ICS 440 – Cryptography and Blockchain Applications

TERM 231 – Sultan Almuhammadi

Term Project

The goal of the term project is to enhance the understanding of the concepts related to the course material. You may choose the project in one of the following topics related to cryptography and blockchain:

1. **AES Enhancement:** You are expected to design and implement AES with extended key lengths. This option requires basic programming skills and knowledge of using software libraries (such as OpenSSL).
2. **Blockchain Implementation:** You are expected to design and implement a small blockchain from scratch using basic concepts you learn about blockchain. This option requires good understanding of blockchain and basic programming skills in Python.
3. **Blockchain Design:** You are expected to design a solution using blockchain technology to a real problem. It requires knowledge of the problem, and a deep understanding of blockchain technology.
4. **RSA Cryptanalysis:** You are expected to do some cryptanalysis or experiment with RSA. This project requires a good understanding of number theory, knowledge of the RSA, and basic programming skills.

More details on the problems in each of the above topics are given below and can be further discussed on the Blackboard/MS-Teams. You will work in teams (of 5 students each, with one serving as a team leader). The evaluation varies based on the delivery of objectives and the depth of understanding. Each student is expected to demonstrate an adequate understanding of the project details in order to obtain a fair evaluation.

Milestones, Deadlines, and Evaluation:

Project proposal:	10% (Due Thursday, 16 November)
Progress report:	15% (Due Thursday, 30 November)
Final report draft (+Code):	40% (Due Saturday, 9 December)
Presentation (+Demo):	35% (10 – 1 3 December)
Revised report/term paper	+10% (Due Sunday, 17 December)

Term Project – Topic 1: (AES Enhancement)

In this project, you implement AES using OpenSSL or any other library of your choice. Then you expand the implementation to allow keys of lengths 320, 384 and 512 bits. You need to design and implement the required parts (such as Rcon Table and extra rounds) to support the new key length. You need to test your code and conduct a comparative analysis of the performance with different key lengths.

Problem and Requirements: (See Blackboard/Teams for updates)

Study AES and familiarize yourself with the encryption process and the key schedule.

(a) Implement AES using OpenSSL or any other library. Test the code to ensure that it works properly.
(b) Design and implement the extended Rcon Table and the additional rounds needed for the larger keys (320, 384, and 512 bits).
(c) Implement AES with the new key lengths (320, 384, and 512 bits).
(d) Perform an experiment for a comparative analysis of the performance of AES with different key lengths: 128, 192, 256, 320, 384, 512 bits.
(e) Report the outcomes of the experiment in (d).
(f) Discuss the security and the performance of the enhanced AES with the new key lengths.
(g) Submit a technical report or a term paper that includes all the details of the project and share the code on GitHub with your instructor.

Evaluation:

The evaluation of this project is based on the security and efficiency of the design, the correctness of implementation, and the provided details in the report.

Term Project – Topic 2: (Blockchain Implementation)

This project helps you understand blockchain (inside out). You will implement your own blockchain from scratch using Python. You will test your blockchain by creating transactions, mining blocks, and add them to the blockchain. You will synchronize blockchains between nodes. You also need to add extra features, like network difficulty and obfuscation, the more the better.

Problem and Requirements: (See Blackboard/Teams for updates)

Study Chapter 1 (Lee 2019) to have a general understanding of blockchain. Also read Chapters 2 to have a general understanding of the project.

(a) Implement your own blockchain as explained in Chapter 2 and test your implementation by adding blocks to your blockchain and find the correct nonce.
(b) You will Increase the difficulty and test the blockchain. Change the difficulty by gradually adding additional leading zeros to the difficulty target and report the time it takes to mine the blocks.
(c) Create at least 4 nodes (one node for each member) and synchronize the blockchain between the nodes. Test the blockchain with some transactions. Use your SID as the last 3 digits of localhost and addresses for payment whenever applicable.
(d) Add extra features to your blockchain, like difficulty level and obfuscation of data. Thus, implement a difficulty level as a floating-point number instead of target-hash string. Also encrypt the amount in the transaction using a simple cipher (like additive shift cipher or transposition).
(e) Add rules to check the validity of the transactions, like accept only transactions using unspent coins after verification of the senders.
(f) Submit a technical report or a term paper that includes all the details of the project and share the code on GitHub with your instructor.

Evaluation:

The evaluation of this project is based on the correctness of the implementation, the the added extra features, and testing experiments and reported results.

Term Project – Topic 3: (Blockchain Design)

In this project, you will design a solution using blockchain technology to a real problem related to your work, or a hypothetical problem. You need to include the necessary details related to the integrity and the security of your design. Implementation is not required at this point, but you should provide adequate details such that a developer can implement your design.

Problem and Requirements: (See Blackboard/Teams for updates)

Identify a process or a service as a proposed problem that can be solved using blockchain technology.

(a) Explain why you choose such a problem. What makes it suitable for blockchain?
(b) Design a blockchain-based solution for the proposed problem. Identify the peers or the nodes in this system.
(c) Identify the type of blockchain needed for the proposed problem (public, private, or semiprivate blockchain).
(d) Explain who can create blocks, how the blocks are linked to the blockchain, and how the consensus is achieved.
(e) Discuss the integrity of the design and analyze its security.
(f) Identify the features of the blockchain solution.
(g) Formally define your consensus algorithms.
(h) Submit a technical report or a term paper that includes all the details of the project.

Evaluation:

The evaluation of this project is based on the efficiency of the design, the provided details, the integrity and the security analysis. (Hint: formal definition makes the analysis much easier).

Term Project – Topic 4: (RSA Cryptanalysis)

In this project, you will do some cryptanalysis and experiment some attacks on RSA. You need to report the necessary details related to each attack. This project requires additional readings on RSA attacks and programming skills for the implementation.

Problem and Requirements: (See Blackboard/Teams for updates)

Given an RSA scheme, your goal is to find some weakness in the scheme by implementing and testing some of known RSA attacks. In each of the following attack, you need to setup an RSA scheme with certain parameters that allow you to demonstrate the attack. You may consider the following attacks:

(a) Factorization
(b) Chosen-ciphertext attack
(c) Encryption exponent
(d) Decryption exponent
(e) Plaintext (short messages, cyclic, unconcealed, …etc.)
(f) Common modulus
(g) Timing attack

Submit a technical report that includes all the details of the project and share the code on GitHub with your instructor.

Evaluation:

The evaluation of this project is based on the quality of the examples presented in each attack. Decent examples get high evaluations, while trivial examples may get poor evaluations.