التعمية اللاتناظرية

د. غسان شدود

السلام عليكم ورحمة الله وبركاته

تحدثنا في المحاضرة السابقة عن التعمية وبشكل خاص التعمية التناظرية وكذلك تحدثنا عن نظام التشفير Cipher والفرق بين ال Stream Cipher و Block Cipher وكذلك بعض معايير تشفير البيانات (DES, 3DES) ومعايير التشفير المتقدمة مثل AES.

الأفكار التي سنتناولها في هذه المحاضرة:

- Public – Key Cryptography
- التعمية اللاتناظرية "تعمية المفاتيح"
- One – Way Functions (OWF)
- خوارزمية ال RSA
- خوارزمية ال EL Gamal
- أطوال المفاتيح

- تحدثنا في المحاضرة السابقة عن التعمية التناظرية ولكن هل تحقق الخدمات الأمنية سنجاوب على سؤالنا السابق كما يلي:
  - **السرية:**

    هل يتم تحقيق السرية من خلال التعمية التناظرية؟

    نعم، وذلك لأنه لا يمكن فك التشفير إلا بوجود المفتاح السري، (السرية لا تعتمد على الرسالة بل على سرية المفتاح) والسرية مؤمنة طالما أن المفتاح متاح فقط لطرفي الاتصال.
  - **Authentication:**

    هل يتم ضمان هوية المرسل أم لا؟

    أو هل الرسالة التي تم فك تشفيرها بنجاح من قبل المستقبل تضمن صحة هوية المرسل؟

    الجواب هو: نعم.

- :Integrity

هل تضمن أن الرسالة لم يتم تعديلها من لحظة خروجها من المرسل حتى وصولها للمستقبل؟

طالما تم فك التشفير بنجاح فالرسالة لم يتم تعديلها.

ملاحظة:
يجب التنويه إلا أن خوارزميات التعمية دائماً تفك التشفير ولا يمكن التأكد من صحة فك التشفير إلا من خلال النظر إلى الخرج إن كانت المعلومات فيه منطقية أم لا.

- عدم النكران:

هل الرسالة المشفرة C والتي تم فك تشفيرها بنجاح لتعطي M تمنع المرسل من إنكار إرسال الرسالة؟

لا، وذلك لأن النص المشفر C يمكن أن ينتج من قبل طرفي الاتصال.

إذاً التعمية التناظرية تؤمن السرية وال Authentication وال Integrity أما عدن النكران فهو غير مؤمن.

إن التعمية التناظرية فعالة وسريعة لكنها تحتاج إلى نظام إدارة للمفاتيح (أي مجموعة من العمليات لتوليد وتحديث وتوزيع المفاتيح للأطراف المعنية)، ولهذا ستتحدث عن نوع آخر من التعمية وهو ال Public-Key Cryptography

Public-Key Cryptography

التعمية اللاتناظرية / تعمية المفاتيح

تستخدم هذه التعمية مفتاحين:

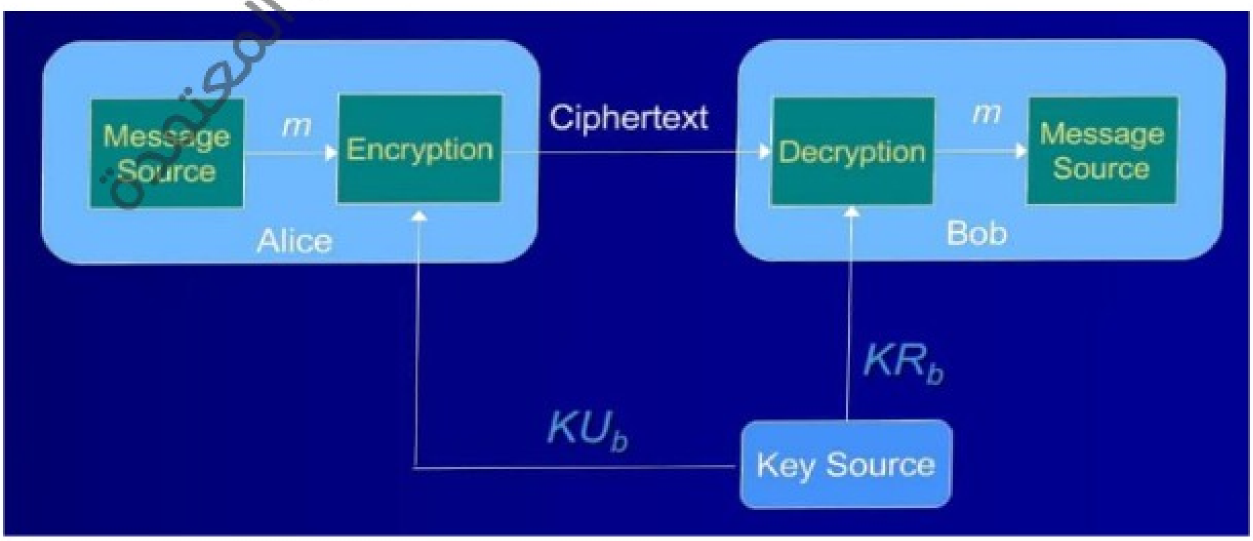
الأول: عام (Ku) Public Key يتم توزيعه على كل الجهات التي ترغب بإرسال رسالة مشفرة إلى تلك الجهة

الثاني: خاص (Kr) Private Key يستخدم لفك التشفير ولا يكون موجود إلا عند المستقبل.

مثال:

ليكن لدينا Alice وتريد أن ترسل رسالة سريعة m إلى Bob.

يجب على Bob أن يملك مفتاحين (Kr) private و (Ku) Public، قبل تشفير الرسالة فإن Alice تتلقى نسخة موثوق منها من مفتاح Bob العام



في هذه التعمية فإنه حتى الجهة التي قامت بالتشفير لا يمكنها فك تشفير الرسالة.

لا يجب أن يكون من الممكن الحصول على النص الأصلي من خلال النص المشفر والمفتاح العام.

تكون العلاقة بين ال Public Key وال Private Key مبنية على توابع وحيدة الاتجاه One-Way Function وكذلك لا يجب أن يكون من الممكن الحصول على المفتاح الخاص من معرفة المفتاح العام.

One - Way Functions (OWF)

وهي توابع سهلة الحساب ولكنها صعبة العكس من الأمثلة عليها:

-Multiplication of two primes

-Modular exponentiation

▪ Multiplication of two primes:

يعتبر تابع وحيد الاتجاه أي إذا كان لدينا p وq عددان أوليان فإنه من السهل إيجاد n = p . q لكن بدءاً من n من الصعب إيجاد p وq ضمن زمن معين.

تذكرة في الرياضيات:

أي عدد يمكن أن يكتب بطريقة وحيدة بدلالة الأعداد الأولية.

▪ Modular exponentiation:

عملية ترقية عدد هي رفع العدد إلى قوة معينة، حيث رفع العدد a إلى قوة b: a^b أي ضرب a بنفسه b مرة أي:

$$a^b = a_1 \times a_2 \times a_3 \times \dots\dots \times a_b$$

ME تعني حساب a^b ثم إيجاد باقي قسمتها على عدد n أي $a^b \bmod n$ ويتم حسابها بالشكل:

$$\left(\left(\left((a \times a) \bmod n\right) \times a\right) \bmod n\right) \times a) \bmod n \dots$$

حساب ME سهل لكن إذا كان لدينا n, a^b, a حيث (n عدد أولي) فإن حساب b هو المشكلة.

تسمى هذه العملية ب Discrete Logarithm Problem أي يكون لدينا a وn أولي فإن التابع:

$f(b) = a^b \bmod n$ هو (OWF).

خوارزمية RSA

-تعتبر خوارزمية التشفير الأكثر استخداماً المستعملة لمفتاح التشفير العام.

-توفر ميزة التشفير والتوقيعات الرقمية.

▪ خطوات الخوارزمية:

نحسب ال p وال q حيث يمكن أن يكون ال n, e هو المفتاح العام وتتم الخوارزمية كما يلي:

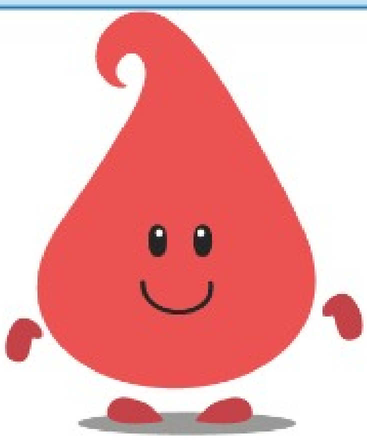
نحسب ال p و q بحيث يكونان عددان أوليان حجمهما كبير ونحسب المقدار n والذي يساوي $(n = p.q)$.

نختار ال e بحيث تحقق شرطين أساسيين:

1. $e < (p-1).(q-1)$
2. أن تكون أولية مع $(p-1).(q-1)$.

ملاحظات:

- المقدار Q(n) = (q-1) .(p-1).
- نقوم بحساب d حيث يقوم الشخص الذي يحسبها بتحليل e إلى عواملها الأولية فيوجد p وq وعندما نحسب d نكون قد كسرنا الخوارزمية.
- إن المفتاح العام في الخوارزمية هو (e , n).
- إن المفتاح الخاص في الخوارزمية هو (d) والذي يبقى سري.



مثال عن خوارزمية ال RSA:

نفترض أن p = 7 **و** q = 11 **فيكون لدينا** n = p.q = 11 * 7 = 77

Q(n) = (p -1). (q -1) = 10 * 6 = 60 **والآن علينا إيجاد ال e:**

لتكن 17: أصغر من Q (n)**، أولي مع** Q (n)

فلنحسب d: d = 53 **ومنه** (53 * 17) mod (60) = 1

والآن نقوم بتوزيع المفاتيح حيث نعطي (s) ال e وال n.

خطوات:

- **عملية التشفير (encryption):**

  ينفذها ال s حيث يأخذ ال m ويضربها بنفسها e (مرة) n mod ويضع الناتج في ال C:

  $$C = m^e \ mod \ n$$

  عملية الإرسال: حيث نرسل ال C إلى A.

- **عملية فك التشفير:**

  نستخدم ال d لنحسب: $m = C^e \ mod \ n$

  نفصل قليلاً: حيث نأخذ ال C ونضربها ببعضها d مرة وباقي قسمة هذا الناتج على n يكون هو m.

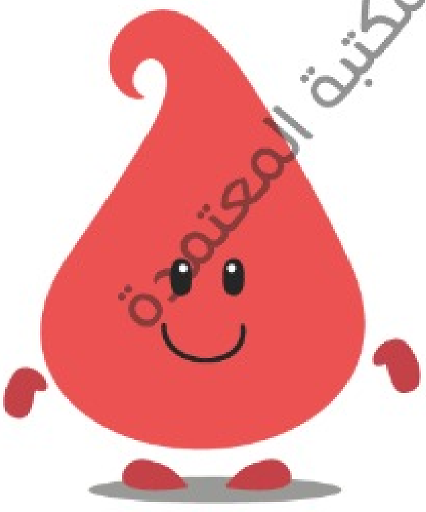
مثال: الرسالة Hello على المثال السابق فتكون الرسالة كالتالي: [07 04 11 11 14] **والآن نشفر:**

$$(07)^{17} \ mod \ 77 = 28$$
$$(04)^{17} \ mod \ 77 = 16$$
$$(11)^{17} \ mod \ 77 = 44$$
$$(11)^{17} \ mod \ 77 = 44$$
$$(14)^{17} \ mod \ 77 = 42$$

نرسل للمستقبل [28 , 16 , 44 , 44 , 12]

عندما يستقبل الرسالة يستخدم المفتاح الخاص (KRb)، d = 53

وذلك ليفك تشفير الرسالة كما يلي:



$(28)^{53} \ mod \ 77 = 07$ H

$(16)^{53} \ mod \ 77 = 04$ E

$(44)^{53} \ mod \ 77 = 11$ L

$(44)^{53} \ mod \ 77 = 11$ L

$(42)^{53} \ mod \ 77 = 14$ O

لا أحد يمكنه قراءة الرسالة وفهمها إلا المستقبل لأنه وحده من يملك المفتاح الخاص اللازم للتشفير.

أطوال المفاتيح :

- قد تكون الأطوال تناظرية أو غير تناظرية.
- قوة الخوارزمية RSA التي طول مفتاحها 1024 bit تعادل من ناحية القوة الأمنية خوارزمية تشفير تناظري قوة مفتاحها 80 bit.

RSA key length (bits)	Symmetric key length (bits)
1024	80
2048	112
3072	128
15360	256

ملاحظة:

- حتى نصل لنفس مستوى Security الذي في خوارزمية ال 128 bit EAS يجب أن يكون طول المفتاح في ال RSA هو 3072 bit.
- وإذا أردنا أن نصل لمستوى Security :ESA: 256 bit يجب أن يكون طول مفتاح ال RSA هو 15360 ولكن عند استخدام هذه الأطوال تصبح الخوارزمية بطيئة جداً لذلك تستخدم غالباً عندما يكون طول الرسالة قصير.

خوارزمية ال EL Gamal

هي خوارزمية تعتمد على تشفير المفتاح العام، لكن لماذا ندرسها؟

- نتعلم خوارزميات أخرى مختلفة عن ال RSA تعتمد على تشفير المفتاح العام ونعلم أنها ليست الوحيدة.
- نعرض نظام تشفير المفتاح العام بالإعتماد على تابع وحيد الإتجاه مختلف عن طريق تحليل العدد لعوامل أولية.

تتألف الخوارزمية من ثلاث مراحل:

1- توليد المفتاح:

يقوم مولد المفاتيح A باختيار المفاتيح بحيث يحقق:

-رقم أولي كبير من 1024 bit.

-صفوف زمرة *Zp بحيث يكون فيها كل مواصفات الزمرة o كل عدد له نظير.

-كل عددين نضربهم ببعض يكون الناتج ضمن الزمرة ومعنى ذلك أنك إذا اخذت g ورفعتها لأي عدد صحيح يبقى الناتج ضمن الزمرة ونحن باستخدام g يمكننا حساب عناصر الزمرة.

2- نختار X بحيث يحقق:

$$1 \leq X \leq P-2$$

3-نحسب Y وهي المفتاح العام:

$$Y = g^{x} \; mod \; P$$

A's public key is (P, g, y) to be published

A's private key is x

> ملاحظة:
>
> Each Entity A creates a public key and a corresponding private key (To be kept secret by A)

مثال:

نفرض p = 2357 ونعتبر ال 2 هي generator للمجموعة هذه حيث: g = 2 of Z 2357، نختار عشوائياً X = 1751

ونحسب Y المفتاح العام حيث:

$Y = 2^{1751} \; mod \; 2357 = 1185$

Public key is (2357, 2, 1185)

Private key is 1751

- **عملية التشفير:**

لتشفير الرسالة نستقبل المفاتيح (P, g, y) ونحول الرسالة بشكل عددي بحيث تكون المفاتيح في المجال [0, P-1] نختار رقم K صحيح حيث: $1 \leq K \leq P-2$

ونحسب ال Y من:

$$Y = g^{k} \; mod \; P \;\; and \;\; \delta = m.Y^{k} \; mod \; P$$

نرسل C = (y , δ) إلى المستقبل ليفك تشفيرها.

> **ملاحظة:**
>
> - حجم الرسالة قبل التشفير يساوي P، أما بعد التشفير فهو يساوي 2P أي أن التشفير يضاعف حجم الرسالة.

- **عملية فك التشفير:**

يقوم مولد المفاتيح A بفك التشفير كما يلي:

سيعين X لنحسب Z كما يلي: $Z = Y^{P-1-X}$

نستخدم ال Z مع المرتبة الثانية δ: $M = Z \,.\, \delta \bmod P$ **وتكون m هي الرسالة الأصلية.**

مثال: سنعتمد على المثال السابق:

Public key is (2357, 2, 1185)

Private key is 1751

- **التشفير:**

يكون كما يلي حيث أن m = 2035:

نولد K **حيث** K = 1520

بعد أن نتأكد من أن 2035 **أصغر من** P **نحسب:**

$$Y = 2^{1520} \, mod \, 2357 = 1430$$
$$\delta = 2035 \times 1185 \, mod \, 2357 = 697$$

نرسل C = (1430 , 697).

ملاحظة:
- إذا حولنا الرسالة لشكل عددي وكانت قمتها أكبر من P يتوجب علينا تقطيعها.

- **فك التشفير:**

$$Z = Y^{P-1-X} \, mod \, P = 1430^{605} mod \, 2357 = 872$$

$$m = 872 \times 697 \, mod \, 2357 = 2035$$

ملاحظات:
- طبيعة الارتباط بين المفتاحين العام والخاص في خوارزمية EL Gamal مختلفة عن طبيعة الارتباط في RSA.
- خوارزمية ال EL Gamal تضاعف حجم الرسالة عند تشفيرها.
- الذي يميز خوارزمية ال EL Gamal هو العشوائية أي أنه من الممكن أن نرسل الرسالة نفسها مرتين وتكون في كل مرة النتيجة مختلفة.
- ال RSA تعتمد على صعوبة تحليل العدد لعوامله الأولية أما ال EL Gamal فإنها تعتمد على discrete logarithm problem.
- نستخدم ال RSA بشكل أكبر من ال EL Gamal لأسباب عملية (حجم الرسالة قبل وبعد التشفير) وليس لأسباب أمنية.
- كلتا الخوارزميتين أقل كفاءة (كاستهلاك موارد) من الخوارزميات التناظرية.
- تعتبر ال EL Gamal أساس للعديد من الخوارزميات مثل: DSA.
- يوجد سلايدات أخرى عن خوارزميات باقي القسمة والأرقام (28 – 40) فيرجى الاطلاع عليهم.

THE END