Information Technology Univeristy

Department of Computer Science
http://www.itu.edu.pk

Assist. Prof. Dr. Muhammad Umar

Blockchain

Assignment # 01

100 Marks

Objective of Assignment

To understand and implement fundamental cryptographic principles and algorithms essential for blockchain security. This assignment will cover hashing, encryption/decryption, and digital signature creation and verification using any programming language. You are encouraged to use https://www.cryptool.org/en/ to practically explore these concepts.

Task 1: Hashing Algorithms

Study five hashing algorithms (MD5, MD4, MD2, SHA-1, SHA-256, SHA-3). Create a file (1KB-10KB) with sample content. Develop a program to compute and store the file's hash using each algorithm. Compare these hashes to evaluate their security (collision resistance and brute-force difficulty). Use CrypTool to generate hash values for the file with the same algorithms and compare these with your program results.

Task 2: Encryption and Decryption

Choose an encryption algorithm (e.g., AES or RSA). Encrypt the file from Part 1 using this algorithm, then decrypt it to verify the original content is restored. Use CrypTool to perform the same encryption and decryption on the file and compare the results with your program.

Task 3: Digital Signatures

Create a digital signature for the file using a cryptographic library (e.g., PyCryptodome). Verify the signature to ensure the file's authenticity and integrity. Use CrypTool to perform the same tasks and compare the results with your program.

Task 4: Practical with CrypTool

Use CrypTool to perform hashing, encryption, decryption, and digital signature tasks from Task 1-3. Take screenshots of each step to document your process.

Task 5: Report Writing

Write a report summarizing the tasks from Tasks 1-4, including code snippets and CrypTool screenshots. Analyze the security of different hashing and encryption methods, and reflect on your experience with CrypTool.

Evaluation Criteria:

- Understanding and correct implementation of hashing algorithms (20%)
- Successful file encryption and decryption (20%)
- Proper creation and verification of digital signatures (20%)
- Practical exploration using CrypTool with relevant screenshots (20%)
- Quality and clarity of the report (20%)

Important Notes:

- Collaboration is encouraged, but each student must submit their work independently.
- All code and reports should be original. The use of external libraries is allowed, but they must be cited properly.

Using https://www.cryptool.org/en/ is highly encouraged to gain hands-on experience and enhance your understanding of cryptographic principle.

Submission Details:

- Single zip file with the name FirstName_RollNumber_01.zip
- Your report must contain output of your program and explanation of your results.
- Submit a single zip file containing

  (a) Code file (b) Pdf Report (c) Code Output & Cryptool screenshots
- Follow the naming convention.
- For each convention, there is a 3% penalty if you don't follow it.
- Email instructor or TA if there are any questions.
- Plagiarism will lead to a straight zero with additional consequences as well.
- 10% (of obtained marks) deduction per day for a late submission.
- **Submission Deadline: September 8, 2024**