المحاضرة الثانية عشر

تشفير المفتاح العام Public – Key Algorithm

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

تشفير المفتاح العام Public – Key Algorithm

- يستخدم في خوارزم DES وتقنيات التشفير الأخرى مفتاحاً واحداً في التشفير وفك التشفير لرسالة ما
- يجب علي كل من المرسل والمستلم أن يعرف المفتاح ويبقياه سراً
- يكون الخوارزمي في حالة ال DES معروفاً لدي الجميع لكن المفاتيح تبقي سرية
- قد تظهر احدي مساوي ال DES في تطبيقات البريد الإلكتروني والتحويل المالي إلكترونياً إذ وجب المستخدم توزيع المفتاح السري علي عدة عملاء
- مثل هذا التوزيع يزيد من خطورة كشف الرسالة أو وقوعها بيد أشخاص غير مخولين

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خوارزم المفتاح العام

- يصمم خوارزم المفتاح العام (PKA) المقدم لتقليل هذه المخاطر وذلك باستعمال مفتاحين
- احدي المفتاحين يستخدم لتشفير الرسالة ويعمم أو ينشر والمفتاح الأخر يستعمل لحل الشفرة ويبقي سراً
- إن نجاح هذا الخوارزمي ناتج من أن حقيقة أن معكوس دوال التشفير التي نحتاجها في حل الشفرة لا يمكن اشتقاقها حتي لو عرفت دوال التشفير
- هذا يناقض مع مع الشفرات التي نستطيع فيها إيجاد دالة حل الشفرة لمعرفة دالة التشفير وهذا لا يمكن أن في PKA

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

خوارزم المفتاح العام

- يستعمل ال PKA دوال رياضية خاصة تعرف بدوال باب المصيدة ذي الممر الواحد Trap door one way functions وتكون دوال الممر الواحد هذه سهلة الاشتقاق ولا يمكن اشتقاق معكوس الدالة بمجرد وصف الدالة
- تعمل دالة الممر الواحد علي هيئة مفتاح تشفير ويكون في متناول اليد للاستعمال العام ولا يكون المعكوس أو مفتاح حل الشفرة شائعاً ولا يستطيع من يري دالة التشفير العام أن يستنتج معكوسها

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نظام التشفير العام

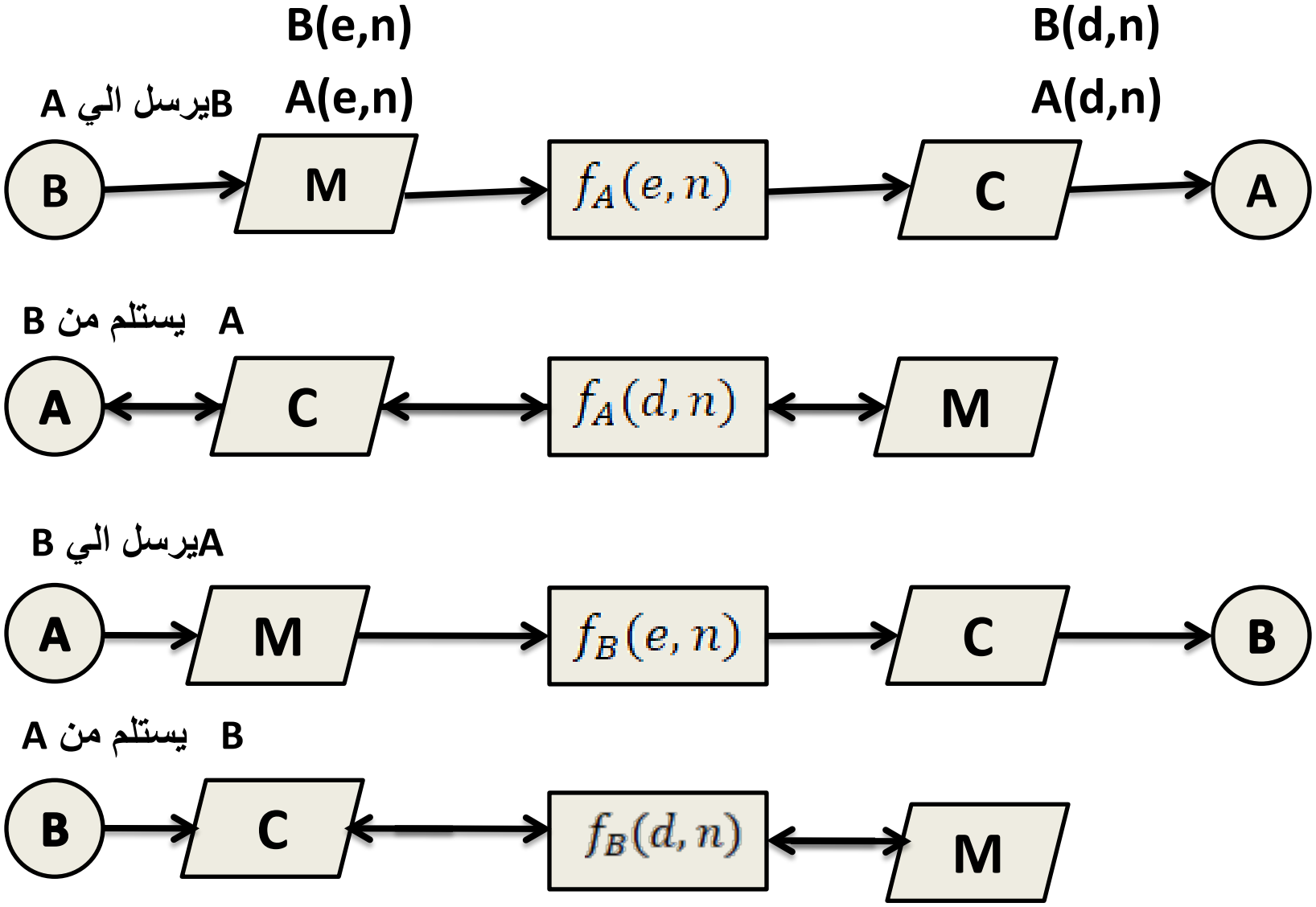
- في نظام تشفير المفتاح العام يعلن الشخص A مفتاح التشفير الخاص به (العددان e,n)
- يستطيع الشخص B إرسال رسالة مشفرة إلي A باستعمال دالة باب المصيدة f وهذا سيكشف عن الرسالة الصريحة الأصلية
- يبين الشكل التالي هذا النظام حيث أن الرسالة الصريحة M النص المشفر C دالة باب المصيدة للتشفير حل الشفرة F
- مفتاح التشفير(عددان صحيحان موجبان)= e,n

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نظام التشفير العام

- مفتاح حل الشفرة(عددان صحيحان موجبان)= d,n
- مرسل/ مستلم = B
- مستلم/ مرسل = A
- هنالك خاصية مفيدة أخري لنظام تشفير المفتاح العام في مجال البريد الإلكتروني أو التحويل المالي هي توقيع الرسالة (message signature)
- مثل هذا التوقيع يكفل للمستلم أن المرسل هو الشخص الذي يفترض أن تكون الرسالة قد أرسلت منه وليس شخص اخر

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري



نظام تشفير النظام العام

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نظام التشفير العام

- نظام التشفير العام سمي ب RSA وهذه الحروف تمثل الحروف الأولي من أسماء المصممين لهذا النظام ريفست وشاميروالدمان
- يستخدم هذا النظام الأعداد الأولية والحساب المعياري لتوليد المفاتيح العامة والخاصة (السرية) للتشفير وحل التشفير كما يستخدم للتوقيع الإلكتروني

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الأعداد الأولية Prime Numbers

- يكون العدد أولياً إذا كان لا يقبل القسمة إلا علي نفسه وعلي واحد فقط
- أي عدد صحيح قابل القسمة علي أي عدد أخر يكون غير أولي مثلاً العدد 10 عدداً غير أولياً لأنه يقبل القسمة علي 2,1,10,5
- أمثلة للأعداد الصحيحة الأولية هي 2,3,5,7,11,13,17,19,23,29,31

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

القاسم الأعظم المشترك Great Common Divisor

- القاسم المشترك الأعظم المشترك (GCD) لزوج من الأعداد الصحيحة أو أكثر يمكن أن تقسم عليه مجموعة معينة من الأعداد فمثلاً 3 هي GCD للعددين 6,15

GCD(6,15)=3

- لإيجاد ال (GCD) نستطيع أولاً أن نجد قائمة بالأعداد المقسوم عليها والأرقام الناتجة ومن ضمنها الرقم نفسه وبعد ذلك نأخذ أكبر عدد مقسوم عليه يظهر في كل من القائمتين
- قواسم العدد 6:1,2,3,6
- قواسم العدد 15:1,3,5,15

GCD(6,15)=3

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

القاسم الأعظم المشترك Great Common Divisor

- يمكن أيضاً إيجاد ال GCD باستعمال خوارزم إقليدس وهذا الخوارزمي يقودنا إلي GCD بدون الحاجة إلي إيجاد قائمة تشمل جميع الأعداد المقسوم عليها
- يمكن تطبيقها كما يلي إذا أعطينا العددين 135,42 نقسم الأكبر علي الأصغر والباقي 9 ونستطيع أن نكتب

GCD(42,135)=GCD(9,42)

- تكرر هذه العملية عدة مرات وتتوقف عند الخطوة قبل أن يكون ناتج القسمة بدون باقي

GCD(42,135)=GCD(9,42)=GCD(6,9) =GCD(3,6) =2

- الخطوة الأخيرة هي GCD(3,6) والتي تعطي 3 علي أنه الجواب

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

الحساب المعياري Modular Arithmatic

- الحساب المعياري هو جزء من دراسة أكبر يعرف بنظرية الأعداد
- حاجتنا تستدعي فهم العلاقة بين ثلاثة أرقام معرفة كما يلي

$$a \equiv b \ modulus \ m$$

- حيث إن a و b هما عددان صحيحان و m عدد صحيح موجب وهذه الجملة تعني أن a هو باقي b/m علي سبيل المثال

14 mod12=2 , 70 mod15=10, 72 mod26=20

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نظام تشفير النظام العام

- هنا نحتاج إلي مفتاحين هما

  مفتاح عام (e,n)

  مفتاح سري (d,n)

- تتبع الخطوات الآتية لبناء هذا النظام

a) في البداية كل مستلم يولد ثلاث أعداد

  رقم كبير أولي p

  رقم كبير أولي q

  رقم كبير n

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نظام تشفير النظام العام

- يتم اختيار هذه الأرقام بصورة عشوائية

b) أحسب n=pxq المفتاح العام عندئذ (e,n)

c) بعد ذلك أحسب قيمة المفتاح السري

$$d = e^{-1} modulo\ \emptyset(n)$$

$$\emptyset(n) = (p-1)(q-1)$$

$$d = \frac{mod\emptyset(n)}{e}$$

d) تأكد من أن e,d صحيحان وذلك بملاحظة أن

$$e \times d\left(mod\emptyset(n)\right) = 1$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نظام تشفير النظام العام

- المفتاح السري عندئذ يكون (d,n)
- توجد طريقة أخري لإيجاد d وهي

$$d = \frac{k\emptyset(n) + 1}{e}$$

- تشفر الرسالة كالأتي

$$C_i = M_i^e \ modulo \ n$$

- تحول الرسالة M إلي مجاميع من الأعداد بواسطة تعويض قيم الحرف الهجائية علي سبيل المثال A=1, B=2, ...,Z=26

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

نظام تشفير النظام العام

- عند جهة المستقبل يقوم المستلم باستخدام مفتاحه السري (d,n) للحصول علي الرسالة الأصلية

$$M_i = C_i^d \ modulo \ n$$

$$M_1 = C_1^d \ modulo \ n$$

$$M_2 = C_2^d \ modulo \ n$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التوقيع الرقمي Digital Signature

- يتم هذا التوقيع بالخطوات التالية

١) يستعمل الشخص المرسل مفتاح حل الشفرة العائد له (d,n) لحساب التوقيع

$$S_i = M_i^d \text{ modulo } n$$

٢) يقوم هذا الشخص بخطوة ثانية اختيارية لضمان خصوصية إضافية وذلك بتشفير التوقيع أيضاً باستعمال المفتاح العائد للمستلم أي أن

$$S = S_i^e \ modulo \ n$$

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري

التوقيع الرقمي Digital Signature

- يستخلص المستلم M_i كما يلي :-

١) باستعمال مفتاح حل الشفرة السري العائد له (d,n)

$$S_i = S^d \ modulo \ n$$

٢) ينظر إلي المفتاح العائد للمرسل (e,n) سوف يجد أن

$$M_i = S_i^e \ modulo \ n$$

- الذي سوف يبين توقيع المرسل ويوثق أصل النص المشفر

د عثمان محمد دفع الله
أستاذ مشارك جامعة كرري