المحاضرة الثالثة

التشفير التقليدي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير التقليدي

- هذا التشفير يعرف بالتشفير التماثلي أو التشفير ذو المفتاح الواحد
- فيه تحول الرسالة إلي رسالة عشوائية ليس لها معني واضح
- يحتاج إلي مفتاح ولوغرثم رياضي
- ليس من الضروري جعل اللوغرثم الرياضي سرا ولكن من الضروري جعل المفتاح سرا

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير التقليدي

- اذا كان لدينا مصدرا للمعلومات ينتج رسائل نص صريح يرمز لها بالرمز X حيث

$$X = \{x_1, x_2, \dots\dots\dots\dots x_n\}$$

- أيضا يتم توليد مفتاح K حيث

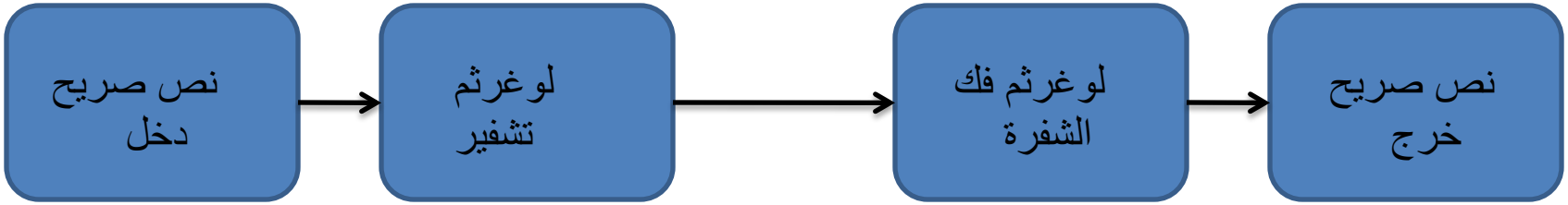
$$K = [k_1, k_2, k_3, \dots\dots\dots\dots k_m]$$

- هذا المفتاح يجب أن يكون مؤمن بين المصدر والطرف النهائي المراد إرسال الرسالة إليه

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير التقليدي

- الشكل التالي يبين نموذج مبسط لنظام تشفير تقليدي



- الدخل بالنسبة لهذه المنظومة هي الرسالة X والمفتاح K وباستخدام لوغرثم التشفير تكون لدينا رسالة مشفرة Y

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

$$Y = [y_1, y_2, y_3, \ldots\ldots\ldots y_N]$$

$$Y = E_K(X)$$

- عند جهة الاستقبال تتم عملية فك الشفرة ويجب أن يتوفر المفتاح المخصص لذلك وبعد ذلك يمكن الحصول علي الرسالة الأصلية

$$X = D_k(Y)$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أنظمة التشفير

- تقوم أنظمة الترميز بتحويل كلمات النص الصريح إلي كلمات نظام الترميز ولكن أنظمة التشفير تركز علي كل حرف من الكلمة
- هنالك نوعان من الشفرات
- شفرات أبدالية
- شفرات تحويلية

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أنظمة التشفير

- الشفرات الابدالية تتضمن عملية التشفير التي تقوم بتغير النمط الاعتيادي للأحرف الموجودة ضمن النص الصريح للرسالة
- إذ تتم عملية مزج أحرف النص الصريح وفق طريقة محددة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

أنظمة التشفير

- هذه الطرق تشمل الأتي
- - عكس الرسالة
- -الأنماط الهندسية
- - إبدال المسلك
- - الإبدال العمودي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

عكس الرسالة

- تحتاج عملية تشفير الرسالة باستخدام عكس الرسالة إلي كتابة النص الصريح بصورة معكوسة لتوليد النص المشفر
- إذا كان النص الصريح للرسالة
- MEET ME MONDAY MORNING
- الرسالة المشفرة بهذه الطريقة تكون كالأتي
- GNINROM YADNOM EM TEEM

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الأنماط الهندسية

- إن الطريقة الاعتيادية لكتابة الرسالة تتبع نمط معين حسب اللغة المستخدمة
- هذه الرسالة تشكل نمط هندسي علي شكل مستطيل
- كل شكل يمكن قراءته وفهمه لأن النمط الهندسي هو شكل قياسي لإغراض إرسال المعلومات المطبوعة
- أي نمط هندسي أخر سيؤدي إلي تمويه الرسالة إلا في حالة أن القاري علي علم بالمفتاح المستخدم في تشفير النص

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الأنماط الهندسية

- الرسالة CONCEL ALL MESSAGES تشكل خطا أفقيا واحدا يمكن إبدالها إلي أشكال مستطيلة علي هيئة عموديتان متساويين في الطول بواسطة كتابة النص الصريح عموديا كالأتي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الأنماط الهندسية

- أو علي هيئة صفين متساويين في الطول أفقيا
- CONCEALAL
- LMESSAGES
- إن عدد الأنماط المستطيلة المختلفة يعتمد علي أحروف الرسالة إضافة إلي حجم الصفحة
- في الرسالة السابقة كان هنالك ١٨ حرفا يمكن تحويلها الي أربعة مستطيلات 2X9 و 9x2 و 6X3 و3X6

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الأنماط الهندسية

- عملية إبدال النص الصريح باستخدام طريقة التشفير المبنية علي الأشكال الهندسية فقط تعطي أمنية ذات درجة محدودة جدا للرسالة
- هذه الأنماط الهندسية تكون ذات فائدة عند استخدامها لمرحلة وسطية لعملية تشفير أخري تسمي إبدال المسلك

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

إبدال المسلك

- إن طرق إبدال المسلك توفر مزجا إضافيا للرسائل ذات الأشكال الهندسية
- إذا كان لدينا الرسالة SEND HELP SOON فيمكن كتابتها علي شكل مستطيل 6X2 بإتباع المسلك من اليسار إلي اليمين مع أخذ حرفين في كل مرة

S	E
N	D
H	E
L	P
S	O
O	N

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

إبدال المسلك

- بما أن المسلك من اليسار إلي اليمين فإن الرسالة سهلة الفهم لذلك فإن هذه الطريقة توفر أمنية قليلة جدا
- يمكن الحصول علي زيادة في المزج في حالة إستخدام الشكل 6X2 بصفته مرحلة وسطية
- النص المشفر التالي يبين إبدال المسلك
- النص الصريح هو SEND HELP SOON
- S N H L S O
- E D E P O N

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

إبدال المسلك

- إن هذه الطريقة تسمي إبدال المسلك المتعرج (Zig Zag) في هذه الحالة يقسم النص إلي أطوال ثابتة
- احد الأطوال يحتوي علي كل الأحرف الوترية والأخر علي زوجية الموقع بالنسبة للرسالة
- هنالك طريقة أخري تسمي إبدال المسلك المتعرج المعكوس
- في هذه الطريقة تبدأ عملية عملي التشفير من اخر حرف من النص الصريح وتستمر رجوعا حتي بادية الرسالة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

إبدال المسلك

- تؤخذ الأحرف وترية الموقع أولا ثم زوجية الموقع ثانيا
- النص الصريح
- SEND HELP SOON
- N O P E D E
- O S L H N S

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري