MINISTRY OF EDUCATION
Imam Abdulrahman Bin Faisal University
College of Computer Science & Information Technology
Department of Computer Science

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

وزارة التعليم
جامعة الامام عبد الرحمن بن فيصل
كلية علوم الحاسب وتقنية المعلومات
قسم علوم الحاسب

CYS507 and CYS 406: Individual Assignment on Cryptosystems

Assignment #1, Term2, 2021/2022

You are required to learn how to design and implement **RSA and ECC cryptosystems. We prefer to use Python.**

Q1: RSA

Design and implement a simple package based on the RSA algorithm to provide encrypting/decrypting and digital signature signing and verifying.

a. Generate two prime numbers: p and q.
b. Miller Rabin: to test the prime number.
c. Euclid’s algorithm: to find the encryption key (e)
d. Extended Euclid’s algorithm (EEA): to find the decryption key (d).
e. choose any hash function which is available as free source
f. A main method to show different usage of RSA including dialogues between two parties (Alice and Bob) that reflect encrypting/decrypting and digital signature signing and verifying

Q2: Elliptic-curve cryptography (ECC).

Design and implement a simple ECC package to provide encrypting/decrypting and digital signature signing and verifying.

a. Operations on the underlying Zp field, where p is either 11, 23, or 37, and E(Zp) is defined.
b. choose any hash function which is available as free source.
c. Represent a message on an EC. you can use free source code or library function, but you have to understand it.
d. A main method to show different usage of ECC including dialogues between two parties (Alice and Bob) that reflect encrypting/decrypting and digital signature signing and verifying.

Submission

1- Submit a report about the design and implementation of the above tasks (softcopy on BB).
2- Submit the code along with screenshots that show testing scenarios. This should be submitted in one folder to BB.
3- The code should be well documented.
4- There are many free sources on the Web and you can study them. However, you must write your own code.
5- As a part of evaluation process of this assignment, a session will be conducted to verify your understanding of the code and the related design and implementation issues.