المحاضرة الرابعة

تغيرات المسلك

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تغيرات المسلك

- إبدال المسلك يمكن أن تأخذ اتجاهات متعددة ومختلفة ومنها
- أفقي
- – عمودي
- – خط قطري
- – مع عقرب الساعة
- – عكس عقرب الساعة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المسالك الأفقية

- إذا إستحدمت الرسالة SEND HELP SOON بشكل هندسي 3X4 يمكن توضيح عدد من إبدال المسلك كما يلي
- S E N D (1)
- H E L P
- S O O N
- N O O S (2)
- P L E H
- D N ES

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

المسالك العمودية

(1)
- S D L O
- E H P O
- N E S N

(2)
- N S E N
- O P H E
- O L D S

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

مسالك باتجاه عقرب الساعة

(1)
- S E N D
- O O N H
- S P L E

(2)
- E L P S
- H N O O
- D N E S

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

مسالك باتجاه عكس عقرب الساعة

- (1) S O S P
- E O N L
- N D H E

- (2) E H D N
- L N O E
- P S O S

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- التشفير بطريقة الإبدال العمودي تحتاج إلي إزاحة أعمدة الرسالة ذات النص الصريح والتي تكون علي شكل نمط هندسي مستطيل
- إذا كان لدينا الرسالة
- SHIP EQUIPTMENT ON THE FOURTH OF JULY
- أولا يجب إتخاذ القرار بخصوص قياس الصفوف والأعمدة للمستطيل المطلوب إستخدامه

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- الرسالة أعلاه تحتوي علي 30 حرفا ومن الممكن أن تأخذ الأشكال الآتية
- 3X10—10X3—6X5—5X6 -- 15X2 -- 2X15 في حالة أن الرسالة أعلاه مكونة من عدد فردي مثلا 29 حرفا أو عدد لا يمكن الحصول منه علي شكل هندسي من الأحرف يضاف حرف زائد أو ملغي مثلا الحرف Z أو X الي النص الصريح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- في الرسالة السابقة إذا أردنا كتابة النص الصريح في شكل مصفوفة تتكون من ستة صفوف وخمسة أعمدة نحصل علي الأتي

- 1 2 3 4 5
- S U T F O
- H I O O F
- I P N U J
- P M T R U
- E E H T L
- Q N E H Y

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- هذا النص المشفر أعلا يمكن قرأته بسهوله ودرجة تأمينه منخفضة جدا
- لزيادة درجة تامين هذا النص يمكن إزاحة الأعمدة وبذلك يمكن الحصول علي ما يسمي بلإبدال العمودي
- يمكن إزاحة مواقع الأعمدة 5 4 3 2 1 بصورة اعتيادية الي المواقع 1 2 4 5 3 والإبدال الناتج هو

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- 3 5 4 2 1
- T O F U S
- O F O I H
- N J U P I
- T U R M P
- H L T E E
- E Y H N Q

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- يمكن الحصول علي تحسينات إضافية لأمنية النص الصريح عند تدوين الرسالة التي تم إبدالها علي هيئة مجاميع تتكون من خمسة أحروف تؤخذ أفقيا من المستطيل وبذلك نحصل علي النص المشفر النهائي
- SHIP EQUIPMENT ON THE FOURTH JOULY
- TOFUS OFOIH NJUPI TURMP HLTEE EYHNQ

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- أيضا يمكن أخذ الحروف من المستطيل علي هئية أعمدة ذات خمسة أحرف كالأتي
- TONTH EQFJU LYFOU RTHUI PMENS HIPEQ
- النص المشفر عموديا لا يمكن قراءته بسهولة دون معرفة القاري لمعلومات عن طرق التشفير المتبعة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- يجب علي مستلم النص المشفر أن تكون لديه المعلومات التالية
- يجب عليه الإلمام بطريقة أخذ النص المشفر أن تكون لديه المعلومات الآتية

❖ يجب عليه الإلمام بطريقة أخذ النص المشفر من الشكل الهندسي أفقيا ، راسيا أو قطريا أو غير ذلك

❖ يجب عليه معرفة الصفوف والأعمدة للمستطيل

❖ يجب معرفة المفتاح الذي أستخدم لعملية تشفير الرسالة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- حتى الآن اقتصر طول المفتاح لشفرة الإبدال علي خمسة أرقام 1,2,3,4,5 وهذه الأرقام يمكن أن توفر احتمالية 120 مفتاح مختلفة تعتبر طريقة المحاولة والخطأ لإيجاد المفتاح إلي وقت طويل
- ولكن فك الشفرة ليس مستحيلا باستخدام الحاسوب الذي جعل المهمة سهلة جدا

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- من أجل زيادة أمنية المفتاح من محاولة اكتشافه نستطيع زيادة عدد الأرقام إلي القيم 0,1,2,3,4,5,6,7,8,9 و من هذه الأرقام العشرة نستطيع اشتقاق مفاتيح مختلفة ذات خمسة أرقام
- عدد المفاتيح $= \frac{10!}{(10-5)!} = \frac{n!}{(n-r)!}$
- وهي عبارة عن 30240 مفتاح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- باستخدام هذه الأرقام الإضافية يمكن أن يكون للمفتاح معني اخريستطيع كل من المرسل والمستلم الاتفاق عليه مثلا استخدام احدي الأعوام 1965 بصفته مفتاحا أو الشهر والسنة معا مارس 1970 فيصبح المفتاح 31970
- لتوضيح استخدام هذا المفتاح يمكن استخدام نفس الرسالة السابقة
- أولا توضع هذه الرسالة بطريقة الإبدال العمودي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- 1 2 3 4 5
- S U T F O
- H I O O F
- I P N U J
- P M T R U
- E E H T L
- Q N F H Y

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- المفتاح المستخدم هو 31970 والأعمدة هي 12345 ولأجل تشفير النص الصريح بحيث تكون القيمة العليا للمفتاح تمثل العمود الأخير والقيمة الدنيا تمثل العمود الأول وهكذا
- في هذا المثال لدينا الأتي
- 3 1 9 7 0 قيم مفتاح النص
- 1 2 3 4 5 مواقع الأعمدة
- 3 2 5 4 1 مواقع النص المشفر

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- ويكون الإبدال العمودي كالأتي
- 3 1 9 7 0
- 3 2 5 4 1
- T U O F S
- O I F O H
- N T J U I
- T M U R P
- H E L T E
- E N Y HQ

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- ويمكن إرسال الرسالة أفقيا علي شكل خمسة أحرف كالأتي
- TUOFS OIFOH NPJUI TMURP HELTE ENYHQ
- أو عموديا علي شكل خمسة أحرف
- TONTH EUITM ENOFJ ULYFO URTHS HIPEQ
- يمكن استخدام الكلمات كمفتاح وفي هذه الحالة في مواضع النص المشفر تعتمد علي التسلسل الهجائي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- مثال لذلك إذا كان المفتاح هو كلمة FIGHT يكون التسلسل الهجائي هو
- 1 2 3 4 5 المواقع
- F I G H T كلمة المفتاح
- 1 4 2 3 5 مواقع الأعمدة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- الأعمدة حسب المفتاح كما يلي

1 2 3 4 5	1 4 2 3 5
S U T F O	S F U T O
H I O O F	H O I O F
I P N U J	I U P N J
PM T R U	P R M T U
E E H T L	E T E H L
QN E H Y	Q H N E Y

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الإبدال العمودي

- عند أخذ كل صف يصبح النص المشفر كالآتي
- SFUTO HOHOF IUPNJ PRMTU ETEHF QHNEY
- يمكن أيضا اخذ النص المشفر علي هيئة أعمدة ذات خمسة أحروف
- SHIPE QFOUR THUIP MENTO NTHEO FJULY
- أو أخذ العمود من أسفل ألي اعلي
- QEPIH SNEMP IUEHT NOTHT RUOFY LUJFO

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري