Cairo University
Faculty of Engineering
Computer Engineering Department

جامعة القاهرة
كلية الهندسة
قسم هندسة الحاسبات

27 May 2015	تأمين الحاسبات وحالات استشارية Computer Security and Consultations	CMP 425 رابعة – هندسة الحاسبات

Answer as much as you can:-

TIME : Part-1 15 Pages 69 Minutes
Part-2 8 Pages 24 Minutes
All Exam : 23 Pages 120 Minutes

Use back pages if needed.

PART-1 Cryptography and Network Security

هذا الجزء مخصص له 96 دقيقة فقط من زمن الامتحان ومخصص له 80% من الدرجة الكلية للتحريرى

Assume any Missing data and State and Justify your assumptions.

1- There are 5 modes of operations of DES Block. One of these modes is Output Feedback (OFB). These modes involve how the different blocks are related together or how feedback is used.

1-a: State the five Cipher Modes of Operation and explain in one line.

-
-
-
-
-

1-b: Draw the block diagram of Out Feedback OFB cipher (SKETCH)

1-c: State and Explain the advantages and Disadvantages of Out Feedback OFB cipher.

Advantages Out Feedback OFB cipher	Disadvantages Out Feedback OFB cipher

1-d: For each of the modes of operation in the DES protocol named: ECB ,CBC and CTR

- Identify which decrypted blocks Px will be corrupted if there is an error in block C4 of the transmitted cipher text. (Explain).

2-a: Write the Deffie-Hellman Key Exchange technique .
Show in detail the details of your derivation and how Diffie-Hellman works.

Users A and B use the Diffie-Hellman key exchange technique with a Common prime q = 71 and a primitive root = 7.

- **If user A has private key $X_A = 5$, what is A's public key Y_A?**

- **If user B has private key $X_B = 12$, what is B's public key Y_B?**

- **What is the shared secret key?**

2-b: Describe Triple DES with 2 Keys (use only the space below).

2-c: What is the Double DES version of the 56-bit DES with 2 Keys each 56 bits.

2-d: Explain why Double DES with 2 Keys each 56 bits is much less secure than a single 112-bit DES? (Explain in detail and use sketch when possible).

3-a: You are asked to design a secure hash function. What are the characteristics needed in a secure hash function?

The characteristics of a secure hash function are:

1.

2

3

4

5

3-b: State and describe briefly the phases of operation of a virus or worm.

3-c: Describe how does a worm propagate

3-d: What is a honey pot ?

3-e: What is the main drawback of the one time pad cryptosystem?

4-a: Assume you have a Public Key distribution authority. Sketch the diagram showing how Public key Encryption is used to distribute Secret Keys. [PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation].

4-b: Sketch the diagram showing how Certificates are used in a Public Key distribution encryption. [PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation].

5-a: Assuming you can do 1 (ONE) encryption per second and the key size is 40 bits, how long would a brute force attack take? Give a scenario where this would be practical and another where it wouldn't. What happens if you double the key size?

5-b: About how many times more does a brute force key search take against a 112-bit DES than against a 56-bit DES?

5-c: What types of attacks are addressed by message authentication?

State and describe briefly at least 3 types of attack.

-
-
-
-

6-a: Draw, in detail, one round of the DES Algorithm.
[PUT on your sketch all necessary explanation to show how the operation is performed, its order and any necessary explanation].

6-b: Briefly define a group, ring, and field.

A group

A ring

A field

6-c: Use extended Euclidean algorithm to find the multiplicative inverse (if exists) of 826 mod 2789. Show steps in detail.

Cairo University
Faculty of Engineering
Computer Engineering Department

جامعة القاهرة
كلية الهندسة
قسم هندسة الحاسبات

May 2015	تأمين الحاسبات وحالات استشارية Computer Security and Consultations	CMP 425 رابعة – هندسة الحاسبات

Answer as much as you can:-

TIME : Part-1 15 Pages 96 Minutes
Part-2 8 Pages 24 Minutes
All Exam : 23 Pages 120 Minutes

Use back pages if needed.

PART-2 Consultation and Law

هذا الجزء مخصص له 24 دقيقة فقط من زمن الامتحان ومخصص له 20% من الدرجة الكلية للتحريرى

Take 24 Minutes Only to answer - 20% OF THE Total EXAM MARKS

Assume any Missing data and State and Justify your assumptions.

1- تقدم أحد الموردين لمناقصة لتوريد 200 حاسب شخصى لكلية الهندسة وتمت الترسية على عرضه طبقا للمواصفات الفنية التى تقدم بها فى عرضه وكان أقصى موعد لتسليمه الحاسبات بالكلية يوم 5 ديسمبر 2011 وقام بتوريد الحاسبات الشخصية الى مخازن الكلية ناقش الحالات التالية:

إذا قام المورد بتلسيم الكميات التالية فى المواعيد المحددة امام كل منها :

أ. عدد 40 حاسب شخصى فى 28 نوفمبر 2011
ب. عدد 30 حاسب شخصى فى 8 ديسمبر 2011
ج. عدد 20 حاسب شخصى فى 14 ديسمبر 2011
د. عدد 35 حاسب شخصى فى 22 ديسمبر 2011
ه- عدد 45 حاسب شخصى فى 15 يناير 2012

وكانت جميع الدفعات مطابقة للمواصفات المطلوبة والمقدمة فى عرض المورد وكان سعر الحاسب الشخصى الواحد 4000 جنيه طبقا لعرض المورد.

1-أ: ما هى الإجراءات التى يجب على الكلية اتخاذها قبل المقاول عند صرف مستحقاته لباقى الدفعات من أ الى هـ؟

a) كيفية صرف قيمة 40 حاسب شخصى والتى تم توريدها فى 28 نوفمبر 2011

b) كيفية صرف قيمة 30 حاسب شخصى والتى تم توريدها فى 8 ديسمبر 2011

c) كيفية صرف قيمة 20 حاسب شخصى والتى تم توريدها فى 12 ديسمبر 2011

d) كيفية صرف قيمة 35 حاسب شخصى والتى تم توريدها فى 17 ديسمبر 2011

c) كيفية صرف قيمة 45 حاسب شخصى والتى تم توريدها فى 15 يناير 2012

1-ج: احسب بالتفصيل القيمة الكلية لمستحقات المقاول (حدد بالتفصيل كيفية حساب القيمة وأكتب بلغتك الخاصة كيفية معالجة القانون لهذا الوضع)

2-1. اذكر قائمة بمحتويات المظروف الفني في المناقصة (بدون شرح) بلغتك الخاصة ورتب القائمة بطريقة منطقية (الأهم فالمهم نصف درجة السؤال تكون على منطقية ترتيب العناصر المكونة للعرض الفني ويجب ملاحظة أهمية ترتيب هذه المحتويات بطريقة منطقية الأهم فالمهم لتحديد مدى تقديرك لأهمية العناصر المختلفة للعرض الفني:

-1

-2

-3

-4

-5

-6

-7

-8

-9

-10

-11

-12

-13

-14

-15

-16

2-ب برأيك الشخصى لماذا نص القانون على تقديم العروض فى مظروفين فنى ومالى ويتم فتح المظروف الفنى أولا وبعد إعلان نتيجة التقييم الفنى يتم فتح المطروق المالى:

2-ج: أذكر أسماء اللجان التى يتم تشكيلها فى حالة المناقصة العامة من وقت الإعلان حتى الترسية على أحد العروض واستلام الأصناف بعد توريدها من الشركة الموردة واشرح فى جملة واحدة أو جملتين دور كل لجنة:

- لجنة
- لجنة
- لجنة

3-أ : أعلنت جامعة القاهرة عن مناقصة لتوريد (200) مائتين من الحاسبات الشخصية وتقدمت شركة القنال الهندسية مع 5 شركات أخرى للمناقصة (كان سعر الحاسب الواحد لشركة القنال الهندسية 5500 جنيه مصرى) وتمت دراسة العروض الفنية والمالية من اللجان الفنية والمالية بجامعة القاهرة لمدة 80 يوما بعد تاريخ فتح المظاريف الفنية وتمت ترسية المناقصة على شركة القنال الهندسة بسعر الحاسب الشخصى 5500 جنيه مصرى ولكن نظرا لحاجة الجامعة لكمية مختلفة عن الكمية المطروحة أصدرت الجامعة أمر توريد لشركة القنال بعدد مختلف من الحاسبات الشخصية عما جاء بكراسة الشروط والمواصفات للمناقصة ،

بعد انتهاء أعمال اللجان وأثناء التعاقد قررت جامعة القاهرة زيادة الكمية المطلوبة فى أمر التوريد وأصدرت الجامعة أمر توريد لعدد 300 حاسب شخصى بدلا من 200 حاسب ناقش موقف الشركة القانونى فى حالة عدم رفبتها فى زيادة الكمية من 200 الى 300 حاسب

هل من الضرورى التزام الشركة بزيادة الكنية وتوريد 300 حاسب شخصى اى 100 جهاز أكثر من كمية المناقصة نعم / لا:

<u>ناقش القضية من الناحية القانونية</u>

3-ب: قمت بافتتاح شركتك الخاصة لتوريد الحاسبات ومستلزماتها وأعلنت وزارة الصناعة عن مناقصة عامة لتوريد ما يلى:
100 حاسب شخصى وكان سعر الحاسب الذى تبيعه شركتك 5000 جنيه
100 طابعة ليزر من نوع HP1102 وكان سعر بيع الطابعة فى شركتك 2200 جنيه

حدد ما يلى: لكل نوع من أنواع التأمين أنواع التأمين المختلفة المتوقع تسليمها للإدارة المختصة بوزارة الصناعة وحدد فى كل حالة:

أولا: التأمين الذى يسلم مع المظاريف اسمة التأمين :. . . . .

قيمة التأمين المتوقعة: . . . . . جنيه مصرى

ثانيا: التأمين الذى يؤدى اذا تمت الترسية على شركتك اسمه التأمين: .. ..

قيمة التأمين المتوقعة: .. ..جنيه مصرى

ثالثا: حدد الطرق المختلفة التى يمكن لشركتك أداء التأمين بها :

-1

-2

-3

-4

-5

-6

4-أ: تقدم أحد الموردين لمناقصة لتوريد 300 حاسب شخصى لكلية الهندسة وتمت الترسية على عرضه طبقا للمواصفات الفنية التى تقدم بها فى عرضه وكان أقصى موعد لتسليمه الحاسبات بالكلية يوم 7 ديسمبر 2011 وقام بتوريد حاسبات الشخصية الى مخازن الكلية فى الموعد المحدد طبقا لما يلى:

- عدد 200 حاسب شخصى مطابق للمواصفات المطلوبة والمقدمة فى عرض المورد
- عدد 100 حاسب شخصى تم رفضها من لجنة الاستلام بسبب عدم مطابقتها للمواصفات المطلوبة

وكان سعر الحاسب الشخصى الواحد 4000 جنيه طبقا لعرض المورد مع العلم أن العرض المطابق للمواصفات **والتالى** للعرض كان بمبلغ 4500 جنيه وأغلى عرض مطابق للمواصفات بمبلغ 4700 جنيه

وضح تفصيلا الإجراءات التى يجب على الكلية اتخاذها قبل المقاول وكيفية التعامل معه بخصوص الأجهزة الغير مطابقة للمواصفات؟ وناقش الحالات المختلفة فى حالة عدم موافقته على إعادة توريد الحاسبات المرفوضة وما يطبق من إجراءات:-

5-ب : ما المقصود بالسلطة المختصة في قانون المناقصات والمزايدات

5-ت : أذكر الإجراءات التي يقوم بها رئيس لجنة فتح المظاريف التي تقدمت في جلسة فتح المظاريف وأذكر هذه الإجراءات بالعناك الخاصة وبترتيب منطقي من لحظة استلامه للعطاءات المغلقة (الفنية والمالية) وحتى انتهاء اللجنة من عملها

ويجب ملاحظة أهمية ترتيب الإجراءات بطريقة منطقية الأهم فالمهم لتحديد مدى تقديرك لأهمية العناصر المختلفة لعمل اللجنة:

-1

-2

-3

-4

-5

-6

-7

-8

-9

-10

-11

-12

-13

-14