CORRECTED

COM 402 Midterm, 9.04.2019

Identification
Please encode your SCIPER on the right (one digit per column), and write your first and last names below.

Firstname and lastname:

.....

.....

☐0	☐0	☐0	☐0	☐0	☐0
☐1	☐1	☐1	☐1	☐1	☐1
☐2	☐2	☐2	☐2	☐2	☐2
☐3	☐3	☐3	☐3	☐3	☐3
☐4	☐4	☐4	☐4	☐4	☐4
☐5	☐5	☐5	☐5	☐5	☐5
☐6	☐6	☐6	☐6	☐6	☐6
☐7	☐7	☐7	☐7	☐7	☐7
☐8	☐8	☐8	☐8	☐8	☐8
☐9	☐9	☐9	☐9	☐9	☐9

Please wait for instructions before opening this document

- This is a **closed book** exam. Books, notes and electronic devices are not allowed.

Multiple choice questions:

- There are 16 multiple choice questions
- Only one answer is correct, there are no penalties for wrong answers
- Make a mark *inside* the box corresponding to your answer
- Use an eraser or white-out fluid if you ticked the wrong answer
- If you use white-out fluid, do not try to re-draw the boxes.

Open text questions:

- There are 4 open text questions
- Please write your answers in the corresponding text boxes
- Do not write more than three lines
- Any text outside of the boxes or after three lines will be ignored
- Do not tick the w, p, c boxes of the top of the text boxes.

Questions and leaving during the exam

- The supervisors will not answer any questions regarding the content of the exam questions
- You can not leave and come back during the exam.

Question 1 Which is a good setting for protecting memory pages ?

- !w and x (you can never write but you can always execute data in a page)
- x xor w (either you can execute or you can write data in a page)
- r xor x (either you can read, or you can execute data in a page)
- r xor w (you can either read or write to a memory page)

Question 2 Private information retrieval

- PIR does not allow “write" operations in the database.
- PIR works only if the database has a single user.
- For IT-PIR to work, all data have to be encrypted while being at rest in the database.
- IT-PIR and cPIR are synonym (they designate the same operating principle).

Question 3 What is a rootkit?

- A rootkit is a malware that encrypts all music files
- A rootkit modifies a system to hide the presence of malware
- A rootkit is used by the root user to search for malware
- A rootkit is a malware that propagates automatically

Question 4 If a hash function is pre-image resistant, this means that

- given an input to the hash function there is no way to find two different outputs of the function
- it is not possible to find any two inputs of the hash function that would hash to the same output
- given an output of the hash function, there is no way to find an input that would generate the same output
- given an input and an output, there is no way to find a second input that would generate the same output

Question 5 Let us assume the following anonymized database:

Zip code	Age	Salary
345**	2*	10K
234**	5*	10K
563**	3*	30K
345**	2*	30K
234**	5*	10K
563**	3*	30K
234**	3*	30K

If you publish this database you can be sure that, by using the database:

- Nobody can learn the salary of people in their 20s living in zip code 234**.
- Nobody can guess the salary of people in their 20s with an error smaller than 30K.
- Nobody can learn the salary of people in their 30s.
- Nobody can learn the salary of people in their 50s living in zip code 234**.

Question 6 Let message m=user_role|timestamp be a content of a session cookie, where user_role is an authenticated user's role on the website (one of moderator, admin, student), and timestamp is a Unix timestamp. What format of the resulting cookie *is sufficient* to prevent tampering of the message (K is the secret key used in the HMAC function by the website owner):

- base64(m)|HMAC(K,base64(m))
- m|HMAC(K,m)
- none of the HMAC constructions, since the user could use K to calculate any HMAC
- both HMAC constructions

Question 7 According to the privacy by confidentiality paradigm, one of the goals of privacy technologies is to distribute trust when it comes to safeguarding users privacy. Let us assume that we have a cryptographic primitive that allows to split the users' data into shares (such that all shares are needed to recover the original data). A good approach to comply with the distributed trust goal is to:

- Store the shares encrypted in one server
- Store the shares in virtual machines hosted in different cloud providers.
- Store the shares in different virtual machines in Amazon Cloud.
- Store the shares in different servers owned by the same entity.

Question 8 What is a typical drawback of symmetric encryption?

- it requires a secure transfer of the key
- it is slower than asymmetric encryption
- it can not be used to authenticate messages
- All of the above

Question 9 Which is the best way to protect against SQL injections ?

- use only indirect object references
- escape all occurrences of single and double quotes (' → \', " → \")
- reject any input that contains SQL keywords (e.g. union, select)
- use prepared statements

Question 10 The Republic of Nonexistingstan wants to release a census of their population every week. They use differential privacy to increase privacy when releasing statistics with $\epsilon = 0.001$. Every week, they draw fresh differentially-private noise and add it to the raw counts. Then, they compute the statistics. After doing three weeks doing this process:

- The citizens never have privacy.
- The citizens have more privacy than the first week.
- The citizens have less privacy than the first week.
- The citizens have the same privacy as the first week.

Question 11 Homomorphic encryption

- An encryption scheme is called partially homomorphic if it supports one arithmetic operation.
- Homomorphic cryptography is generally faster in terms of execution time than symmetric cryptography.
- Paillier is a fully homomorphic encryption scheme.
- Homomorphic encryption cannot be used with cloud computing.

Question 12 Stream ciphers are malleable because:

- You can encrypt text of arbitrary length
- If you encrypt the cleartext twice, you get the cleartext
- If you flip a bit in the cipher text, the same bit of the clear text will be flipped
- If you use the same IV twice, the cipher stream is identical

Question 13 During the execution of a function call, what is the relation of the stack pointer and the base pointer ?

- the stack pointer contains the address of the base pointer
- the base pointer contains the address of the stack pointer
- the address of the base pointer is *greater* than the address of the stack pointer
- the address of the base pointer is *smaller* than the address of the stack pointer

Question 14 Let us assume that Instaclan, an application to upload group photos, provides users with three privacy settings. 1) the photo will be seen only by your friends, 2) the photo will be seen by your friends and their friends, 3) the photo will be seen by only one friend to be selected. All of these settings ensure that:

- The Internet Service Provider cannot see the photo.
- Nobody that is not a friend of the user can see the data.
- The service provider cannot see the photo, since the service provider is not a friend.
- None of the above.

Question 15 A web application uses the following link `https://is-aca/show_info_and_grades?sciper=493813` to display information and the grades of a logged-in student. If the programmer was not careful, which type of vulnerability might be exploitable in this page?

- SQL injection
- Cross Site Scripting
- Insecure direct object reference
- all of the above

Question 16 Databases typically provide the following types of access control:

- role based (RBAC) and discretionary (DAC)
- read xor write access
- role based but not discretionary
- discretionary but not role based

Question 17 In 3 lines, explain a concrete application of attribute-based credentials of your choice, not seen at the lecture, and mention the key properties that are fulfilled by the use of this technique.

☐w ☐p ■c

.....

.....

.....

Question 18 Why does ASLR protect against buffer overflow attacks?

☐w ☐p ■c

.....

.....

.....

Question 19 Give two reasons why it is important to salt password hashes

☐w ☐p ■c

.....

.....

.....

Question 20 Morty wants to play a prank on Rick. The prank involves posting several comments signed by a pretty Alien on a website hosted by Rick. Because he is afraid that Rick will send him to another dimension if he does not like the prank, Morty uses Tor. The onion router he uses as an entry node is controlled by Rick. As an additional protection, Morty also posts the same message on websites hosted by other members of the family using Tor. Does this method provide Morty with Unlinkability and/or Anonymity with respect to Rick? And the other family members? (Justify)

☐w ☐p ■c

.....

.....

.....

Corrected