميز الإرسال
- أستحدث هذا النظام في عام 1967 من قبل المعهد الوطني الأمريكي للمقاييس لغرض توفير نظام الترميز القياسي لأجهزة الحاسوب والاتصالات
- إضافة إلي مجموعة رموز البتات السبعة BCD الخاص بالأحرف يوجد هنالك أيضا نظام ترميز أسكي لقيم الأعداد الصحيحة الخاصة بمجموعة حروف لغة البرمجة بيسك بالنسبة للأحرف الهجائية A إلي Z

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

قيم أسكي كمفتاح

- مجموعة الرموز هي القيم من 65 للحرف A إلي 90 للحرف Z
- A 65 B 66 C 67 D 68 E 69 F 70 G 71 H 72
- I 73 J 74 K 75 L 76 M 77 N 78 O 79 P 80
- Q 81 R 82 S 83 T 84 U 85 V 86 W 87 X 88
- Y 89 Z 90

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

قيم أسكي كمفتاح

- في حالة وجود أحروف متكررة في المفتاح فإن مواضع الإبدال العمودي تبقي معتمدة علي المواضع النسبية للأحرف الهجائية لكل حرف في المفتاح
- بالنسبة للأحرف المتكررة تخصص لها مواضع تبدأ من اليسار (أقل) نحو اليمين (عالي)
- أفرض أن المفتاح هو كلمة PEACE والتي تحتوي علي الحرف المكرر E
- باستخدام هذا المفتاح يصبح التسلسل

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

قيم أسكي كمفتاح

- A C E E P حروف المفتاح
- 1 2 3 4 5 تخصصات الأعمدة
- 5 3 1 2 4 تسلسل الإبدال
- P E A C E المفتاح
- عند إختيار كلمة المفتاح فإن من الحكمة عدم استخدام كلمات يمكن تخمينها مثال علي ذلك أسماء المرسل والمستلم أسماء شركات وهكذا ويجب كذلك عدم استخدام العناوين وأرقام الهواتف وأيام الميلاد كمفتاح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

طرق لإبدال الأخرى

- هنالك طرق إبدال أخري تشمل
  - ❖الإبدال العمودي المزدوج
  - ❖الإبدال الحرفي المتعدد
- بالنسبة للإبدال العمودي المزدوج يشفر النص المشفر مرة أخري باستخدام مفتاح أخر
- إذا كان لدينا الرسالة الاتية
- NEGOTIAIONS STALLED SEND INSTRUCTIONS TODAY

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

طرق لإبدال الأخرى

- شفر هذا النص أعلاه باستخدام المفتاح (4213)والمفتاح (5926)

1	2	3	4
N	N	E	T
E	S	N	I
G	S	D	O
O	T	I	N
T	A	N	S
I	L	S	T
A	L	T	O
T	E	R	D
I	D	U	A
O	S	C	Y

4	2	1	3
T	N	N	E
I	S	E	N
O	S	E	N
N	T	O	I
S	A	T	N
T	L	I	S
O	L	A	T
D	E	T	R
A	D	I	U
Y	S	O	C

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

طرق لإبدال الأخرى

- باستخدام المفتاح 5926 يشفر النص المشفر الي
- 5 9 2 6
- N E T N
- S N I E
- S D O G
- T I N O
- A N S T
- L S T I
- L T O A
- E R D T
- D U A I
- S C Y O

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

طرق لإبدال الأخرى

- عند كتابة النص المشفر علي شكل مجاميع رباعية مأخوذة أفقيا نحصل علي الأتي
- NETN SNIE SDOG TINO ANST LSTI LTOA ERDT DUAI SCYO

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبداع الحرفي المتعدد

- باستخدام وحدة مؤلفة من حرفين يمكن تشكيل نمط ذي أربعة أعمدة من النص الصريح السابق كالأتي

1	2	3	4
NE	NS	EN	TI
GO	ST	DI	ON
TI	AL	NS	ST
AT	LE	TR	OD
IO	DS	UC	AY

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبداع الحرفي المتعدد

- باستخدام المفتاح (LIFE) التي تقوم بتحويل الأعمدة إلي التسلسل 4321 نحصل علي الإبدال الأتي
- 4 3 2 1
- TI EN NS NE
- ON DI ST GO
- ST NS AL TI
- OD TR LE AT
- AY UC DS IO

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبداع الحرفي المتعدد

- بعد أخذ المعلومات أفقيا علي شكل مجموعات ذات ثلاث وحدات نحصل علي الأتي
- TIENNS NEONDI STGOST NSALTI ODTRLE ATAYUC DSIOXY
- هذا النص المشفر ونلاحظ أن الحرفين الأخريين XY أضيفا للمجموعة الأخيرة لموازنة المجموعة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

إبدال كلمة الدلالة

- نفرض أن كلمات النص الصريح لها كلمات نظام ترميز الكلمات وعلي النحو التالي

• JMXY	INSTRUCTION
• KEWB	NEGOTIATIONS
• LSRB	SEND
• MLMA	STALLED
• NMBB	TODAY

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

وحدات ذات حرفين

- عند تشكيل وحدات ذات حرفين علي شكل خمسة أعمدة نحصل علي الأتي
- 1 2 3 4 5
- KE L LS JM NM
- WB MA RB XY BB
- باستخدام المفتاح العددي (81978) الذي يعطي مواضع الأعمدة (31524) تكون النتيجة علي الشكل التالي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

وحدات ذات حرفين

- تكون النتيجة علي الشكل التالي
- 3 1 5 2 4
- LS KE NM ML JM
- RB WB BB MA XY
- نلاحظ أن المفتاح الرقمي يحتوي علي مكرر الرقم (8) خصص الرقم (8) الأول لموضع العمود الثالث والثاني لموضع العمود الرابع

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

وحدات ذات حرفين

- أي أن أرقام المفتاح (17889) هي مكافئة لمواضع 12345
- النص المشفر النهائي يكون علي شكل مجموعات رباعية أفقية هو
- LSKE NMML JMRB WBBB MAXY

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أمنية المعلومات ونظام التشفير

- من الممكن القيام بعمليات التشفير وفك الشفرة يدويا بالنسبة للرسائل القصيرة والتي تستخدم شفرات بسيطة
- باستخدام الحاسوب فإنه من السهولة إجراء عدد كبير من العمليات وهذا يؤدي إلي سهولة حل الشفرة
- من الناحية المثالية لا يمكن للأشخاص غير المخولين اعتراض الرسائل المشفرة
- في حالة اعتراض الرسائل المشفرة بواسطة خبير محترف فانه من الممكن فك هذه الشفرات

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أمنية المعلومات ونظام التشفير

- يمكن استخدام الشفرات البسيطة للرسائل ذات الأولوية الأقل درجة
- الشفرات الأكثر تعقيدا فإنها تستخدم في الرسائل ذات الأولوية العالية
- إذا تم تثبيت منظومة تشفير تعتمد علي نوعية معينة من المفاتيح يجب في هذه الحالة القيام بتغير المفتاح بصورة منتظمة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أمنية المعلومات ونظام التشفير

- يجب عدم ترك أرقام المفاتيح أو كلمات المفاتيح مكتوبة علي قصاصات من الورق أو مثبتة علي المحطات الطرفية للحاسوب
- إضافة إلي ذلك في حالة استخدام طريقة إبدال المسلك فان أحسن تطبيق عملي تغير الاتجاه (عمودي أفقي)
- من الأمور المهمة الواجب تذكرها هي أن منظومة التشفير الأمنية هي ليست أفضل من الأشخاص ذوي التفكير الأمني الذين يستخدمونها

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري