COM 402 Final Exam, 17.06.2019

Name: **name**

Sciper: **123456**

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 10 multiple choice questions, counting 1 point each.
- Only one answer is correct, *there is a 0.25pt penalty for wrong answers*
- Make a mark *inside* the box corresponding to your answer
- Use a pen to mark your answers. Pencils are not allowed.
- Use a white-out fluid or tape if you ticked the wrong answer
- If you white-out a wrong answer, do not try to re-draw the boxes.

Open text questions:

- There are 21 open text questions, counting 1 point each.
- 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

- The supervisors will not answer any questions regarding the content of the exam questions

Disclaimer: Some of the material has not been covered in the fall semester 2019.

Question 1 The Moodle developers would like to enable the posting of comments that give plausible deniability to the students regarding being the author of the message. Which technology would you recommend to the Moodle developers to look into:

□ K-anonymity
□ Differential privacy
■ Anonymous credentials
□ Default privacy settings

Question 2 In buffer overflow the assignments, you probably added a `NOP` sled in the attack buffer. Which of the following is true?

□ Adding NOPs is necessary to overflow a buffer
□ NOP sleds bypass ASLR (address space layout randomization)
■ Using a NOP sled, the attacker needs to approximately but not precisely guess the address of the shellcode
□ To execute the shellcode, the NOP sled can be placed either before or after the shellcode, as long as the control flow jumps somewhere in the NOP sled

Question 3 Which of the following statements about blockchains is true:

□ In Bitcoin, it is impossible to relate two transactions involving the same user
■ Ethereum supports smart contracts
□ In a private (or permissioned) blockchain, anyone can join the blockchain provided it has enough computing capabilities
□ To break a cryptocurrency such as Bitcoin, it is sufficient for a miner to control 1/3 of the total computing power

Question 4 The *no write-up* rule states that subjects may not write or modify objects that are at a higher level. In which type of access control is this rule used:

□ Discretionary access control
■ Mandatory access control, when protecting integrity
□ Role based access control
□ Mandatory access control, when protecting confidentiality

Question 5 Consider the following command that defines some access to columns of a database table:

```
grant SELECT,UPDATE,INSERT (name, address) ON com402.students to bob@localhost;
```

This is a typical example of which type of access control:

□ Mandatory access control, when protecting confidentiality
□ Role based access control
□ Discretionary access control
■ Mandatory access control, when protecting integrity

Question 6 Private Information Retrieval…

□ Can be implemented exclusively in an information-theoretic setting

□ Is the best solution in the case where write operations in a database need to be concealed from the database manager

□ Requires the usage of fully homomorphic encryption

■ Can support multiple users accessing the same database

Question 7 Model stealing is an attack whereby an adversary is able to reconstruct a machine learning model by observing its outputs. If the model is linear, we have seen in the class that to recover d variables, the adversary needs $d+1$ queries. When the model is non-linear (e.g., a neural network), however:

□ The adversary needs d^n queries where n is the number of layers

■ The adversary can steal by using inputs and outputs to train an equivalent model

□ The model is so complex that model stealing is not possible

□ Model stealing is possible using adversarial examples

Question 8 A core operation in RSA decryption is $a^d \; mod \; n$, with secret key d. A very similar operation is involved in ElGamal, DSA, and ECC. The following pseudocode represents the square and multiply algorithm, frequently used to implement this operation.

```
Function exp_by_squaring_iterative(x, n)
  if n < 0 then
    x := 1 / x;
    n := -n;
  if n = 0 then return 1
  y := 1;
  while n > 1 do
    if n is even then
      x := x * x;
      n := n / 2;
    else
      y := x * y;
      x := x * x;
      n := (n − 1) / 2;
  return x * y
```

Your friend decides to write his own implementation, which you can see below.

```
typedef unsigned long long uint64;
typedef uint32_t uint32;

/* This really wants to be done with long integers */
uint32 modexp(uint32 a, uint32 mod, const unsigned char exp[4])
  int i,j;
  uint32 r = 1;
  for(i=3;i>=0;i--) {
    for(j=7;j>=0;j--) {
      r = ((uint64)r*r) % mod;
      if((exp[i] >> j) & 1)
        r = ((uint64)a*r) % mod;
    }
  }
  return r;
}
```

Which of the following is true?

☒ The implementation is not secure because not all calls execute the code in the *if* branch

□ The implementation is secure whether or not an attacker knows the source code

□ The implementation is not secure because not all calls execute all the iteration of the second *for* loop

□ The implementation is secure as long as an attacker does not know the source code

Question 9 You configure the *com402.epfl.ch* server to include in its HTTP response header: `Strict-Transport-Security: max-age=31536000"`. The com402 server is not in the HSTS-preload list of any browser. Which of the following statements are true:

□ This is an example of certificate pinning

■ Clients that observe this response header can tell for future connections whether they are victim of an attack that converts an HTTPS connection into an HTTP connection

□ An attacker cannot perform a man-in-the-middle HTTP-downgrading on the very first connection of a user to the com402 server

□ The server must use a self-signed certificate

Question 10 Swiss e-voting protocols use verification codes to implement individual verifiability. These codes protect against

□ breaking vote secrecy on the client

□ breaking vote secrecy on the server

□ modification of votes on the server

■ modification of votes on the client

Two factor authentication

Consider the following two-factor authentication methods that can be used to authenticate on a web site:

- An OTP token that displays a new one-time-password every time you click on a button
- A U2F token that stores private keys and uses them to sign a challenge provided by a web server you want to connect to.

Question 11 Describe an attack where the attacker can log into the victims account when OTP is used.

□w □p ■c

....

....

....

Question 12
Explain why this attack would not work if the account was protected by an U2F token.

□w □p ■c

....

....

....

Format strings

Question 13 Why does a stack canary not protect against format string vulnerabilities?

□w □p ■c

....

....

....

Kerberos

Question 14 The Kerberos protocol makes use of tickets and authenticators.
What are the authenticators used for ?

□w □p ■c

....

....

....

Question 15 For more security, Kerberos can use pre-authentication, which means that an authenticator is already sent by the client with the first request.

What is the security advantage that pre-authentication provides?

□w □p ■c

....

....

....

Stream ciphers

Question 16 Why is it particularly important to use unique IVs when encrypting data with a stream cipher?

□w □p ■c

....

....

....

XSS

Question 17 Describe the difference between a reflexive and a persistent cross-site scripting attack.

□ w □ p ■ c

....

....

....

Question 18 Which of both attacks has the greater impact ? justify

□ w □ p ■ c

....

....

....

Selecting Machine Learning Models

You are the new VP for Education at EPFL. Your team tells you that they want to install a new plagiarism detection mechanism. They propose to buy a tool called *YouAreCaught* for Master theses. In the specifications of this tool they promise that:

- *YouAreCaught* misses 10% of the True plagiarism cases
- *YouAreCaught* makes mistakes on 3% of the False plagiarism cases, flagging them as plagiarism

Question 19 You know that at EPFL students are very honest, i.e., only 5 in 1000, plagiarise in their Master thesis. Is *YouAreCaught* a good tool for you? Justify

□w □p ■c

....

....

....

Question 20 What percentage of students need to be cheating for *YouAreCaught* to provide good performance?

□w □p ■c

....

....

....

Selecting Privacy Enhancing Technologies

A friend asks you to recommend a good privacy technology. What would you recommend if:
(Justify all answers – think about potential adversaries)

Question 21 Your friend is a journalist that wants to inform another journalist about some corrupted behaviour of the Editor-in-Chief. The documents that incriminate the Editor-in-Chief are on her machine at the newspaper's headquarters, and so is the computer of the receiving journalist. Your friend does not have a USB stick or any other hardware to protect herself. Thus she wishes to send the documents over an anonymous communication channel.

□w □p ■c

Question 22 Your friend is a nurse that wants to inform a journalist about some corrupted behaviour of the Head of Medicine in his hospital. The documents that incriminate the Head of Medicine are on his machine at the hospital. The computer of the journalist is in the newspaper headquarters. Your friend does not have a USB stick or any other hardware to protect himself. Thus, he wishes to send the documents over an anonymous communication channel.

□w □p ■c

Question 23 Your friend is building an new mobile game. To ensure that the game is not a burden for users' devices your friend wants to make sure it does not consume too much battery. However, your friend is aware that if the app sends the exact consumption of the users then she will be able to identify them and track them over time. Thus, he wants a technology to understand the game's consumption in a privacy-preserving way.

□w □p ■c

Pallier Homomorphic Encryption

Recall the Paillier encryption scheme. Let p and q be two independent primes subjected to $gcd(pq, \phi(p,q)) = 1$ with $\phi : (a,b) \to (a-1)(b-1)$.

We define $n = pq$ a RSA modulus and $\lambda = \phi(n) = \phi(p,q)$.
Let $\mu = [\phi(n)]^{-1} \mod n$.

Denote by $\mathcal{P}$ the plaintext space and $\mathcal{C}$ the ciphertext space.

Let (λ, μ) be the private key and n the public key.

For $m \in \mathcal{P}$ and a nonce r sampled from $\mathbb{Z}_n^*$ uniformly at random:

$$Enc(m) = (1+n)^m \cdot r^n \mod n^2$$

$$Dec(c) = \frac{[c^{\phi(n)} \mod n^2] - 1}{n} [\phi(n)]^{-1} \mod n$$

Question 24 1. Show that this scheme is homomorphic between $\mathcal{P}$ and $\mathcal{C}$.
For m_1, $m_2 \in \mathcal{P}$, for $r_1, r_2 \in \mathbb{Z}_n^*$,

□w □p ■c

....

....

....

Question 25 Chose $p, q \leq 6$ and encrypt the message m=2 using a nonce r=1. Explain why 2,3 is not a good choice for p, q.

□w □p ■c

....

....

....

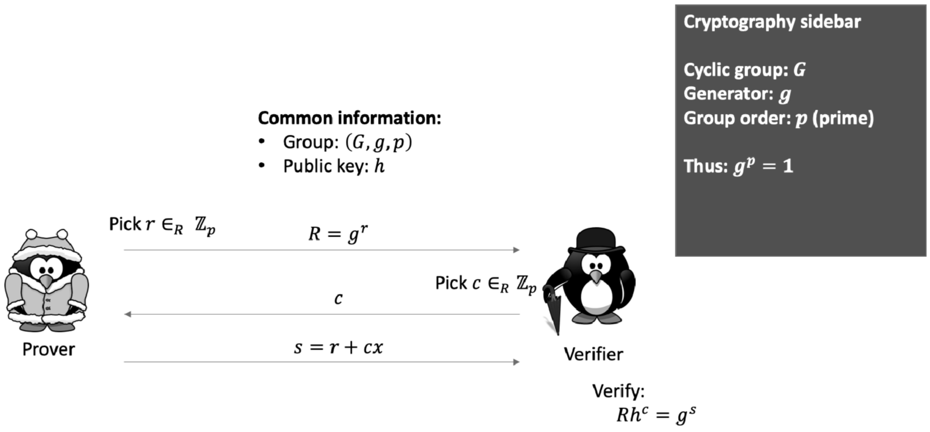
Zero-Knowledge Proofs

Question 26 Which of the following properties need to be satisfied by a zero-knowledge proof? Write **ONLY** the three required properties.

- Completeness
- Quantum security
- Soundness
- Anonymity
- Non-repudiation
- Zero-Knowledge
- Non-interactive
- Homomorphic

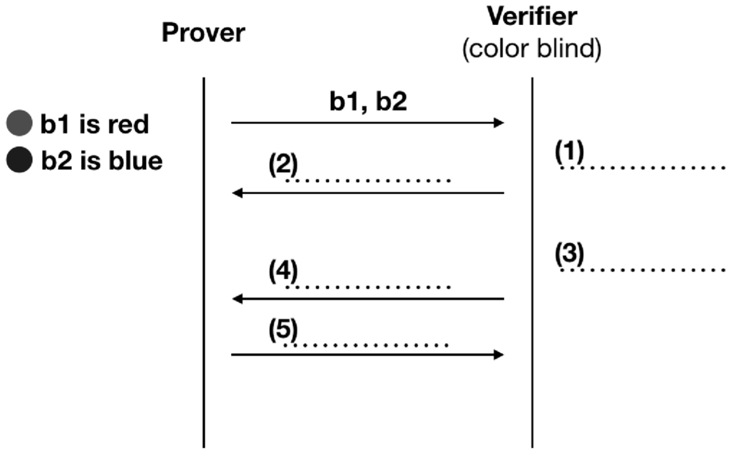
□w □p ■c

Question 27 In the following protocol (Figure below), which relation is proved by the prover?



□w □p ■c

Question 28 Consider the following setup. A prover owns two balls ($b1, b2$) of two different colors. The prover wants to prove to a color-blind verifier that he is not color-blind and that he can distinguish one ball from the other one. Design a zero-knowledge protocol to achieve this utility with soundness 1/2.



Fill in the dashed lines (1) to (5). Dashed lines at the verifier side represent actions. Dashed lines over an arrow represent a message.

□ w □ p ■ c

Differential Privacy

Question 29 Let $f : D \to \mathbb{N}$ be a query function that takes as input a dataset $X \in D$ and returns an integer output. Recall the Laplace mechanism for achieving differential privacy: The Querier obtains $f(x) + \texttt{noise}$, where $\texttt{noise}$ is sampled from $\mathsf{Laplace}(\frac{\mathsf{sensitivity}(f)}{\varepsilon})$. This mechanism is ε-DP. Consider the following mechanism: The Querier obtains $\lfloor |f(x) + \texttt{noise}| \rceil + 1$ (rounded and absolute value so that the output domain of the mechanism is $\mathbb{N}$). What is the epsilon-value of DP that this mechanism satisfies? Why? Use the compositionality or post-processing properties of differential privacy to justify.

□ w □ p ■ c

....

....

....

PIR

Consider a multi-party IT-PIR protocol where m servers, each denoted as S_j, all hold the same dataset $X \in \{0,1\}^n$ (each *record* in the dataset is a bit). A Querier wants to privately obtain the i-th record from the dataset. For that, she builds a query vector $q \in \{0,1\}^n$ as follows:

$$q_j = \begin{cases} 1, & \text{if } j = i \text{ is the element that the Querier wants to obtain} \\ 0, & \text{otherwise} \end{cases}$$

For all servers but the last one, she randomly generates a bit vector $s_j \in \{0,1\}^n$. For the last server t, she generates the s_t such that the following holds:

$$q = \bigoplus_{j=1}^{m} s_j,$$

Then, she sends each s_j to the server S_j. Then, each server S_j computes the response r_j:

$$r_j = \bigoplus_{k=1}^{n} [s_{jk} \wedge X_k]$$

and sends back the result r_j to the Querier.

Question 30 ow many servers does an adversary need to control to de-anonymize the query? Disrupt the operation? Justify.

□ w □ p ■ c

....

....

....

Password cracking

Question 31 Explain the advantage of dictionary password-cracking attacks as compared to brute-force attacks.

□ w □ p ■ c

....

....

....