IIT Kanpur
Department of CSE
APPLIED CRYPTOGRAPHY

Assignment 2, Semester 2025

Due Date: 11.59 pm, 4 July 2025

Introduction

This assignment is marked out of 200 marks, and will contribute to 20% final subject marks. It consists of two parts.

Part 1 [75 marks (7.5%)]: Answer the questions in this file. You are required to type your answer in a separate file and submit as PDF. Handwritten, scanned images, screenshots, and/or Microsoft Word submissions are not acceptable. Note that indicating the Question number and writing your answer are sufficient - do not copy and paste the questions again into your submission.

Part 2 [130 marks (12.5%)]: Finish the questions in the Jupyter notebook file directly. The Jupyter notebook can be opened offline by setting up the Jupyter Notebook on your local machine (`https://jupyter.org/install`), or online by using Google Colab. You **MUST** use Python 3. It should be fine for any sub-versions of Python 3. However, we recommend you test your implementation under Python 3.10.16, as we will run your submission under this environment. **Before your submission, please rename your Jupyter notebook as {YOUR_STUDENT_NUM}.**

** If you are using Google Colab, some images may not correctly display. You need to re-configure the path to those images. However, you can leave it. Instead, you can inspect the source code in each question body and manually open the corresponding image inside the *img* folder for view.

Part 1 Questions

1. [10 marks] A manager selects two large primes, p and q, where $p \neq q$, to set up a secure communication channel between three employees, Alice, Bob, and Carlo, using RSA encryption. He first computes $n = pq$ and corresponding $\phi(n)$. Then, he uses this $< p, q >$ pair to generate three RSA key pairs (with different e being relatively prime to each other and corresponding d), assigns them to the staff individually, and destroys $p, q, \phi(n)$ immediately afterwards (meaning nobody knows the values). The following lists the key pairs:

$$\text{Alice: } < n, e_A >,\ < n, d_A >$$
$$\text{Bob: } < n, e_B >,\ < n, d_B >$$
$$\text{Carlo: } < n, e_C >,\ < n, d_C >$$

   Answer the following questions with detailed justification.

(a) [5 marks] Alice wants to send a message M to both Bob and Carlo, so she calculates $C_B = M^{e_B} \bmod n$ and $C_C = M^{e_C} \bmod n$. Explain how an adversary can recover the message M without knowing private keys d_B and d_C.

(b) [5 marks] Carlo is interested in messages sent to Alice. Outline a strategy that may help Carlo recover an alternative private key d'_A that can perform the same function as d_A to decrypt messages sent to Alice.

2. [30 marks] Hash Functions.

(a) [15 marks] Consider the following hash function based on RSA function. The key $< n, e >$ is known to the public. A message M is represented by blocks of predefined fixed size $\{M_1, M_2, M_3, ..., M_m\}$ such that $0 \leq M_i < n$. We can assume that n is large enough to hold the RSA assumptions. The hash value is calculated by:

$$H(M) = ((M_1 \oplus M_2 \oplus ... \oplus M_m)^e) \bmod n$$

Does this hash function satisfy each of the following requirements? Justify your answers. You can give examples, if necessary, to support your arguments.

i. [3 marks] Fixed output size

ii. [3 marks] Efficiency (easy to calculate)

iii. [3 marks] Preimage resistant

iv. [3 marks] Second preimage resistant

v. [3 marks] Collision resistant

(b) [15 marks] Explain how to efficiently find collisions in the following hash functions:

i. [5 marks] The function $H_a : \{0,1\}^{512} \to \{0,1\}^{256}$ is defined as follows:

$$H_a(x, y) = F(y, x \oplus y) \oplus y.$$

Let the pair F, F^{-1} be a public secure symmetric key block cipher with block size and key length 256. That is, y is interpreted as the 'symmetric key', and $x \oplus y$ is the 'plaintext' for F. To compute H_a, we first XOR y with x, then apply the block cipher to the result, and finally XOR the block cipher output with y one more time to get the final output.

ii. [5 marks] $H_b = F(y \oplus x, x)$, where F, F^{-1} is as in last question (i). $y \oplus x$ is the 'key' and x is the 'plaintext'.

iii. [5 marks] $H_c : \{0,1\}^{257} \to \{0,1\}^{256}$ is defined as follows: Let $H : \{0,1\}^* \to \{0,1\}^{256}$ be a collision-resistant hash function for arbitrary-length messages, then for $x||b \in \{0,1\}^{257}$, $H_c(x, b) = H(x)$ if $b = 0$ and $H_c(x, b) = H(H(x))$ if $b = 1$. Here, $a||b$ refers to concatenating a and b together as a single string.

3. [20 marks] ElGamal.

(a) [10 marks] ElGamal Encryption

A variant of ElGamal crypto system over the prime field $GF(q)$ is given as follows. Assume the parameters are as discussed in the lectures. Let $y_A = a^{x_A} \mod q$, be the public address of Alice, where $x_A, 1 < x_A < q-1$, is Alice's private key. Encryption function is defined as follows:

$$E(M) = [C_1, C_2],$$

where $C_1 = a^k \bmod q$, where k is a random integer $1 \leq k \leq q-1$, $C_2 = K \oplus M$, where $K = y_A^k \bmod q$ and $\oplus$ is binary XOR applied to binary representation of K and M.

i. [5 marks] Describe the Decryption Function $D(C_1, C_2)$ that Alice can use to recover the message.

ii. [5 marks] Show how the security of the encryption function is based on Computational Diffie-Hellman (CDH) problem.
CDH Problem: Let q be a prime number and a be a generator of the multiplicative cyclic group of modulo q. Given a^x, a^y, the CDH problem is to compute a^{xy}.

(b) [10 marks] ElGamal signature.

Let's consider a variant of ElGamal signature over the prime field $GF(q)$. Let H be a public hash function and let $y_A = a^{x_A} \bmod q$ be the public key of Alice, where $x_A, 1 < x_A < q-1$ is the private key and a is a primitive element in the field. Alice uses the following equation to define a related ElGamal signature scheme by using:

$$m\ S_2 + x_A S_1 = k \bmod (q-1),$$

where $m = H(M)$, M an arbitrary message, k a random number, $S_1 = a^k \bmod q$ and S_2 are signature parameters. The signature for a message M is represented as $[M, S_1, S_2]$.

i. [5 marks] What are the signing and verification equations?

ii. [5 marks] Is this shceme secure? Justify your answer with reasons.

4. [15 marks] We studied the Needham–Schroeder protocol in lectures. An alternative key distribution method suggested by a network vendor is illustrated in the figure below.

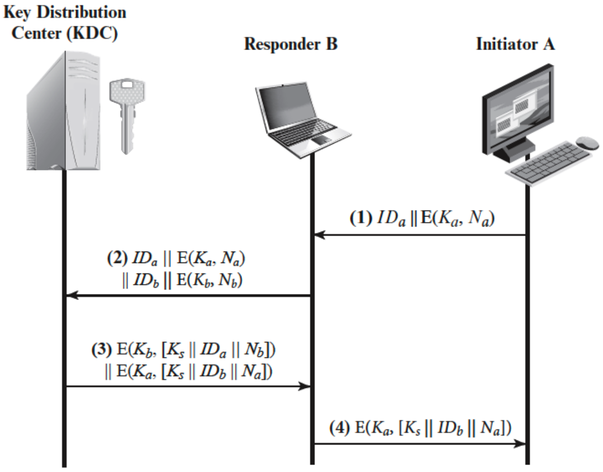
Key Distribution
Center (KDC)
Responder B
Initiator A
(1) $ID_a \| E(K_a, N_a)$
(2) $ID_a \| E(K_a, N_a) \| ID_b \| E(K_b, N_b)$
(3) $E(K_b, [K_s \| ID_a \| N_b]) \| E(K_a, [K_s \| ID_b \| N_a])$
(4) $E(K_a, [K_s \| ID_b \| N_a])$

Figure 1: Key Distribution Between A and B.

(a) [5 marks] How do A and B know that the key is freshly generated?

(b) [5 marks] How could A and B know that the key is not available to other users in the system?

(c) [5 marks] At this stage, A and B cannot authenticate with each other. Explain why and extend the scheme with a few steps so that A and B can authenticate with each other. Your modifications should be based on symmetric key methods used in this key distribution protocol, not public key primitives.

Part 2 Questions

Please finish the Part 2 questions in the Jupyter Notebook '2025asg2.ipynb'. Do not forget to rename the file with your student number before the submission.

Submission and Evaluation

- You must submit a PDF document for the part one, and the Jupyter notebook for the part two, via the Assignment 1 submission entry on the LMS by the due date. Handwritten, scanned images, screenshots, and/or Microsoft Word submissions are not acceptable — if you use Word, create a PDF version for submission.

- Late submission will be possible, but a late submission will attract a penalty of 10% per day (or part thereof). Requests for extensions on medical grounds will need to be supported by a medical certificate. Any request received less than 48 hours before the assessment date (or after the date) will generally not be accepted except in the most extreme circumstances.

- This assignment will be marked out of 200 marks, and will contribute to 20% of your total marks in this subject. Marks are primarily allocated for correctness of your thinking and clarity of your communication, rather than (only) the correct result without justification.

- We expect your work to be neat — parts of your submission that are difficult to read or decipher will be deemed incorrect. Make sure that you have enough time towards the end of the assignment to present your solutions carefully. Time you put in early will usually turn out to be more productive than a last-minute effort.

- You are reminded that your submission for this assignment is to be your own individual work. For many students, discussions with friends will form a natural part of the undertaking of the assignment work. However, it is still an individual task. You are welcome to discuss strategies to answer the questions, but not to share the work (even draft solutions) on social media or discussion board. It is University policy that cheating by students in any form is not permitted, and that work submitted for assessment purposes must be the independent work of the student concerned.

If you have any questions, you are welcome to reach out the teaching team.