المذاكرة الأولى

القسم الأول: (4 علامات للسؤال الأول و5 علامات للثاني)

1. في حال أردنا تأمين السرية والوثوقية للمعطيات أثناء النقل، والسرية فقط للمعطيات أثناء التخزين، صف باستخدام مجموعة من الآليات الأمنية (تشفير، توقيع رقمي، تابع البصمة، كود وثوقية رسالة، معمي تناظري، معمي لا تناظري، مفتاح مشترك سري، مفتاح عام، مفتاح خاص) آلية مناسبة لتبادل وحفظ المعلومات.

المرسل: رسالة واضحة، يتم تشفيرها باستخدام المفتاح العام للمستقبل، وحساب تابع البصمة للرسالة الواضحة ومن ثم تشفير البصمة باستخدام المفتاح الخاص للمرسل
المستقبل: يستلم الرسالة المشفرة والتوقيع، يتم فك تشفير الرسالة المشفرة باستخدام المفتاح الخاص ومن ثم حساب بصمة الرسالة، يتم ايضاً فك تشفير التوقيع باستخدام المفتاح العام للمرسل والتأكد من مطابقة الناتج مع بصمة الرسالة المستلمة بعد فك تشفيرها، للتخزين يتم تخزين الرسالة المستلمة المشفرة فقط دون الحاجة إلى تخزين البصمة المشفرة (التوقيع الرقمي).

2. وصف الجمل التالية لتشكيلها لنقطة ضعف أو تهديد؟

#	السؤال	الجواب
a	معطيات هامة مرسلة عبر الشبكة بشكل غير مشفر	نقطة ضعف
b	استخدام كلمة مرور بشكل غير شرعي	تهديد
c	نفاذ غير مخول إلى المخدمات الشبكية	تهديد
d	برنامج التدريب الأمني (Security training) للموظفين غير مناسب	نقطة ضعف
e	فيروس كومبيوتر (computer virus)	تهديد
f	الادعاء بأن تكون عامل صيانة خارجي.	تهديد
g	لا يوجد مختص بأمن المعلومات.	نقطة ضعف
h	عدم مراقبة الباب الخارجي للمؤسسة.	نقطة ضعف
i	عدم وضع سياسة أمنية من قبل إدارة المؤسسة.	نقطة ضعف
j	النفاذ غير القانوني إلى الانترنت.	تهديد

جامعة الجزيرة الخاصة
ALJAZEERA PRIVATE UNIVERSITY

القسم الثاني: اختر الإجابة الأكثر دقة لكل منها، ولكل سؤال علامة واحدة

1. إن قطع الكبل الشبكي (وسيط النقل) المستخدم يعد تهديداً لـ:

a. السرية confidentiality
b. الوثوقية authentication
c. الإتاحة availability
d. السلامة integrity

2. في حال أردنا تأمين الحماية للمعطيات المتبادلة عبر الانترنت، أي من المعميات (أو الخوارزميات) التالية تؤمن السلامة في حال لم يكن الكيان المستقبل كائنا بشرياً؟

a. RSA
b. AES (Advanced Encryption Standards)
c. HMAC
d. ElGamal

3. أي من الأهداف الأمنية التالية تستطيع أن تمنع الأشخاص غير المخولين من الاطلاع على المعطيات المتبادلة بين جهازين حاسوبيين عبر الشبكة؟

a. السرية
b. وثوقية كيان
c. الإتاحة
d. وثوقية رسالة

4. أي من الآليات الأمنية التالية تستطيع أن تحقق السلامة (Integrity) وعدم النكران (Non-repudiation) معاً؟

a. المعميات التناظرية	b. المعميات اللاتناظرية
c. التوقيع الرقمي	d. MAC (Message Authentication Code)
e. تابع البصمة	f. الخياران b و c

5. أي من الآليات الأمنية التالية يعد الأنسب من أجل تحقيق السلامة؟

a. المعميات التناظرية	b. المعميات اللاتناظرية
c. لا يوجد	d. MAC (Message Authentication Code)

6. في حال أردنا تأمين السرية وعدم النكران فقط للمعطيات المتبادلة بين طرفي الاتصال، أي من الجمل التالية غير صحيحة؟

a. يمكن للمستقبل التأكد من صحة التوقيع باستخدام مفتاح المرسل العام.
b. يمكن أن يستخدم المستقبل مفتاحه الخاص لفك تشفير الرسالة.
c. لا يحتاج المستقبل لتخزين الرسالة المستقبلة مشفرةً.
d. لا يحتاج المستقبل لتخزين التوقيع المرفق بالرسالة.

مع التمنيات بالتوفيق

د.باسم صقور