CS 449 Assignment 1

Release Sep 21st, 2024; Due Oct 6th, 2024

Instructions

The homework is due on Oct 6th 23:59:59 EST. The whole assignment has been tested on a 64-bit Ubuntu 24.04 virtual machine. Using a Linux virtual machine to set up the environments and complete this assignment is recommended. If you have trouble running a Linux virtual machine on your own computer, you can go to the UNIX/PC Lab (M-3-731), Web Lab (M-3-732), or IT Lab (M-3-730) of our department where you can find computers pre-installed with virtualization software, including VMware Workstation Pro and Oracle VirtualBox.

Your submissions must have two folders, Q1 and Q2. Place the files in the appropriate folder, and use the exact names and conventions specified in the question text. Please zip the two folders without encryption, rename the zip file as CS449A1.first_name.last_name.studentID.zip, and submit it on Blackboard.

Question 1 (5 points)

Performance holds significant importance when implementing cryptographic techniques across various applications. We have discussed several symmetric and asymmetric ciphers during the class, where symmetric ciphers often outperform asymmetric ciphers in terms of encryption and decryption speed. In this question, you will use the `openssl speed` tool (`https://www.openssl.org/docs/manmaster/man1/openssl-speed.html`) to run a performance benchmark of `AES` (symmetric) and `RSA` (asymmetric) algorithms.

(a). Running benchmarks of `aes-128-cbc`, `aes-192-cbc`, `aes-256-cbc`, and `rsa` for 1 second respectively. Capture the screen snapshot of the commands you use for running them as well as the returning results.

(b). Describe the performance trends of `AES` in relation to varying block and key sizes and discuss the underlying factors driving these trends.

(c). Describe the performance trends of `RSA` in relation to varying key sizes and discuss the underlying factors driving these trends. Compare the signing (decryption) and verifying (encryption) speeds of `RSA` and analyze the reason for their differences.

Submission Instructions: Write a report containing your answers to the abovementioned subquestions. The report should be in PDF format and named as Q1.pdf. It should be placed under the Q1 folder of the submission.

Question 2 (5 points)

The block cipher mode of operation plays a critical role in the security of applying block ciphers to encrypt data whose size is larger than one block. During the class, we have learned that using the wrong mode of operation can lead to leakage of the plaintext's patterns in the ciphertext. In this question, you will apply `AES` to encrypt several bitmap images with different modes of operation and assess whether patterns from the plaintext are leaked in the resulting ciphertext.

(a). Use `openssl enc` `https://wiki.openssl.org/index.php/Enc` to perform encryption using AES-128 with ECB and CTR modes on the 3 given bitmap images (bmp24.bmp, greenland.bmp, and blackbuck.bmp). For ease of grading, please use **140b41b22a29beb4061bda66b6747e14** as the key and use **36f18357be4dbd77f050515c73fcf9f2** as IV for the CTR mode when encrypting all of these files.

If the plaintext file name is x.bmp (e.g., bmp24.bmp), name the encrypted file name as x_ecb.bmp (e.g., bmp24_ecb.bmp) and x_ctr.bmp (e.g., bmp24_ctr.bmp) respectively.

(b). Step (a). will give you the encrypted images. However, you cannot open them as images because the header was encrypted as well, preventing any photo-viewing software from displaying them as images correctly. Since all bmp format images have a 54 bytes long header, the simplest way to display the encrypted images is copying the first 54 bytes from a plaintext image to overwrite the first 54 bytes in the encrypted image. One way to do this is using the `dd` commands in Linux (`https://en.wikipedia.org/wiki/Dd_(Unix)`).

First, make a copy of each encrypted images (e.g., bmp24_ecb.bmp) and name them as x_ctr_display.bmp or x_ecb_display.bmp (e.g., bmp24_ecb_display.bmp). Then copy the first 54 bytes from each plaintext image (e.g., bmp24.bmp) to overwrite the first 54 bytes of the corresponding copied encrypted image (e.g., bmp24_ecb_display.bmp). Now, you will be able to open the encrypted images. Take a look at them and compare images encrypted in ECB mode with the ones encrypted in CTR mode.

(c). Run decryption on each encrypted images (e.g., bmp24_ecb.bmp) and compare the results with the plaintext images (e.g., bmp24.bmp) to make sure that encryption and decryption are performed correctly.

Submission Instructions: You need to submit 12 files for Question 2. Those files are: bmp24_ecb.bmp, bmp24_ctr.bmp, bmp24_ecb_display.bmp, bmp24_ctr_display.bmp, greenland_ecb.bmp, greenland_ctr.bmp, greenland_ecb_display.bmp, greenland_ctr_display.bmp, blackbuck_ecb.bmp, blackbuck_ctr.bmp, blackbuck_ecb_display.bmp, and blackbuck_ctr_display.bmp. Place all of them under the Q2 folder of the submission.