Chapters 5, 8, 12, 13, 14, 15

We didn't have enough time to accomplish our mission of finishing the full book :D so we didn't study these chapters during the year.

Chapters 1, 3, 4, 7, 16

I think there were no questions in these chapters.

Chapter 2

1

Using a playfair matrix (It was drawn in the exam), encode the word "university" and show your steps clearly.

Answer: Page 41

Chapter 6

2

Output Feedback (OFB) is one of the DES modes. List the other four modes.

Answer: Page 181

3

Draw the block diagram of the OFB DES mode and illustrate it. Use symbolic forms in your illustration.

Answer: Page 187

4

Why is it not good to encrypt two plain texts using the same key in stream ciphers?

Answer: Page 191

Chapter 9

5

Draw the public-key cryptosystem that provides both authentication and secrecy. Illustrate it.

Answer: Page 265

Chapter 10

6

Draw the public-key distribution scenario. Illustrate it.

Answer: Page 293

7

How Diffe-Hellman Works? Show the derivation. What is it used for?

Answer: Page 289, 299

8

Two users are using Diffe-Hellman with alpha = 7 and q = 71. If Xa = 5, compute Ya. If Xb = 12, compute Yb. Compute the secret key. (this question is identical to problem 10.1 in the book)

Answer: Ya = (alpha)^Xa mod q … Yb = (alpha)^Xb mod q … k = (Ya)^Xb mod q = (Yb)^Xa mod q

Chapter 11

9

What are the three ways to do authentication?
Answer: Message Encryption, MAC, Hash Function

10

What are the requirements for a strong hash function?
Answer: Page 335

11

What is the difference between the weak collision resistance and the strong collision resistance?
Answer: Page 335

Chapter 17

12

What is the difference between SSL session and SSL connection?
Answer: 532

13

What are the SET participants? Draw the figure of them. How does it work?
Answer: 551, 552, 553

14

What are the SSL features that prevent the following attacks?
Note: there was a huge table consists of maybe 6 rows. There is an attack in each row (e.g. replay attack) and you have to write the SSL features that prevent it. Unfortunately and of course, I didn't have the time to read this entire huge table so I don't have anything to say.

Chapter 18

15

What is Salt? What is it used for?
Note: take care of this question … it is important to the extent that it was repeated in the exam … 20 pages, of course there will be duplicate questions.
Answer: Page 582

16

What are the two ways to protect passwords? (Actually I don't remember the question so well … I am also not sure of my answer of course … and for sure can't find it in the book :D)
My suspicious Answer: Encryption, Hashing

17

What are the four ways to eliminate guessable passwords? Tell a statement about each.
Answer: Page 587

Chapter 19

18

What are the four phases of viruses and worms?
Answer: 532

19

What are the functions performed by the propagation phase of a worm?
Answer: Page 607

Chapter 20

20

Fill a packet-filtering rules table given the explained rules in English.

Answer: Page 627 contains a table and full explanation of how to fill it. The one in the exam was very near to that table.

Concept Questions

21

Alice thinks that she has invented a protocol that makes her authenticate her peer (i.e. making sure that it's Bob who is talking to her). The protocol proceeds as follows:
1- Alice generates a pseudorandom number
2- Alice encrypts this number with a previously shared key with Bob (i.e. assume no one knows the key except Alice and Bob)
3- Alice sends the cipher text
4- Bob receives the cipher text
5- Bob decrypts the cipher text using the same shared key
6- Bob encrypts the output of step (5) using the same encryption key
7- Bob sends the output of step (6) to Alice
8- Alice receives this then decrypts using the same shared key
9- If Alice found the output of (8) the same number generated in (1), then It's true that Bob is the peer of Alice. Else, it’s not Bob who is communicating with Alice.

The question is: Is there an error in this protocol and if there is can you modify it to fix this error?

22

كان فى جدول لعروض تم تقييمها فنيا وكان موجود التقييم الفنى كرقم من 100 وكانوا كلهم زى بعض والسعر المعروض ودولة الشركة وبيقول اختار انهى شركة يرسى عليها المناقصة

فكنت المفروض تختار العرض الاقل فى السعر

23

زى السوال 22 بالظبط بس رغم ان الشركة المصرية كانت مقدمة عرض اعلى من اقل شركة فكان لازم تختارها هى لان عرضها كان اعلى ب اقل من 15% لكن فى السوال 22 كانت اعلى من الشركة صاحبة العرض الاقل باكثر من 15%

24

نفس الجدول بس التقييم الفنى كان مختلف بقى والاسعار مختلفة ... فكان المفروض تقسم القيمة المالية على التقييم الفنى وتختار الشركة الاقل

25

محتويات المظروف الفنى

26

مورد عمل توريد لاجهزة ... بعضهم لجنة الفحص وافقت عليه وبعضهم ماكانش مطابق للمواصفات ... ايه الخطوات اللى تتبعها الشركة بالنسبة للمورد وبالنسبة للاجهزة التالفة ... ويحصل ايه لو المورد مارضيش يغير الاجهزة ده ... الشركة ترد باجراء ايه؟

27

انواع التامين الاتنين ... وقيمتها وغرضها وامتى تسترد

28

شركة فى محافظة اسوان عايزه تعمل مناقصة ... ايه الاختيارات اللى قدامه واكتب جملة عن كل واحدة ... اللى هما مناقصة عامة ومحدودة ومحلية وممارسة محدودة وعامة

29

المفروض يتكتب ايه فى الاعلان عن مناقصة

30

ايه هما اللجان اللى بتعمل الاجراءات من ساعة ما يتم الاعلان عن المناقصة واكتب جملة على كل لجنة

1- Playfair cipher encrypt University using worldcup
2- BOb & Alic
3- Chapter 10 Pubic Key distribution using Authority
4- Chapter 9 , Securece & Authentication (A encrypts with PUb, PRa) ...
5- Chapter 10 , Deffie Hellman Algorithm , when it is used and a problem on it
6- a-The life cycle of Virus & Worms
   b-the propagation of worms
7- a-Write the block cippher modes (EBC, CTR, C,,)
   b- Draw the diagram for OFB
8- a- SSL session & SSL connection
   b- 3 ways to do MAC
   c- SET diagram and scenario steps
9- a- 6 requirements of public key
   b- Attacks that ccan be handled with MAC
10- a- Why Stream Cipher is not recommended to use same key?
    b- Requirements of strong hash fn.
    c- compare between weak collision and strong collision?
11- a- What is SALT in UNIX password managment?
    b- 2 different ways to keep a password file secure(I guess)?
    c- 4 methods to get passwords that are not gessable
12- a large table related to SSL taking about each attach and how to overcome it , (copy paste from book)
13- A problem on firewall ,it looks similar to the table in the book (src ,dst ,port , allow or disallow)

Mon2sat :
1- it is really important to know that the law favours egyptians over forigeners with a certain percentage .(3 problems on it , choose who will win the job)
2- a- 2nw3 el t2meen
   b- 15 points of mazroof fany
3- kolyat handasa 3malt mon2sat wa rasyat 3la wa7ed yawrd 300 computer
   gab 200 motabkeen lel mawsfat wa 100 mesh motbkeen
   ehh elyy ya7sal ,, and some more questions on that