اسم المادة : إدارة شبكات الاتصال وأمنها

تجمع طلبة كلية التكنولوجيا والعلوم التطبيقية - جامعة القدس المفتوحة

acadeclub.com

وُجد هذا الموقع لتسهيل تعلمنا نحن طلبة كلية التكنولوجيا والعلوم التطبيقية وغيرها من خلال توفيروتجميع كتب وملخصات وأسئلة سنوات سابقة للمواد الخاصة بالكلية, بالإضافة لمجموعات خاصة بتواصل الطلاب لكافة المواد:

للوصول للموقع مباشرة اضغط هنا

وفقكم الله في دراستكم وأعانكم عليها ولا تنسوا فلسطين من الدعاء ♡

اسم المقرر: إدارة شبكات الاتصال وأمنها
رقم المقرر: 1475
مدة الامتحان: ..ساعة ونصف.....
عدد الاسئلة: ...ستة.....

اسم الطالب: .....
توقيع الطالب: .....
تاريخ الامتحان: ...../...../.....

بسم الله الرحمن الرحيم

جامعة القدس المفتوحة
إجابة الامتحان النهائي البديل (غير المكثف)
للفصل الثاني "1162"
2017/2016

-- نظري --

السؤال الاول ضع إشارة صح(✓) أو خطأ(×) في الجدول الأول في دفتر الإجابة (20علامة)

1. خطر التنكر هو أن ينكر المرسل إرساله للرسالة. خ و5 ص 148
2. يعتمد التشفير بشكل أساسي على صعوبة معرفة خوارزمية التشفير من قبل الخصم. خ و5 ص 155
3. يمكن تنفيذ بعض خوارزميات التشفير الحديثة على شكل رقاقات إلكترونية ICs. ص و5 ص 158 س
4. في طريقة الكتاب الإلكتروني المرمز: تتم عملية فك التشفير لكل كتلة بشكل مستقل عن الكتة السابقة لها. ص و6 ص 227
5. في طريقة العداد: عمليتي التشفير وفك التشفير تتطلبان خوارزمية التشفير فقط دون الحاجة إلى خوارزمية فك التشفير. ص و6 ص 231
6. تستخدم خوارزمية دس مفتاحا رئيسياً يتكون من 48 خانة ثنائية لانتاج 14 مفتاحا فرعيا. خ و6 ص 218
7. يمكن استخدام خوارزميات تشفير المفتاح العام في التوقيع الرقمي. ص و7 ص 271
8. توجد علاقة رياضية بين المفتاح العام والمفتاح الخاص، وبمعرفة أحدهما يمكن بسهولة حساب الآخر. ص و7 ص 247
9. تستخدم شهادات مواقع الويب للتحقق من هوية المستخدم لدى الموقع . خ و8 ص 289
10. عند اصدار شهادة المفتاح العام من قبل الجهة المخولة: يتم نشر المفتاح العام على شبكة الإنترنت لإثبات ملكيته للجهة الطالبة. خ و8 ص 290

جدول رقم (1)

اجابة السؤال رقم (1) من نوع (أجب بنعم أو لا) او (√ او×) (20 علامة)(2 علامات لكل فرع)

الفرع	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
الصحيحه	×	×	✓	✓	✓	×	✓	✓	×	×										

السؤال الثاني اختر رمز الإجابة الصحيحة ثم انقل اجابتك في دفتر الإجابة في الجدول الثاني (30 علامة)

1. الهدف من تشفير الرسالة منع الخصم من ..... ج و5 ص 149
أ) تأخير الرسالة ب) تحليل حركة المرور ج) الاطلاع على محتوى الرسالة د) جميع ما ذكر

2. باستخدام شيفرة قيصر: ناتج تشفير النص "bee" يمكن أن يكون ..... أ و5 ص 164
أ) ehh ب) xyy ج) eeb د) جميع ما ذكر

3. تعتبر شيفرة هل مثالاً على التشفير ..... د و5 ص 170
أ) أحادي الأبجدية ب) متعدد الأبجدية ج) أحادي الأحرف د) متعدد الأحرف

4. في التشفير أحادي الأبجدية: إذا سمحنا باستبدال الحرف الأصلي بحرف آخر بغض النظر عن ترتيبه الأبجدي، سنتمكن من انتاج ..... من المفاتيح د و5 ص 167
أ) 10^{26} ب) 26^{10} ج) 2^{26} د) 26!

5. ناتج الجولة الواحدة من خوارزمية فستل $f_k(L,R)$ = ... أ و6 ص 202
أ) (F(R) xor L, R) ب) (F(L), L xor R) ج) (L, L xor F(R)) د) (F(L) xor F(R))

6. بطريقة الكتل المشفرة المتسلسلة: ناتج عملية تشفير الكتلة الثانية C_2 هو ..... د و 6 ص 230
أ) $E(C_1) \text{ xor } E(P_1)$ ب) $E(C_2) \text{ xor } E(P_1)$ ج) $E(C_2 \text{ xor } P_2)$ د) $E(C_1 \text{ xor } P_2)$

7. صناديق إس S-Boxes هي مصفوفات تستخدم من قبل خوارزمية DES بهدف تحقيق ..... ب و6 ص 239
أ) التشتت ب) التشويش ج) أ و ب معاً د) لا شيئ مما ذكر

8. على مستوى الأمان: خوارزمية دس الثلاثية ( ) تكافئ خوارزمية تستخدم مفتاحاً واحداً يتكون من..... ج و6 ص 225
أ) 56 ثنائية ب) 128 ثنائية ج) 168 ثنائية د) 24 ثنائية

9. يجب أن تتصف دالة تشفير المفتاح العام بأنها ..... ب و7 ص 248
أ) Hash Function ب) One-way Function ج) Computationally Difficult د) Unconditionally Secure

10. من الاعتداءات التي تتعرض لها خوارزمية RSA ..... ج و7 ص 270
أ) اعتداء الالتقاء في المنتصف ب) هجوم عيد الميلاد ج) الاعتداء التوقيتي د) لا شيئ مما ذكر

11. تتطلب عملية توقيع الرسالة وتشفيرها معاً وقتاً طويلاً في معظم الأحيان، ولتسريع هذه العملية فإننا نقوم بتشفير الرسالة باستخدام ..... و تشفير قيمة الهاش باستخدام ..... ج و7 ص 252

أ) المفتاح العام للمستقبل / المفتاح الخاص للمرسل ب) المفتاح الخاص للمرسل / المفتاح العام للمستقبل
ج) خوارزمية تماثلية بمفتاح سري / المفتاح الخاص للمرسل د) المفتاح الخاص للمرسل / خوارزمية تماثلية بمفتاح سري

12. من البرمجيات المستخدمة لضمان أمن البريد الإلكتروني ..... د و8 ص 312

أ) PGP ب) GnuPGP ج) GPG4WIN د) جميع ما ذكر

13. من مواصفات دالة الهاش الجيدة أن تنتج عدداً ..... من الخانات. ج و7 ص 273

أ) متناسباً مع حجم الرسالة ب) مختلفاً في كل مرة ج) متساوياً في كل مرة د) أولياً في كل مرة

14. مركز توزيع المفاتيح هو جهة موثوقة توكل لها مهمة توزيع ..... على المستخدمين. أ و8 ص 319

أ) المفاتيح السرية ب) المفاتيح الخاصة ج) المفاتيح العامة د) شهادات المفاتيح

15. عند تحليل حركة المرور وأنماط الاتصال فإن الرسائل القصيرة والمتبادرة بسرعة قد تعني ..... ب و8 ص 303

أ) التخطيط لأمر ما ب) مرحلة تفاوض ج) موافقة على أمر ما د) رفض مع مبررات

جدول رقم (2)

اجابة السؤال رقم (2) من نوع (اختيار من متعدد) (30 علامة)(2 علامات لكل فرع)

الفرع	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
الصحيحه	ج	أ	د	د	أ	د	ب	ج	ب	ج	ج	د	ج	أ	ب					

السؤال الثالث : اجباري (15علامة)

أ) يمكن تصنيف خوارزميات التشفير من حيث قدرتها على توفير الأمن للنص الأصلي إلى صنفين. أذكرهما مع شرح كيفية ضمان الأمن لكل منهما. و5 ص 160 **(9 علامات)**

1. خوارزميات آمنة دون شروط.
   - لا يحتوي النص المشفر على أية معلومات يمكن استخدامها للحصول على النص الأصلي
   - كل ما يستطيع فعله الخصم تخمين محتوى الرسالة.
2. خوارزميات أمنة حسابياً. لا يمكن كسر الشيفرة إلا بتوفر أحد الشرطين أو كلاهما:
   - أن تكون تكلفة كسر الشيفرة كبيرة جداً بحيث تفوق ثمن البيانات نفسها.
   - أن يكون الوقت المستغرق لكسر الشيفرة كبير جداً بحيث لا تكون البياتات مفيدة بعد انقضاء تلك الفترة.

ب) هناك ثلاثة شروط لا بد من توافرها لكي يتم استخدام نظام تشفير المفتاح العام بطريقة علمية وآمنة، أذكرها. و7 ص 247 **(6 علامات)**

1. أن تكون عملية التشفير سهلة حسابياً، ولا تتطلب وقتاً كبيراً لإتمامها.
2. أن تكون عملية فك التشفير سهلة حسابياً لمن يملك المفتاح الخاص
3. أن تكون صعبة حسابياً لمن لا يعرف المفتاح الخاص حتى وإن عرف المفتاح العام.

السؤال الرابع : اجباري (15 علامة)

أ) اذكر الخطوات الرئيسية التي تتكون منها خوارزمية دس المبسطة SDES . و6 ص 207 **(10 علامات)**

1. إعادة الترتيب المبدئية Initial Permutation وهي إعادة ترتيب الخانات في الكتلة الرئيسية حسب الدالة IP
2. تشفير النصف الأيسر للكتلة النصية بتطبيق الدالة fk عليها مع المفتاح الفرعي k1
3. تبديل نصفي الكتلة النصية الأيمن والأيسر تمهيداً لتشفير باقي النص.
4. تشفير النصف الأيسر (الأيمن قبل التبديل) من الكتلة النصية بتطبيق الدالة fk عليها مع المفتاح الفرعي k2 .
5. إعادة ترتيب الكتلة الناتجة بإرجاع كل خانة إلى مكانها الأصلي قبل عملية الترتيب المبدئية IP وذلك باستخدام الدالة IP^{-1} .

ب) أذكر الخطوات الرئيسية للحصول على المفاتيح المؤقتة بدون طرف وسيط. و8 ص 295 **(5 علامات)**

1. يرسل المرسل A طلباً للمستقبل B يطلب فيه مفتاحاً مؤقتاً مع قيمة عددية N1 يختارها بنفسه
2. يقوم B بتشكيل المفتاح الفرعي Ks ويرسله إلى A مشفراً باستخدام المفتاح الرئيسي بينهما إضافة إلى قيمة F(N1) مع قيمة جديدة N2 يختارها بنفسه
3. يقوم A بفك تشفير الرسالة وإرسال قيمة F(N2) إلى B مشفرة بالمفتاح المؤقت الجديد Ks.

السؤال الخامس : اختياري **(20 علامة)**

ج) اذا كانت a=11 و b=5 في خوارزمية RSA قم بتشكيل المفتاح العام والمفتاح الخاص موضحا طريقة الحل. (قم باختيار قيمة مناسبة لـ k وليكن أقل من 10) و7 متعدد الصفحات ـ استيعاب **(11 علامة)**

نقوم بحساب قيمة n

$n = a * b = 5 * 11 = 55$

ثم نحسب قيمة $\Phi(n)$

$\Phi(n) = (a-1) * (b-1) = 10 * 4 = 40$

يختار الطالب قيمة مناسبة لـ k بحيث تكون عدداً أولياً بالنسبة لـ $\Phi(n)$ ، ولتكن k= 7 ، ثم يكمل الطالب الحل بناء على قيمة k التي اختارها

- المفتاح العام = $(n, k) = (55, 7)$

نقوم بحساب قيمة k' على أساس $k * k' \bmod \Phi(n) = 1$

نجد أن العدد 23 يحقق المعادلة

- المفتاح الخاص = $(n, k') = (55, 23)$

د) أذكر نقطة ضعف كل من: و 8 متعدد الصفحات **(9 علامات)**

1. **شيفرة قيصر :** قلة عدد المفاتيح يجعل الخصم قادراً على تجربة كل المفاتيح الممكنة بسهولة
2. **شيفرة هل :** ضعيفة في وجه اعتداء النص المعروف، فإذا عرف الخصم مجموعة من الأزواج المشفرة وما يقابلها من النص الأصلية فيمكن استنتاج مصفوفة المفتاح لأن العلاقة بين المفتاح والنص المشفر علاقة خطية.
3. **شيفرة فيجينير:** لا تخفي كل تراكيب النص الأصلي. فكلما كان النص المشفر كبيراً يعطي فرصة أكبر للخصم لمعرفة طول المفتاح.

السؤال السادس : اختياري **(20 علامة)**

أ) قم بتشكيل المفاتيح الفرعية لخوارزمية SDES بناء على المعطيات التالية: و6 ص 214 **(10 علامات)**

K = "1011010011"

Permuted Choice-1 = 3,5,2,7,4,10,1,9,8,6

Permuted Choice-2 = 6,3,7,4,8,5,10,9

1. نقوم بإعادة ترتيب خانات المفتاح حسب الدالة Permuted Choice-1 ليصبح = "1000111101"
2. نقسم الخانات العشر إلى قسمين "11101" و "10001"
   ثم ازاحة دائرية لكل منهما إلى اليسار خانة واحدة ليصبحا "11011" و "00011" = "0001111011"
3. نطبق الدالة Permuted Choice-2 على الناتج لتشكيل k1 = " 10110111"
4. نقوم بعملية ازاحة دائرية النصفين من ناتج الخطوة الثانية خانتين لليسار ليصبحا " 01111 " و " 01100" = "01100 01111"
5. نطبق الدالة Permuted Choice-2 على الناتج لتشكيل k2 = " 01101011 "

ب) في تشفير النهايات: على من تقع مهمة التشفير وفك التشفير؟ ولماذا؟ واذكر فوائد تلك الطريقة. و8 ص 300
(10 علامات) (4 علامات على مهمة من والسبب و علامتان لكل فائدة)

– تقع مهمة التشفير وفك التشفير على عاتق المرسل والمستقبل اللذين عليهما الاتفاق على مفتح تشفير سري.

– فوائد طريقة تشفير النهايات:

1. أن المستقبل فقط من يستطيع فك تشفير الرسالة والاطلاع على محتواها.
2. تعطي المستخدم حرية اختيار خوارزمية التشفير التي تناسبه.
3. تمكن المستقبل من التأكد من هوية المرسل لأن المفتاح السري متفق عليه بين الطرفين.

انتهت الإجابة

اسم المقرر: إدارة شبكات الاتصال وأمنها اسم الطالب: .....
رقم المقرر: .....1475..... رقم الطالب: .....
مدة الامتحان: ..ساعة ونصف..... تاريخ الامتحان: ...../...../.....
عدد الاسئلة: ...ستة.....

بسم الله الرحمن الرحيم
جامعة القدس المفتوحة
اجابة الامتحان النهائي
للفصل الثاني "1152"
2016/2015
FUTURE LIBARARY

-- نظري --

السؤال الاول ضع إشارة صح(✓) أو خطا(×) في الجدول الأول في دفتر الإجابة (20علامة)

1. يقصد بكسر الشيفرة استخدام المفتاح في عملية استرجاع النص الأصلي من النص المشفر. و5 ص 155
2. إن إضافة نص عشوائي إلى الرسائل المشفرة والمرسلة عبر الشبكة يزيد من إمكانية تعرضها لكسر الشيفرة. و5 ص153
3. يمكن تنفيذ بعض خوارزميات التشفير الحديثة على شكل رقاقات إلكترونية ICs. 5 ص 158 س
4. تستخدم شيفرة فيجنر نفس الخوارزمية للتشفير وفك التشفير مع عكس ترتيب المفاتيح الفرعية فقط. 6 ص 203 س
5. يمكن كسر دس الثنائية Double DES بواسطة نوع من الاعتداءات يدعى Meet in the Middle Attack. و6 ص 223
6. عند استبدال المرحلة الوسطى من خوارزمية دس الثلاثية بمرحلة فك تشفير، فذلك سيقلل من مستوى الأمان أو يلغيه تماماً. و6 ص 225
7. توجد علاقة رياضية بين المفتاح العام والمفتاح الخاص، وبمعرفة أحدهما يمكن بسهولة حساب الآخر. و7 ص 247
8. باستخدام التوقيع الرقمي يطمئن المستقبل إلى هوية المرسل وإلى أن الرسالة وصلت سليمة أيضاً. و7 ص 251
9. تكمن مشكلة تشفير النهايات في أن الخصم يستطيع تحديد هوية المستقبل وحجم الرسالة. و8 ص 300
10. تتطلب عملية توزيع المفاتيح السرية بطريقة المفتاح العام طرفاً ثالثاً لتأمين وصول المفتاح إلى الطرفين دون أي اعتداءات. و8 ص 297

جدول رقم (1)

اجابة السؤال رقم (1) من نوع (أجب بنعم أو لا) او (√ او×) (20 علامة)(2 علامات لكل فرع)

الفرع	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
الصحيحه	×	×	√	√	√	×	×	√	√	×										

السؤال الثاني اختر رمز الإجابة الصحيحة ثم انقل اجابتك في دفتر الإجابة في الجدول الثاني (30 علامة)

1. تعتبر شيفرة هل مثالاً على التشفير ..... 5 ص 170
أ) أحادي الأبجدية ب) متعدد الأبجدية ج) أحادي الأحرف د) متعدد الأحرف

2. من أحد الشيفرات الآمنة دون شروط 5 179
أ) قيصر ب) فيجينير ج) ون تايم باد د) هل

3. في التشفير أحادي الأبجدية: إذا سمحنا باستبدال الحرف الأصلي بحرف آخر بغض النظر عن ترتيبه الأبجدي، سنتمكن من انتاج .... من المفاتيح و5 ص 167
أ) 10^{26} ب) 26^{10} ج) 2^{26} د) !26

4. من إحدى نقاط ضعف شيفرة فيجنير أنها .... و5 ص 117
أ) أحادية الأبجدية ب) لا تخفي كل التراكيب النسبية ج) تستخدم مفتاح واحد فقط د) صغر حجم المفتاح

5. على مستوى الأمان: خوارزمية دس الثلاثية ( ) تكافئ خوارزمية تستخدم مفتاحاً واحداً يتكون من... و6 ص 225
أ) 56 ثنائية ب) 128 ثنائية ج) 168 ثنائية د) 24 ثنائية

6. بطريقة العداد للتشفير: (حيث أن العداد = I) فإن ناتج عملية التشفير على النحو التالي... و 6 ص 231
أ) Ci = E(I) XOR Pi ب) Ci = I XOR Pi ج) Ci = I XOR E(Pi) د) Ci = Pi mod I

7. في طريقة الكتل المشفرة المتسلسلة: يتم تطبيق عملية أو الاستثنائية XOR على الكتلة النصية الأصلية P مع .... و6 ص 229
أ) ناتج تشفير الكتلة السابقة ب) ناتج تشفير الكتلة اللاحقة ج) النص الأصلي السابق د) النص الأصلي اللاحق

8. تتطلب عملية توقيع الرسالة وتشفيرها معاً وقتاً طويلاً في معظم الأحيان، ولتسريع هذه العملية فإننا نقوم بتشفير الرسالة باستخدام .... و تشفير قيمة الهاش باستخدام .... و7 ص 252
أ) المفتاح العام للمستقبل / المفتاح الخاص للمرسل ب) المفتاح الخاص للمرسل / المفتاح العام للمستقبل

ج) خوارزمية تماثلية بمفتاح سري / المفتاح الخاص للمرسل د) المفتاح الخاص للمرسل / خوارزمية تماثلية بمفتاح سري

9. يمكن استخدام عملية الضرب في التشفير غير التماثلي، ويجب أن تكون العلاقة ما بين K و 'K كالتالي: و7 ص 256

أ) K = K' * 26 ب) K' = K * 26 ج) K * K' mod 26 = 1 د) K * K' mod 1 = 26

10. واحدة من الدوال التالية ليست من دوال الهاش هي : و7 ص 273

أ) MD5 ب) POP3 ج) SHA-1 د) RIPEMD

11. يجب أن تتصف دالة تشفير المفتاح العام بأنها ... و7 ص 248

أ) Hash Function ب) One-way Function ج) Computationally Difficult د) Unconditionally Secure

12. لا تحتوي شهادة المفتاح العام على: و 8 ص 289

أ) تاريخ الإصدار ب) المفتاح الخاص ج) المفتاح العام د) تاريخ الانتهاء

13. البرمجية التي تستخدم على نطاق واسع لضمان امن الرسائل الالكترونية هي : و8 ص 313

أ) PGP ب) KDC ج) SLT د) KS

14. مركز توزيع المفاتيح هو جهة موثوقة توكل لها مهمة توزيع ..... على المستخدمين. و8 ص 319

أ) شهادات المفاتيح ب) المفاتيح الخاصة ج) المفاتيح العامة د) المفاتيح السرية

15. برامج تقوم في الظاهر بأشياء مفيدة، ولكن تحتوي على برامج خفية للتجسس على الأرقام السرية ومعلومات أخرى. و8 ص 131

أ) أحصنة طروادة ب) حلقة المفاتيح ج) Proxy د) Spam

جدول رقم (2)

اجابة السؤال رقم (2) من نوع (اختيار من متعدد) (30 علامة)(2 علامات لكل فرع)

الفرع	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
الصحيحه	د	ج	د	ب	ج	أ	أ	ج	ج	ب	ب	ب	أ	د	أ					

السؤال الثالث : اجباري (15علامة)

أ. تحل عملية التشفير عدداً من مشاكل الاعتداءات التي قد تتعرض لها البيانات. أذكر خمسة من تلك الاعتداءات وكيف يمكن لعملية التشفير حل مشكلة كل منها. و5 ص 150 (10 علامات)

1. اطلاع الأشخاص غير المخولين على محتوى الرسالة : يرسل المرسل رسالة مشفرة عبر قنوات الاتصال، فلو استطاع الخصم الحصول على نسخة منها فمن المفترض ألا يستطيع فك أو كشر الشيفرة لعدم معرفته بالمفتاح
2. تغيير محتوى الرسالة : من الممكن أن يستطيع الخصم تغيير محتوى الرسالة ولكن من السهل اكتشاف ذلك عند فك الشيفرة من قبل المستقبل
3. تأخير الرسالة : من الممكن أن يستطيع الخصم تأخير الرسالة ، ولكن بتضمين الوقت والتاريخ في الرسالة قبل تشفيرها يسهل اكتشاف ذلك عند فك الشيفرة.
4. العبث بترتيب : من الممكن أن يستطيع الخصم تغيير ترتيب الرسائل، ولكن بتضمين رقم متسلسل للرسائل قبل تشفيرها يمكن اكتشاف ذلك أيضاً عند فك الشيفرة وفحص التسلسل
5. التنكر : لوجود مفتاح سري متفق عليه بين المرسل والمستقبل، إذا استطاع المستقبل فك الشيفرة بذلك المفتاح وحصل على نص سليم فغالباً ما يستطيع المستقبل الجزم بأن المرسل هو الشخص الذي إتفق معه على ذلك المفتاح

- ويمكن للطالب اضافة بعض الاعتداءات كإنكار المرسل والمستقبل وغيرها وكذلك طريقة حل تلك المشاكل. ويترك لعضو هيئة التدريس تقييمها

ب. ما هي الشروط الواجب توفرها في خوارزمية التشفير لكي تكون آمنة حسابياً؟ و5 ص 161 (5 علامات)

1. أن تكون تكلفة كسر الشيفرة كبيرة جداً تفوق قيمة البيانات نفسها
2. أن يكون الوقت اللازم لكسر الشيفرة كبير جداً بحيث لا تكون البيانات مفيدة بعد انقضاء تلك المدة

السؤال الرابع : اجباري (15 علامة)

أ. عدد العوامل المؤثرة على مستوى الأمان في شبكات/خوارزمية فستل و6 ص 202 (5 علامات)

1. الدالة F وما تقوم به من عمليات
2. حجم المفتاح

3. حجم الكتلة النصية
4. عدد الجولات
5. المفاتيح الفرعية وكيفية الحصول عليها

ب. قارن بين خوارزميتي SDES و DES من حيث **(10 علامات)**

1) حجم المفتاح
2) حجم الكتلة المشفرة
3) عدد الجولات
4) عدد و حجم المفاتيح الفرعية
5) عدد و حجم صناديق S-Boxes

وجه المقارنة	SDES	DES
حجم المفتاح	10	56
حجم الكتلة المشفرة	8 Bits	16 Bits
عدد الجولات	2	16
عدد و حجم المفاتيح الفرعية	28 Bits مفتاح فرعي كل منها يتكون من	1648 Bits مفتاح فرعي كل منها يتكون من
عدد و حجم صناديق S-Boxes	4 X 24 صندوق كل منها	84 X16 صناديق كل منها

السؤال الخامس : اختياري (20 علامة)

أ) اذا كانت a=11 و b=5 في خوارزمية RSA قم بتشكيل المفتاح العام والمفتاح الخاص موضحا طريقة الحل. (قم باختيار قيمة مناسبة لـ k وليكن أقل من 10) و7 متعدد الصفحات - استيعاب **(12 علامة)**

نقوم بحساب قيمة n

$n = a * b = 5 * 11 = 55$

ثم نحسب قيمة $\Phi(n)$

$\Phi(n) = (a-1) * (b-1) = 10 * 4 = 40$

يختار الطالب قيمة مناسبة لـ k بحيث تكون عدداً أولياً بالنسبة لـ $\Phi(n)$ ، ولتكن k= 7 ، ثم يكمل الطالب الحل بناء على قيمة k التي اختارها

- المفتاح العام = (n, k) = (55, 7)

نقوم بحساب قيمة k' على أساس $k * k' \bmod \Phi(n) = 1$

نجد أن العدد 23 يحقق المعادلة

- المفتاح الخاص = (n, k') = (55, 23)

ب) ما هي مواصفات دالة الهاش الجيدة؟ و7 ص 272 **(8 علامات)**

1. أن تنتج الدالة عدداً ثابتاً من الخانات Bits بغض النظر عن حجم الرسالة
2. أن يصعب معرفة محتوى الرسالة إذا عرفت بصمتها
3. اذا علمت الرسالة M1 أن يكون من الصعب حسابياً إيجاد M2 لها نفس البصمة
4. أن يكون من الصعب إيجاد رسالتين M1 و M2 بحيث H(M1) = H(M2)

السؤال السادس : اختياري (20 علامة)

أ) أذكر أنواع شهادات المفتاح العام، وما هي خطوات الحصول على شهادة مفتاح عام؟ و8 ص 289 **(12 علامة)**

علامتان للأنواع و 10 علامات للخطوات

- أنواع شهادات المفتاح العام
1. شهادات شخصية
2. شهادات مواقع الويب
- خطوات الحصول على شهادة المفتاح العام
1. زيارة الموقع الخاص بالجهة التي يود الحصول منها على الشهادة
2. يعبئ المستخدم النموذج الخاص ببياناته ورقم بطاقة الائتمان
3. يقوم المستكشف بتوليد زوج من المفاتيح (العام والخاص) بناء على طلب الموقع ويرسل المفتاح العام فقط إلى الموقع
4. يتم إرسال بريد الكتروني من الموقع إلى عنوان المستخدم
5. عند الرد على تلك الرسالة تصدر شهادة بالمفتاح العام وترسل وتحمل في برنامج المستخدم الخاص بالبريد الإلكتروني

ب) يعتمد عمل سرية طبقة الاتصال TLS على أربع مراحل. اذكرها مع شرح مبسط. و8 ص 306 **(8 علامات)**

1. مرحلة التفاوض: تبدأ عندما يقوم المستكشف بطلب اتصال آمن ثم يتم التفاوض على خوارزمية التشفير
2. مرحلة التحقق من الهوية : بإرسال شهادة المفتاح العام للموقع إلى المستكشف (المستخدم) وأحيانا إرسال شهادة المستخدم إلى الموقع.
3. مرحلة تبادل المفاتيح السرية : يقوم المستكشف بإرسال المفتاح السري الذي سيستخدم لتشفير البيانات مشفراً بالمفتاح العام إلى الموقع.
4. مرحلة تبادل الرسائل المشفرة: إرسال واستقبال الرسائل المشفرة بالمفتاح السري

انتهت الإجابة

اسم المقرر: إدارة شبكات الاتصال وأمنها
رقم المقرر: 1475
مدة الامتحان: ساعة ونصف
عدد الأسئلة: 6

الصنف الطالب: خاص مكتبة فيوتشر
رقم الطالب: الوسطى
تاريخ الامتحان: ...../...../2015

-- نظري --

عزيزي الطالب:
1. عبىء كافة المعلومات المطلوبة عنك في دفتر الاجابة وعلى ورقة الاسئلة.
2. ضع رقم السؤال ورموز الاجابة الصحيحة للاسئلة الموضوعية (ان وجدت) على الجدول المخصص في دفتر الاجابة
3. ضع رقم السؤال للاسئلة المقالية واجب على دفتر الاجابة.

السؤال الأول: اجب بنعم أو لا على الأسئلة التالية واضعا الإجابة في الجدول المخصص (جدول رقم 1). (20 علامة)

1. تشفير الرسائل (Encryption) إحدى وسائل حماية البيانات.
2. نقطة الضعف في شيفرة هل (Hill Cipher) أنها قابلة للكسر إذا عرف الخصم عددا كافيا من النصوص الأصلية والنصوص المشفرة المقابلة لها.
3. تعتبر خوارزمية RSA أول خوارزمية تشفير مفتاح عام وأقلها استخداما.
4. إن تبادل المفاتيح السرية يعتبر من أهم تطبيقات تشفير المفتاح العام.
5. أسلوب القوة الجبارة (Brute force attack) هو أحد أساليب تشفير البيانات.
6. من عيوب خوارزمية تشفير المفتاح العام أنها بطيئة.
7. المفتاح السري هو المفتاح الذي يستخدم من قبل خوارزمية التشفير التماثلية.
8. تعتبر خوارزمية دس DES من أقل الخوارزميات الحديثة استخداما في عصرنا هذا.
9. تستخدم طرق التشفير غير التماثلية مفتاحا للتشفير وآخر لفك التشفير.
10. طريقة تشفير قناة الاتصال (Link Encryption) تعطي المستخدم الحرية في اختيار خوارزمية التشفير التي يريد.

السؤال الثاني: اختر الإجابة الصحيحة واضعاً رمزها في الجدول المخصص (جدول رقم 2). (30 علامة)

1. من أنواع شهادات المفتاح العام

أ) شهادات شخصية ب) شهادات عليا ج) شهادات مواقع ويب د) أ + ج

2. تعتبر كوابل _____ الأفضل من الناحية الأمنية إذ يصعب نسخ الإشارات التي تمر من خلالها.

أ. الكبلات المجدولة (Twisted - pair) ب) الألياف الضوئية (Fiber optics)
ج) الكبلات المحورية (Coaxial) د) أ + ب

3. تتلخص وسائل حماية البيانات من معظم الاعتداءات باستخدام

أ) تشفير الرسائل ب) التوقيع الرقمي ج) إشغال شبكة الحاسوب بشكل منتظم د) جميع ما ذكر

4. طرق التشفير التقليدية تستخدم _____ في عمليتي التشفير وفك التشفير.

أ) مفتاحا واحدا ب) مفتاحان ج) ثلاثة مفاتيح د) أربعة مفاتيح

5. تعتبر خوارزمية دِس (Des) خوارزمية

أ) غير تماثلية ب) تماثلية ج) مزدوجة د) جميع ما ذكر

6. يسمى مفتاح فك التشفير بـ

أ) المفتاح الذهبي ب) المفتاح العام ج) المفتاح المزدوج د) المفتاح الخاص

7. عدد جولات التشفير في خوارزمية دِس (Des) المبسطة هي

أ) 5 جولات ب) 3 جولات ج) جولتان د) 5 جولات

8. إن خوارزمية المفتاح العام تتطلب وقت تنفيذ

أ) طويلا نسبيا ب) قصيرا نسبيا ج) متوسط نسبيا د) لا شيء مما ذكر

9. تستخدم خوارزمية (RSA) العملية الحسابية التالية

أ) الجمع ب) الطرح ج) الضرب د) الأس

10. تستخدم خوارزمية دس (Des) مفتاحا فرعيا يتكون من _____ خانة ثنائية.

أ) 20 ب) 65 ج) 56 د) 41

السؤال الثالث: (20 علامة)

أ) هناك عدة اعتداءات محتمله قد تتعرض لها البيانات أثناء تبادلها عبر شبكات الحاسوب أذكرها. (8 علامات)

ب) وضع العالم شانون (Shannon) في العام 1945 صفتين للشيفرة الجيدة وضحهما باختصار. (6 علامات)

ج) هناك ثلاثة أنواع لتصنيفات أنظمة التشفير أذكرها. (6 علامات)

السؤال الرابع: (20 علامة)

أ) إذا كان لديك كتلة من البتات 10010010 وتم تنفيذ إعادة ترتيب مبدئية لها حسب الدالة التالية: (10 علامات)

IP							
2	6	3	1	4	8	5	7

ب) تحتوي شهادات المفاتيح العامة على عدة معلومات أذكرها. (6 علامات)

ج) يتكون TLS من أربعة مراحل أذكرها. (4 علامات)

أجب عن أحد السؤالين التاليين

السؤال الخامس: (10 علامات)

وضح المقصود بكل مما يلي :

1- أحصنة طروادة (Trojan Horses)
2- التوقيع الرقمي (Digital Signature)
3- صناديق إس S-Boxes
4- هجوم القوة الجبارة (Brute-force Attack)

السؤال السادس: (10 علامات)

إذا كانت لديك الرسالة الأصلية Palestine وكان المفتاح المستخدم هو k= 5 ماذا ستصبح الرسالة بعد تشفيرها باستخدام طريقة شيفرة قيصر (Caesar Cipher) ؟ استعن بالجدول التالي:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

انتهت الأسئلة

اسم المقرر: إدارة شبكات الاتصال وأمنها
رقم المقرر: 1475
مدة الامتحان: ساعة ونصف
عدد الأسئلة: 6

اسم الطالب: .....
رقم الطالب: .....
تاريخ الامتحان: ...../...../.....

بسم الله الرحمن الرحيم

جامعة القدس المفتوحة
إجابة الامتحان النهائي البديل (غير المكتمل)
الفصل الثاني "1142"
2015/2014

FUTURE LIBRARY

-- نظري --

جدول رقم (1)

إجابة السؤال رقم (1) من نوع (أجب بنعم أو لا) أو (√ أو ×) (20 علامة) (علامتان لكل فرع)

الفرع	1	2	3	4	5	6	7	8	9	10
الصحيحة	نعم	نعم	لا	نعم	لا	نعم	نعم	لا	نعم	لا
رقم الصفحة	149	198	245	297	155	275	291	195	150	301
الوحدة	5	6	7	8	5	7	8	6	5	8

جدول رقم (2)

إجابة السؤال رقم (2) من نوع (اختيار من متعدد) (20 علامة)(3 علامات لكل فرع)

الفرع	1	2	3	4	5	6	7	8	9	10
الصحيحة	د	ب	د	أ	ب	د	ج	أ	د	ج
رقم الصفحة	289	299	149	162	198	274	206	249	264	218
الوحدة	8	8	5	5	6	7	6	7	7	6

السؤال الثالث: (20 علامة)

أ) هناك عدة اعتداءات محتمله قد تتعرض لها البيانات أثناء تبادلها عبر شبكات الحاسوب أذكرها (الوحدة 5 صفحة 147)
(8 علامات)(علامة لكل نقطة)

1. الاطلاع على محتوى الرسالة.
2. تعديل المحتوى.
3. تأخير الرسالة.
4. العبث بترتيب الرسالة.
5. التنكر.
6. إنكار المرسل.
7. إنكار المستقبل.
8. تحليل حركة المرور وأنماط الاتصال.

ب) وضع العالم شانون (Shannon) في العام 1945 صفتين للشيفرة الجيدة وضحهما باختصار (الوحدة 6 صفحة 199)
(6 علامات) (3 علامات لكل نقطه)

1. التشتت (Diffusion) : إن على الشيفرة الجيدة أن تشتت التكرارات والأنماط الإحصائية للنص الأصلي في النص المشفر مثل عدد المرات التي تتكرر فيها الأحرف والتراكيب الثنائية والثلاثية.

2. التشويش (Confusion): تهدف إلى جعل العلاقة بين النص المشفر الناتج والمفتاح المستخدم في التشفير علاقة معقدة غير خطية وذلك لجعل فرص الخصم في استنتاج المفتاح ضعيفة.

ج) هناك ثلاثة أنواع لتصنيفات أنظمة التشفير أذكرها. (الوحدة 5 صفحة 162)
(6 علامات) (علامتان لكل نقطه)

1. عدد المفاتيح المستخدمة
2. العملية المستخدمة في التشفير.
3. حجم النص المشفر.

السؤال الرابع: (20 علامة)

أ) إذا كان لديك كتلة من البتات 10010010 وتم تنفيذ إعادة ترتيب مبدئية لها حسب الدالة التالية: (10 علامات)

IP							
2	6	3	1	4	8	5	7

الناتج هو :

0	0	0	1	1	0	0	1

ب) تحتوي شهادات المفاتيح العامة على عدة معلومات أذكرها. (الوحدة 8 صفحة 289) (6 علامات، علامة لكل نقطة)

تحتوي على :

1- رقم الإصدار
2- اسم صاحب المفتاح
3- تاريخ إصدار المفتاح
4- المفتاح العام نفسه
5- نوع خوارزمية التشفير الممكن استخدام هذا المفتاح معها
6- تاريخ الانتهاء

ج) يتكون TLS من أربعة مراحل أذكرها. (الوحدة 8 صفحة 307) (4 علامات، علامة لكل نقطة)

1- مرحلة التفاوض
2- مرحلة التحقق من الهوية
3- مرحلة تبادل المفاتيح
4- مرحلة تبادل الرسائل المشفرة

أجب عن أحد السؤالين التاليين

السؤال الخامس: (10 علامات)

وضح المقصود بكل مما يلي : (10 علامات) (2.5 علامة لكل مصطلح)

1- أحصنة طروادة (Trojan Horses) (الوحدة 8 صفحة 318)

هي برامج عدائية تقوم بأعمال في ظاهرها مفيدة ولكن قد تقوم بأعمال عدائية بشكل خفي مثل سرقة البيانات السرية الخاصة بالمستخدم مثل كلمات السر والبيانات المالية.

2- التوقيع الرقمي (Digital Signature) (الوحدة 7 صفحة 278)

هو عملية تتطلب تشفير الرسالة المرسلة (أو ملخص لها مستخرج باستخدام دالة هاش) باستخدام المفتاح الخاص للمرسل.

3- صناديق إس S-Boxes (الوحدة 6 صفحة 239)

مصفوفات تستخدم من قبل خوارزمية دِس في عملية تعويض معقدة تهدف إلى تحقيق التشويش اللازم.

4- هجوم القوة الجبارة (Brute-force Attack) (الوحدة 5 صفحة 189)
هو الذي يحاول كسر الشيفرة وكشف النص الأصلي وذلك بمحاولة فك تشفير النص الأصلي مستخدما جميع القيم الممكنة للمفتاح إلى أن يحصل على نص ذي معنى سليم.

السؤال السادس: (10 علامات)

(الوحدة 5 صفحة 164)
إذا كانت لديك الرسالة الأصلية Palestine وكان المفتاح المستخدم هو k= 5 ماذا ستصبح الرسالة بعد تشفيرها باستخدام طريقة شيفرة قيصر (Caesar Cipher) ؟ استعن بالجدول التالي:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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

بالاعتماد على الجدول أدناه والمعادلة التالية: $C=E(P)=(P+4) \mod 26$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
P	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
C	F				J				N			Q		S		U			X	Y						

E(P)=(15+5) mod 26= 20
E(A)=(0+5) mod 26= 5
E(L)=(11+5) mod 26= 16
E(E)=(4+5) mod 26= 9
E(S)=(18+5) mod 26= 23
E(T)=(19+5) mod 26= 24
E(I)=(8+5) mod 26= 13
E(N)=(13+5) mod 26= 18

النص بعد التشفير : UFQJXYNSJ

انتهت الإجابة