جامعة المنارة الخاصة
كلية الهندسة
هندسة الروبوت والأنظمة الذكية

مهارات الحاسوب

Computer Skills UNRC101

مدرس المقرر
أ.د. مثنى علي القبيلي

الفصل الدراسي الأول | الاثنين 28/11/2022 | العام الدراسي 2022-2023

عناوين المحاضرة

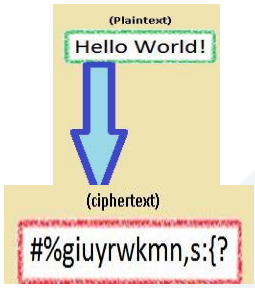
- ما المقصود بعلم التعمية؟
- مفاهيم أساسية
- خوارزميات التشفير
  - ✓ خوارزميات التشفير المتناظر
  - ✓ خوارزميات التشفير غير المتناظر

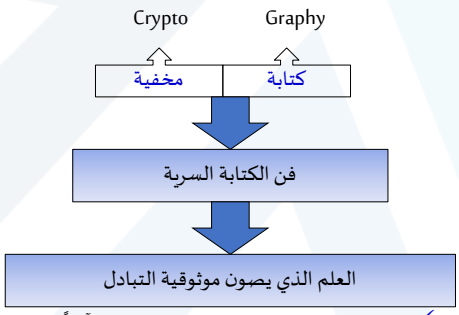
مقدمة في علم التعمية cryptology (1/2)

❖ 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):

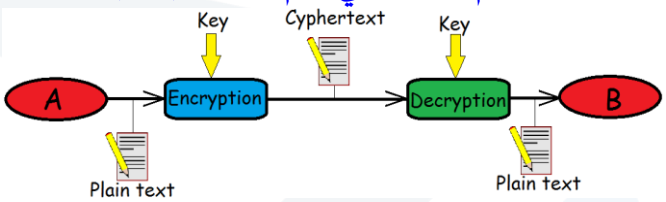
✓ فن كسر تشفير الرسائل المشفرة

- 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:

- خوارزميات التشفير المتناظر
- خوارزميات التشفير غير المتناظر

تبعا لـ

المفاتيح المستخدمة في عمليتي التشفير و فك التشفير

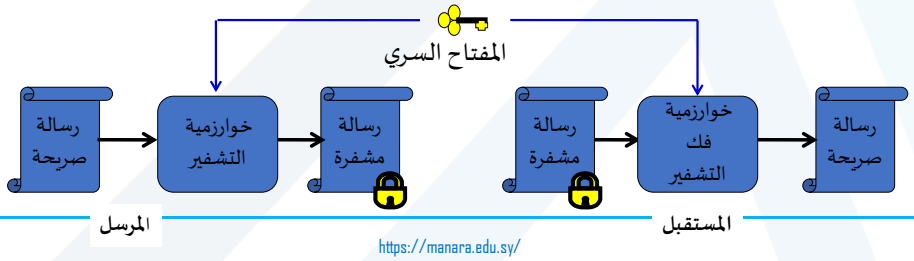
خوارزميات التشفير المتناظر (1/7)
(Symmetric Encryption Algorithms)

✓ **تعريفها :**

هي الخوارزميات التي تستخدم المفتاح نفسه لعمليتي التشفير وفك التشفير.
يسمى هذا المفتاح بالمفتاح السري Secret Key

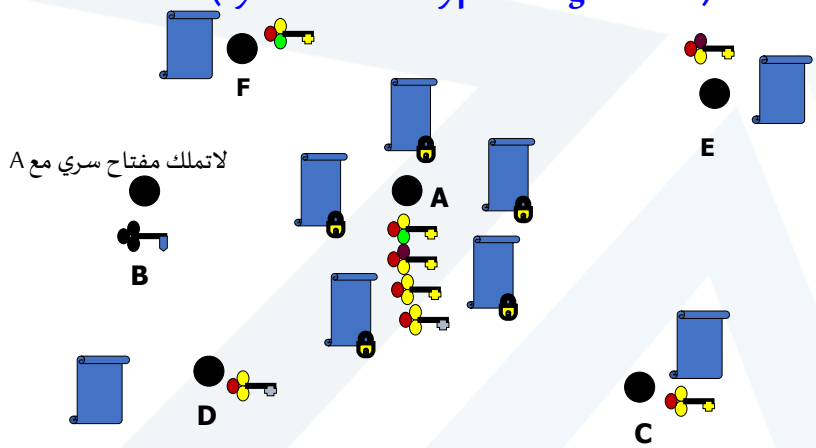
✓ يشترك المرسل والمستقبل بهذا المفتاح

✓ يستخدم المرسل هذا المفتاح لتشفير الرسالة ويقوم المستقبل باستخدامه لفك تشفير الرسالة



خوارزميات التشفير المتناظر (2/7)
(Symmetric Encryption Algorithms)

➢ مثال:



خوارزميات التشفير المتناظر (3/7)
(Symmetric Encryption Algorithms)

✓ يوجد نوعان:

1. 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 الـ64 بت)
- وهناك أيضاً:..... AES (Advanced Encryption Standard)
- يوجد خمسة أنماط لعمليات التشفير الكتلي هي :

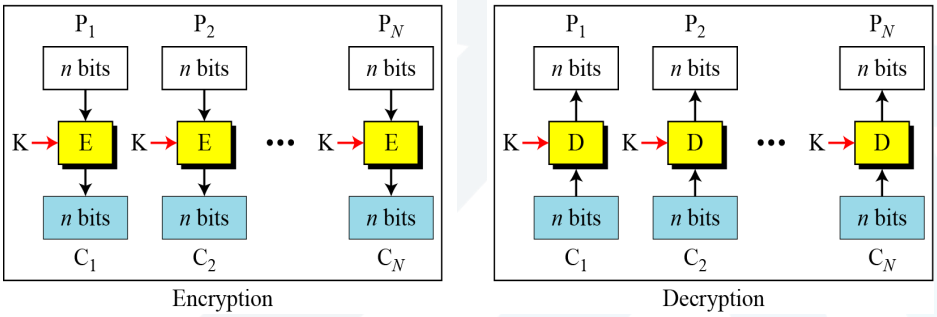
أنماط التشفير الكتلي

❖ يوجد عدة أنماط لعملية للتشفير الكتلي هي:

- ECB = electronic codebook mode
- CBC = cipher block chaining mode
- CFB = cipher feedback mode
- OFB = output feedback mode
- CTR = counter mode

ECB = electronic codebook 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)

إذ 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

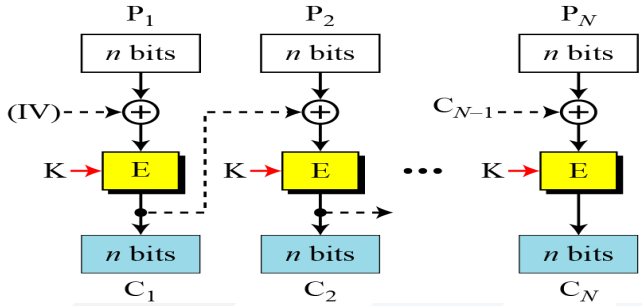
➢ تطبيقاته:

- ❑ تأمين إرسال المعلومات القصيرة مثلاً إرسال مفتاح مؤقت.

CBC = cipher block chaining mode

➢ يعد النمط الأكثر شيوعاً

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



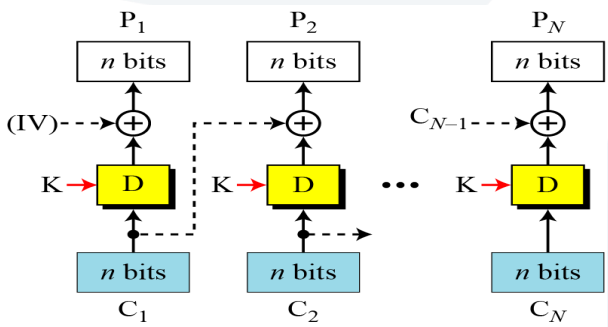
$$C_i = E_K(C_{i-1} \oplus P_i)$$
$$C_0 = IV$$

حيث IV هو شعاع تهيئة يستخدم لبدء العملية

CBC = cipher block chaining mode

➢عملية فك التشفير تتم بطريقة معاكسة

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



ملاحظة: 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 .

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 نصاً مشفراً خاطئاً وبالنتيجة نصاً صريحاً خاطئاً

➢تطبيقاته:

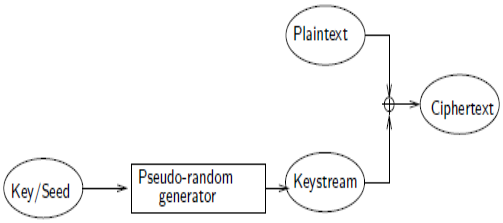
❑كل عمليات الارسال التي تعتمد على إرسال كتل

خوارزميات التشفير المتناظر (4/7)

(Symmetric Encryption Algorithms)

✓ يوجد نوعان:

2. خورازميات التشفير التسلسلي (Stream Cipher):



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

الخوارزميات الأكثر استخداماً ضمن هذا النوع :

- Ron Rivest 1987 :RC4
- SEAL(Software Encryption Algorithm) :
Don Coppersmith and Phillip Rogaway ,IBM 1993

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

مثال عن التشفير التسلسلي (Stream Cipher)

شيفرة قيصر

يتم في هذه الطريقة تبديل كل حرف من حروف الأبجدية بالحرف الذي يقع في المرتبة الثالثة بعده.

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

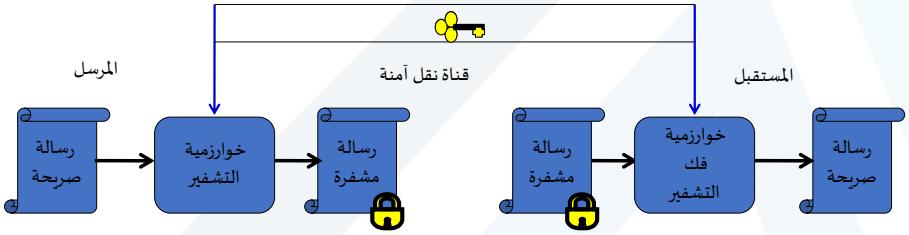
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

النص الصريح		النص المشفر
SECRET	→	VHFUHW

خوارزميات التشفير المتناظر (5/7)
(Symmetric Encryption Algorithms)

✓ يتم الحصول على المفتاح السري :

- ❑ إما أن يتم تخزينه في المرسل والمستقبل في مرحلة تهيئة الشبكة
- ❑ إما أن يتم إرساله من المرسل إلى المستقبل في قناة محمية
- ❑ إما أن يتم توزيعه إلى كل من المرسل والمستقبل من قبل طرف ثالث في قناة محمية



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

خوارزميات التشفير المتناظر (6/7)
(Symmetric Encryption Algorithms)

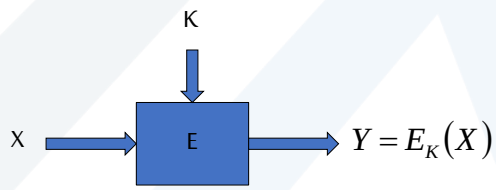
✓ يعبر عن عملية التشفير باستخدام المفتاح السري K كما يلي:

$$Y = E_K(X)$$

حيث: X:الرسالة / النص الصريح

Y:الرسالة / النص المشفرة

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

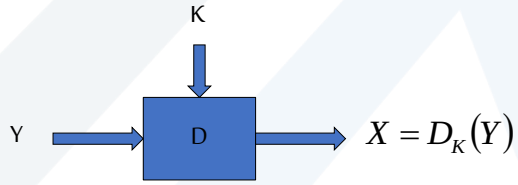


خوارزميات التشفير المتناظر (7/7)
(Symmetric Encryption Algorithms)

✓ 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 Yبتطبيق خوارزمية فك التشفير D باستخدام المفتاح السري K



خوارزميات التشفير غير المتناظر (1/8)
(Asymmetric Encryption Algorithms)

✓ **تعريفها:**

هي الخوارزميات التي تستخدم زوجاً من المفاتيح, مفتاح عام (Public Key) و مفتاح خاص (Private Key) ,
يتم استخدام أحدهما للتشفير والثاني لفك التشفير .
تسمى أيضاً خوارزميات المفتاح العام (Public Key)

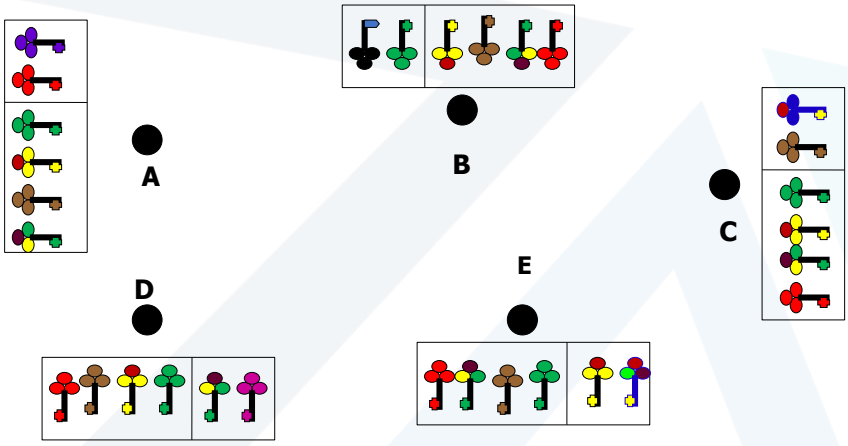
✓ **المفتاح العام (Public key):** و هو المفتاح الذي يكون معلوماً من قبل جميع عقد الشبكة ويستخدم من قبل أي منها لتشفير الرسائل المرسلة إلى مالك هذا المفتاح. نرمز له بـ K_{pub}

✓ **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 تم تشفيرها بالمفتاح العام المقابل له.
نرمز له بـ K_{pri}

ملاحظة: تتعلق صعوبة كسر هذا النوع من الخوارزميات بصعوبة استخلاص المفتاح الخاص من المفتاح العام.

خوارزميات التشفير غير المتناظر (2/8)
(Asymmetric Encryption Algorithms)

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

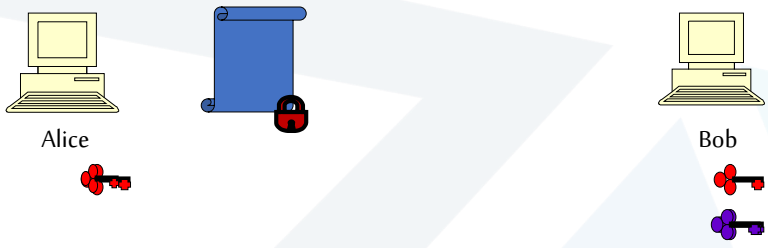


خوارزميات التشفير غير المتناظر (3/8)
(Asymmetric Encryption Algorithms)

✓ **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})	$\{K_{Pub_B}, K_{Pub_C}, K_{Pub_A}, K_{Pub_D}\}$

خوارزميات التشفير غير المتناظر (4/8)
(Asymmetric Encryption Algorithms)



المفتاح العام لـ Bob

المفتاح الخاص لـ Bob

خوارزميات التشفير غير المتناظر (5/8)
(Asymmetric Encryption Algorithms)

- ✓ يعتمد مستوى أمن هذه الخوارزميات على صعوبة استخلاص المفتاح الخاص من المفتاح العام وبالتالي صعوبة استخلاص النص الصريح من النص المشفر

- ✓ لكن ينتج هذا النوع حملاً حسابياً عالٍ مقارنة بالخوارزميات المتناظرة
  --> غير مناسب لعدد كبير من التطبيقات

- ✓ يتم استخدام هذا النوع عادة لإرسال المفتاح المتجانس السري الذي يستخدم لتشفير البيانات.

خوارزميات التشفير غير المتناظر (6/8)
(Asymmetric Encryption Algorithms)

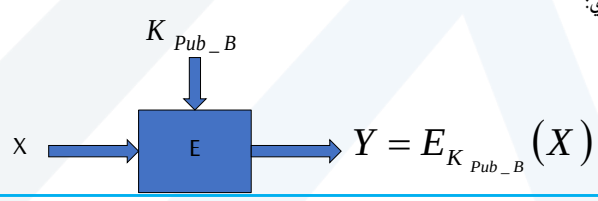
- ✓ إذا فرضنا السيناريو الآتي:

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

عندها : 1. يقوم المرسل A بتشفير الرسالة باستخدام المفتاح العام لـB

$$Y = E_{K_{Pub_B}}(X)$$

أي:



خوارزميات التشفير غير المتناظر (7/8)
(Asymmetric Encryption Algorithms)

✓ إذا فرضنا السيناريو الآتي:

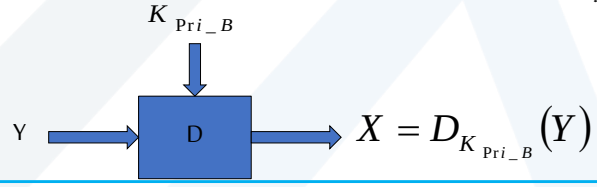
تريد عقدة A أن ترسل إلى العقدة B رسالة ما (X) بشكل آمن باستخدام خوارزمية تشفير غير متناظر .

عندها :

1. يقوم المرسل A بتشفير الرسالة باستخدام المفتاح العام لـB
2. عندما تستقبل العقدة B الرسالة تقوم باستخدام مفتاحها الخاص لفك تشفير الرسالة

أي:

$$X = D_{K_{Pri_B}}(Y)$$

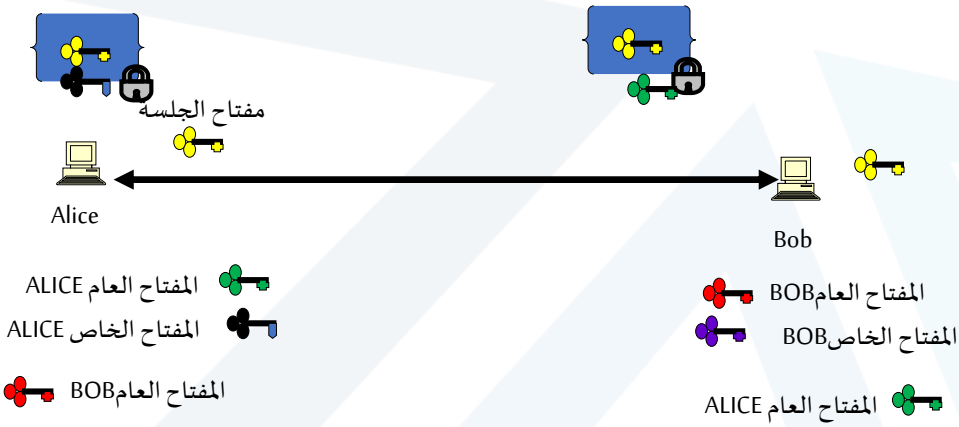


خوارزميات التشفير غير المتناظر (8/8)
(Asymmetric Encryption Algorithms)

➢ أهم تطبيقات هذه الخوارزميات هي:

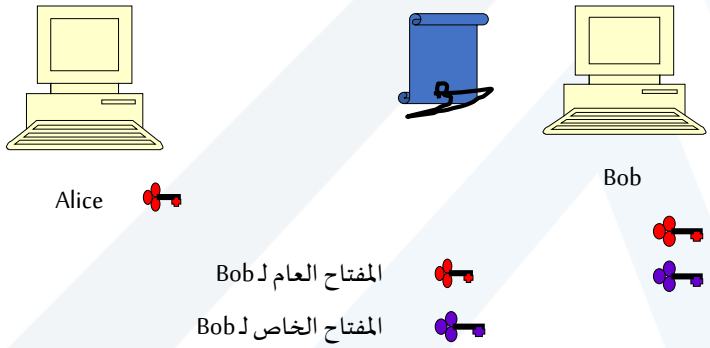
- ❑ التعمية/ فك التعمية: يستخدم المرسل المفتاح العام للمستقبل في التشفير.
- ❑ تبادل المفاتيح : يقوم الطرفان بتبادل مفتاح الجلسة . يستخدم لذلك المفتاح الخاص لأحدهما أو لكليهما.
- ❑ التوقيع الرقمي : يستخدم المرسل مفتاحه الخاص ليوقع على الرسالة، وذلك باستخدام المفتاح الخاص له مع خوارزمية التشفير على الرسالة أو جزء منها.

تبادل المفاتيح باستخدام خوارزمية التشفير غير المتناظر



تحقق المصادقة باستخدام خوارزمية التشفير غير المتناظر

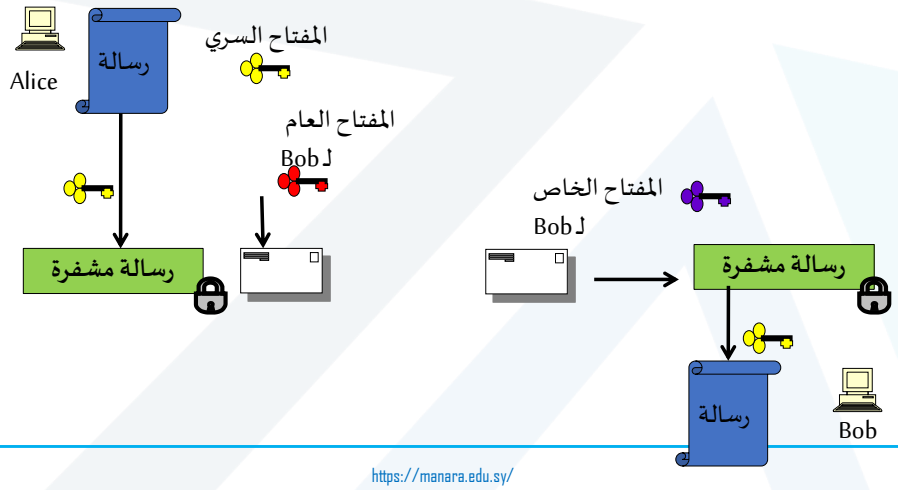
يستخدم المرسل المفتاح الخاص لتشفير الرسالة, يمكن فك تشفير هذه الرسالة باستخدام المفتاح العام المطابق فقط. هكذا يتأكد المستقبل من أن المرسل هو حقاً من أرسل الرسالة كونه الوحيد الذي يملك المفتاح الخاص



خطوات عمل الخوارزميات التشفير غير المتناظر

- يولد /يخزن كل مستخدم زوجاً من المفاتيح لاستخدامه في التشفير وفك التشفير
- يضع كل مستخدم أحد المفاتيح (المفتاح العام) في ملف ما يمكن الدخول إليه من قبل الجميع. أما الآخر فهو المفتاح الخاص به , و الذي يحتفظ به لنفسه
- إذا أراد مستخدم ما (A) إرسال رسالة آمنة لمستخدم آخر (B), فسيقوم ذلك المستخدم بتشفيرها مستخدماً المفتاح العام للمرسل إليه
- عند استقبال المستقبل B للرسالة، يقوم بفك التشفير مستخدماً مفتاحه الخاص

استخدام الخوارزميات المتناظرة وغير المتناظرة معاً



تمارين

السؤال الأول

1. اختر الإجابة الصحيحة

1.يهدد هجوم الانقطاع متطلب:

A .عدم التنصل B. الموثوقية C. التوافرية D. الترخيص

2. يمثل قيام المهاجم بإنشاء رسائل جديدة و إرسالها ضمن الشبكة هجوماً هو :

A . التعديل B.الانقطاع C. الاعتراض D. التزييف

3. من أنواع التحكم الفيزيائي بأمن المعلومات:

A. سلوك الأفراد B . مضادات الفيروسات C.كاشفات الحركة D.البطاقات الذكية

السؤال الثاني (1/2)

أجب بـ صح أو خطأ مع التعليل:

1. تعد برامج الجدران النارية أحد أهم أنواع التحكم الإداري بأمن المعلومات.

خطأ.بل هو أحد أنواع التحكم المنطقي لأن هذا النوع من التحكم يشمل جميع برمجيات التحكم بالوصول

2. تو افرية المعطيات هي متطلب الأمن الذي يسمح بضمان وصول البيانات كما أرسلت.

خطأ.لأن توافرية المعطيات تتعلق بضمان استمرار الحصول على المعطيات من قبل المخول لهم بذلك عند طلبهم لها، ولا تتعلق أبداً بأي تعديل يجرى عليها.

3. هجوم التعديل هو هجوم سلبي.

خطأ. لأنه يتسبب بأذى للنظام، فقد يتسبب التعديل باتخاذ قرارات خاطئة تضر بالنظام كاملاً مما يجعله هجوماً إيجابياً وليس سلبياً

السؤال الثاني (2/2)

أجب بـ صح أو خطأ مع التعليل:

4. ينفذ المهاجم هجوم التعديل عن طريق إنشاء رسائل جديدة و إرسالها ضمن الشبكة

خطأ.يقوم هجوم التعديل على تعديل جزء من النظام موجود مسبقاً (محتوى رسالة مثلاً) ، و لا يقوم على إنشاء رسائل جديدة غير موجودة سابقاً

5.في شبكة مكونة من عقد محدودة الطاقة، ينتهك هجوم إعادة الارسال متطلب التو افرية.

صح.لأن هجوم إعادة الإرسال يتسبب في زيادة عدد الرسائل التي تستقبلها العقد و بالنتيجة زيادة في استهلاك الطاقة ، الأمر الذي قد يتسبب في موت العقد و توقف الخدمة المقدمة من الشبكة وهذا ما يتسبب بانتهاك متطلب التوافرية

6. تعد الهجمات الإيجابية أخطر من الهجمات السلبية.

صح.لأن الهجمات الإيجابية تهدف إلى إيذاء النظام بينما تهدف الهجمات السلبية إلى الحصول على المعلومات لكن دون الإضرار بالنظام مثل التنصت

السؤال الثالث(1/2)

بفرض لدينا شبكة حساسات لاسلكية متجانسة مكونة من مجموعة من عقد محدودة الطاقة ومركز معالجة رئيسي يدعى SINK. الهدف من هذه الشبكة هو مراقبة بستان مشجر للإنذار عن الحريق . في حال وجود عقدة مهاجمة ضمن الشبكة. المطلوب:

1. إذا توضعت هذه العقدة في موقع ضمن الشبكة سمح لها بمنع وصول أية رسالة إلى مركز المعالجة الرئيسي للشبكة. ما اسم هذا الهجوم مع التعليل؟ ما نوعه مع التعليل؟

اسم الهجوم: هجوم حجب الخدمة (الثقب الأسود Blackhole Attack)

التعليل: لأن العقدة المهاجمة أوقفت الخدمة المقدمة من قبل الشبكة بمنع وصول أية رسالة إلى المركز من قبل العقد، فعندما تولد عقدة رسالة إنذار عن الحريق لن تصل إلى المركز، وبالنتيجة لن تتحقق الخدمة التي وجدت من أجلها الشبكة.

نوع الهجوم: إيجابي

التعليل: لأنه أدى إلى الإضرار بالشبكة بإخراجها من الخدمة

السؤال الثالث(2/2)

2. إذا قامت هذه العقدة بإرسال رسالة إنذار كاذبة وصلت إلى مركز المعالجة، فقام بدوره المركز بإصدار أمر للإطفاء للتوجه إلى مكان الحريق. ما اسم هذا الهجوم؟ وما نوعه مع التعليل؟

اسم الهجوم: هجوم التزييف **نوع الهجوم:** إيجابي

التعليل: لأنه أدى إلى اتخاذ قرار خاطئ و بالنتيجة أضر بالنظام

3. استقبلت هذه العقدة رسالة إنذار عن الحريق من إحدى عقد الشبكة في لحظة t1 . فقامت بتمرير هذه الرسالة بشكل طبيعي واحتفظت بنسخة منها. و من ثم أرسلت الرسالة ذاتها في اللحظات (t2,t3,t4,t5). ماذا يسمى هذا الهجوم ؟ وما نوعه مع التعليل؟

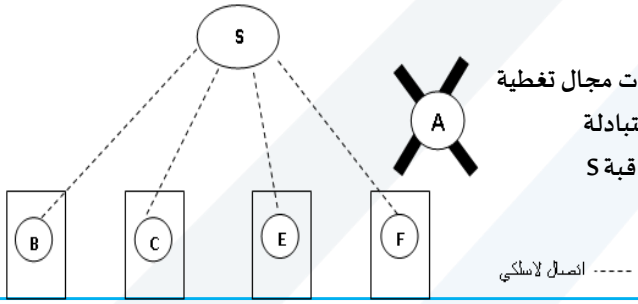
اسم الهجوم: هجوم إعادة الإرسال **نوع الهجوم:** إيجابي

التعليل: تتسبب إعادة الإرسال بزيادة استهلاك الطاقة، وهذا يضر بالشبكة كون العقد محدودة الطاقة، إضافة إلى تسببه في إصدار عدة قرارات خاطئة من المركز

السؤال الرابع(1/4)

إذا كان لدينا شبكة مكونة من عقد حساسات لاسلكية قادرة على قياس درجة الحرارة . هذه الشبكة موزعة ضمن بناء مكون من أربعة مخازن .

الهدف الأساسي هو الإنذار ضد الحريق، وذلك عن طريق قياس درجة الحرارة وإرسال رسالة كل 5 دقائق إلى مركز المراقبة S متضمنة عنوان العقدة المرسلة وعنوان المركز ودرجة الحرارة ، الذي يقارن درجات الحرارة الواصلة إليه مع العتبة $T_{thershold} = 35^{o}C$ لتحديد وجوب إطلاق إنذار عن الحريق وتشغيل رذاذ إطفاء الحريق في المخزن المعني أم لا.



إذا كان لدينا العقدة المهاجمة A ذات مجال تغطية يمكنها من الاستماع إلى الرسائل المتبادلة بين العقد B,C,E,F, وبين مركز المراقبة S والمطلوب:

السؤال الرابع(2/4)

1. في البداية استمعت العقدة A إلى الرسائل المرسلة ولم تقم بأي إجراء. ماذا نسمي هذا الهجوم؟ وما نوعه ولماذا؟

اسم الهجوم: هجوم التنصت نوع الهجوم: سلبي

التعليل: لأن العقدة جمعت معلومات من الشبكة و لكنها لم تضر بها

2. في حال قامت العقدة A بإرسال الرسالة: $\{ID_C, ID_S, T = 45^{o}C\}$ ماذا نسمي هذا الهجوم؟ وما نوعه ولماذا؟

اسم الهجوم: هجوم التخفي (سرقة الهوية) نوع الهجوم: إيجابي/فعال

التعليل: لأنه تسبب الاضرار بالنظام من خلال إرسال رسالة تؤدي إلى اتخاذ قرار خاطئ مثل تشغيل الرذاذ.

السؤال الرابع(3/4)

3. في حال أرسلت العقدة C رسالة تتضمن $\{ID_C, ID_S, T = 15^O C\}$ قاطعت العقدة A الرسالة ومن ثم أرسلتها كالآتي: $\{ID_C, ID_S, T = 50^o c\}$

ماذا نسمي هذا الهجوم؟ وما هو متطلب الأمن الذي انتهك؟ و ماذا قد ينتج عن هذا الهجوم؟

اسم الهجوم: هجوم التعديل **المتطلب:** التكاملية

ينتج عنه: اتخاذ قرار خاطئ بالإنذار بالحريق في المستودع C

4. نشب حريق ضمن المخزن E،تحسس الحساس الحريق و قام بإرسال الرسالة الآتية:

$$\{ID_E, ID_S, T = 40^O C\}$$

لكن العقدة A قامت بالتشويش مما أعاق وصول هذه الرسالة إلى العقدة S، و بالنتيجة لم يتخذ المركز S أي إجراء. ماذا نسمي هذا الهجوم؟ و ما هو متطلب الأمن الذي يتم انتهاكه و لماذا ؟

اسم الهجوم: هجوم حجب الخدمة **المتطلب:** التوافرية

التعليل:لأنه منع وصول إلى الخدمة التي يقدمها المركز من تشغيل الرذاذ و إطفاء الحريق

السؤال الرابع(4/4)

5. في حال طبق التشفير المتناظر التقليدي على الشبكة المبينة بالشكل. ما هو عدد المفاتيح المخزنة من قبل كل عقدة؟ ما عدد المفاتيح التي يخزنها المركز؟ مع التعليل

تخزن كل عقدة مفتاح واحد فقط

يخزن المركز مفتاح واحد فقط

التعليل: لأنه في التشفير المتناظر التقليدي تخزن كل عقد الشبكة مفتاح واحد فقط للتشفير وفك التشفير

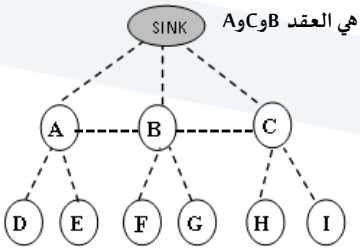
6. في حال طبق التشفير المتناظر الثنائي على الشبكة المبينة بالشكل. ما هو عدد المفاتيح المخزنة من قبل كل عقد مع التعليل ؟ ما عدد المفاتيح التي يخزنها المركز مع التعليل ؟ وما عدد المفاتيح على مستوى الشبكة مع التعليل؟

تخزن كل عقدة مفتاح واحد فقط لأن العقدة تتصل مع المركز فقط أي تحتاج مفتاح واحد فقط

يخزن المركز 4 مفاتيح لأن المركز يتصل مع الحساسات الأربعة بحيث يستخدم مفتاح مختلف لتأمين كل وصلة

عدد المفاتيح على مستوى الشبكة : مفاتيح1x4+4=8

السؤال الخامس



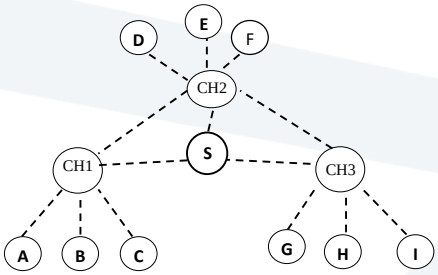
أولاً. بفرض لدينا الشبكة اللاسلكية المجاورةحيث المركزهو الSINK و قادة العناقيد هي العقد AوCوB
حيث عقد العنقود A هي D,E و عقد العنقود B هي F,G و عقد العنقود C هي H,I
الوصلات في الشبكة تمثل بالخطوط المنقطة.
إذا كان نظام التشفير المستخدم هو نظام تشفير هجين كالآتي:
يستخدم نظام تشفير متناظر ثنائي بين قادة العناقيد و المركز.
يستخدم نظام تشفير غير متناظر فيما بين قادة العناقيد.
يستخدم نظام تشفير متناظر تقليدي بين كل قائد عنقود و عقد العنقود التابعة له.
و المطلوب:

1. حدد مع التعليل عدد المفاتيح الذي يختزنه كل من الSINK و قادة العناقيد (B وCوA) و العقد D,F,H.
2. في حال غادرت العقدة I العنقود C. ما هو الإجراء الأمني الذي يجب القيام به لضمان أمن الشبكة، ولماذا؟

ثانياً. لدينا السيناريو الآتي:
موظف في شركة مسؤول عنجدولة رواتب الموظفين و تثبيت قيم المكافآت الشهرية باستخدام برنامج محاسبة.
بينما كان يعمل، أحس بالتعب، فقرر أن يذهب لتناول القهوة، وترك جهازه في حالة عمل، و باب مكتبه مفتوحاً.
فدخل أحد الموظفين و قام بالعبث بجداول المكافآت وتغيير بعض القيم فهل زيادة و أخرى نقصاناً. بر أيك:

1. ما نوع التحكم بأمن المعلومات الذي أهمل في هذا السيناريو؟ مع التعليل.
2. ما اسم الهجوم الذي حدث في السيناريو؟ وما نوعه؟ وما هو المتطلب الأمني الذي انتهك مع التعليل؟

السؤال السادس



أولاً. إذا كان لدينا الشبكة المعطاة بالشكل الآتي :
حيث S هو مركز الشبكة. CH1 قائد عنقود يتضمن العقد A,B,C
CH2 قائد عنقود يتضمن العقد D,E,F CH3 قائد عنقود يتضمن العقد G,H,I
---- الاتصال المسموح به.
و المطلوب:
إذا طبق نظام تشفير هجين كالآتي:

1. نظام تشفير ثنائي بين المركز S وقادة العناقيد.
2. نظام تشفير غير متناظر بين قادة العناقيد.
3. نظام تشفير متناظر تقليدي بين عقد العنقود وقائد العنقود التابعة له.

أ. ما عدد المفاتيح (مع التعليل) الذي يختزنه المركز S وكل من قادة العناقيد الثلاث والعقدة A.
ب. ما هو تأثير سيطرة المهاجم على العقدة H التابعة لقائد العنقود الثالث CH3 ؟ وما هو الإجراء الأمني الذي يجب اتخاذه في هذه الحالة؟
ج. إذا علمت أن كل من العقد A,B,C تتحسس لنسبة الرطوبة، في لحظة زمنية ما أرسلت نسب الرطوبة الآتية إلى قائد العنقود CH1 :
HU_A=70% ,HU_B=80%, HU_C=75%. قام CH1 بإرسال نسبة الرطوبة الأعظمية الواصلة إليه إلى المركز. إذا كانت نسبة الرطوبة الواصلة إلى المركز من CH1 هي 40% . من خلال المقارنة مع العتبة الإحصائية لنسبة الرطوبة في تلك المنطقة(HU_{TH}=60%) رفض المركز القيمة معتبراً أن CH1 قد هوجم. ماذا نسمي هذا الهجوم (مع التعليل)؟ ما هو المتطلب الأمني الذي انتهك نتيجة هذا الهجوم؟ وما هي التقنية الأمنية التي تقترح استخدامها لتجنب حدوث هذا الهجوم؟

Thanks