الجمهورية العربية السورية
جامعة قرطبة الخاصة
كلية الهندسة / تكنولوجيا هندسة الاتصالات والمعلومات

ملخص محاضرة خاصة بمقرر مادة
"وثوقية وأمن المعلومات"
" تطبيقات وثوقية وأمن المعلومات 1"
للفصل الثاني للعام الدراسي 2020/2019
بعنوان:

الغوريتم التشفير (RSA)

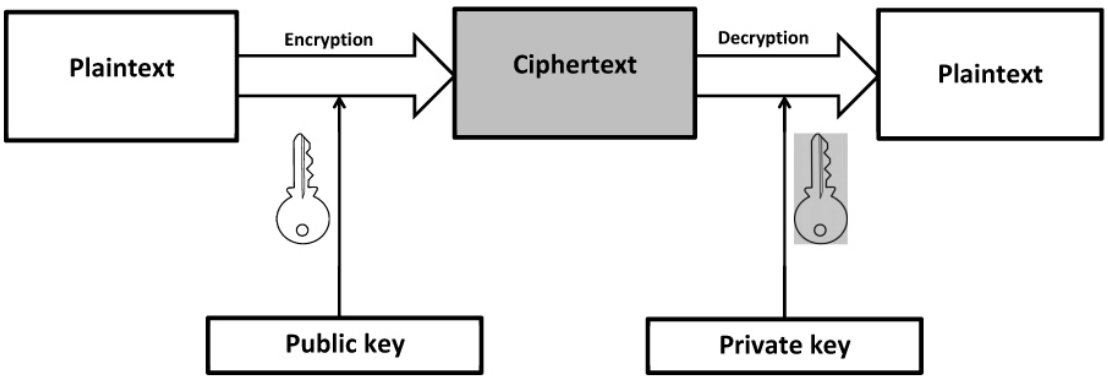
RSA Encryption Algorithm

I. ما هو الغوريتم التشفير(RSA) RSA Encryption Algorithm:

- هو الغوريتم تشفير غير متماثل (يستخدم مفتاحين)
- يستخدم الأعداد الأولية
- أوجده عام 1977 كلٍ من (Rivest, Shamir and Adelman RSA)

• مبدأ العمل لألغوريتم التشفير RSA:

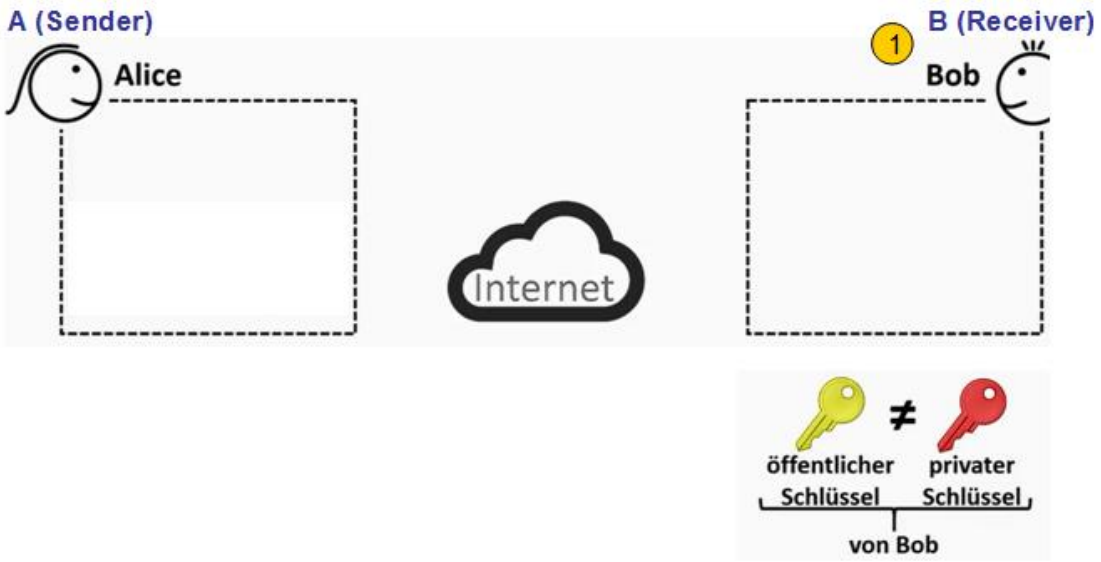
يتم تشفير النص الأصلي Plaintext بعملية التشفير Encryption باستخدام المفتاح العام Public key.
كما يتم فك تشفير النص المشفر Ciphertext بعملية فك التشفير Decryption باستخدام المفتاح الخاص Private key. كما هو موضح بالشكل (1):



شكل (1)

• مراحل الغوريتم التشفير RSA (إنشاء المفتاحين الخاص والعام من قبل المستقبل):
يتكون الغوريتم التشفير RSA من المراحل الثلاث التالية:

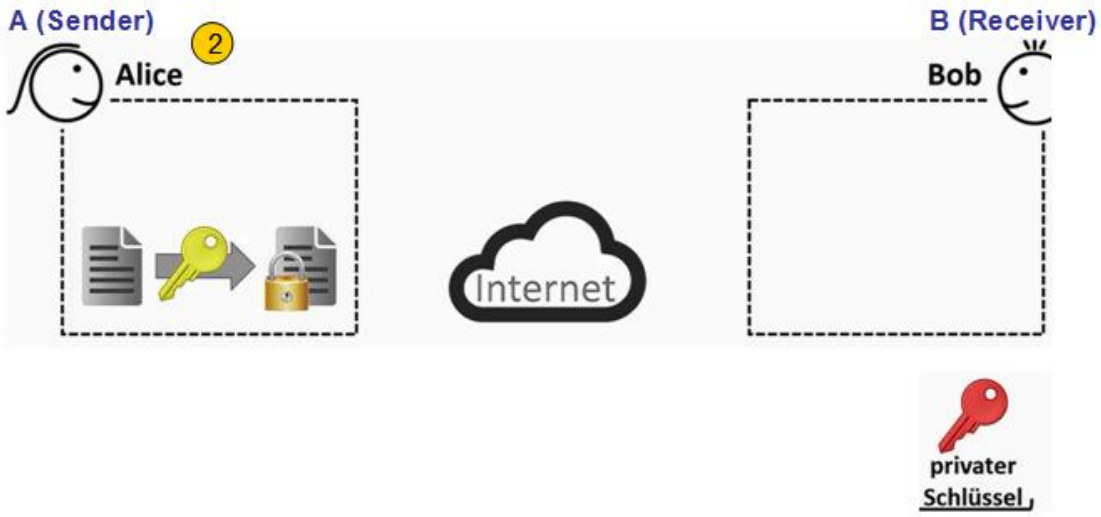
1- يقوم المستقبل* B (Receiver) بإنشاء مفتاحين غير متماثلين:
- (مفتاح خاص Private) يحتفظ به
- (مفتاح عام Public) يرسله للمرسل A
كما هو موضح في الشكل (2):



شكل (2)

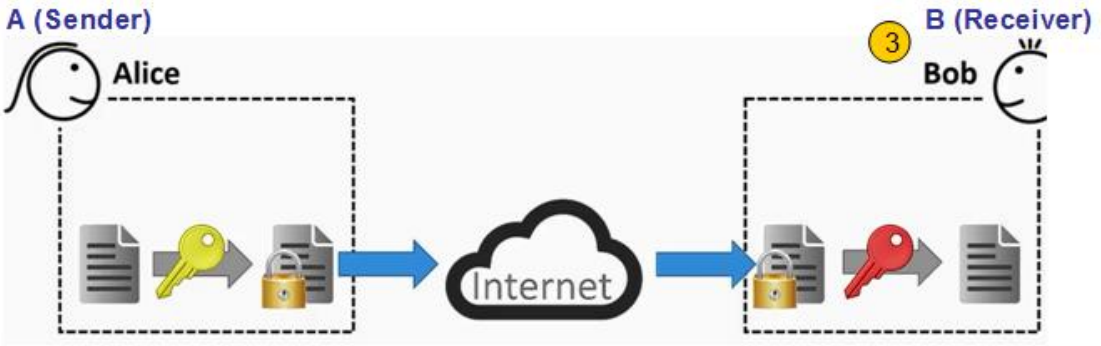
*) تأكيد: المستقبل (وليس المرسل)!

2- يقوم المرسل A (Sender) بتشفير النص باستخدام المفتاح العام ويرسله للمستقبل B
كما هو موضح في الشكل (3):



شكل (3)

3- يقوم المستقبل B بفك تشفير النص باستخدام المفتاح الخاص
كما هو موضح في الشكل (4):



شكل (4)

• **عبارات حساب الغوريتم التشفير RSA:**

يتم فرض العددين الأوليين p & q ومن ثم يتم حساب n&m باستخدام العلاقات التالية:

1- حساب n:

$$n = p * q$$

2- حساب m:

$$m = (p-1) * (q-1)$$

بينما يتم تعيين العددين الأوليين d & e وفق الشروط التالية:

3- تعيين e: يتم تعيين e وفق الشروط التالية:

- عدد أولي
- ليس من مضاعفات m
- أصغر من m

4- تعيين d: يتم تعيين كعدد موجب يحقق العلاقة التالية:

$$0 < d, d * e \bmod m = 1$$

5- حساب النص المشفر V:

$$V = T^e \bmod n$$

6- حساب النص الأصلي T:

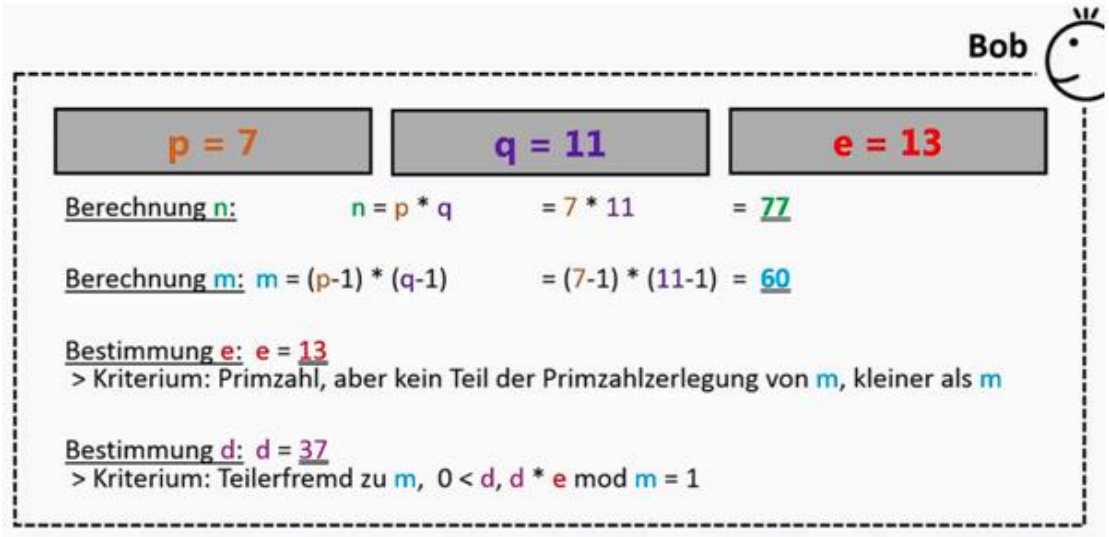
$$T = V^d \bmod n$$

II. حساب الغوريتم التشفير RSA Encryption Algorithm:

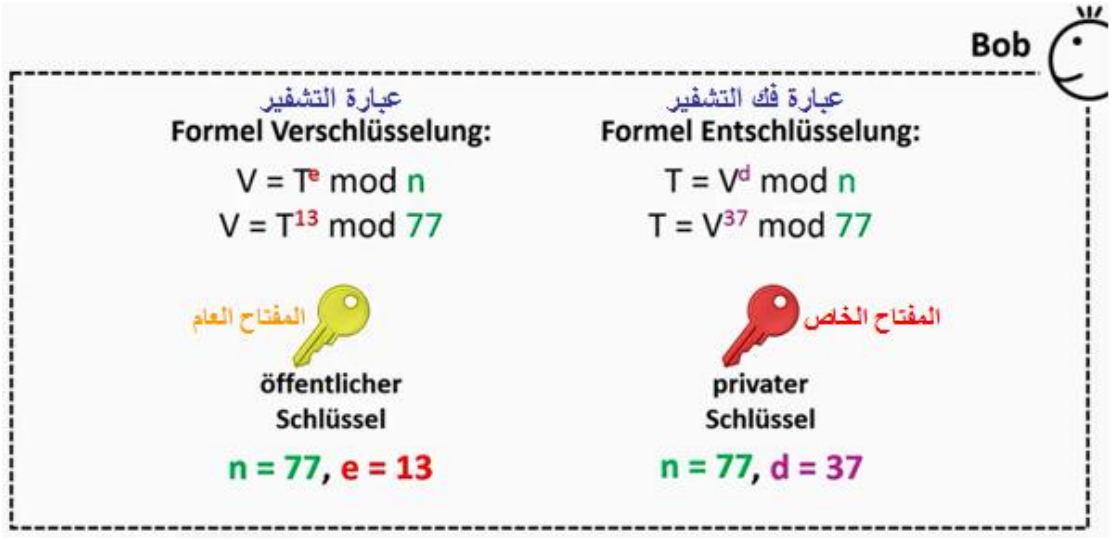
• **مثال عملي حساب الغوريتم التشفير RSA (Example):**

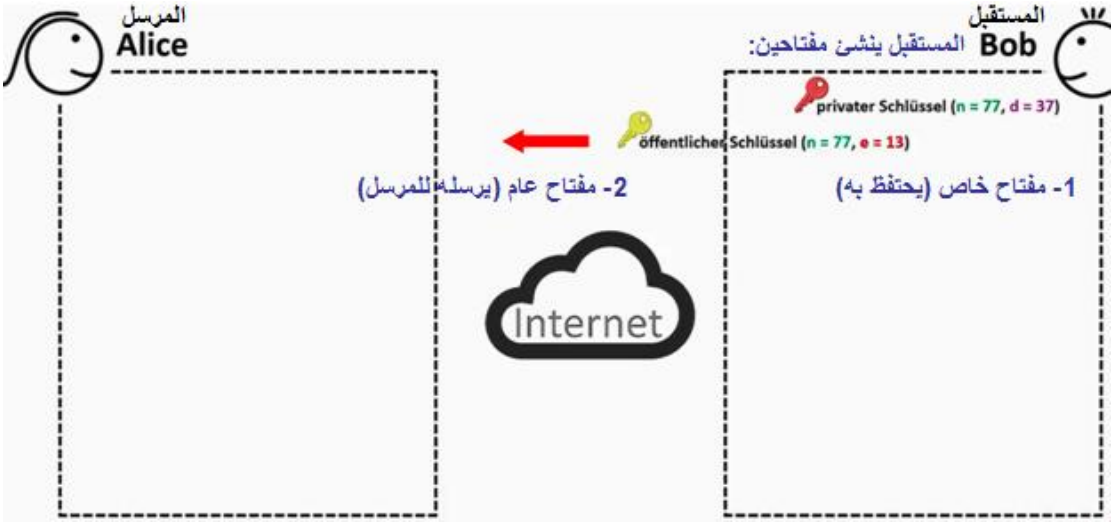
بفرض المعطيات التالية: p=7 ، q=11 ، e=13

1- حساب n&m وتعيين e&d:



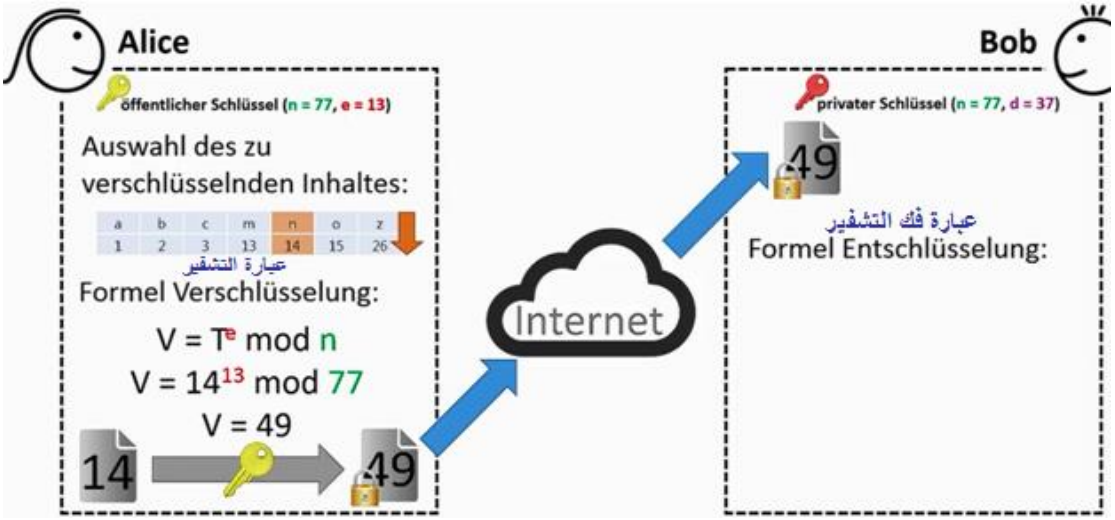
2- حساب عبارتي التشفير V وفك التشفير (أو النص الأصلي) T:



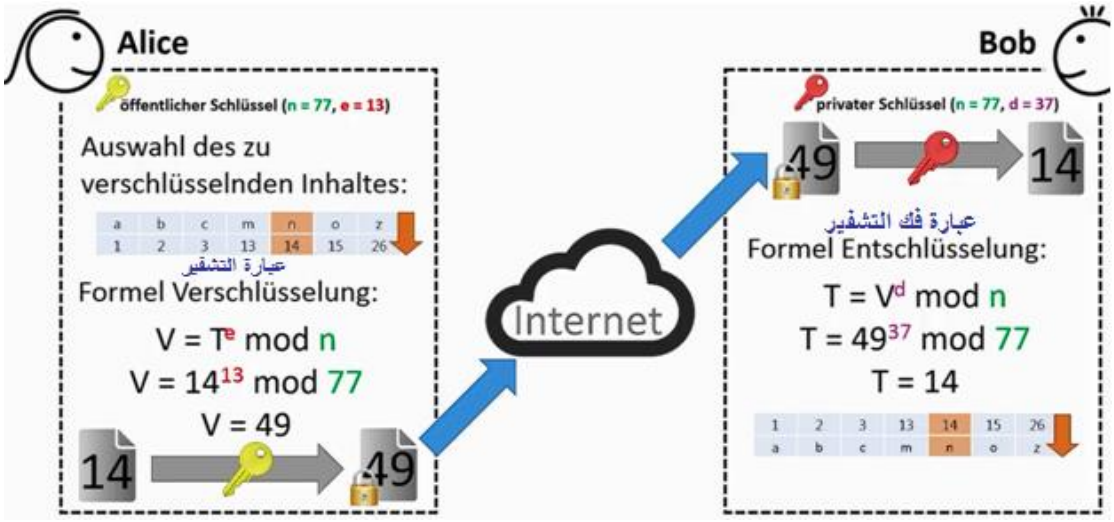


نلاحظ أن النص المرسل هو "n" ترتيبه 13

باستخدام عبارة التشفير أصبح ترتيبه 49:



الآن باستخدام عبارة فك التشفير تم استرجاع الترتيب الأصلي 14
وبالتالي تم استرجاع النص الأصلي المقابل وهو "n".



وعليه إذا تم معرفة المعلومات المرسلة من قبل Man in the Midel (MitM) يكون الرقم 49 (وهو الرقم الذي قد يتم الحصول عليه ومعرفته من قِبَل الأشخاص أو الهيئات المتطفلة) وليس 13 الذي لا يعبر عن النص الأصلي الذي تم إرساله وهو "n".

وبالتالي نكون بطريقة التشفير هذه على سرية ووثوقية المعلومات التي تم إرسالها.

- **ملاحظة1:**

بعض المراجع تسمي الجداء

$$m = (p-1) * (q-1)$$

بتابع أويلر Euler عوضاً عن m:

$$\Phi(n) = (P-1) * (Q-1)$$

كما تسمي النص المشفر Ciphertext بـ C عوضاً عن V و النص الأصلي Plaintext بـ Message (m) عوضاً عن T. وعليه تصبح عبارات حساب الالغوريتم RSA كما يلي*:

Key generation	$n = P * Q$ $d * e = 1 \bmod \Phi(n)$
Encryption	$c = m^e \bmod n$ Public Key(n,e)
Decryption	$m = c^d \bmod n$ private key (d)

*) كلتا الطريقتين صحيحة ويترك للطالب حرية الاختيار!

• **ملاحظة2:** يتوفر حالياً تطبيقات حاسوب تسمح باختيار نوع التشفير (RSA, DES, 3Des, ...) تقوم آلياً بحساب الالغوريتم المطلوب. بناءً عليه يطلب فقط معرفة وحفظ العبارات الأساسية دون الخوض في التفاصيل.

***

حلب 2020/4/15

مع كل التمنيات بالنجاح والتوفيق

مدرس المقرر: **الدكتور حسن مسلماني**