INFO-F514: protocols, cryptanalysis and mathematical cryptology
Examples of exam questions

Liran Lerman and Christophe Petit
Université libre de Bruxelles

January 30, 2026

Your knowledge and understanding of the course content will be assessed through an oral exam. During the exam, you will receive a question and get some time to prepare your answer to it, before presenting it to us. We may ask follow-up questions during your presentation to better assess your understanding of the material (a typical follow-up question will start with "Why?").

This document includes a list of potential exam questions, organized by chapter. The lists are provided to help you gauge our expectations, and are not meant to be exhaustive.

1 e-voting

1. Explain the meaning of "end-to-end verifiable voting system". Describe how advanced cryptographic tools can be used to build these systems.
2. Here is a research paper [...] Choose one advanced cryptographic tool covered in the lectures, and explain how it is used to build an e-voting protocol in this paper.
3. Here is a sketch of an e-voting scheme [...]. Explain how to realize step 3 of the protocol using advanced cryptographic tools.
4. Compare the homomorphic encryption and mixnet approaches for e-voting. What are their respectives advantages and drwabacks?
5. Suppose a weighted election with three categories of voters V_1, V_2, V_3 voting yes (1) or no (0), and respective weights ω_1, ω_2 and ω_3, ie the result of the election is $v = \omega_1(\sum_{v \in V_1} v) + \omega_2(\sum_{v \in V_2}) + \omega_3(\sum_{v \in V_3})$. Explain how to use exponential ElGamal to encrypt the individual votes when $\omega_1 = 1/3$, $\omega_2 = 1/4$ and $\omega_3 = 5/12$, and then compute an encryption of the result. Describe the confidentiality guarantees provided by such a system.
6. Reduce the security of exponential ElGamal to the security of ElGamal.
7. Explain what is a treshold encryption scheme, and describe one construction.
8. Describe the Helios voting system.

2 Provable security

1. Explain the "provable security" methodology, then illustrate it with an example.
2. "If a system is provably secure, then it is probably not secure." Do you agree with this statement? Motivate your answer.

3. Suppose a new attack is found on finite field discrete logarithm problem, with a complexity $L(1/5)$. Discuss the potential impact of this attack on our digital security infrastructures.

4. Define IND-CPA security, and show that ElGamal encryption scheme is IND-CPA secure.

5. Consider the following variant of ElGamal encryption scheme [...]. Explain how CCA attacks on ElGamal are defeated in this variant.

6. Consider the following (informal) security definition : let $\mathcal{F}$ be a family of functions, and consider a security game for a public key encryption scheme where the challenger picks a pair of keys (SK, PK); then the adversary can make *related key queries* and receive answers, then the adversary sends two messages to the challenger and receives back the encryption of one, and finally the adversary can choose and receive answers from more *related key queries*. A *related key query* consists of a function $f \in \mathcal{F}$ and a ciphertext c, and its answer is a valid decryption of c under the secret key $f(SK)$. We say the encryption scheme is secure against $\mathcal{F}$-related key queries if any probabilistic polynomial time adversary wins this game with at most negligible probability. Compare this security definition with IND-CPA and IND-CCA(2) definitions, and discuss whether it could be relevant in practice.

7. Give a pseudo-code to generate secure Diffie-Hellman parameters, and justify its security.

8. Explain how Sony's ECDSA secret key could be recovered. Does it mean that ECDSA itself is not secure?

9. What is a fault attack? Give an example against RSA. Does this attack mean RSA is insecure? Motivate your answers.

3 Homomorphic encryption

1. Suppose you want to compute statistics on the marks the class obtained for INFOF514 course, but none of you wants to reveal their mark to the rest of the class. Propose a methodology using homomorphic encryption, and discuss a choice of system to use if you want to compute the average mark. Show an example assuming there are 3 people in the class.

2. Suppose you want to compute statistics on the marks the class obtained for INFOF514 course, but none of you wants to reveal their mark to the rest of the class. Propose a methodology using homomorphic encryption, and discuss a choice of system to use if you want to compute the average mark and its standard deviation. Show an example assuming there are 3 people in the class.

3. Here is an exponential El Gamal public key and ciphertext. What is the corresponding plaintext?

4. Suppose you want to set up an election with a binary choice (yes/no) and veto power to each power, ie the result of the election is yes if they all voted yes, and no if at least one voter voted no. Suggest a homomorphic encryption scheme that could be suitable for this election, explain how to use it and work out an example with three voters.

5. Here are parameters and keys for Pailler cryptosystem, and a ciphertext. What is the corresponding plaintext?

6. Here are parameters and keys for Boneh-Goh-Nissim cryptosystem, two ciphertexts C_1 and C_2, and pairing values $e(P,P)$, $e(P,Q)$, $e(Q,Q)$ and $e(C_1,C_2)$. Knowing that C_1 and C_2 encrypt messages $m_1, m_2 \in \{0,1\}$, what is the value of $m_1 m_2$? Show your calculations.

7. Here is the lattice scheme described in the lectures, and parameters and keys for it. Here is also a ciphertext c for plaintext $m \in \{,1\}$. What is the value of m? (show your calculation). Explain how to compute a ciphertext of nm and m^n, where n is a known integer. What are the maximal values of n one can take in both case to ensure decryption works without error?

8. Explain how to build a fully homomorphic encryption scheme from a somewhat homomorphic encryption scheme. Discuss the advatanges and drawbacks of both schemes.

4 Zero-knowledge proofs

1. Define zero-knowledge proofs. What are their main security requirements?
2. Soundness and zero-knowledge may seem to contradict each other, as "Special soundness requires that the witness can be recovered, while zero-knowledge requires that the witness remains secret." Recall the exact definitions of special soundness and zero-knowledge, and explain why they do not in fact contradict each other.
3. Here are two graphs and an isomorphism between them [...]. Explain how you can prove to someone that you know this isomorphism, without revealing anything about it.
4. Here is a graph and a 3-coloring for that graph [...]. Explain how you can prove to someone that you know this 3-coloring, without revealing anything about it.
5. Suppose you have ZK protocols for languages $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$. Deduce a ZK protocol for the language $\mathcal{L} = \mathcal{L}_1 \cup (\mathcal{L}_2 \cap \mathcal{L}_3)$.
6. Suppose you have ZK protocols for languages $\mathcal{L}_1, \mathcal{L}_2, \mathcal{L}_3$. Deduce a ZK protocol for the language $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2 \cup \mathcal{L}_3$.
7. Let $p, g, x = [...]$. Let also $h := g^x \bmod p = [...]$. Apply Schnorr protocol and Fiat-Shamir transform to produce a non interactive zero-knowledge proof of knowledge of x satisfying $h := g^x \bmod p$.
8. Let $p, x, \{g_i := g^{x^i} | i = 0, \ldots, 3\}$. Give a ZK protocol to prove that such a tuple is well-formed. Sketch a proof that your protocol is sound and zero-knowledge.
9. Here are parameters for ElGamal encryption scheme [...]. Compute an encryption of 0, and a non interactive ZK proof that your ciphertext does indeed contain an encryption of 0.
10. Here are parameters for ElGamal encryption scheme [...]. Using the secret key, check that the ciphertext $c = [...]$ encrypts the message $m = [...]$, and compute a non interactive ZK proof of this fact.

5 Cryptanalysis

1. Estimate the odds that two students in the course are born the same day of the year and the same hour of the day, knowing that 105 students are enrolled in the course this year. Estimate the odds that two girls are born the same day and the same hour in September.
2. Let p, g, h be [...]. Run the Baby Step Giant Step algorithm to recover x such that $h = g^x$. Discuss the complexity of this algorithm.
3. Let p, g, h be [...]. Run Pollard's rho algorithm to recover x such that $h = g^x$. Discuss the complexity of this algorithm.
4. Let p, g, h be [...]. Run the Pohlig-Hellman algorithm to recover x such that $h = g^x$. Discuss the complexity of this algorithm.
5. Let $n = [...]$. Run Pollard's rho factoring algorithm to recover two prime numbers p, q such that $n = pq$.
6. Let $n = [...]$. Run Pollard's $p - 1$ factoring algorithm to recover two prime numbers p, q such that $n = pq$.

6 Post-Quantum cryptography

- Let $n =$ and let $T =$ such that $g^x \bmod n = g^{x+T} \bmod n$. Compute the factorization of n from this data.
- Let $p, g, h =$ [...] and let $(t_1, t_2) =$ such that $g^x h^y \bmod p = g^{x+t_1} h^{y+t_2} \bmod p$. Compute x such that $h = g^x$ from this data.
- Let $p, g, h =$ [...] and let $(t_1, t_2) =$ such that $g^{3x} h^{4y} \bmod p = g^{3x+t_1} h^{4y+t_2} \bmod p$. Compute x such that $h = g^x$ from this data.
- Let $q =$ ..., let $f \in \mathbb{Z}_q[X]$ and let $a \in \mathbb{Z}[X]/(f(X))$. Define Ajtai's hash function for the ideal lattice generated by a. Compute the hash value for message $m =$ ..., $f =$ ... and $a =$ .... Discuss its security when $f(X) = X^{128} + 1$ and when $f(X) = (X-1)(X-2)\dots(X-128)$.

7

8