المحاضرة الثانية

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

علم التشفير

- حدثت طفرة كبيرة جدا في علم التشفير نتيجة للتطبيقات الحديثة والتي تحتاج إلي حماية وتامين عالي
- هذه التطبيقات تمثلت في برمجيات الحاسوب والبريد الإلكتروني والتلفون الخلوي والبنوك وكذلك المجالات الطبية
- في الماضي كان التشفير في رسائل البعثات الدبلوماسية ومكاتبات الدول ذات الخصوصية العالية وكذلك في رسائل الجيوش

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

علم التشفير

- علم التشفير يقسم إلي

١. تشفير الرسائل Cryptography

٢. فك الشفرة Cryptanalysis

- مثلما أن طرق التشفير مهمة فإن طرق فك الشفرة مهمة للغاية والتي من خلالها يمكن التعرف علي مدي قوة الشفرة المستخدمة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

علم التشفير

- يمكن تقسيم التشفير إلي

❖لوغرثم تماثلي Symmetric Algorithm

في هذا النوع فإن عملية التشفير وفك التشفير تستخدم نفس المفتاح ويستخدم بصورة واسعة في عمليات تشفير البيانات وكذلك التحقق من تكاملية البيانات

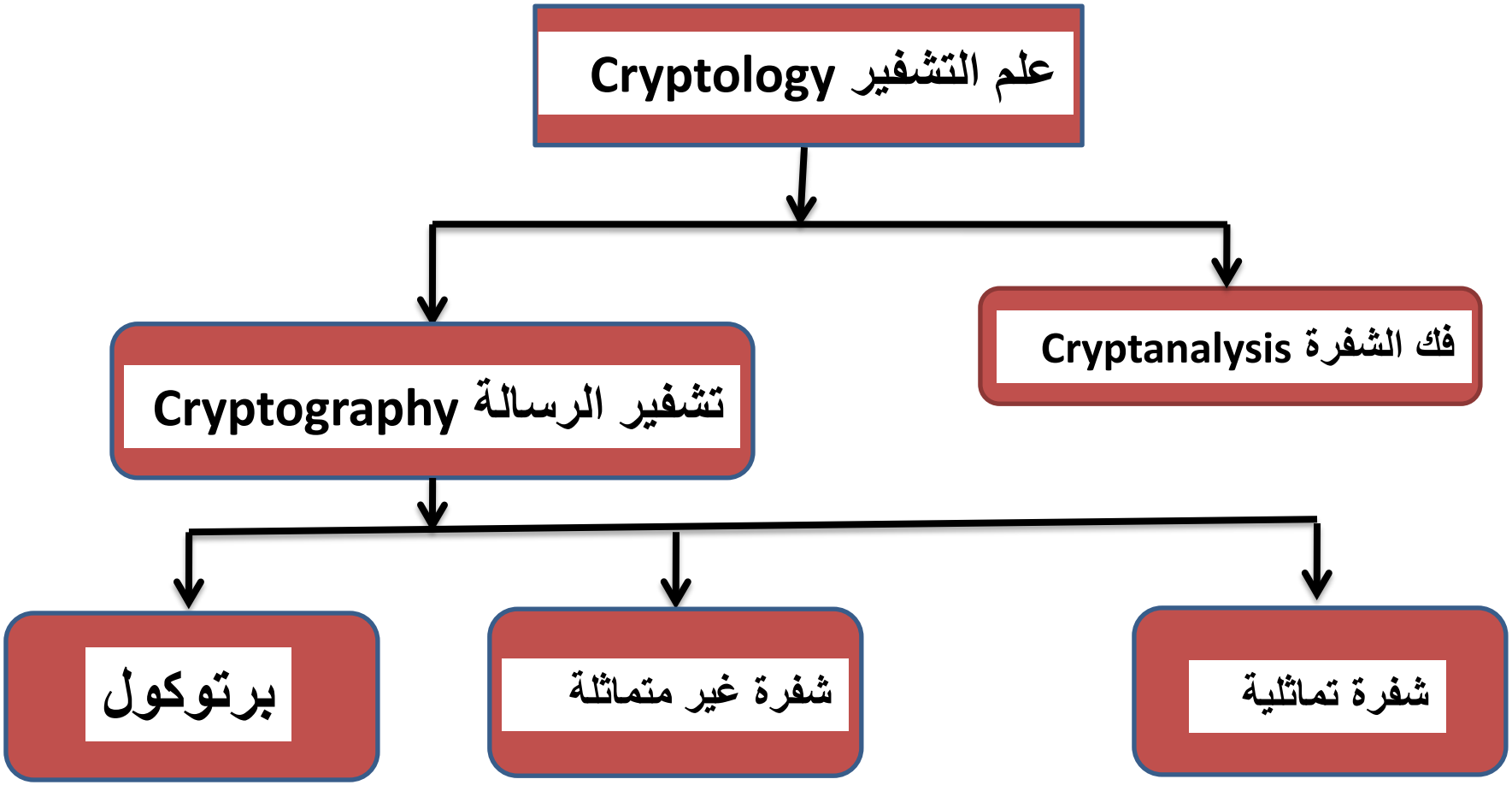
❖لوغرثم غير متكامل Asymmetric ويسمي المفتاح العام وفي هذا النوع فإن المستخدم يمتلك مفتاح خاص به وكذلك مفتاح عام ويستخدم هذا النوع في التوقيع الالكتروني وتشفير البيانات

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

علم التشفير

- برتوكولات التشفير Cryptographic Protocols ونعني بالبروتوكولات المستخدمة في عملية التشفير مثل الانترنت وطبقة النقل المخطط التالي يوضح علم التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري



د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

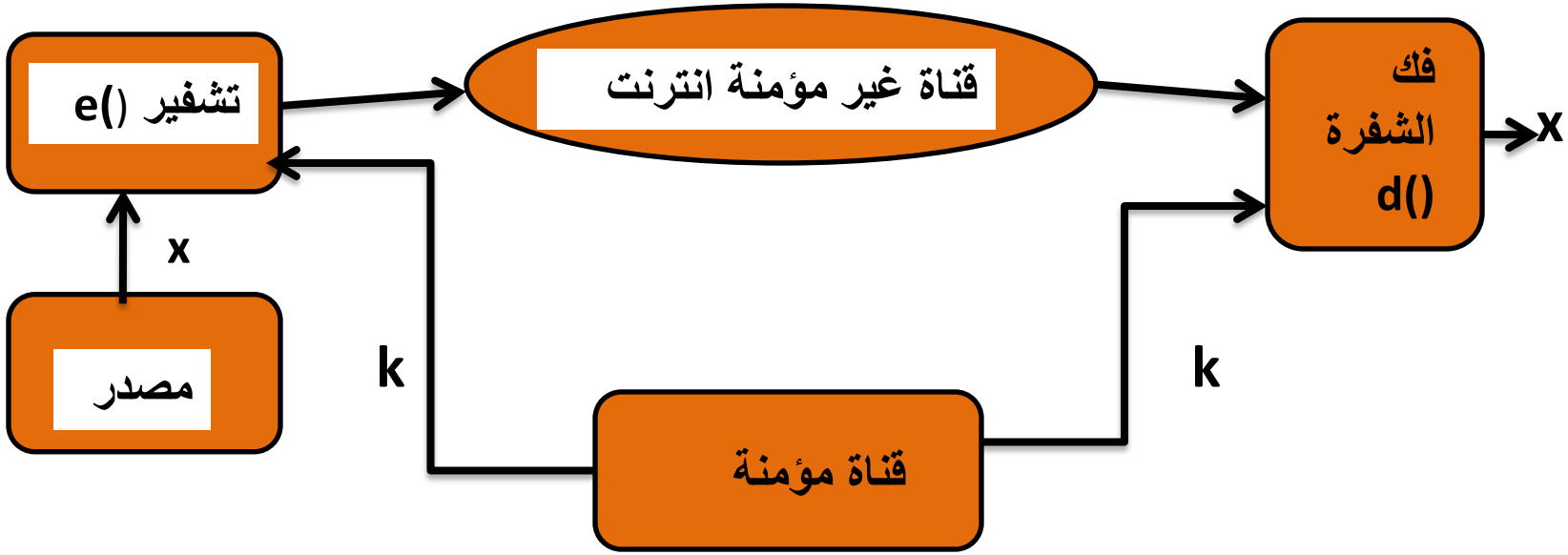
علم التشفير

- أغلب تطبيقات التشفير تستخدم اللوغرثم التماثلي والغير تماثلي وكذلك دالة الهاش معا وتسمي بالهجين Hyprid

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير المتماثل Symmetric

- يسمي أيضا بالمفتاح المتماثل أو المفتاح الواحد الشكل التالي يوضح التشفير المتماثل



د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير المتماثل Symmetric

- من الشكل نلاحظ ان المفتاح k هو المستخدم في عمليتي التشفير وفك التشفير
- هنالك طرق أخري للتشفير المتماثل مثال علي ذلك طرق التعويض التي يبدل الحرف فيها بحرف أخر عشوائيا
- يتم ذلك بعمل جدول عشوائيا ولذلك يصعب علي المهاجم أن يخمن الحرف المعني ويجب أن يؤمن المفتاح بين الجانبين
- هنالك نوع من الهجوم يسمي Brute force attack وفيه يمكن للمهاجم أن يحصل علي عنوان الرسالة أو جزء منها

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التشفير المتماثل Symmetric

- يقوم المهاجم بفك تشفير هذا الجزء من الرسالة بإستخدام كل المفاتيح المتاحة
- إذا طابق هذا الناتج الجزء القصير من الرسالة يكون المهاجم قد تحصل علي المفتاح الصحيح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

هجوم Brute force

- أفرض أن (x,y) تمثل النص الصريح و k يمثل حقل المفاتيح حيث

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

- يقوم هجوم Brute force بفحص كل المفاتيح للحصول علي المفتاح الصحيح

$k_i \in K$ هذا يعني أن $d_{k_i}(y) = x$

إذا تحقق ذلك فإن المفتاح يكون صحيحا وإذا لم يكن يستخدم المفتاح الذي يليه إلي الوصول إلي المفتاح الصحيح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

هجوم Brute force

- عمليا هجوم Brute force أكثر تعقيدا لأن المفاتيح الخطأ قد تعطي نتائج إيجابية غير حقيقية
- نظام هجوم Brute force بالنسبة لأنظمة التشفير المتماثلة من حيث المبدأ ممكنة ولكنها عمليا تعتمد علي حقل المفتاح وكلما كان الحقل كبيرا فإن العمليات الحسابية تكون كبيرة جدا وتأخذ وقتا طويلا
- من هذه الناحية فإن التشفير المتماثل يكون مأمنا ضد هجوم Brute force

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

مثال

- أفرض أنك تريد تحديد حقل المفتاح بالنسبة للتشفير التعويضي
- أفرض أنك اخترت تعويض حرف A عشوائيا من بين ال 26 حرف ال K ثم تبديل حرف B من بقية ال 25 المتبقية
- من ذلك فإن حقل المفتاح بالنسبة للتشفير التعويضي تكون كالأتي

$$K = [k_1, k_2, \dots \dots k_i] = 26.25 \dots \dots .3.2.1 = 26! \approx 2^{88}$$

- من ذلك نلاحظ صعوبة الحصول علي المفاتيح والزمن الذي تأخذه أقوي الحواسيب للحصول علي المفتاح

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تحليل تردد الحروف

- بالنسبة لهجوم Brute force فإنه ينظر إليه كصندوق مغلق ولا يتطرق إلي تحليل التركيبة الداخلية للشفرة
- في هذا النوع من الهجوم فإن لكل حرف من أحرف اللغة الإنجليزية تردد أكثرها هو حرف E ويمثل 13% ثم حرف T وهكذا كما موضح بالجدول أدناه

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

Letter	Frequency	Letter	Frequency
A	0.0817	N	0.0675
B	0.0150	O	0.0751
C	0.0278	P	0.0193
D	0.0425	Q	0.0010
E	0.1270	R	0.0599
F	0.0223	S	0.0633
G	0.0202	T	0.0633
H	0.0609	U	0.0276
I	0.0697	V	0.0098
J	0.0015	W	0.0236
K	0.0077	X	0.0015
L	0.0403	Y	0.0197
M	0.0241	Z	0.0007

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تحليل تردد الحروف

- وطريقة تحليل أو فك الشفرة بهذه الطريقة فإننا نأخذ تردد حروف الرسالة المشفرة ومن ثم نجد حرف النص الصريح كما يوضح المثال التالي
- النص المشفر هو
- lq ifcc vqqr fb rdq cfjwhwz hr bnnb hcc h wwhbsqvqbre hwq vhlq
- النص الصريح هو WE WILL MEET IN THE MIDDLE OF THE LIBRARY AT NOON ALL ARRANGEMENTS ARE MADE

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تحليل تردد الحروف

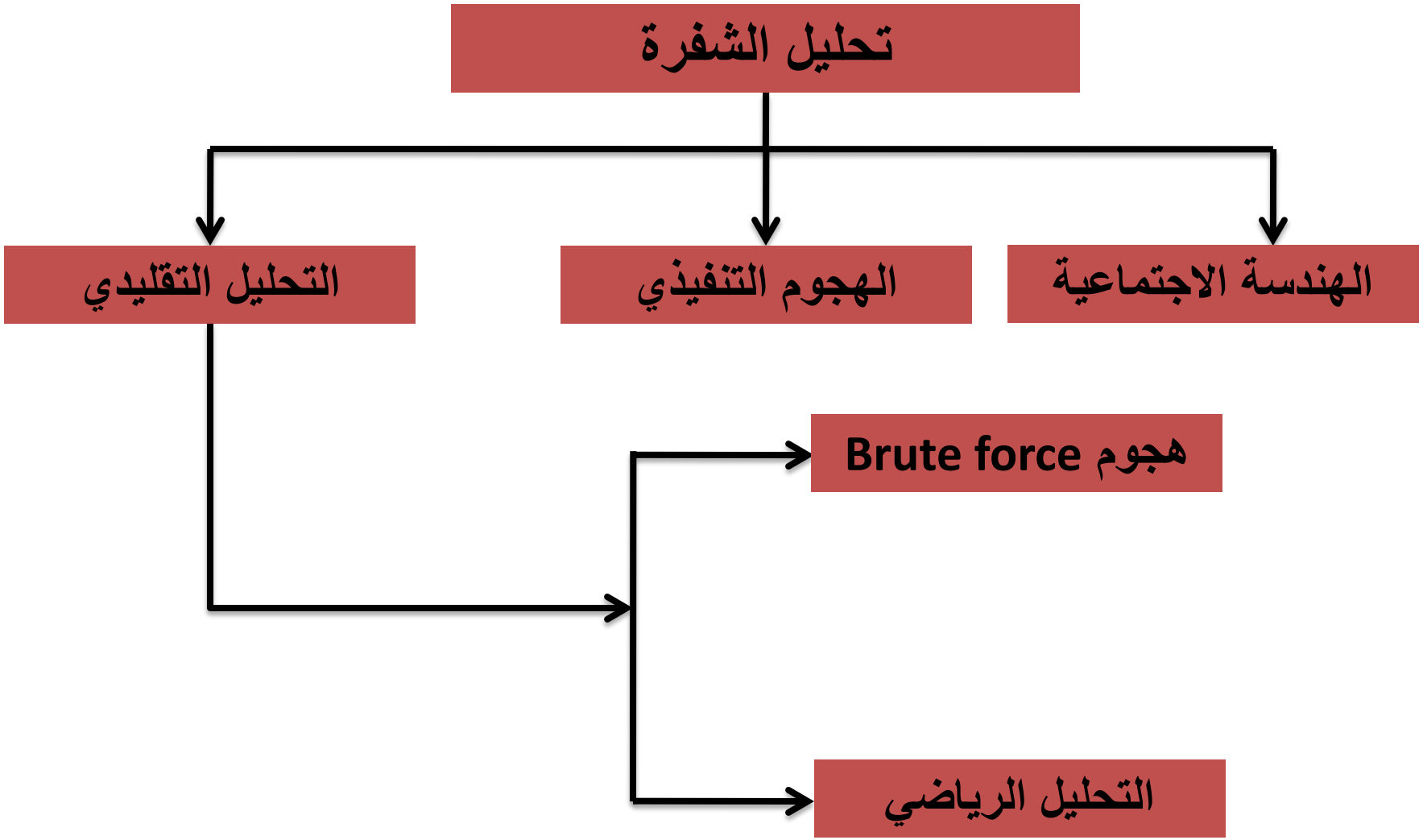
- إخفاء المشفر الجيد إخفاء الخصائص الإحصائية بالنسبة للرسالة المشفرة وتكون الرسالة المشفرة عشوائيا كذلك كبر حقل المفتاح لا يعني بالضرورة قوة دالة التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تحليل الشفرة Cryptanalysis

- هي طرق تستخدم لكسر الشفرة ولذلك لا بدأ من أن يكون التشفير المستخدم ذات درجة عالية من الأمنية بحيث يصعب كسر الشفرة حتي إذا عرف المهاجم اللوغرثم المستخدم
- هنالك طرق متعددة تستخدم لكسر الرسالة المشفرة موضحة بالشكل التالي

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري



الشكل أعلاه يوضح طرق تحليل الشفرة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تحليل الشفرة التقليدي

- تحليل الشفرة التقليدي يقصد علم إرجاع النص الصريح x من النص المشفر y أو كشف المفتاح المستخدم k من النص المشفر k ويقسم إلي

١. التحليل الرياضي
٢. هجوم Brute force

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التحليل الرياضي

- التحليل الرياضي هو تحليل البنية الداخلية لطريقة التشفير المستخدمة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

هجوم Brute force

- وهو يعامل الشفرة كصندوق مغلق ويقوم بإختباركل المفاتيح المستخدمة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الهجوم التنفيذي

- هو تحليل جزء من القناة وبذلك تقاس الطاقة المستهلكة في المعالجات الدقيقة التي تعمل علي المفتاح السري أيضا الإشعاعات الكهرومغناطيسية وكذلك سلوك زمن التشغيل علي اللوغرثم المعني

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

هجوم الهندسة الاجتماعية

- هجوم الهندسة الاجتماعية يعتمد علي إجبار أو إغراء الأشخاص الذين يعلمون بالمفتاح السري بطرق مختلفة حسب طبيعة الشخص المعني
- دائما المهاجم يبحث عن أضعف نقطة أو جانب بالنسبة للوغرثم المستخدم في تشفير الرسالة

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

مبدأ كرنكوف

- مبدأ كرنكوف ينص علي أنه يجب أن يكون نظام التشفير علي درجة عالية وكافية حتى إذا عرف المهاجم كل التفاصيل المتعلقة بنظام التشفير عدا المفتاح السري ويجب أن يكون النظام قويا حتى إذا عرف المهاجم كذلك نظام التشفير وفك التشفير

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري