جامعة العلوم والتقانة
كلية علوم الحاسوب وتقانة المعلومات
دبلوم تقنية شبكات الحاسوب

إمتحانات نهاية الفصل للعام 2017-2018
السنة **الثالثة** الفصل **السادس** الدفعة NWD 2016/2015
المقرر: **أمن الشبكات**
التاريخ: الأربعاء 2018/5/9 م **الزمن : ثلاث ساعات**

80 درجة

الإسم ..... الرقم .....

أجب عن جميع الأسئلة

ورقة الإمتحان تشتمل على عدد 5 صفحات

22 Marks

السؤال الأول:

(أ) ضع علامة [✓] أمام العبارة الصحيحة وعلامة [X] أمام العبارة الخاطئة في كل مما يلي: (درجة لكل)

1- يقصد بالإتاحية أن اى مستخدم شرعى فى النظام يمكنه او يستطيع الوصول للمعلومات [ ]

2- تعتبر مواقع الويب من الأصول الفيزيائية [ ]

3- التشفير هو التقنية الوحيدة المستخدمة لحماية سرية البيانات [ ]

4- توفر خدمة التكاملية يعنى توفر القدرة على الحفاظ على صحة ودقة البيانات [ ]

5- التحكم في الوصول هو ايجاد الدليل ان المرسل قد ارسل الرسالة وان المستقبل قد استلم الرسالة [ ]

6- الثغرة ه ي اى ظرف او حدث يحتمل أن ينتج عنه اذى للنظام [ ]

7- يمكن لأي جهة إصدار الشهادات الرقمية [ ]

8- يستخدم التوقيع الرقمي لغرض التعريف بالأجزاء مثل شخص معين أو جهاز معين [ ]

9- يمكن بإستخدام SSL توفير خدمة التحقق من الهوية [ ]

10- سياسة التصريح الافتراضي تنص على ما هو ممنوع صراحة ويكون غير ذلك مصرح به [ ]

(ب) إملأ الفراغ فيما يلي بما يناسبه: (درجة لكل فراغ)

1- الموارد الخاصة بالنظام والتى يجب حمايتها تسمى ..... ويمكن أن تكون ..... أو .....

2- يتم الإختراق عادة باستخدام تقنيات تمكن المهاجم من استغلال .....

3- هجوم ..... يعتمد على قدرة المهاجم فى إرسال بياناته للنظام المستهدف بعنوان مصدر غير عنوانه الحقيقي.

4- ..... تعنى حماية المعلومات الشخصية والخاصة المتعلقة بالمستخدم.

5- في أكثر طرق تشفير المفتاح العام ان هناك مفتاحين أحدهما ..... والآخر .....

7- ..... هي وثيقة رقمية تحتوي على مجموعة من المعلومات التي تقود إلى التحقق من هوية الشخص أو المنظمة.

8- تقنية الشبكات الإفتراضية يمكن تطبيق..... أو .....

9- في ..... يقوم المهاجم بمراقبة لاتصالات بحيث لا تتداخل مع قناة الاتصال الفعلية بدون شعور مستخدمي النظام بشئ غريب.

السؤال الثاني

15 درجة

بإختصار قارن بين الآتي: (3 درجات لكل)

(أ) الهجوم الفعّال (Active attack) والهجوم الخامل (Passive attack)

……

……

……

……

(ب) الشفير بالإحلال (Substitution Cipher) و الشفير بالإنتقال (Transposition Cipher)

……

……

……

……

(ج) شفرة الكتل (Block Cipher) و شفرة التدفق (Stream Cipher)

……

……

……

……

(د) الانتشار (Confusion) و الغموض (Diffusion)

……

……

……

……

(هـ) الشفير أحادي الأبجدية (Monoalphabetic cipher) و الشفير متعدد الأبجدية (Polyalphabetic cipher)

……

……

……

20 درجة

السؤال الثالث (4 درجات لكل)

(أ) تحدث عن هجوم الإغراق الموزع (Smurf).

……

……

……

……

(ب) تحدث عن إثنين من التقنيات التى يمكن من خلالها توفير الامن للشبكات.

……

……

……

……

(ج) عدد محتويات الشهادة الرقمية.

……

……

……

……

(د) عدد الدوال الخمسة المستخدمة في خوارزمية التشفير البيانات القياسية DES.

……

……

……

……

……

(هـ) عدد العناصر الأساسية التي تقيم بها نظم التشفير.

……

……

……

……

9 درجات

السؤال الرابع:

بالرسم فقط وضح الآتي: (3 درجات لكل)

(أ) هجوم إغراق الجهاز المستهدف بحزم التزامن (TCP SYN Attack)

(ب) هيكلية فيستل Feistel Structure

(ج) التشفير بالمفتاح العام(التشفير المتماثل)

15 درجة

السؤال الخامس (5 درجات لكل)

(أ) مستخدما التشفير بطريقة **Rail Fence** قم بتشفير النص "**This exam is three hours**".

……

……

……

……

……

……

……

(ب) معطى الكلمة المفتاحية **NETWORK ومفتاح خاص g** مستخدما خوارزمية **Key Phrase cipher** قم بتشفير النص "**Final Exam**".

……

……

……

……

……

……

……

(ج) معطى (**p = 11, q = 17, e = 7; M = 5**) قم بعمليتي التشفير وفك التشفير بإستخدام خوارزمية **RSA**.

……

……

……

……

……

……

……

بالتوفيق،،،