EECE 455/632 - Cryptography and Network Security

Projects

The aim of this project is to investigate the most important classical encryption techniques as well as some basic tools needed in cryptography. Hence, 10 projects are described below. The subject you will work on is determined by your AUB ID number. You will work in groups of 3. In each group, you will take the last digit of your AUB ID, add them up (we should add three numbers) and do a modulo 10. The resulting number is your project topic number. Once you form your groups, you have to send an email to hn49@aub.edu.lb cc rmm71@mail.aub.edu with the list of names of each group and the project topic number. The subject assigned to you is determined as follows:

- If your result is 0, select Project 0
- If your result is 1, select Project 1
- If your result is 2, select Project 2
- If your result is 3, select Project 3
- If your result is 4, select Project 4
- If your result is 5, select Project 5
- If your result is 6, select Project 6
- If your result is 7, select Project 7
- If your result is 8 select Project 8
- If your result is 9, select Project 9

For the selected topic, you are required to write a detailed report.

Most of these subjects and their implementation can be found online. However, the main purpose of this project (besides fully understanding the functionality of the code) is to create a nice and easy graphical user interface (GUI) and make them user friendly and suitable for educational purposes.

Plagiarism Warning:

As per AUB rules and regulations, all students are required to submit their own work (project) and avoid plagiarism. You will be penalized for any act of plagiarism as per AUB rules and regulations.

Declaration of No Plagiarism by Student (to be signed and submitted by the student with project folder):

I hereby declare that the submitted project is a result of my own efforts and that I have not plagiarized or copied any person's work. I have provided all references for the information used in this project (all applicable references and quotes are inserted).

Name of Student: ……..
Student ID: ……..
Signature: ..……...
Date: ……

Project-0. ***Polynomial Arithmetic***

The code will allow a user to perform arithmetic operations on polynomials in GF (2^8) with:

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

The operations to be performed are modulo reduction, finding the inverse, addition, subtraction, multiplication, and division. The software should allow inputs and display outputs in either Binary or Hexadecimal.

Project-1. ***Polynomial Arithmetic***

The code will allow a user to perform arithmetic operations on polynomials in GF(2^m) with m = 163. The operations to be performed are modulo reduction, finding the inverse, addition, subtraction, multiplication, and division. The implementation should be modular and can be easily extended to other standard powers such as: 163, 233, 239, 283, 409, 571.

The software should allow inputs and display outputs in either Binary or Hexadecimal.

Project-2. ***Stream Cipher***

Implement RC4 and A5 for GSM encryption.

Project-3. ***Number Theory***

Implement code to perform: Prime Factorization, Totient function computation, Miller Rabin Algorithm, Fast Exponentiation.

Project-4. ***Public Key Cryptography***

Implement RSA with key sizes of 1024 and 2048 bits.

Project-5. ***Elliptic Curve Cryptography***

Given an Elliptic Curve $E_p(a, b)$, write code to find all points on the curve, add two points on the curve and multiply a point by a scalar.

Project-6. ***Elliptic Curve Cryptography***

Implement ECC encryption/decryption based on a curve $E_p(a, b)$.

Project-7. ***El-Gamal***

Implement the algorithms for El-Gamal Encryption and Decryption.

Project-8. ***ECC Digital Signature***

Implement the Elliptic Curve Digital Signature Algorithm (***ECDSA***)

Project-9. ***ECC D-H Key Exchange***

Implement the ***Curve25519,*** which is an elliptic curve offering 128 bits of security and is designed to be used alongside the elliptic curve Diffie–Hellman (***ECDH***) key agreement scheme.