جامعة المنارة

كلية الهندسة

قسم المعلوماتية

أمن المعلومات

مدرسة المقرر

د.بشرى علي معلا

عناوين المحاضرة الثانية

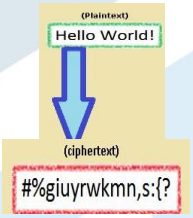
- ما المقصود بعلم التعمية؟
- مفاهيم أساسية
- خوارزميات التشفير
  - خوارزميات التشفير المتناظر
  - خوارزميات التشفير غير المتناظر

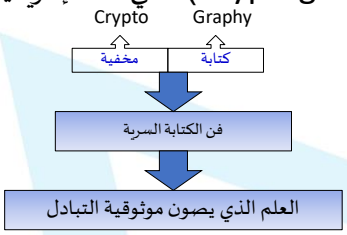
مقدمة في علم التعمية cryptology (1/2)

❖ هو العلم الذي يبحث في عمليتي التعمية (Cryptography) وتحليل التعمية (Cryptanalysis)

➢ **عملية التعمية (Cryptography):**

✓ كلمة (Cryptography) هي كلمة إغريقية مكونة من مقطعين :





✓ هدف التعمية :جعل الاتصال بين طرفين آمناً، بحيث لا يستطيع أي طرف ثالث اختراق هذا الاتصال أو فهم الموضوع الذي يدور حوله الاتصال

مقدمة في علم التعمية cryptology (2/2)

❖ هو العلم الذي يبحث في عمليتي التعمية (Cryptography) وتحليل التعمية (Cryptanalysis)

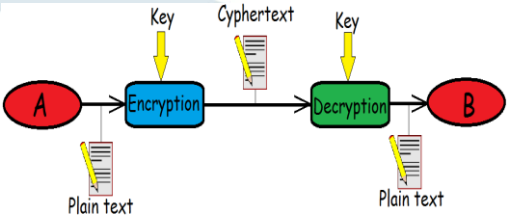
➢ تحليل التعمية (Cryptanalysis):

✓ فن كسر تشفير الرسائل المشفرة

- استغلال مميزات الخوارزمية بهدف محاولة استنتاج الرسالة الأصلية أو المفتاح المستخدم
- تجريب جميع المفاتيح الممكنة على جزء من النص المشفر للحصول على النص الأصلي

✓ هدف عملية تحليل التعمية **إيجاد نقاط ضعف خوارزمية التشفير المطبقة**، والعمل على كسرها، أي العمل على كسر التعمية.

مفاهيم أساسية في علم التعمية(1/2)



- **النص الصريح (Plain text):** هو الرسالة / المعلومات الأصلية.
- **النص المشفر (Cipher text):** هو الرسالة / المعلومات المشفرة.
- **المفتاح (key):** المعلومات السرية التي تستخدم مع خوارزمية التشفير لإنتاج النص المشفر من النص الأصلي.
- **التشفير (encryption) :**هو يمثل عملية تحويل النص الأصلي الواضح إلى نص مشفر مبهم .
- **فك التشفير (Decryption) :**هو يمثل عملية تحويل النص المشفر المبهم إلى شكله الأصلي الواضح .

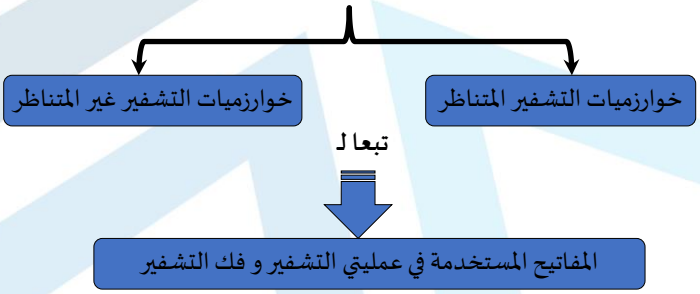
مفاهيم أساسية في علم التعمية(2/2)

- الخوارزمية الآمنة حسابياً : هي الخوارزمية التي تحقق الشرطين الآتيين:
  - ✓ كلفة كسر النص المشفر تفوق قيمة المعلومات المشفرة.
  - ✓ الزمن اللازم لكسر النص المشفر يفوق الفترة المفيدة من حياة المعلومات.

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/μs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

خوارزميات التعمية/التشفير

❖ تقسم إلى:



مفهوم خوارزميات التشفير المتناظر (1/2)
(Symmetric Encryption Algorithms)

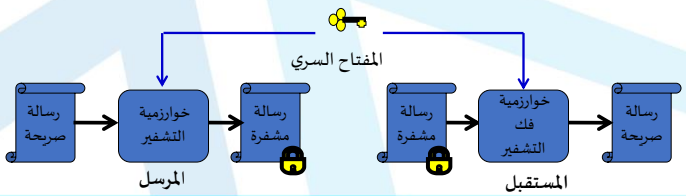
❖ **تعريفها :**

هي الخوارزميات التي تستخدم المفتاح نفسه لعمليتي التشفير وفك التشفير.

يسمى هذا المفتاح بالمفتاح السري Secret Key

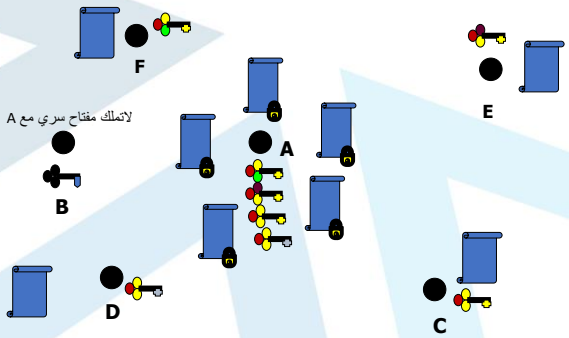
✓ يشترك المرسل والمستقبل بهذا المفتاح

✓ يستخدم المرسل هذا المفتاح لتشفير الرسالة ويستخدمه المستقبل لفك تشفير الرسالة



مفهوم خوارزميات التشفير المتناظر (2/2)
(Symmetric Encryption Algorithms)

➢ مثال:



أنواع خوارزميات التشفير المتناظر (1/2)

تقسم خوارزميات التشفير المتناظر من حيث التعامل مع النص المطلوب تشفيره إلى نوعين هما :

١. خوارزميات التشفير الكتلي (Block Cipher)

٢. خوارزميات التشفير التسلسلي (Stream Cipher)

أنواع خوارزميات التشفير المتناظر (2/7)

١. خوارزميات التشفير الكتلي (Block Cipher):

يقسم النص الصريح إلى كتل (بلوكات) ذات طول ثابت (عادة 64 بت) ومن ثم تشفر كتلةً كتلةً.

- مثال : خوارزمية DES (حيث يكون طول المفتاح 56 بت، على طول الكتلة ذات الـ 64 بت)
- وهناك أيضاً:..... AES (Advanced Encryption Standard)
- يوجد خمسة أنماط لعمليات التشفير الكتلي هي :

ECB = Electronic CodeBook mode

CBC = Cipher Block Chaining mode

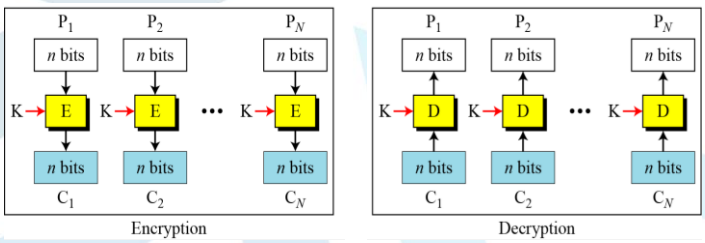
CFB = cipher feedback mode

OFB = output feedback mode

CTR = counter mode

ECB = Electronic Code Book mode

➢ تشفر فيه كل كتلة معطيات بشكل مستقل عن الكتلة التي قبلها أو بعدها



$C_i = E_K(P_i)$ حيث:K هو المفتاح السري

n طول الكتلة

$P_i = D_K(C_i)$

ECB = Electronic CodeBook mode

إيجابياته:

- ✓ القدرة على تشفير عدة كتل على التوازي في آن واحد.
- ✓ أخطاء الارسال محصورة بكل كتلة بشكل منعزل عن باقي الكتل
- ✓ بساطته

سلبياته:

- ✓ ضعيف تجاه هجوم تحليل الحركية (traffic analysis)

حيث أن تشفير الكتلة التي تحتوي معطيات ثابتة يعطي في كل مرة نفس الكتلة المشفرة باستخدام نفس المفتاح المتناظر مما يسهل كسر التشفير في حال وجود كتلتين متماثلتين

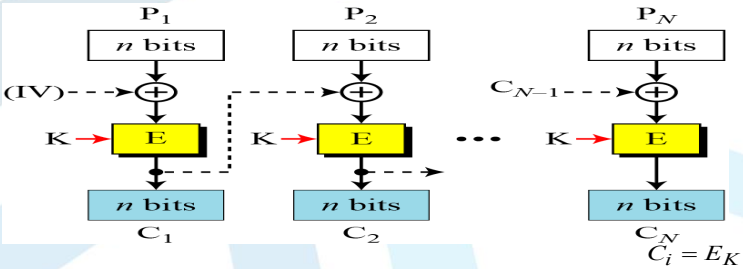
تطبيقاته:

- ✓ تأمين إرسال المعلومات قصيرة مثلاً إرسال مفتاح مؤقت

CBC = Cipher Block Chaining mode

يعد النمط الأكثر شيوعاً

ينتج النص المشفر عن تشفير ناتج عملية XOR بين الكتلة المشفرة السابقة والنص الصريح للكتلة الحالية.



$$C_i = E_K(C_{i-1} \oplus P_i)$$
$$C_0 = IV$$

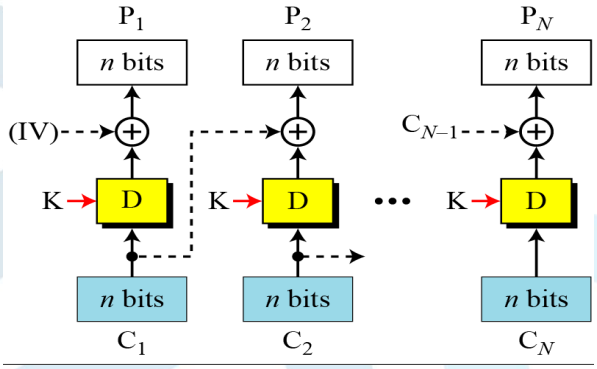
حيث IV هو شعاع تهيئة يستخدم لبدء العملية

جَـامعة

CBC = Cipher Block Chaining mode

➢تنفذ عملية فك التشفير بطريقة معاكسة

$$P_i = C_{i-1} \oplus D_K(C_i)$$
$$C_0 = IV$$



ملا حظة: إن قيمة شعاع التهيئة IV إما أن يكون قد اتفق عليها سابقاً بين المرسل والمستقبل أو يمكن أن تكون قيمة ثابتة أومرسلة مشفرة باستخدام النمط ECB .

جَـامعة المَـنارة

CBC = Cipher Block Chaining mode

➢**إيجابياته:**

✓ أكثر مقاومة لهجوم تحليل الحركة من النمط السابق.

➢**سلبياته:**

✓ إن حدوث خطأ في بت واحد في إحدى الكتل قد يؤثر على كل الكتل و يعطي نص مشفر خاطئ و بالنتيجة نص صريح خاطئ

➢**تطبيقاته:**

✓ كل عمليات الارسال التي تعتمد على إرسال كتل

CTR = COUNTER Mode

➢ **الفكرة الأساسية :**

بدلاً من تشفير البيانات مباشرة، يُشفر العداد (counter) مع NONCE من ثم يستخدم الناتج لتشفير البيانات باستخدام الـXOR .

➢ **المكونات الأساسية:**

- ✓ **المفتاح (K)**:المفتاح السري المشترك بين المرسل والمستقبل.
- ✓ **العداد (Counter)**: قيمة عداد تزيد بشكل منتظم (قد يبدأ من الصفر أو الواحد)
- ✓ **Nonce (Number Used Once)**: قيمة عشوائية أو شبه عشوائية **يجب أن تكون فريدة** لكل رسالة

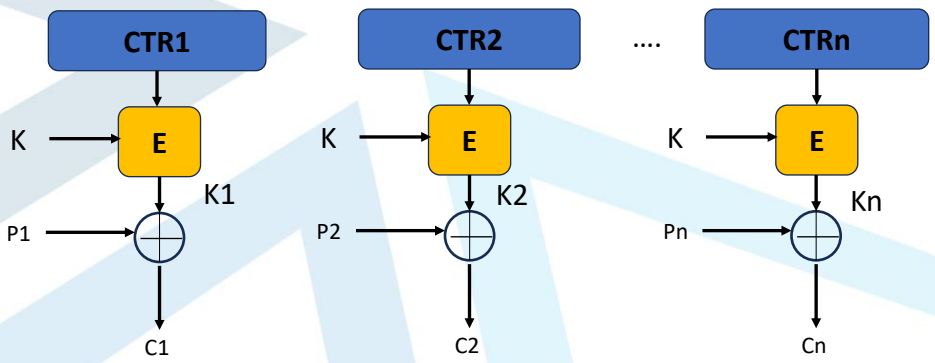
CTR = COUNTER Mode

➢ **عملية التشفير**

تدمج قيمة العداد مع قيمة الـ NONCE بحيث . **CTR_i = Nonce || (Counter_Value + i)**

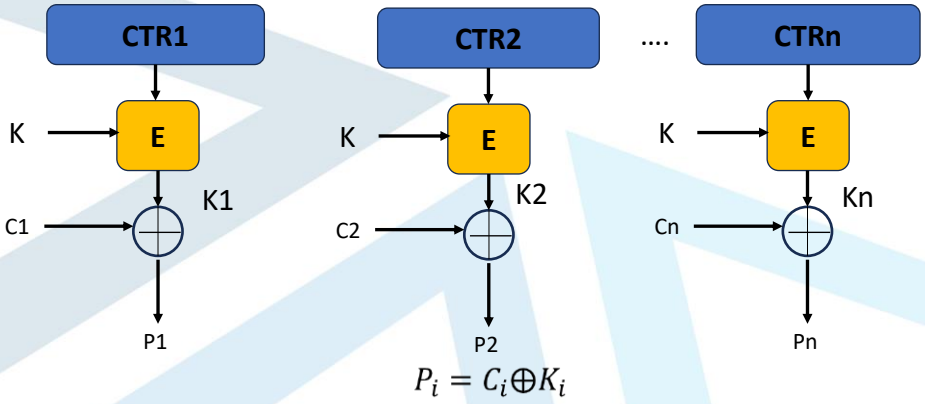
$K_i = E(K, CTR_i)$

$C_i = P_i \oplus K_i$



CTR = COUNTER Mode

➢ عملية فك التشفير



$$P_i = C_i \oplus K_i$$

CTR = COUNTER Mode

➢ إيجابياته:

- ✓ يعمل على التوازي
- ✓ لا يحتاج غالباً إلى حشو (padding) لأنها إذا كانت الكتلة الأخيرة من البيانات غير مكتملة، فإننا ببساطة نستخدم جزء **فقط** من Ki المفتاح المقابل لها لعملية XOR هذا ويوفر مساحة.
- ✓ يستخدم عملية التشفير فقط وهذا يجعل تطبيقه أقل تعقيداً

➢ سلبياته:

- ✓ ضعيف تجاه هجوم التحليل الإحصائي ، يظهر في حال أعيد استخدام الزوج (counter, nonce)
  - إذا كان لدينا: $C_1 = P_1 \text{ XOR } KS$ و$C_2 = P_2 \text{ XOR } KS$
  - فإن المهاجم يمكنه ببساطة حساب:

$$C_1 \text{ XOR } C_2 = (P_1 \text{ XOR } KS) \text{ XOR } (P_2 \text{ XOR } KS) = P_1 \text{ XOR } P_2$$

- معرفة $P_1 \text{ XOR } P_2$ تعطي المهاجم معلومات كبيرة ويمكنه، باستخدام تحليل إحصائي، استعادة أجزاء من النصين الأصليين.

➢ تطبيقاته:

- ✓ تشفير البيانات على التوازي

أنواع خوارزميات التشفير المتناظر (2/2)

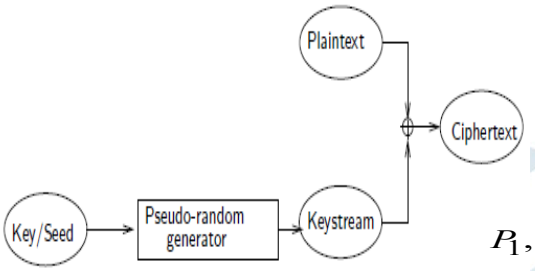
جامعة المنارة

٢. خوارزميات التشفير التسلسلي (Stream Cipher):

تكون فيها الكتلة ذات بعد صغير جداً (1 Octet, 1 Bit)

الخوارزميات الأكثر استخداماً ضمن هذا النوع:

- RC4: Ron Rivest 1987



✓ أساسيات التشفير التسلسلي (Stream Cipher)

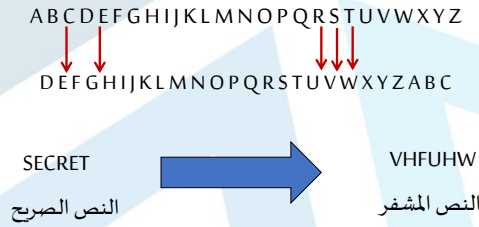
- عملياً ، يعالج النص الصريح بايت بايت
- لذا سيكون النص الصريح عبارة عن سلسلة من البايتات: $P_1, P_2, P_3, \ldots\ldots$
- يستخدم المفتاح K كقيمة لتوليد سلسلة من المفاتيح: $k_1, k_2, k_3, \ldots\ldots$
- يكون النص المشفر هو: $C_1, C_2, C_3, \ldots\ldots$
- حيث تعرف عملية التشفير كالآتي: $C_i = P_i \oplus k_i$
- تختلف خوارزميات التشفير التسلسلي عن بعضها البعض بطريقة توليد سلسلة المفاتيح

جامعة

مثال عن التشفير التسلسلي (Stream Cipher)

شيفرة قيصر (Caesar Cipher)

تعتمد شيفرة قيصر على استبدال كل حرف من الحروف الأبجدية بالحرف الذي يقع في المرتبة الثالثة بعده.



مثال عن التشفير التسلسلي (Stream Cipher)

شيفرة قيصر(Caesar Cipher)

مثال: بفرض أننا نريد فك تشفير النص المشفر MUUJPUH باستخدام شيفرة قيصر علماً أن المفتاح يساوي 6 .

G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

MUUJ PUH
النص المشفر

GOOD JOB
النص الصريح

مثال عن التشفير التسلسلي (Stream Cipher)

شيفرة قيصر(Caesar Cipher)

مثال: بفرض أننا نريد تشفير الرسالة الصريحة GOOD JOB باستخدام شيفرة قيصر علماً أن المفتاح يساوي 6 .

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

G H I J K L M N O P Q R S T U V W X Y Z **A B C D E F**

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

G H I J K L M N O P Q R S T U V W X Y Z A B C D E F

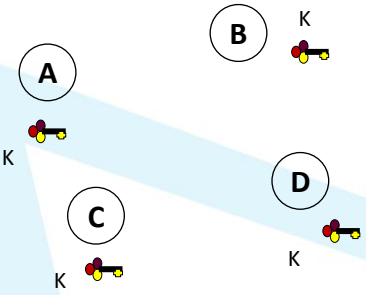
GOOD JOB
النص الصريح

MUUJ PUH
النص المشفر

أنواع خوارزميات التشفير المتناظر

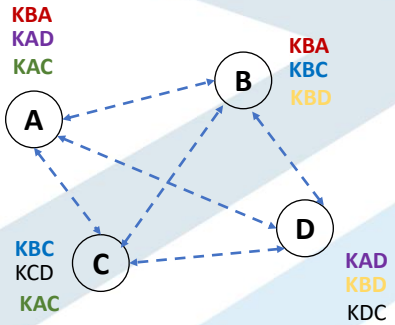
❖ تشفير متناظر تقليدي

✓ كل العقد الشرعية تملك نفس المفتاح



❖ تشفير متناظر الثنائي

✓ مفتاح سري مشترك لكل عقدتين.



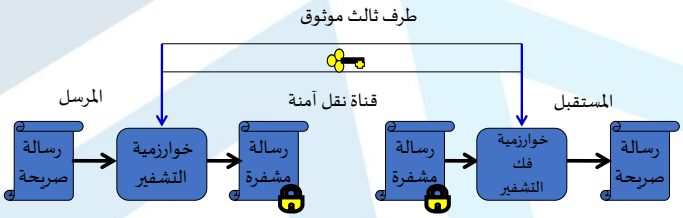
مصدر المفتاح السري في خوارزميات التشفير المتناظر

❖ يتم الحصول على المفتاح السري :

✓ إما أن يخزن في المرسل والمستقبل في مرحلة تهيئة الشبكة

✓ إما أن يرسل من المرسل إلى المستقبل في قناة محمية

✓ إما أن يوزع إلى كل من المرسل والمستقبل من قبل طرف ثالث في قناة محمية



<-- لذا لا ينجح استخدام مثل هذه الخوارزميات في التجارة الالكترونية عبر الانترنت

التعبير الرياضي عن خوارزميات التشفير المتناظر(1/2)

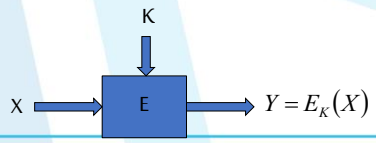
✓ يعبر عن **عملية التشفير** باستخدام المفتاح السري K كما يلي:

$$Y = E_K(X)$$

حيث:

Y:النص المشفر X:النص الصريح

و تقرأ: Y هو عبارة عن الرسالة المشفرة الناتجة من تشفير الرسالة X بتطبيق خوارزمية التشفير E باستخدام المفتاح السري K

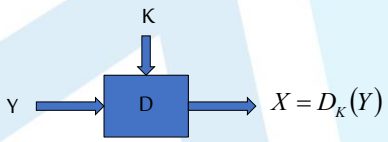


التعبير الرياضي عن خوارزميات التشفير المتناظر(2/2)

✓ يعبر عن **عملية فك التشفير** باستخدام المفتاح السري K كما يلي:

$$X = D_K(Y)$$

و تقرأ: X هي عبارة عن الرسالة الصريحة الناتجة من فك تشفير الرسالة Y بتطبيق خوارزمية فك التشفير D باستخدام المفتاح السري K



مفهوم خوارزميات التشفير غير المتناظر (Asymmetric Encryption Algorithms)

- ✓ **تعريفها:**

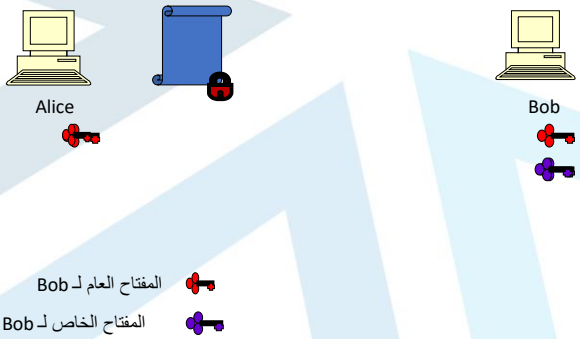
هي الخوارزميات التي تستخدم زوجاً من المفاتيح، مفتاح عام (Public Key) و مفتاح خاص (Private Key) ،يستخدم أحدهما للتشفير والثاني لفك التشفير .

- ✓ تسمى أيضاً خوارزميات المفتاح العام (Public Key)
- ✓ **المفتاح العام (Public key):** هو المفتاح الذي يكون معلوماً من قبل جميع عقد الشبكة الشرعيين ويستخدم من قبل أي منها لتشفير الرسائل المرسلة إلى مالك هذا المفتاح. نرمز له بـ K_{pub}
- ✓ **المفتاح الخاص (Private key):** هو المفتاح الذي تحتفظ به العقدة بشكل سري، أي يكون معلوماً من قبلها فقط ، يستخدم هذا المفتاح لفك تشفير الرسائل التي ترسل إليها مشفرة باستخدام مفتاحها العام. نرمز له بـ K_{pri}
- ✓ تتعلق صعوبة كسر هذا النوع من الخوارزميات بصعوبة استخلاص المفتاح الخاص من المفتاح العام.
- ✓ يستخدم هذا النوع عادة لإرسال المفتاح السري الذي يستخدم لتشفير البيانات.
- ✓ لكن ينتج هذا النوع حملاً حسابياً عالٍ مقارنة بالخوارزميات المتناظرة

خطوات عمل الخوارزميات التشفير غير المتناظر (1/2)

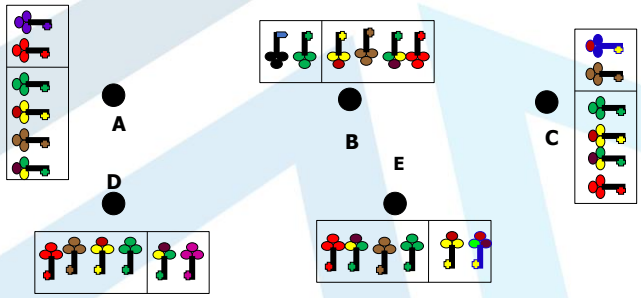
- يولد /يخزن كل مستخدم زوجاً من المفاتيح (مفتاح عام و مفتاح خاص) لاستخدامه في التشفير وفك التشفير
- يضع كل مستخدم أحد المفاتيح (هو المفتاح العام) في ملف ما يمكن الدخول إليه من قبل الجميع. أما الآخر فهو المفتاح الخاص به ،و الذي يحتفظ به لنفسه فقط
- إذا أراد مستخدم ما (A) إرسال رسالة آمنة لمستخدم آخر (B): سيشفرها المستخدم (A) مستخدماً المفتاح العام للمرسل إليه(B)
- عند استقبال المستقبل B للرسالة، سيفك التشفير مستخدماً مفتاحه الخاص

خطوات عمل الخوارزميات التشفير غير المتناظر (2/2)



مثال عن خوارزميات التشفير غير المتناظر (1/2)
(Asymmetric Encryption Algorithms)

✓ **مثال:** شبكة مكونة من N = 5 عقد. كل عقدة تختزن N+1 مفتاح أي 6 مفاتيح



مثال عن خوارزميات التشفير غير المتناظر (2/2)
(Asymmetric Encryption Algorithms)

✓ **مثال:** شبكة مكونة من N = 5 عقد. كل عقدة تختزن N+1 مفتاح أي 6 مفاتيح

العقدة	زوج المفاتيح المختزنة	المفاتيح الإضافية المخزنة
A	(K_{Pub_A}, K_{Pri_A})	$\{K_{Pub\_B}, K_{Pub\_C}, K_{Pub\_D}, K_{Pub\_E}\}$
B	(K_{Pub_B}, K_{Pri_B})	$\{K_{Pub\_C}, K_{Pub\_E}, K_{Pub\_A}, K_{Pub\_D}\}$
C	(K_{Pub_C}, K_{Pri_C})	$\{K_{Pub\_B}, K_{Pub\_E}, K_{Pub\_A}, K_{Pub\_D}\}$
D	(K_{Pub_D}, K_{Pri_D})	$\{K_{Pub\_B}, K_{Pub\_C}, K_{Pub\_A}, K_{Pub\_E}\}$
E	(K_{Pub_E}, K_{Pri_E})	$\{K_{Pub\_B}, K_{Pub\_C}, K_{Pub\_A}, K_{Pub\_D}\}$

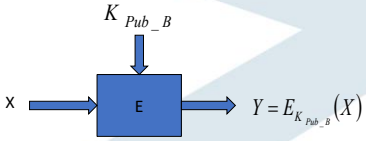
التعبير الرياضي عن خوارزميات التشفير غير المتناظر

✓ إذا فرضنا السيناريو الآتي:

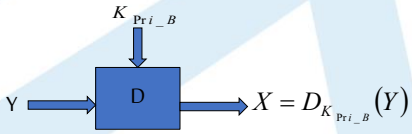
تريد عقدة A أن ترسل إلى العقدة B رسالة ما (X) بشكل آمن باستخدام خوارزمية تشفير غير متناظر .

عندها :

١. يشفر المرسل A الرسالة باستخدام المفتاح العام لـ B أي: $Y = E_{K_{Pub\_B}}(X)$



٢. عندما تستقبل العقدة B الرسالة تفك تشفير الرسالة باستخدام مفتاحها الخاص أي: $X = D_{K_{Pri\_B}}(Y)$



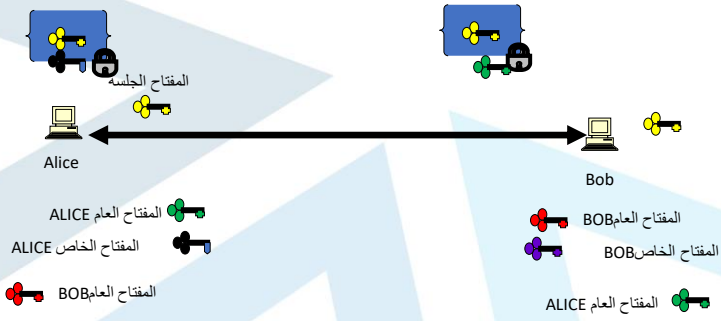
أهم تطبيقات خوارزميات التشفير غير المتناظر

- التعمية/ فك التعمية: يستخدم المرسل المفتاح العام للمستقبل في التشفير، و يستخدم المستقبل مفتاحه الخاص في فك التشفير.
- تبادل المفاتيح : يقوم الطرفان بتبادل مفتاح الجلسة (المفتاح السري للجلسة). يستخدم لذلك المفتاح الخاص لأحدهما أو لكليهما.
- تحقيق المصادقة (التوقيع الرقمي) : يستخدم المرسل مفتاحه الخاص ليوقع على الرسالة، مما يؤكد هوية المرسل كونه الوحيد الذي يملك هذا المفتاح.

تبادل المفاتيح باستخدام خوارزمية التشفير غير المتناظر

- عندما تريد أليس إرسال مفتاح الجلسة إلى بوب مستخدمة خوارزمية تشفير غير متناظر ستقوم بالآتي:
  - ✓ تشفر مفتاح الجلسة باستخدام مفتاحها الخاص
  - ✓ يستقبل بوب الرسالة المشفرة
  - ✓ يفك التشفير باستخدام المفتاح العام لأليس

تبادل المفاتيح باستخدام خوارزمية التشفير غير المتناظر

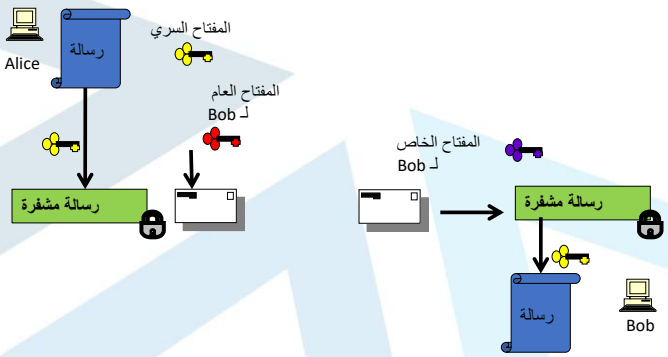


تحقق المصادقة باستخدام خوارزمية التشفير غير المتناظر

يستخدم المرسل المفتاح الخاص لتشفير الرسالة، يمكن فك تشفير هذه الرسالة باستخدام المفتاح العام المطابق فقط. هكذا يتأكد المستقبل من أن المرسل هو حقاً من أرسل الرسالة كونه الوحيد الذي يملك المفتاح الخاص

مثلاً:

استخدام الخوارزميات المتناظرة وغير المتناظرة معاً(1/2)



استخدام الخوارزميات المتناظرة وغير المتناظرة معاً(2/2)

- ✓ تريد أليس أن ترسل رسالة مشفرة إلى بوب
- ✓ تشفر أليس الرسالة باستخدام المفتاح السري للجلسة بينها وبين بوب فتنتج **الرسالة مشفرة ١**
- ✓ تشفر أليس **الرسالة مشفرة ١** باستخدام المفتاح العام لبوب فينتج **الرسالة المشفرة ٢** و ترسلها
- ✓ يستقبل بوب الرسالة المشفرة الأخيرة ، لكي يحصل على محتوى الرسالة يقوم بالخطوات:
  - يفك تشفير الرسالة المستقبلة باستخدام مفتاحه الخاص فتنتج الرسالة المشفرة ١
  - يفك تشفير الرسالة المشفرة ١ باستخدام مفتاح الجلسة الرسالة الصريحة

جَامعة المَنارة
MANARA UNIVERSITY

نهاية المحاضرة الثانية