The German University in Cairo
Dpt. for Media Engineering and Technology
Assoc. Prof. Georg Jung, Eng. Mohamed Khamis

May 26, 2013

CSEN 1001: Computer and network security

Spring 2013

Final exam

Barcode

Instructions. Please read carefully before proceeding.

(a) The duration of this exam is **180 minutes**.

(b) Non-programmable calculators are allowed.

(c) No books or other aids are permitted for this test.

(d) This exam booklet contains a total of **12 pages**, including this one. Two extra sheets of scratch paper are attached and have to be kept attached. **Note that if one or more pages are missing, you will lose their points. Thus, you must check whether your exam booklet is complete.**

(e) Write your solutions into the space provided. If you need more space, write on the back of the sheet containing the problem or on the two extra sheets and indicate that clearly on the problem page. **Scratch sheets will not be graded unless a reference on the problem page indicates that the solution extends to the scratch sheets.**

(f) When you are told that time is up, stop working on the test.

Please checkmark your major and exam type!

☐ CS (computer science)

☐ DMET (digital media engineering and technology)

☐ Regular final

☐ Midterm/final (excused for midterm)

☐ Makeup / second makeup

Good luck!

Do not write anything below this line.

Exercise	1	2	3	4	5	6	7	Σ
Possible marks	6	16	6	15	5	12	Bonus: 3	**60**
Final marks								

Exercise 1 Key Management (6 Marks)

Alice and Bob have each generated a public and private key pair. However, they do not know each others' keys yet. Now they are trying to exchange a message M over a network.

(a) What is the procedure to exchange the message confidentially, if only passive attacks need to be considered? (3 Marks)

(b) What can be done to mitigate the risk if active attacks are possible? (3 Marks)

Exercise 2 MCQ (16 Marks)
Mixed trivia and understanding

(a) Choose the correct answer and **state the reason**.

(i.) When exchanging a key, Diffie-Hellman is used to counter ... attacks (3 Marks)

☐ Passive
☐ Active

Reason:

(ii.) In Public/Private key cryptography, even the sender will no longer be able to read the message after encrypting it with the receiver's public key. (3 Marks)

☐ True
☐ False

Reason:

(iii.) In the Advanced Encryption Standard (AES) cipher, "shift rows" is a step that contributes to... (3 Marks)

☐ Confusion
☐ Diffusion

Reason:

(iv.) RSA is an example of ... ciphers. (3 Marks)

☐ Symmetric
☐ Asymmetric

Reason:

(b) Check **all** that apply

(i.) The Data Encryption Standard (DES) is based on (2 Marks)

☐ Feistel Cipher
☐ Stream Cipher
☐ Rijndael Cipher
☐ Vigenère Cipher
☐ Caesar Cipher

(ii.) The Caesar Cipher is a(n) (2 Marks)

☐ SP-Network
☐ Block Cipher
☐ Stream Cipher
☐ Substitution Cipher
☐ Permutation Cipher

Exercise 3 Mathematical cipher attacks (6 Marks)
Diffie-Hellman key exchange

Alice and Bob use the Diffie-Hellman algorithm to exchange a secret key. Eve intercepts the following values:

$$p = 283$$
$$g = 12$$
$$A = 77$$
$$B = 196$$

(a) What are the steps for Eve to compute s? (3 Marks)

(b) You are Eve. Actually compute s. (3 Marks)

Exercise 4 Stream and Block ciphers (15 Marks)
Vigenère, One-time-pad, and Running Key cipher

In this exercise we develop a relatively secure cipher from the idea of the Vigenère cipher but still find a vulnerability. The scenario is that Alice wants to communicate a message (a lengthy text in English) to Bob without Eve being able to read it.

(a) Imagine that instead of a password of finite length, Alice and Bob chose a virtually infinite password (*i. e.*, the password is at least as long as the message) for a Vigenère cipher. For simplicity they secretly agree on using the text of the five books of the "Hitchhiker's Guide to the Galaxy" trilogy by Douglas Adams as the password (keystream).

Which of the following attacks **works** on a standard Vigenère cipher but **does not work/is not feasible** on this variation? Check all that apply and give a short explanation: (5 Marks)

☐ Frequency analysis

☐ Previously computed table of discrete logarithms

☐ Kasiski analysis

☐ Pattern word attack

☐ Brute force

Note. This type of cipher is called a **Running Key cipher**.

(b) Since the Vigenère lookup in the tabula recta is tedious to implement on a computer, Alice and Bob decide to use the ASCII code representation of message M and keystream K and instead of the table lookup perform a bitwise XOR ("$\oplus$") to obtain the ciphertext C, so

$$C = E_K(M) = M \oplus K, \text{ and}$$
$$M = E_K(C) = C \oplus K.$$

Is the cipher now more secure (*yes* or *no*)? Explain! (2 Marks)

☐ Yes.
☐ No.

(c) Regardless of what you found out above, let us assume that encrypting English text with English text is **insecure**. In other words, if $C = M \oplus K$ and M and K are both English texts, then there is an attack on C that can reveal M and K.

If Alice and Bob decide to use a high quality pseudo random number generator for the keystream instead of the Douglas Adams novels, will the cipher be more secure (*yes* or *no*)? Explain! (2 Marks)

☐ Yes.
☐ No.

(d) Again, assume that encrypting English text with English text is **insecure**, and for this part assume that encrypting English text with a good random stream is **secure**.

Alice sends to Bob two messages M_1 and M_2 of the same length, encrypted using the same high quality pseudo random keystream K_0 with the same seed, so with exactly the **same key twice**:

$$C_1 = M_1 \oplus K_0, \text{ and}$$
$$C_2 = M_2 \oplus K_0.$$

Unfortunately, Eve intercepts both messages. Show how (under the above assumptions) Eve can extract both messages M_1 and M_2 from only C_1 and C_2. (6 Marks)

Hint. Note that $\oplus$ is commutative and that for all X we have that $X \oplus X = 0$ (self inverse). What else?

Exercise 5 Avalanche effect (5 Marks)

(a) Given an encryption function $f(x)$, what kinds of trials can you do in order to check whether or not it achieves diffusion? (2 Marks)

(b) Which of the main components of an SP-Network contributes to confusion, and which contributes to diffusion? and why? (3 Marks)

Exercise 6 Security management (12 Marks)
Cloud service

You are responsible for the security of a cloud storage and computing service. Naturally, you need to protect your customers' data by fully encrypting their reserved blocks on your server. You distinguish:

IT team. This team has access to the server and all system files for maintenance.

Executive team. This team has access to customers' addresses and billing data.

The customers. Each customer has access to his reserved block on the file system.

(a) When a customer enters/edits their billing data, it has to be protected from unauthorized access. Choose one of the following encryption schemata (explain your choice): (1 Mark)

- ☐ triple DES
- ☐ RSA
- ☐ AES

(b) Given your choice above, write for each group which key should be available to them (write the key type or "*none*"): (1 Mark)

- IT team:
- Executive team:
- Customer:

(c) The IT team has access to the system files, including sensitive files such as `/etc/passwd`. Describe how you prevent them from using an executive team member's credentials. (2 Marks)

(d) Sales expert Alice (executive team) does not have PGP/RSA installed on her private e-mail client, however she does have a public/private key pair which she uses when communicating over her corporate mail client. She wants to send a sensitive message to sales expert Bob as she often does, however she currently cannot use the corporate client. She considers two options:

(1) She sends this one e-mail unencrypted.
(2) She uses an online encryption/decryption service she found at `www.isilver.com`, where she can submit the message and Bob's public key and receives a ciphertext which she sends to Bob. Bob can likewise decrypt the ciphertext by uploading it together with his private key to the same site.

Which option poses the **greater** security risk? Please explain! (2 Marks)

(e) Which algorithm would you use to secure the customers' data inside their blocks? Explain your answer. (2 Marks)

- ☐ AES
- ☐ DES
- ☐ RSA

(f) Based on your choice above, who should hold which key for the customer data? Write the key type or "*none*": (1 Mark)

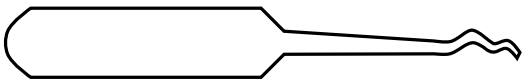
- IT team:
- Executive team:
- Customer:

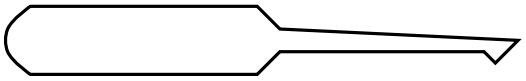
(g) Propose a mitigation against flooding of your service by bots masking as new customers. (1 Mark)

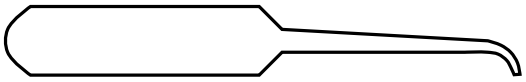
(h) Which precautions are necessary at a minimum to mitigate customer-interface-side attacks on your site? (2 Marks)

Bonus Exercise 7 Physical security (3 Marks)
Simple devices

Please name instruments given below as schematics

(a)  (1 Mark)

(b)  (1 Mark)

(c)  (1 Mark)

Scratch paper sheet 1

contents of the scratch paper will not be graded unless a reference on the problem page indicates that a solution extends here

Scratch paper sheet 2

contents of the scratch paper will not be graded unless a reference on the problem page indicates that a solution extends here