Concordia University of Edmonton (CUE)
Assignment 2 (Fall, 2023)
IT 270A: Applied Cryptography
Total marks: 50 (plus 10 bonus marks)
Version: v1

Problem 1. (10 marks) Alice wants to send an encrypted message to Bob. Bob first computes his RSA parameters. He then sends Alice his public key. Alice encrypts the message and sends the ciphertext y to Bob. Bob decrypts y using his private key. For the two prime numbers $p = 5$ and $q = 7$, and the plain message $x = 4$, show the

1. **(4 marks)** Key generation process of the RSA encryption algorithm
2. **(3 marks)** Encryption process of the RSA algorithm.
3. **(3 marks)** Decryption process of the RSA algorithm

Problem 2. (8 marks) Suppose Bob wants to send a signed message ($x = 6$) to Alice. The key generation process is exactly the same as it is for RSA encryption. Bob computes his RSA parameters and sends the public key to Alice. In contrast to the encryption scheme, now the private key is used for signing while the public key is needed to verify the signature. For two prime numbers $p = 5$ and $q = 11$, and for $x = 6$, show the

1. **(2 marks)** Key generation process of the RSA
2. **(3 marks)** Computer the signature.
3. **(3 marks)** Verify the signature.

Problem 3.(8 marks) The Diffie-Hellman public parameters are $p = 41$ and $\alpha = 5$.

a **(3 marks)** Choose the appropriate private keys for both Alice and Bob.

b **(5 marks)** Show the session key estimation process from these two private keys using the Diffie-Hellman algorithm.

Problem 4.(9 marks) There are three central properties that a hash function needs to possess in order to be secure. Define those terms with examples.

a **(3 marks)** Preimage resistance.

b **(3 marks)** Second preimage resistance.

c **(3 marks)** Collision resistance.

Problem 5.(8 marks) How to view an SSL certificate in a browser? Include the SSL certificate details for the domain https://concordia.ab.ca.

Problem 6.(5 marks) How to view the public key of a website that uses https (secure protocol)? Add a screenshot of the public key for the domain https://concordia.ab.ca.

Problem 7.(7 marks) How to view the session key in a browser? Include the session key details for the domain https://concordia.ab.ca.

Problem 8.(5 marks) How to view the cookies in a browser? Add a screenshot of the cookies for the domain https://concordia.ab.ca.