Spring 2023 Cryptography and Network Security

Homework 1

Release Date: 2023/03/09

Due Date: 2023/04/09, 23:59

TA's Email: `cns@csie.ntu.edu.tw`

Instructions

- This homework set is worth 111 points, including 11 bonus points.
- **Submission Guide:** Please submit all your codes and report to NTU COOL. Please refer to the homework instructions slides for information.
- You may encounter new concepts that haven't been taught in class, and thus you're encouraged to discuss with your classmates, search online, ask TAs, etc. However, **you must write your own answer and code**. Violation of this policy leads to serious consequences.
- You may need to write programs in the Capture The Flag (CTF) problems. Since you can use any programming language you prefer, we will use a pseudo extension code**.ext** (e.g., code.py, code.c) when referring to the file name in the problem descriptions.
- In each of the Capture The Flag (CTF) problems, you need to find out a flag, which is in `CNS{...}` format, to prove that you have succeeded in solving the problem.
- Besides the flag, you also need to submit the code you used and a short write-up in the report to get full points. The code should be named **code{problem_number}.ext**. For example, code3.py.
- In some CTF problems, you need to connect to a given service to get the flag. These services only allow connections from 140.112.0.0/16, 140.118.0.0/16, and 140.122.0.0/16.

Handwriting

1. CIA (10%)

Please explain three major security requirements: confidentiality, integrity, and availability. For each security requirement, please give an example in the real world.

2. Hash Function (10%)

Please explain three properties of a cryptographic hash function: one-wayness, weak collision resistance, and strong collision resistance. For each property, please give an example applied in the real world.

3. Multi-prime RSA (15% + 3% Bonus)

We all know how RSA works. First, we choose two prime numbers, and then magic happens. But what if we have more than two primes in the modulus? The idea of using multiple primes

in RSA, often called multi-prime RSA or r-prime RSA, which is as old as regular (2-prime) RSA itself, is that the modulus has multiple **distinct** primes. In fact, we can say that regular RSA is a special case of multi-prime RSA. In this problem, we will look into some advantages and disadvantages of multi-prime RSA.

- Key generation:
  1. Choose r ($r \in \mathbb{N}, r \geq 2$) **distinct** large primes p_i such that $N = \prod_{i=1}^{r} p_i$.
  2. Calculate $\phi(N) = \prod_{i=1}^{r}(p_i - 1)$.
  3. Select e and compute $d \equiv e^{-1} \mod \phi(N)$.
  4. The public key is (e, N) and the private key is $(d, p_1, \cdots, p_r)$.
- Encryption: $c \leftarrow m^e$.
- Decryption: $m \leftarrow c^d$.

a) (3%) Prove the correctness of multi-prime RSA, i.e., decrypting an encrypted message would recover the message.

b) (4%) Explain briefly why RSA, whether 2-prime or multi-prime, must use distinct primes.

c) (5%) As shown in class, the Chinese Remainder Theorem (CRT) can be used to optimize the performance of 2-prime RSA decryption. Apply the CRT to multi-prime RSA decryption and prove its correctness.

d) (3%) What are the advantages and disadvantages of multi-prime RSA over regular RSA? Please give at least two of each. You may mention possible attacks without explaining or proving how they work, but you must explain why one type of RSA is more vulnerable to such an attack than the other. If you notice any advantage or disadvantage in other subproblems, you can mention it here.

e) (Bonus 3%) Most implementations of RSA use the Miller-Rabin primality test with trial division to search for primes. The expected runtime is $O(n^4/\log(n))$ where n is the bit length of the prime[1]. Show that the multi-prime RSA key-generation is more efficient than the regular RSA key-generation when the moduli are of the same size.

4. Fun With Semantic Security (15%)

During the course, we have learned the way of using security reduction and calculating the attacker's advantage in a security game. Let's have more fun with these adorable ciphers!

Let $\mathcal{E} = (Enc, Dec)$ be a cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Assume that one can efficiently sample an element from a uniform distribution over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. Assume that $\mathcal{K}, \mathcal{M}$ are both group with a binary operation $+$.

Assume that $\mathcal{E}$ is semantically secure (using the definition for one-time key). You are requested to prove that the following ciphers $\mathcal{E}' = (Enc', Dec')$, which are constructed from $\mathcal{E}$, are semantically secure (also for one-time key) as well.

a) (5%) $Enc'(k, m)$ is defined by sampling $r \xleftarrow{R} \mathcal{K}$ and output $Enc(k, m)||r$.

[1] In fact, it should be $O(n^4/\log(n)+tn^3)$ with a maximum probability of 4^{-t} for outputting composite numbers. This property does not matter in this problem.

b) (5%) $Enc'(k, m)$ is defined by sampling $r \xleftarrow{R} \mathcal{M}$ and output $Enc(k, m + r)||r$.

c) (5%) $Enc'(k, m)$ is defined by sampling $r \xleftarrow{R} \mathcal{K}$ and output $Enc(k + r, m)||r$.

- Hint: If you are unfamiliar with a formal proof involving a security game, you can refer to this document, which is the complete version of the proof demonstrated in the class.
- Hint: You can prove the semantic security by directly calculating the advantage if you do not need a security reduction.
- Hint: If you use security reduction, you should explicitly state the correctness of your reduction. That is to say, why is your reduction efficient? What is the probability distribution of the messages in your security game reduction?

Capture The Flag

5. Simple Crypto (10%)

> "Welcome to the Crypto World. In this homework, you are going to play with some well-known classical ciphers. Please solve all the classical cipher challenges yourself. Even though classical ciphers are used mostly in the past and most of them can be practically computed and solved, I don't think you can figure it out that easily :P. Be careful and don't use classical ciphers to safeguard your secret!"

You can access the service by `nc cns.csie.org 44398`. If this is your first CTF challenge, we highly recommend that you solve this challenge first.

Hint: If you use Python and pwntools, keep an eye on the return value of Python's builtin function ***`input()`****. Sometimes a trailing newline character may exist with unknown reason.*

6. ElGamal Cryptosystem (10% + 8% Bonus)

After learning about public-key cryptography in his course, Andy wants to implement his own ElGamal Cryptosystem library. He designs several encryption and decryption services and asks you to assess their security. Please help him recognize the fact that he should not implement cryptographic function libraries himself.

a) (4%) flag1: Although Andy's teacher has taught him never to reuse the ephemeral key, he still wants to use his lucky number as the ephemeral key. "How can such a random number compare with my lucky number?" You can access the server by `nc cns.csie.org 6001`. The challenge source is provided in `hw1/ElGamal-Cryptosystem/stage1.py`.

b) (Bonus 8%) flag2: "You decrypted my flag!" said Andy angrily. He has decided not to encrypt messages for you anymore and will only accept messages that have already been encrypted by you. You can access the server by `nc cns.csie.org 6002`. The challenge source is provided in `hw1/ElGamal-Cryptosystem/stage2.py`.

Hint: This problem was inspired by "SECCON CTF 2022 Quals - this_is_not_lsb", and it is much simpler. Just think about what information you can obtain from the two different responses of the server.

c) (6%) flag3: Andy has learned Shamir's secret sharing in class, and he has decided to combine the tricks with his ElGamal encryption to change it into a threshold-ElGamal cryptosystem that requires multiple parties to decrypt the ciphertext. Can you still decrypt it this time? You can access the server by `nc cns.csie.org 6003`. The challenge source is provided in `hw1/ElGamal-Cryptosystem/stage3.py`.

7. Bank (15%)

CNS Bank has launched New User Promotion. During this period, newly registered users can get cashback. Join us right away and enjoy our service.
Visit CNS Bank by `nc cns.csie.org 44377`. Also refer to the source code in `bank/server.py`

a) (5%) flag1: The first thing to do here must be visiting our flag store. You can find good flags here.

b) (10%) flag2: Are you a CNS student? There is a gift for you! Register a student account now to receive the gift!

8. Clandestine Operation (15%)

Sumeru, the nation of wisdom, is led by a group of scholars. They work for the Akademiya, the supreme governing and academic institution in Sumeru. However, these scholars are evil. Due to some reason, they imprisoned Nahida, the god of Sumeru, also the god of wisdom. She is imprisoned in the Akademiya building now.
As a traveler, you meet the spirit of Nahida when you travel in Sumeru (although her body is imprisoned, her spirit can enter anyone's body). Nahida told you these things and hope that you can rescue her.
Start your journey now by `nc cns.csie.org 44399`! Also, the source code is provided in `hw1/clandestine-operation`.

a) (7%) flag1: First you need to sneak into the Akademiya building. You observe that everyone who wants to enter it needs to say the secret word to the guard. Fortunately, someone accidentally lost his ID card and then you picked it up. As the god of wisdom, Nahida told you that the secret word is hidden in the ID card. She will also help you find the secret. Ask Nahida if you have any questions! She will give you some valuable hints.

   Hint: Have you heard of padding oracle?

b) (8%) flag2: After entering the building, the spirit of Nahida told you that she is imprisoned in a place called "Sanctuary of Surasthana". However, only Azar, the supreme leader of the Akademiya, can enter this place. Can you think of a way to get in?