Fall 2019: CSCI 430: Introduction to Computer and Network Security

Assignment 1

Deadline: Sep 20, 2019, 9pm.

Programming language. The preferred programming language is Java, but you could use any language. If we cannot compile your program, you would need to come to office hours and demonstrate your code on your computer.

Submission instructions. Create a private git repo on bitbucket and share the repo with the instructor (mnaveed@usc.edu) and TA (hsaleem@usc.edu). For full credit, only the code pushed to bitbucket before the deadline will be considered. Your programs need to compile without any additional software.

Problem 1: Write a program for the one-time pad encryption scheme. Your program should include key generation, encryption, and decryption procedures.

1. **Input:** your program should take command line arguments, ask the user if they want to encrypt or decrypt the message, if they want to encrypt the message, it would take plaintext message as an input, and if they want to decrypt the message, it would take ciphertext as input.

2. **Output:** your program should print the ciphertext if the user encrypts the message and print the plaintext if the user decrypts the message.

Problem 2: Write two programs to encrypt messages of arbitrary length using AES as a block cipher: the first program should use AES CBC mode and the second should use AES CTR mode. Your programs should include key generation, encryption, and decryption procedures.

1. **Input:** your program should take command line arguments, ask the user if they want to encrypt or decrypt the message, if they want to encrypt the message, it would take plaintext message as an input, and if they want to decrypt the message, it would take ciphertext as input.

2. **Output:** your program should print the ciphertext if the user encrypts the message and print the plaintext if the user decrypts the message.

Problem 3: Write a program to encrypt messages of arbitrary length using AES block cipher in an appropriate authenticated mode of encryption, such that it provides both secrecy and integrity. Your programs should include key generation, encryption, and decryption procedures.

- **Input:** your program should take command line arguments, ask the user if they want to encrypt or decrypt the message, if they want to encrypt the message, it would take plaintext message as an input, and if they want to decrypt the message, it would take ciphertext as input.

- **Output:** If the user wants to encrypt the message, your program should print the ciphertext and the authentication tag and if the user wants to decrypt the message, it should print the plaintext only if the authentication tag is valid and print an "invalid" if the authentication tag is invalid.

Problem 4: Write a program to implement a CBC-MAC for arbitrary length messages using AES as block cipher. Your program should include key generation, tag generation, and verification procedures.

- **Input:** your program should take command line arguments, ask the user if they want to generate or verify the authentication tag, if they want to generate the tag, it would take message as an input, and if they want to verify the tag, it would take both the message and the tag as input.

- **Output:** If the user wants to generate the tag, your program should print the authentication tag and if the user wants to decrypt the message, it should print "valid" if the tag is valid and print "invalid" if it is not.