Third homework

1 Important notices:

- **If you have any questions regarding the tasks, please do not hesitate to contact instructors.**
- This assignment gives you 15% of the final grade.
- **Provide an explicit explanation to your solutions**. Providing answers to the task with no explanation will give you 0 points.
- Your solution must be in the PDF format. You may either scan a handwritten solution or type your solution in Latex (LaTeX) or MS Word. Then export it into PDF. **Solutions submitted in a non-PDF format will receive 0 points**.
- You may write the programming code to solve any task. However, you have to explain explicitly the code logic in your submission and how it helped you solving the task. **Providing the code with no explanations will give you 0 points for the task.** You must submit your code either in the appendix of your submission or to a public repository (Github or Gitlab).
- You may use any online or installed tools to solve a task. However, you must explain how exactly tool helped you solve the task and your personal contribution. The tool must be properly referenced.
- **Plagiarism is prohibited.** Any used sources of information must be referenced. If you are suspected of plagiarism, then you will receive 0 for the task and will be reported to the Dean's office and Program Manager.
- **YOU CANNOT HAVE 0 (zero) as a plaintext in the tasks about RSA and/or ElGamal!**
- This assignment is due **27th of April, 23:59**.

Tasks

Task 1 (RSA cryptosystem). You are working in the company that uses RSA cryptosystem in their solutions. You have been sent the following abstract for the scientific paper. Based on this, would your recommendation to your company and why?

Really, Stop Using RSA: Evidence of a Backdoor

Benoît-Gilles Changerlain
Institut Avancé de Mathématiques de Paris XXI, France

March 9, 2025

Abstract

We report a groundbreaking yet trivial vulnerability in the RSA cryptosystem. Shockingly, we find that if an adversary who does *not* possess the private key d but somehow obtains Euler's totient function value, $\varphi(n)$, they can effortlessly factor the modulus n and completely destruct RSA. Our rigorous theoretical analysis reveals that this backdoor can enable stealthy surveillance by government agencies and bad actors alike—even with FIPS-certified implementations. We urge the cryptographic community to swiftly transition to post-quantum one-end encryption

Task 2 (Security definitions). Suppose you are given the following encryption scheme:

KeyGen() :

1. Sample large prime number p
2. Compute modulus as $n = p^2$
3. Select e to be integer such that GCD$(\phi(n), e) = 1$ and $2 < e < \phi(n)$
4. Calculate d such that $e \cdot d \equiv 1 \mod \phi(n)$
5. Return private key $sk = (d, n)$ and public key $pk = (e, n)$

Enc(pk, m) :

1. Compute ciphertext as $c = m^e \mod n$

Dec(sk, c) :

1. Compute decryption as $m = c^d \mod n$

Your task is to provide an attack that shows that given encryption scheme is not secure with respect to the IND-OT-CPA security definition.

Task 3 (ElGamal encryption). Consider the ElGamal cryptosystem with a public key h and a private key x.

1. Assume that you are given a ciphertext (c_1, c_2) encrypting an unknown message m. Show how you can generate a new ciphertext (c_1', c_2') that encrypts the same m, but with different randomness y' (without decrypting the ciphertext).
2. Assume you are given ciphertext $c = (c_1, c_2)$ that you wants to decrypt, but you do not know corresponding private key sk. Suppose that you have a friend who provides you with the decryption of any other chosen ciphertext $c' \neq c$ using private key sk. Show how can you decrypt c.
3. Assume you are given two ciphertexts $ctx_1 = (c_{11}, c_{12})$ and $ctx_2 = (c_{21}, c_{22})$ that correspond to some plaintext messages (not known to you) m_1 and m_2. What information can you learn about m_1 and m_2, if you observe that $c_{11} = c_{21}$?

4. Bring an example of potential application of ElGamal encryption scheme, where homomorphic property is useful and another example, where it violates the desired security of the application. Justify your answer.

Task 4 (Attack on RSA encryption). You have intercepted two RSA ciphertexts $c_1 = 7$ and $c_2 = 16$ that correspond to the same plaintext – a promo code for the video game. You know that those ciphertexts have been created using corresponding public keys $pk_1 = (e = 3, n = 57)$ and $pk_2 = (e = 5, n = 57)$. What is the promo code m from the intercepted ciphertext?
Note: for this attack, your task is not to find the private key!

Task 5 (Choosing cryptographic primitives). Your company is building a product that heavily relies on usage of cryptography. You receive the following list of security requirements for the system:

1. System should ensure data confidentiality and integrity in transmission,
2. System should ensure data confidentiality and integrity at rest,
3. System should enforce strong authentication mechanisms for users and services to ensure that only authorized entities can access the data,
4. System must be resistant to common attacks, including side-channel attacks and brute force attacks, using strong cryptographic primitives and practices

Your task is to select preferred AI chat bot (LLM), ask it to answer the following question:

You task is for each requirement to provide example of cryptographic scheme(s) (studied in the class) that will ensure that the requirement is met. The last requirement should be taken into account for choosing primitives for the previous requirements. Additionally, recommend the key length for each of the proposed scheme and justify your answer.

Analyse its response and explain with your own words whether you agree or disagree with its conclusion. You are free to provide any additional arguments of your own.

Bonus Task (ElGamal). Show that exponential ElGamal (where the ciphertext is constructed as $c = (c_1, c_2) = (g^y, g^m \cdot s)$) is not IND-CCA2 secure. You are allowed to make single encryption query and single decryption query to the challenger.

PRF task. .

Rules. If you want to improve your grade for the PRF task from the previous homework, you can try to solve this task. Points for this solution overwrite the points that you have gotten for the PRF task in the second homework. The points for this task will go to the 2nd homework submission points. You could solve this task to get full points, even if you did not attempt the second assignment or submitted it late.
Task. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be **a secure PRF**. Do the following functions satisfy definition of pseudo-random function? If the function does not satisfy the definition, provide an attack with respect to the PRF security definition. For those attacks you are allowed to make **a single query** to the challenger.

- $F'(k, m||m') = F(k, m \oplus m')||F(k, 1^n)$, where 1^n is a string of ones of length n.
- $F'(k, m||m') = F(k, m \oplus 0^n) \oplus F(k, m' \oplus 1^n)$, where 0^n is a string of zeros of length n.
- $F'(k, m||m') = F(k, k||m)||F(k, k||m')$, where $m, m' \in \{0,1\}^{n/2}$.