COMP 417 INTRODUCTION TO CRYPTOGRAPHY

HOMEWORK 1 (Total=100 points)

Deadline: 02.11.2023 23:59

Read the questions and rules carefully. They are clear and well defined.

Rules:

1. No Cheating: You are not allowed to collaborate with your friends and use any kind of websites or AI. If your homework gives a sign of any of them, **directly it will be graded as zero**.

2. Goal: Please do your homework alone. Our main aim is to **learn** whatever we cover so far.

3. Submission: Submit your homework in a **single pdf. No other file types will be accepted. No multiple pdf files will be accepted. In these cases, your points will be deducted by 30%.**

QUESTIONS (10x10=100 points)

1. Provide 3 main differences between symmetric cryptography and asymmetric cryptography. Explain.

- **Key Usage** → Symmetric cryptography uses only one key for encryption and decryption unlike asymmetric cryptography. Asymmetric cryptography uses a pair of keys which are called public key and secret/private key.
- **Speed** → Symmetric cryptography is a lot quicker than asymmetric cryptography since the process for asymmetric cryptography requires 2 separate keys.
- **Computational Power** → As I mentioned in the previous difference, symmetric cryptography is a lot quicker than asymmetric cryptography this also leads to it requires less computational power since we can do encryption and decryption with only one key.
- **Use** → Symmetric cryptography is generally used for bulk data encryption like file securing and communicating over a secure channel where you need to share the secret key. On the other hand, asymmetric cryptography is used for integrity, authentication etc. where you do not need to share a key.

2. Explain how you can construct a secure block cipher. What do you use to construct a secure block cipher?

- In order to construct a secure block cipher, we need to find a secure PRP aka Pseudo Random Permutation. So, how can we decide if our PRP is secure? A PRP is **secure** if a random function in Perms[X] is **indistinguishable** from a random function in S_F

Where Let E: K x X → Y be a PRP

Perms[X]: the set of all **one-to-one** functions from X to Y.

S_F = {E (k,.) such that k ∈ K} ⊆ Perms[X,Y]

3. Explain why AES-128 is not quantum resistant but AES-256 is?

- We know that quantum computers can do attacks in time = O ($|X|^{1/2}$) where classical computers do it O(|X|) with best generic algorithm time.

- AES-128 is not quantum resistant since 128-bit key is used during encryption and decryption. Adversaries can attack this key by searching through 2^128 possibilities in 2^64 operations. Thus, it becomes non-resistant against quantum computers.

- However, AES-256 is quantum resistant since 256-bit key is used. Hence, 2^128 operations to attack is quite impossible with today's quantum computational resources. (Which is higher than 2^112)

4. a. Explain the following modes of operation for block ciphers: ECB, CBC, CFB, OFB, CTR.

b. Provide one application area or use-case for each of them.

- **ECB** (Electronic Codebook Book) is a simple mode of operation where a **message is broken into independent blocks** which are encrypted, and each block is a value which is substituted. It can be used **in secure transmission of encryption key.**
- **CBC** (Cipher Block Chaining) is a mode of operation where **each previous cipher block is chained to be input with current plaintext block**. We use Initial Vector and XORs for this mode. The encryption depends on the current and all the blocks before it. It is commonly used in **authentication**.
- **CFB** (Cipher Feed Back) is a mode of operation where **we encrypt the previous ciphertext, then combine with the plaintext block using XOR** (exclusive or) to produce the current ciphertext. The cipher is fed back to combine with the rest of IV. This can be used as a stream cipher. We need to wait for previous encryption process. It can be used as **primary stream cipher and authentication.**
- **OFB** (Output Feedback) is a mode of operation where its scheme is *similar to CFB* but the **output of the encryption function output of cipher is fed back.** Here, **the feedback is independent of message.** So, pre-computation of forward cipher is possible. It can be used as a **stream cipher for transmission over noisy channels.**
- **CTR** (Counter) is a mode of operation where we encrypt the **counter value with the key rather than any feedback**. So, there is **no feedback** in the mode. The counter value will be different for each plaintext. Thus, **blocks can be processed in parallel** since there is no dependence between blocks. It can be used for **high-speed communications**.

5. Provide 3 main differences between stream ciphers and block ciphers. Explain.

- **Data Handling** → Stream ciphers do all the operations bit by bit or byte by byte where block ciphers operate on data in fixed-size blocks (chunks).
- **Pseudorandom Keystream** → Stream ciphers generate a keystream, a sequence of pseudorandom bits/bytes to combine with the plaintext using XOR for getting ciphertexts.
- **Synchronization** → Since the stream ciphers use keystream to generate random values, receiver and sender must be sharing the same initial state for keystream generator.

6. Explain perfect secrecy and computational secrecy and their differences.

- **In perfect secrecy**, there should be **no leak about the information of the plaintext**. Even unlimited computational power should not allow to do it.
- **In computational secrecy,** we accept **a scheme of leaking information with tiny probability to bad guys** with bounded/limited computational resources.

7. Explain why OTP (one-time-pad) stream cipher provides perfect secrecy? Under what condition perfect secrecy is provided?

- OTP uses a key generation that is random and secret that is at least as long as the plaintext. This generated key only used once, hence name. Then, the key is used while XORing with plaintext which will create the ciphertext that is long as the plaintext.
- OTP (one-time-pad) provides perfect secrecy when the essential characteristics are served which are:
    - Using a keystream that is as long as a plaintext,
    - Randomized and secret key,
    - This random and secret key should be used only once.

8. Explain how we can construct a stream cipher from a block cipher. Explain how it works. Give one example.

- We can use block cipher to construct a stream cipher by using them as pseudo random number generators and to combine these generated random bits with the plaintext/message. Block ciphers are used in CFB (Cipher Feedback) where its application is primary stream cipher, OFB (Output Feedback), CTR (Counter).

9. Calculate $7^{123}\ mod\ 145$.

To solve this problem, we can use Modular Exponentiation. It is defined as:

$x^y \bmod n = x^{y \bmod \phi(n)} \bmod n$

if $y = 1 \bmod \phi(n)$ then $x^y \bmod n = x \bmod n$

So, in the question x is 7, y is 123, and n is 145. Then, we will have:

$7^{123}\ mod\ 145 = 7^{123 \bmod \phi(145)} \bmod 145$

Where $\phi(145) = (29 - 1)(5 - 1) = 28 * 4 = 112$ ($145 = 29 * 5$ where both of them are primes)

Then, $7^{123 \bmod \phi(145)} \bmod 145$ becomes $7^{123 \bmod 112} \bmod 145$. Thus $7^1 \bmod 145$ since 123 mod 112 is 1.

As the last step, $7^{123}\ mod\ 145$ will become 7 mod 145 which is **7.**

9. What is the total number of positive numbers less than 2436 and coprime to 2436? Calculateand explain why. Hint: Euler's Totient function ☺

   2436 = 4*3*7*29

   Ø (2436) = Ø (29) Ø (84) = Ø (29) Ø (4) Ø (21) = Ø (29) Ø (4) Ø (7) Ø (3) = 28 * 2* 6 *2 = **672**