

Information System Security أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا



عناوين المحاضرة الرابعة

➤ خوارزمية RSA (Rivest Shamir et Adleman)

✓ الأسس الرياضية لخوارزمية RSA

✓ آلية عمل الخوارزمية

✓ أمن الخوارزمية

✓ استخداماتها الحالية

➤ خوارزمية ديفي هيلمان لتوزيع المفاتيح DH (Diffie-Hellman)

✓ أهمية الخوارزمية

✓ آلية عمل الخوارزمية

✓ أمن الخوارزمية



مقدمة عن خوارزمية RSA

❖ هي عبارة عن خوارزمية تشفير غير متناظر، وضعت من قبل Ronald L. Rivest, Adi Shamir and Leonard M. Adleman في عام 1977، وهي تعتمد على عدة أسس رياضية في نظرية الأعداد.

❖ هي عبارة عن نظام تسمية كتلي

❖ دخله وخرجه عبارة عن أرقام صحيحة تتراوح قيمتها بين $0 - (n-1)$ من أجل قيمة n ، الحجم النموذجي لـ n هي 1024 خانة ثنائية

❖ تعتمد هذه الخوارزمية على صعوبة تحليل الأعداد الكبيرة إلى عواملها الأولية. هذه الأرقام الكبيرة هي عبارة عن ناتج من ضرب عددين أوليين كبيرين.



أسس رياضية لخوارزمية RSA

❖ الأعداد الأولية فيما بينها:

✓ نقول عن عددين أنهما عددين أوليين فيما بينهما إذا كان القاسم المشترك الأكبر لهما هو الواحد
مثال: العددين 10, 21 هما عددين أوليين فيما بينهما لأن 10 يقبل القسمة على 1,2,5,10 و العدد 21 يقبل القسمة على 1,3,7,21 أي لا يوجد بينها معامل مشترك سوى الواحد.

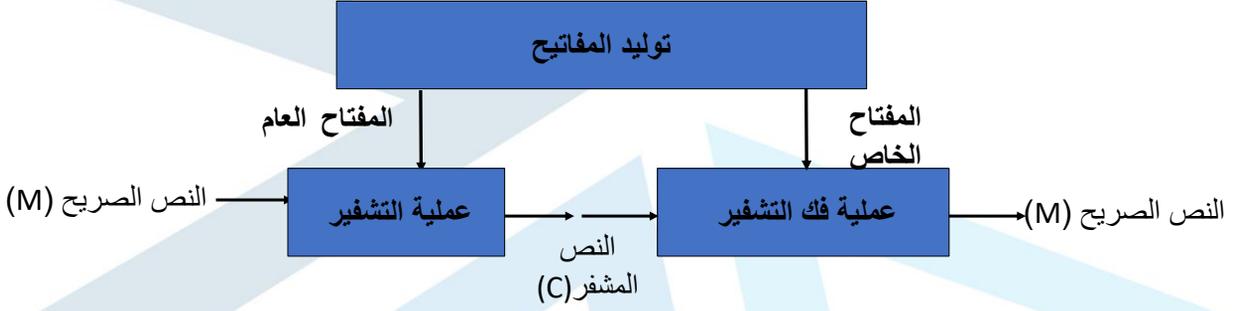
❖ التابع $\phi(n)$:

✓ يعرف التابع $\phi(n)$ على أنه عدد الأعداد الأقل من n والتي تكون أولية مع (n)
مثال: $\phi(6) = 2$. لأن الأعداد الأقل من 6 هي 1,2,3,4,5 لكن نلاحظ أن 1,5 هما فقط العددين الأوليين مع العدد 6 بينما 2,4 يشتركان مع العدد 6 بالمعامل 2 و العدد 3 يشترك مع 6 بالمعامل 3

❖ من أجل أي عدد أولي n يكون: $\phi(n) = n - 1$ مثال: $\phi(7) = 6$



المخطط الصندوقي لخوارزمية RSA



توليد المفاتيح (Key Generation) (المفتاح العام والمفتاح الخاص)

فيكون المفتاح العام:
 $K_{pub} = \{e, n\}$

1. نختار عددين أوليين كبيرين (p, q) و بحيث $p \neq q$

2. نحسب: $n = p \times q$

3. نحسب: $\phi(n) = (p-1) \times (q-1)$

4. نختار عدد صحيح (e) بحيث يكون: $1 < e < \phi(n)$; $\gcd(\phi(n), e) = 1$;

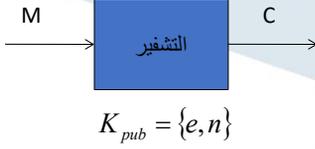
5. نحسب (d) : $d \equiv e^{-1} \pmod{\phi(n)} \rightarrow d \times e \equiv 1 \pmod{\phi(n)}$

فيكون المفتاح الخاص: $K_{pri} = \{d, n\}$



عملية التشفير (Encryption)

يستخدم المفتاح العام للمستقبل

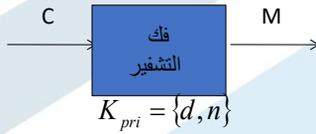


النص الصريح: $M < n$

النص المشفر: $C = M^e \text{ mod}(n)$

عملية فك التشفير (Decryption)

يستخدم المفتاح الخاص للمستقبل



النص المشفر: C

النص الصريح: $M = C^d \text{ mod}(n)$



أمن الخوارزمية RSA (1/2)

❖ توجد عدة هجومات نذكر منها:

➤ الهجوم الأعمى (Brute force):

يتضمن تجريب جميع المفاتيح الممكنة، الحل يكون باستخدام مفاتيح طويلة (قيم e, d)

➤ الهجوم الرياضي (Mathematical Attack):

عادة يتبع الهجوم الرياضي ما يلي: (المفتاح العام معروف من قبل المهاجم)

١. تحليل n إلى عددين أوليين (p, q) بحيث $n = p * q$

٢. حساب تابع أولر $\phi(n) = (p - 1) \times (q - 1)$

٣. إيجاد المفتاح الخاص بمعرفة e $d \equiv e^{-1} \text{ mod } \phi(n)$

يمكن مقاومة هذا الهجوم عن طريق تكبير قيمة n كثيراً ليصعب تحليلها إلى العوامل الأولية.



اختار رقمين أوليين كبيرين p, q عشوائيين و مختلفين عن بعضهما .
لدينا هنا مثال عن أعداد أولية ولدت باستخدام اختبار Rabin-Miller primality tests

p

121310724392112718973236715316124404284724276337014109256345493123019643730420
85619324197365322416866541017057361365214171711713797974299334871062829803541

q

120275242554787488859562207937345121287333878036820754336538999839551798509887
97899869146900809131611153346817050832096022160146366346391812470987105415233



باستخدام هذين الرقمين نحسب $\phi(n)$ و n

n

1459067680075833232301869393490706352924018723753571643995818710198734387990053589383695714026
7014980212181808629246742282815702292207674690654340122488967247240792696998710058129010319931
7858753663710862357656510507883714297115637342788911463535102712032765166518411726859837988672
111837205085526346618740053

$\phi(n)$

1459067680075833232301869393490706352924018723753571643995818710198734387990053589383695714026
7014980212181808629246742282815702292207674690654340122488964831381123227996631730139777785236
5301547848273478871297222058587457152891606459269718119268971163555070802643999529549644116811
947516513938184296683521280



أمن الخوارزمية RSA (2/2)

تاريخ الكسر	العدد التقريبي للبتات الثنائية
1991	332
1992	365
1993	398
1994	428
1999	465
1999	512
2005	664

➤ أمثلة عن كسر الخوارزمية بالهجوم الرياضي :

➤ يعد المفتاح ذو الطول الذي يتراوح [4096-2048] بت آمن .



الاستخدامات الحالية لخوارزمية RSA

❖ تستخدم في WEB Browsers عند Microsoft, Netscape

❖ تستخدم في عدة منتجات برمجية تجارية وفي أنظمة التشغيل مثل Microsoft, Apple, sun, Novell

❖ تستخدم أيضاً في العتاد الصلب كالهواتف الآمنة وبطاقات شبكات الايثرنت، وعلى البطاقات الذكية.

❖ كما تستخدم في أغلب بروتوكولات الاتصالات الآمنة عبر الإنترنت مثل S/MIME وSSL,



أهمية خوارزمية ديفي هيلمان (Diffie-Hellman) DH

تبادل المفتاح السري (المتناظر) بين طرفين (أليس و بوب) يكون باتتبع الخطوات الآتية :

١. يولد بوب المفتاح المتناظر Ks
٢. يشفر بوب المفتاح المتناظر Ks باستخدام المفتاح العام لأليس
٣. تفك أليس التشفير باستخدام المفتاح الخاص لها، و تحصل على المفتاح المتناظر Ks
٤. يشفر كل من بوب و أليس المعلومات باستخدام المفتاح المتناظر و أية خوارزمية تشفير متناظر (DES,3DES...)

المشكلة هنا : ماذا لو أن أحد الطرفين لا يملك مفتاحاً عاماً

الحل: استخدام خوارزمية ديفي هيلمان لتبادل المفاتيح لأنها تسمح بتوليد مفتاح سري بين طرفين دون وجود مسبق لمفتاح عام



الفكرة العامة لخوارزمية ديفي هيلمان

تعتمد على أن الطرفين يتبادلان معلومات ، هذه المعلومات تسمح بتوليد مفتاح متناظر بشكل آمن، يستخدم لتشفير المعلومات المتبادل بينهما



آلية عمل خوارزمية ديفي هيلمان لتبادل المفاتيح (1/3)

1. يتفق الطرفان (أليس و بوب) على معلومات عامة معروفة لكليهما (Common Global Information) هي:
 P : عدد أولي كبير (1024 bits على الأقل) g : مولد وهو جذر أولي لـ P حيث $P > g$
2. يختار بوب عدداً عشوائياً XB (خاص) بحيث: $XB \in [1, P-1]$
3. يولد بوب باستخدام قيمة XB قيمة عامة YB وفق العلاقة:
$$YB = g^{XB} \bmod P$$
4. يرسل بوب القيمة العامة YB إلى أليس
5. تختار أليس عدداً عشوائياً XA (خاص) بحيث: $XA \in [1, P-1]$
6. تولد أليس باستخدام قيمة XA قيمة عامة YA وفق العلاقة:
$$YA = g^{XA} \bmod P$$
7. ترسل أليس القيمة العامة YA إلى بوب



آلية عمل خوارزمية ديفي هيلمان لتبادل المفاتيح (2/3)

$$K = YA^{XB} \bmod P$$

$$K = YB^{XA} \bmod P$$

8. يولد بوب المفتاح السري (المتناظر) وفق العلاقة:

9. تولد أليس المفتاح السري (المتناظر) وفق العلاقة:





آلية عمل خوارزمية ديفي هيلمان لتبادل المفاتيح (3/3)

بوب

يختار عدداً عشوائياً X_B

الاتفاق على قيم P و g

أليس

تختار عدداً عشوائياً X_A

يولد قيمة عامة Y_B وفق العلاقة:

$$Y_B = g^{X_B} \text{mod } P$$

يولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = Y_A^{X_B} \text{mod } P$$

ترسل Y_A

تولد قيمة عامة Y_A وفق العلاقة:

$$Y_A = g^{X_A} \text{mod } P$$

يرسل Y_B

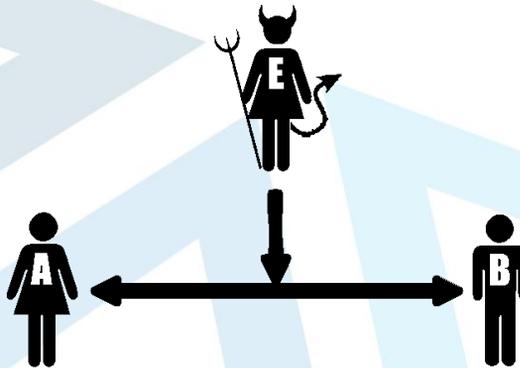
تولد المفتاح السري (المتناظر) وفق العلاقة:

$$K = Y_B^{X_A} \text{mod } P$$



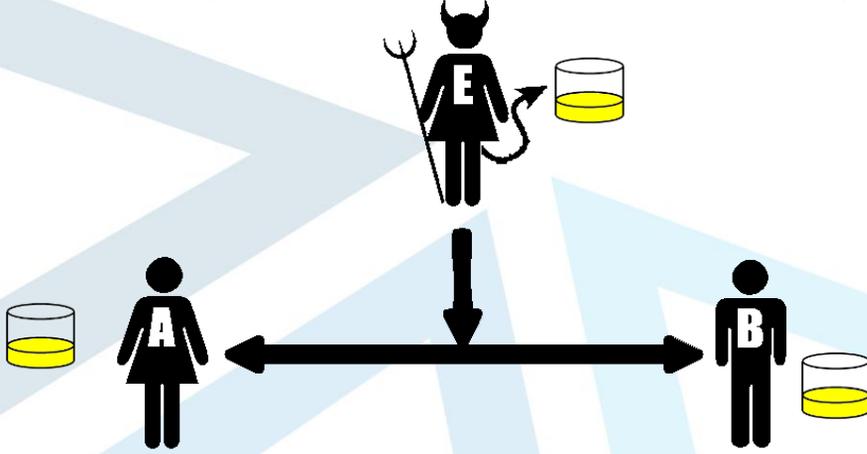
أمن خوارزمية ديفي هيلمان لتبادل المفاتيح

بفرض أن المهاجم **ينصت** لعمليات التبادل التي تجري بين أليس و بوب





سيتفق كلاهما على القيم العامة المعروفة (اللون الأصفر) وكذلك سيحصل عليها المهاجم



MU-EPP-FM-005

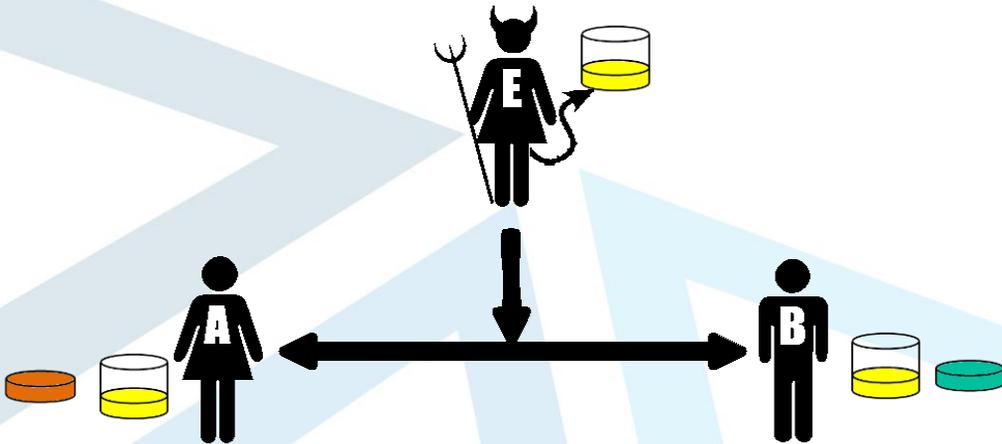
Issue date 17November2025

issue no:1

<https://manara.edu.sy>



يختار كل من الطرفين قيمة سرية (اللون الأخضر لبوب، اللون البرتقالي لأليس)، لا يمكن للمهاجم معرفة أي منهما



MU-EPP-FM-005

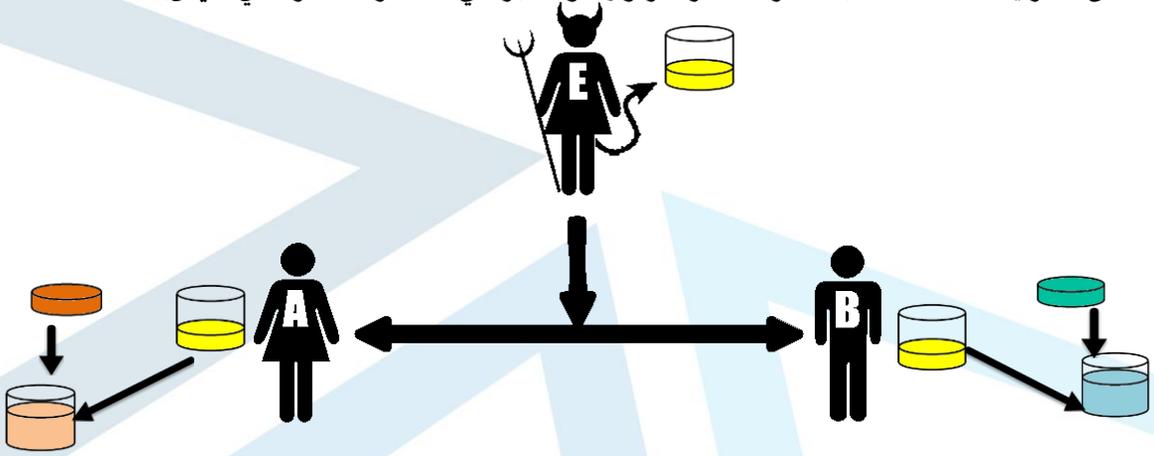
Issue date 17November2025

issue no:1

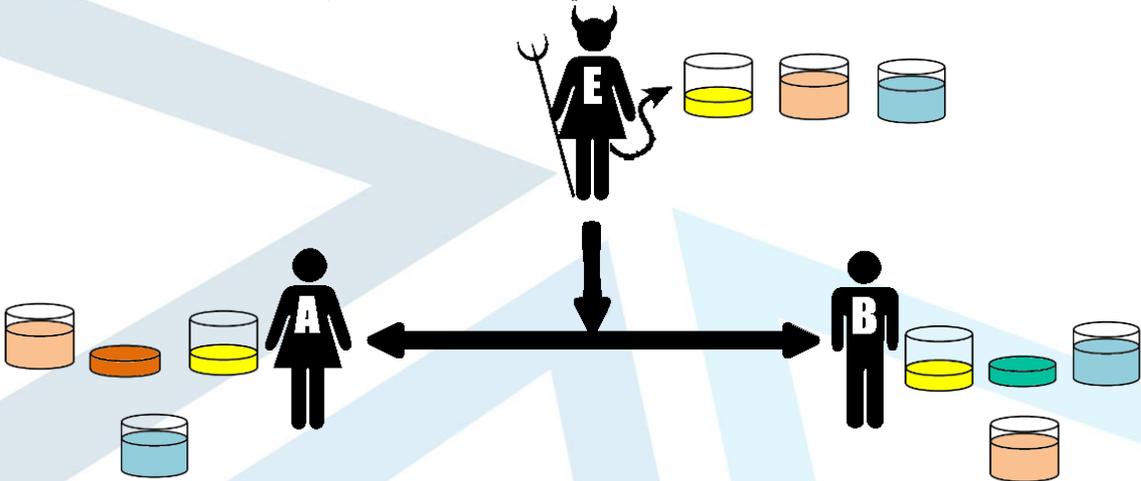
<https://manara.edu.sy>



يولد كل من الطرفين قيمة علنية (أخضر + أصفر = تركواز لبوب، برتقالي + أصفر = أصفر طيني لأليس)



يرسل كل من الطرفين القيمة العلنية للآخر (تركواز، أصفر طيني) فيحصل عليها المهاجم





نهاية المحاضرة الرابعة

MU-EPP-FM-005

Issue date 17November2025

issue no:1

<https://manara.edu.sy>

