مهارات الحاسوب

الدكتور المهندس
مثنى القبيلي

هندسة الروبوتيكس والأنظمة الذكية
كلية الهندسة
جامعة المنارة

الفصل الدراسي الأول ٢٠٢١-٢٠٢٢

عناوين المحاضرة الثامنة

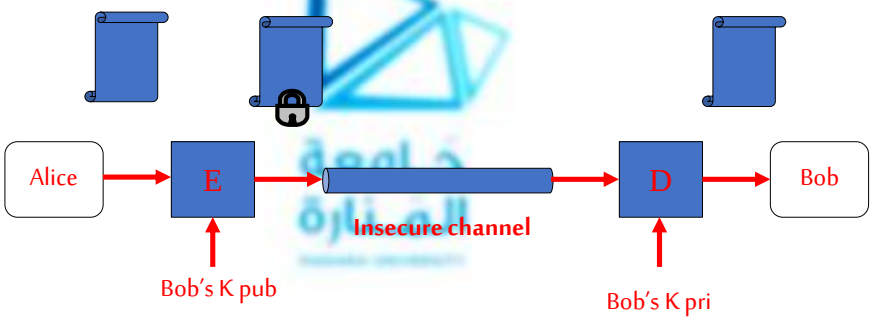
- تذكرة بمفهوم التشفير غير المتناظر
- مفهوم التابع وحيد الاتجاه (one-way function)
- مفهوم تابع الـ mod
- نظام تشفير حقيبة الظهر (knapsack Cryptosystem)
- مقدمة عن خوارزمية RSA(Rivest Shamir et Adleman)
  - ✓ الأسس الرياضية لخوارزمية RSA
  - ✓ آلية عمل الخوارزمية
  - ✓ أمن الخوارزمية
  - ✓ استخداماتها الحالية

عناوين المحاضرة الثامنة

- خوارزمية ديفي هيلمان لتوزيع المفاتيح DH(Diffie–Hellman)
  - ✓ أهمية الخوارزمية
  - ✓ آلية عمل الخوارزمية
  - ✓ أمن الخوارزمية

تذكرة بمفهوم التشفير غير المتناظر

- يعتمد التشفير غير المتناظر على استخدام مفتاحين:
  مفتاح خاص private key و مفتاح عام public key



- يشفر باستخدام المفتاح العام للوجهة ويفك التشفير باستخدام المفتاح الخاص المقابل(للوجهة نفسها)

4

مفهوم التابع وحيد الاتجاه (one way function)

❖ نقول عن تابع y=f(x) أنه تابع وحيد الاتجاه ، إذا تحقق لدينا الشرطين الآتيين:

✓ إذا توفر لدينا x فإنه من السهل حساب y=f(x)

✓ أما إذا توفر لدينا y فإنه لا يمكن حسابياً تحديد قيمة: $y = f^{-1}(X)$

❖ **مثال : تابع حساب العوامل الأولية**

إذا كان لدينا العددين الأوليين الكبيرين p,q من السهل جداً حساب n=pxq

لكن عند معرفة n من غير الممكن معرفة العددين الأوليين اللذين ينتج عنهما n بل يجب تجربة كافة القيم .

❖ قد يعاني تابع وحيد الاتجاه مما يسمى **المصيدة**

❖ **مثال على المصيدة :**

في حساب العددين الأوليين تعد معرفة أحدهما هي مصيدة تتسبب بمعرفة الآخر فمثلاً بمعرفة n مع معرفة q سيكون من السهل معرفة p أي أن q هي مصيدة لحساب p من n

5

مفهوم تابع الـ mod (1/3)

➢ يعرف تابع الـmod بالعلاقة: **a=b mod(n)**

و تعني أن a هو باقي قسمة b على n .

➢ إن الأعداد التي تؤخذ بالحسبان هي فقط الأعداد الصحيحة **غير السالبة** من المعاملات (modulus).

➢ من أجل mod(n) تكون الأعداد الفعالة هي فقط الأعداد من 0 إلى (n-1). ونتائج العمليات ستكون دائماً من 0 حتى (n-1)

مثال:

1=11mod5 تعني أن باقي قسمة 11 على 5 هو 1

4=73mod 23 تعني أن باقي قسمة 73 على 23 هو 4

6

مفهوم تابع الـ mod (2/3)

❖ **الأعداد المتطابقة في القياس:**

✓ نقول عن عددين أنهما عددين متطابقين في القياس إذا كان:

(a mod(n)) = (b mod(n))

✓ و يعبر عن ذلك رياضياً كمايلي : $a \equiv b \bmod(n)$

مثال:

$$\left.\begin{array}{l} 11 \bmod 5 = 1 \\ 1 \bmod 5 = 1 \end{array}\right\} \Rightarrow 11 \equiv 1 \bmod(5)$$

$$\left.\begin{array}{l} 73 \bmod 23 = 4 \\ 4 \bmod 23 = 4 \end{array}\right\} \Rightarrow 73 \equiv 4 \bmod(23)$$

❖ **عمليات الحساب بالقياس:**

$$[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$$

7

مفهوم تابع الـ mod (3/3)

❖ **معكوس الضرب بالنسبة لتابع الـ mod :**

✓ معكوس عدد a بالنسبة لتابع mod(m) هو عدد x بحيث $a * x \equiv 1 mod(m)$

تكون قيمة x ضمن المجال {0,1,2,....m-1}

مثال :

أوجد معكوس العدد 8 للضرب بالنسبة لـ mod(29)

$$8 * x \equiv 1 mod(29)$$

تكون قيمة x ضمن المجال {0,1,2,3,4,5,6,7,8,...28}

$$88 = 1 mod(29) \qquad 8 * 11 = 88$$

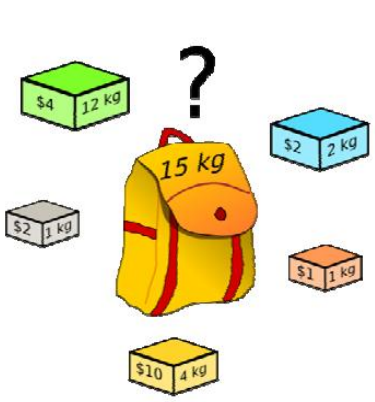
$$8 * 11 \equiv 1 mod(29)$$

أي x=11 هي معكوس الضرب لـ a=8 بالنسبة لـ mod29

8

نظام تشفير حقيبة الظهر (1/2)
knapsack Cryptosystem

❖ يعد أول نظام تشفير غير متناظر ، وضع من قبل العالمين Hellman و Merkel عام 1978 ، يمكن تنظيم هذا النظام كالآتي:



➢ **الفكرة الرئيسية:**

إيجاد حل لمسألة تعبئة حقيبة الظهر

➢ **فرضيات المسألة:**

حقيبة سعتها S

عدد الأغراض K غرض

➢ **المطلوب:**

ما هي مجموعة الأغراض التي يجب اختيارها كي تمتلئ الحقيبة تماماً؟

9

نظام تشفير حقيبة الظهر (2/2)
knapsack Cryptosystem

❖ **التوصيف الرياضي للمسألة:**

حجم الحقيبة : $S = X_1 a_1 + X_2 a_2 + \cdots + X_k a_k$

- حيث:

a_i حجم الغرض i

X_i قيمتها 0 أو 1 حيث : $X_i = 0,$ الغرض i غير موجود ضمن الحقيبة

$X_i = 1$ الغرض i موجود ضمن الحقيبة

10

المخطط الصندوقي لنظام تشفير حقيبة الظهر
knapsack Cryptosystem

11

مراحل نظام تشفير حقيبة الظهر(1/4)

❖ **توليد المفاتيح :** خطوات توليد المفتاح العام و المفتاح الخاص:

من أجل عدد أغراض K:

1. نقوم بتوليد مجموعة متزايدة $b = [b_1, b_2, \dots \dots, b_k]$ بحيث تحقق الشرط

$$b_i \geq b_1 + b_2 + \cdots + b_{i-1}$$

2. نختار قيمة n بحيث تحقق الشرط : $n > b_1 + b_2 + \cdots + b_k$

3. نختار قيمة r بحيث تكون أولية مع n

4. نحسب المصفوفة t باستخدام العلاقة : $t_i = (b_i \times r) mod(n)$

5. ندور t وفق تدوير مفروض و بذلك نحصل على **a المفتاح العام**

6. و يكون المفتاح الخاص هو **القيم b و n و r والتدوير**

12

مثال عن توليد المفاتيح في نظام تشفير حقيبة الظهر(1/2)

بفرض عدد الأغراض K=4 .

1. نقوم بتوليد مجموعة متزايدة $b = [2,3,6,12]$ و هي تحقق الشرط

$$b_i \geq b_1 + b_2 + \cdots + b_{i-1}$$

$3 \geq b_1 = 2$ محقق

$6 \geq b_1 + b_2 = 2 + 3 = 5$ محقق

$12 \geq b_1 + b_2 + b_3 = 2 + 3 + 6 = 11$ محقق

2. نختار n بحيث هي تحقق الشرط $n > b_1 + b_2 + b_3 + b_4$

$n > 2 + 3 + 6 + 12 = 23$

n=25 هي تحقق الشرط

13

مثال عن توليد المفاتيح في نظام تشفير حقيبة الظهر(2/2)

3. نختار قيمة r=7 وهي أولية مع n=25

4. نحسب بعدها المصفوفة t باستخدام العلاقة : $t_i = (b_i \times r) mod(n)$

$t_1 = (b_1 \times r) mod(n) = (2 \times 7) mod(25) = 14$

$t_2 = (b_2 \times r) mod(n) = (3 \times 7) mod(25) = 21$

$t_3 = (b_3 \times r) mod(n) = (6 \times 7) mod(25) = 17$

$t_4 = (b_4 \times r) mod(n) = (12 \times 7) mod(25) = 9$

فتكون المصفوفة t=[14,21,17,9]

5. بفرض أن التدوير هو : [3,2,4,1]

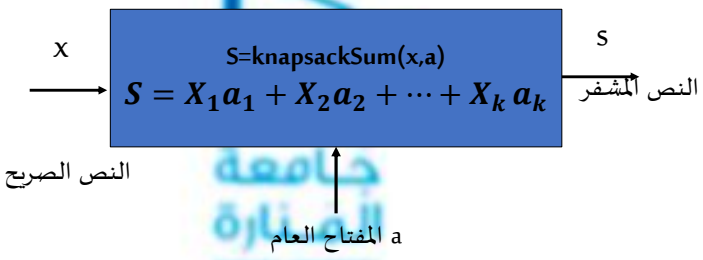
بعد تدوير t ينتج **المفتاح العام** : a=[17, 21,9,14]

ويكون المفتاح الخاص : n=25, r=7,b=[2,3,6,12] و التدوير : [3,2,4,1]

14

مراحل نظام تشفير حقيبة الظهر(2/4)

❖ عملية التشفير

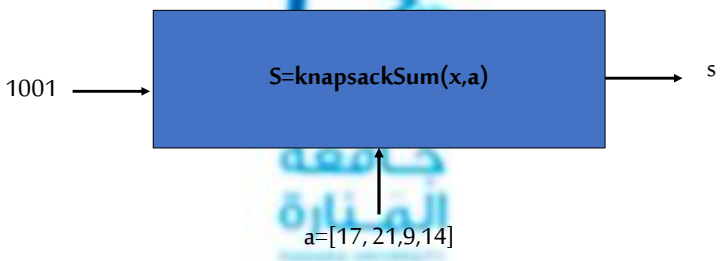


المخطط الصندوقي

15

مثال على عملية التشفير باستخدام حقيبة الظهر

بفرض أن النص الصريح x=1001 . أوجد النص المشفر باستخدام نظام حقيبة الظهر (s) الذي يعتمد القيم المحسوبة سابقاً



$$S = X_1a_1 + X_2a_2 + X_3a_3 + X_4 a_4$$

$S = 1 * 17 + 0 * 21 + 0 * 9 + 1 * 14$=31 النص المشفر

16

مثال2 على عملية التشفير باستخدام حقيبة الظهر

بفرض أن النص الصريح x=00101101 . أوجد النص المشفر باستخدام نظام حقيبة الظهر (s) الذي يعتمد القيم المحسوبة سابقاً

نلاحظ أن طول النص الصريح يساوي 8 وهو أكبر من عدد الأغراض 4

نقسم هذا النص على طول الأغراض فيكون : x1=0010

x2=1101

a=[17, 21,9,14]

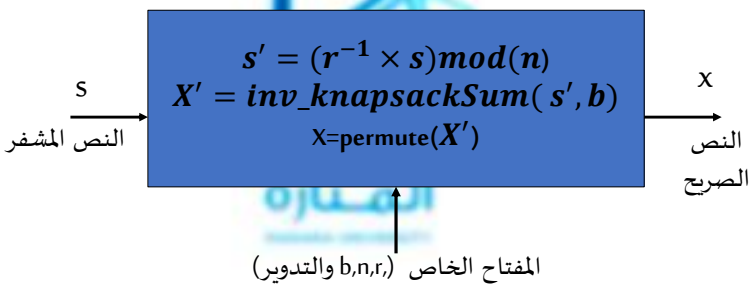
$$S1 = X_1a_1 + X_2a_2 + X_3a_3 + X_4a_4$$
$$S1 = 0.17 + 0.21 + 1.9 + 0.14 = 9$$
$$S2 = X_1a_1 + X_2a_2 + X_3a_3 + X_4a_4$$
$$S2 = 1 * 17 + 1 * 21 + 0 * 9 + 1 * 14 = 52$$

النص المشفر هو : 9 52

17

مراحل نظام تشفير حقيبة الظهر(3/4)

❖ عملية فك التشفير



المخطط الصندوقي

18

مراحل نظام تشفير حقيبة الظهر(4/4)

❖ **خطوات عملية فك التشفير:**

1. لعكس الضرب بـ r نوجد معكوس r بالنسبة لـ mod(n)

$$r^{-1} mod(n) = v$$

بحيث: $r \times v \equiv 1 mod(n)$

2. نحسب $\boldsymbol{s' = (r^{-1} \times s) mod(n)}$

3. نعكس عملية ملء الحقيبة $\boldsymbol{X' = inv\_knapsackSum(s', b)}$

أي نكتب الجداء الذي نحصل من خلاله على القيمة $\boldsymbol{s'}$ اعتماداً على b و بذلك نحصل على قيم X':

$$\boldsymbol{s' = X'_1 b_1 + X'_2 b_2 + \cdots + X'_k b_k}$$

4. ندور قيم X' وفق التدوير المفروض فنحصل على X .

19

مثال عن مرحلة فك التشفير في نظام تشفير حقيبة الظهر

1. معكوس r=7 بالنسبة لـ mod(25)

$$7^{-1} mod(25) = 18$$

بحيث: $7 \times 18\ mod(25) = 126 mod(25) = 1$

2. نحسب

$$\boldsymbol{s' = (r^{-1} \times s) mod(n) = (18 \times 31) mod 25 = 558\ mod 25 = 8}$$

3. لدينا $b = [2,3,6,12]$ فيكون $\boldsymbol{s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_k + X'_4 b_k}$

$$\boldsymbol{8 = 1 \times 2 + 0 \times 3 + 1 \times 6 + 0 \times 12}$$

فتكون قيم X': $\boldsymbol{X' = 1\ 0\ 1\ 0}$

4. ندور قيم X' وفق التدوير المفروض [3,2,4,1] فنحصل على X=1001 .

20

مقدمة عن خوارزمية RSA

❖ هي عبارة عن خوارزمية **تشفير غير متناظر**، وضعت من قبل Ronald L. **R**ivest, Adi **S**hamir and Leonard M. **A**dleman في عام1977، و هي تعتمد على عدة أسس رياضية في نظرية الأعداد.

❖ هي عبارة عن نظام تعمية كتلي دخله وخرجه

❖ دخله وخرجه عبارة عن أرقام صحيحة تتراوح قيمتها بين 0 – (n-1) من أجل قيمة لـ n ، الحجم النموذجي لـ n هي 1024 خانة ثنائية أو 309 خانة عشرية.

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

21

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 بينهما معامل مشترك سوى الواحد.

❖ **التابع** $\phi(n)$:

✓ يعرف التابع $\phi(n)$ على أنه **عدد الأعداد الأقل من** n و التي **تكون أولية فيما بينها**

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 معه بالمعامل 3فيما بينهما

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

مثال: $\phi(7)=6$

22

المخطط الصندوقي لخوارزمية RSA

23

توليد المفاتيح Key Generation

(المفتاح العام و المفتاح الخاص)

1. نختار عددين أوليين كبيرين (q ، p) 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 :

$$\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n)$$

5 .نحسب (d) :

$$d \equiv e^{-1} \bmod \phi(n) \rightarrow d \times e \equiv 1 \bmod \phi(n)$$

فيكون المفتاح العام :

$K_{pub} = \{e, n\}$

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

24

❖ عملية التعمية (encryption) : يستخدم المفتاح العام للمستقبل

النص الصريح: M<n

النص المشفر : $C = M^e \bmod(n)$

❖ عملية فك التعمية (Decryption) : يستخدم المفتاح الخاص للمستقبل

النص المشفر: C

النص الصريح: $M = C^d \bmod(n)$

25

أمن الخوارزمية RSA (1/2)

- توجد عدة هجومات نذكر منها :

➢ **الهجوم الأعمى (Brute force):**

يتضمن تجريب جميع المفاتيح الممكنة، الحل يكون باستخدام مفاتيح طويلة أي لـ e,d

➢ **الهجوم الرياضي (Mathematical Attack):**

عادة يتبع الهجوم الرياضي ما يلي: (بمعرفة المفتاح العام)

١. تحليل n إلى عددين أوليين بحيث n=p*q

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

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

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

26

مثال

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

12131072439211271897323671531612440428472427633701410925634549312301964373042085619324
19736532241686654101705736136521417171171379797429933487106282980354 1

q

12027524255478748885956220793734512128733387803682075433653899983955179850988797899869
14690080913161115334681705083209602216014636634639181247098710541523 3

مثال

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

n

14590676800758332323018693934907063529240187237535716439958187101987343879900535893836
95714026701498021218180862924674228281570229220767469065434012248896724724079269699871
00581290103199317858753663710862357656510507883714297115637342788911463535102712032765
16651841172685983798867211183720508552634661874005 3

$\phi(n)$

14590676800758332323018693934907063529240187237535716439958187101987343879900535893836
95714026701498021218180862924674228281570229220767469065434012248896483138112322799663
17301397777852365301547848273478871297222058587457152891606459269718119268971163555070
80264399952954964411681194751651393818429668352128 0

أمن الخوارزمية RSA (2/2)

- أمثلة عن كسر الخوارزمية بالهجوم الرياضي :

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

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

29

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 SSL S/MIME, ...

30

أهمية خوارزمية ديفي هيلمان(DH(Diffie-Hellman

تبادل المفتاح السري (المتناظر) بين طرفين (أليس وبوب) يكون باتباع 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، وتحصل على المفتاح المتناظر Ks
٤. يشفر كل من بوب و أليس المعلومات باستخدام المفتاح المتناظر وأية 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

31

الفكرة العامة لخوارزمية ديفي هيلمان

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

32

آلية عمل خوارزمية ديفي هيلمان لتبادل المفاتيح (1/2)

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 :

يولد بوب باستخدام قيمة XB قيمة عامة YB وفق العلاقة :

$$YB = g^{XB} mod\ P$$

٣. يرسل بوب القيمة العامة YB إلى أليس

٤. تختار أليس عدداً عشوائياً XA(خاص) بحيث:

تولد أليس باستخدام قيمة XA قيمة عامة YA وفق العلاقة :

$$YA = g^{XA} mod\ P$$

٥. ترسل أليس القيمة العامة YA إلى بوب

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

$$K = (YA)^{XB} mod\ P$$

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

$$K = (YB)^{XA} mod\ P$$

33

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

الاتفاق على قيم Pوg

أليس	بوب
تختار عدداً عشوائياً XA	يختار عدداً عشوائياً XB
تولد قيمة عامة YA وفق العلاقة : $YA = g^{XA} mod\ P$	
ترسل YA →	
	يولد قيمة عامة YB وفق العلاقة : $YB = g^{XB} mod\ P$
← يرسل YB	
تولد المفتاح السري (المتناظر) وفق العلاقة: $K = (YB)^{XA} mod\ P$	يولد المفتاح السري (المتناظر) وفق العلاقة: $K = (YA)^{XB} mod\ P$

34

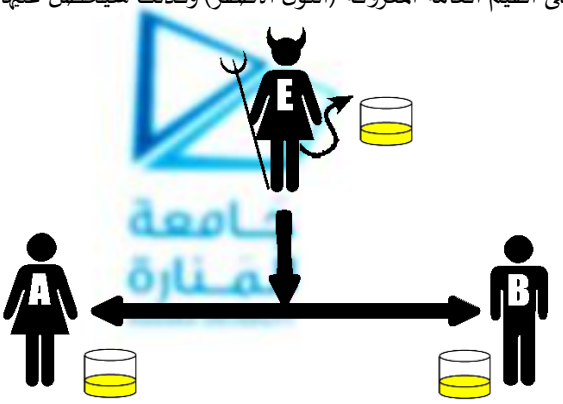
أمن خوارزمية ديفي هيلمان لتبادل المفاتيح (1/6)

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

35

أمن خوارزمية ديفي هيلمان لتبادل المفاتيح (2/6)

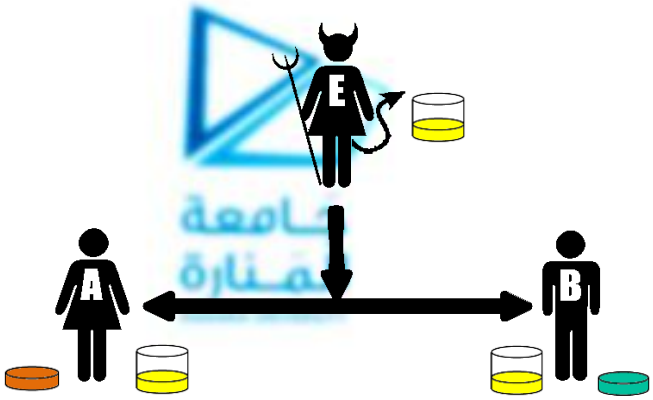
سيتفق كلاهما على القيم العامة المعروفة (اللون الأصفر) وكذلك سيحصل عليها المهاجم



36

أمن خوارزمية ديفي هيلمان لتبادل المفاتيح (3/6)

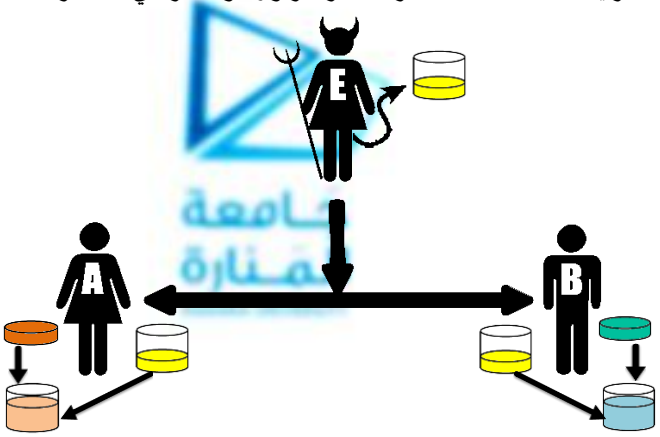
يختار كل من الطرفين قيمة سرية (اللون الأخضر لبوب، اللون البرتقالي لأليس)، لا يمكن للمهاجم معرفة أي منهما



37

أمن خوارزمية ديفي هيلمان لتبادل المفاتيح (4/6)

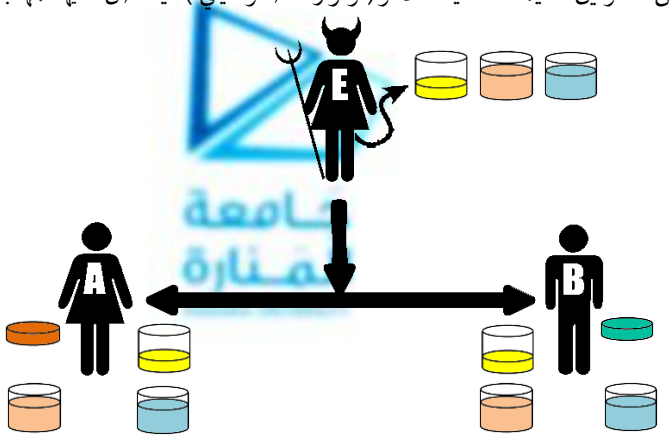
يولد كل من الطرفين قيمة علنية (أخضر +أصفر =تركواز لبوب، برتقالي +أصفر =أصفر طيني لأليس)



38

أمن خوارزمية ديفي هيلمان لتبادل المفاتيح (5/6)

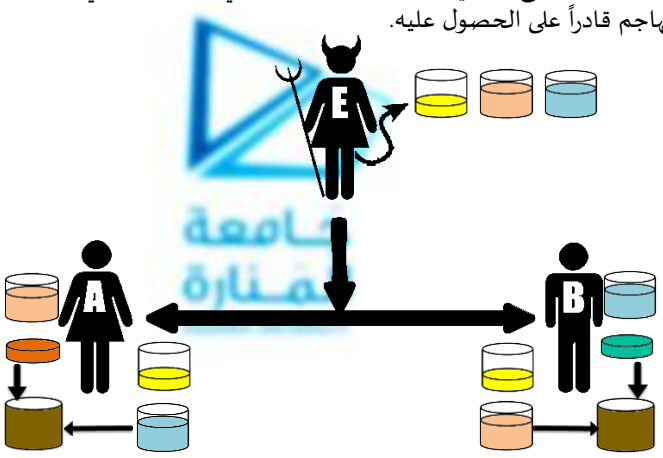
يرسل كل من الطرفين القيمة العلنية للآخر (تركواز، أصفر طيني) فيحصل عليها المهاجم



39

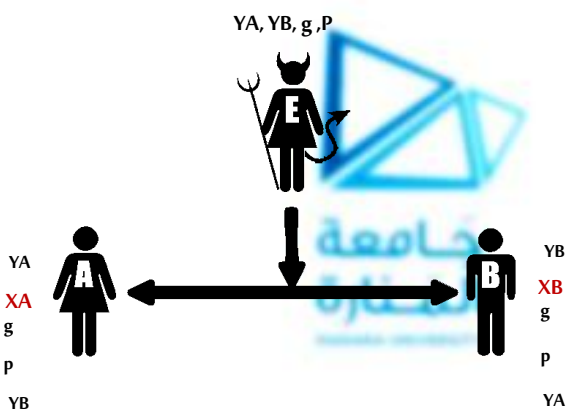
أمن خوارزمية ديفي هيلمان لتبادل المفاتيح (6/6)

يولد كل من الطرفين المفتاح السري لهما بمفرده (أصفر طيني+ أخضر=عفني ، التركواز + برتقالي =عفني) لن يكون المهاجم قادراً على الحصول عليه.



40

أمن خوارزمية ديفي هيلمان لتبادل المفاتيح رياضياً



$$XA = log_g(Y_A mod P)$$

$$XB = log_g(Y_B mod P)$$

من الصعب جداً جداً الحصول على القيم السرية من القيم العلنية

لايمكن للمهاجم الحصول على المفتاح السري أو توليده

41