COMP 4334 Principles and Practice of Internet Security
Assignment 1

Release date: Sept. 23, 2024
Firm Deadline: 11:59 pm, Oct. 2 (Wednesday), 2024

Note: Please remember that you are not permitted to directly exchange ideas about how to solve the problems in this homework. Limited discussions are allowed mainly about the clarity of the questions – you are encouraged to discuss if you feel that some parts of the questions are confusing, and make sure that you understand the questions before proceeding. If you used any conclusions or results not presented in the lecture, please properly provide references to them.

1 Answer the following questions, briefly (max 100 words per question).

1. **Security under different threat models** [**2pts**]. Use Diffie-Hellman key exchange scheme to explain how it is secure in one threat model but not secure in another threat model.

2. **Randomness in encryption** [**2pts**]. Use the ElGamal encryption scheme as an example to explain why it is a bad idea to re-use the random number k in encrypting two different messages.

3. **Public key distribution** [**2pts**]. In public-key cryptography, the encryption key K_p is public so that anyone can encrypt a message using the corresponding public key. Suppose we use the following method to make the public keys publicly known. Everyone in the classroom will write her name and public key on the blackboard. For example, Alice will write (Alice, K_{Alice}) and Bob will write (Bob, K_{Bob}) on the blackboard. What's the possible drawback to distribute the public keys like this?

2 Operation Modes of Block Ciphers. [9 pts]

Consider a block cipher operating in cipher-block chaining mode (CBC). Answer the following two questions. You should explain your answer in detail.

(a) Suppose a message of 100 plaintext blocks is being encrypted with CBC mode. Suppose that, before encryption, one bit of the tenth plaintext block is modified. How many blocks of plaintext, after decryption, are certain to be correct? [**4 pts**]

(b) Same setup as question (a), but this time, one bit of the tenth ciphertext block is changed after encryption but before decryption. How many blocks of plaintext, after decryption, are certain to be correct? [**5 pts**]

3 Secret Dating. [10 pts]

In our Teams channel, there are two students: Alice and Bob. They use the general channel to decide the location and time for their next date. To protect privacy, they will use a public-key encryption scheme to encrypt their messages. Let the public keys of Alice and Bob be PK_A and PK_B, respectively.

Alice and Bob will use the following protocol to communicate.

Step 1 Alice proposes a location and time, denoted as $m = < loc, time >$. Alice then sends the encrypted message $c = Enc(m, PK_B)$ to Bob in the public general channel.

Step 2 When Bob received the ciphertext c, he will decrypt and respond with a "Yes" or "No". That is, Bob will send $Enc(ans, PK_A)$ to Alice, where $ans \in \{Yes, No\}$.

Step 3 Alice will decrypt Bob's answer. If the answer is "Yes", they have an agreement. If the answer is "No", Alice will propose a new option again (i.e., repeat Step 1). The communication ends when Alice and Bob have reached an agreement.

Note: we assume that Alice and Bob will pick one of the Blocks at PolyU for their date. That is, $loc \in \{A, B, C, \cdots, Z\}$. And the time is in 24h format. For example, $time = 22:30$ or $time = 11:00$.
Questions:

1. Suppose you observed several encrypted messages between Alice and Bob in the general channel. Explain how you can figure out the location and time for their next date. [**5pts**]

2. Suppose you are Bob, and you found that there are people following you while you are dating. Make **one single modification** to the plaintext such that people cannot know your dating plan. [**5pts**]

4 Attacks against Textbook RSA [15pts]

In this problem, we will investigate several attacks against the RSA algorithm.

1. Assume that Alice and Bob use RSA to encrypt messages. Specifically, Bob will choose two large primes such that their product n is of more than 1024 bits, i.e. $n > 2^{1024}$. And Bob will choose the public key as $e = 7$. Alice wants to encrypt a message m of 128 bits using Bob's public key. Explain why this is a bad idea and find a way to fix it. [**5pts**]

2. When generating the modulus n for RSA, it is often dangerous to share the same modulus among different parties. Suppose the RSA public keys for Alice and Bob are $(e_A = 3, n)$ and $(e_B = 5, n)$, respectively, where Alice and Bob share the same modulus n. A third person Kevin sent the same encrypted message to Alice and Bob. That is, Kevin sent $c_A = m^{e_A} \bmod n$ to Alice and sent $c_B = m^{e_B} \bmod n$. An eavesdropper Eve obtained the transmitted ciphertext c_A and c_B. Show how Eve can recover the message m from c_A, c_B, and n. (*Hint: utilize extended Euclidean theorem. When encountered multiplicative inverse, assume that it always exists.*) [**5pts**]

3. This problem shows that not padding randomness into the message could be dangerous. Suppose there are three persons A, B, and C, whose RSA public keys are $(e_1 = 3, N_1)$, $(e_2 = 3, N_2)$, $(e_3 = 3, N_3)$, respectively. Assume that N_1, N_2, N_3 are pairwise prime. Suppose that someone sent the same message m (encrypted by the corresponding public keys) to these three persons A, B, and C.

   Suppose the eavesdropper Eve got to know the three ciphertext c_1, c_2, c_3. Show how Eve can recover the message m from the public information. (*Hint: use the Chinese Reminder Theorem. Read the materials in Chapter 8.4 from the textbook.*) [**5pts**]

5 Cryptographic Hash Function [10pts]

Consider a function $H : \{0,1\}^* \rightarrow \{0,1\}^n$, meaning that H will take a bit string of **any length** as input and outputs a bit string of length n. For any two bit strings x and y of the same length, H has the following property:

$$H(x \oplus y) = H(x) \oplus H(y), \tag{1}$$

where $\oplus$ denotes bit-wise XOR operation.

1. Compute $H(\mathbf{0}^k)$. Note, $\mathbf{0}^k$ denotes a bit string of length k consisting of all zeros, where k is a positive integer. [**3 pts**]

2. If H is used as a cryptographic hash function, show that H is not strong-collision resistant. Hint: use the result of the previous question. [**7 pts**]