HW #1: Introduction, and Private Key Cryptography

CS x36: Computer Security
Spring 2015
[100pts]
DUE 02/02/2015 (11am)

Instructions (please read)

- This HW covers Lectures 1 and 2. Please review these thoroughly before starting to work on the HW.
- All soft copy submissions must be turned in via Canvas. Name your files as “Lastname_Firstname_HW1”. Please make sure that you have correctly submitted/uploaded the files.
- You can submit hand-written hard copies, if you wish. However, we would prefer that you submit soft copies. If you choose to submit hard copies in any case, please turn them into my mailbox in the CS office or hand them in before the lectures. Please also make sure that your hand-written solutions and handwriting is legible and easy to understand.
- You must submit by the deadline – 11 am on 02/02/2015 (Monday). This applies to both soft and hard copy submissions. Late submissions will not be graded.
- Problem 5 has two options. You can choose to solve either of them. The first option requires handling a piece of code provided to you. If you need help with the code, please contact the TA.
- You will be graded based on the correctness of your answer and also on the steps that you took to come to that answer. Please try to show all your work.
- The assignment needs to be solved individually by every student. No collaboration of any sort is allowed. No plagiarism is allowed. Please check the course policies against misconduct (discussed in Lecture 1). When in doubt, please consult the instructor.
- Please submit early to avoid any last minute issues.
- Please do start working on the homework early and do not wait until the deadline.
Problem 1 [20pts]

1) [10pts] While logging yourself in using a pair of username and password, say, at a web mailing service, you might have noticed that you are often timed-out after 3 failed attempts. What do you think this might protect against?

2) [5pts] Many people reuse the same password across multiple web sites. What is the problem with such a reuse?

3) [5pts] Define the terms “authentication” and “non-repudiation.”

Problem 2 [15pts]

In the class, we studied the Caesar’s cipher. A similar cipher is called the affine cipher, which works as follows.

*Encryption:* each plaintext letter $P$ is encrypted to obtain the ciphertext letter $C$ such that $C = aP + b \mod 26$, (where $a, b$ are numbers between 0,1,….25, and represent the secret key).

*Decryption:* each ciphertext letter $C$ is decrypted to obtain the plaintext letter such that $P = (C-b)a^{-1} \mod 26$.

I need to send a message to the class: “HELLOCLASSALLOFYOULLGETANAYOUDONOTNEEDTODOTHEHOMEWORK” (I don’t mean it!), and want to send it encrypted using the affine cipher so that the Department chair does not learn the message 😊. The chair intercepts the 8th and 3rd letters of the cipher text, ‘C’ and ‘J’ respectively, and somehow learns the corresponding plaintext letters, i.e., ‘A’ and ‘L’ respectively. Can he decrypt the message (and take a Disciplinary action against me 😊)? If so, explain how? What is the secret key? What is the original ciphertext that I sent out?

Problem 3 [25pts]

Show that DES exhibits a complementation property, i.e., if $C = Enc(K, P)$, then $C^c = Enc(K^c, P^c)$. Here, $P$ is a plaintext. $K$ is the key and $C$ is the ciphertext, and $X^c$ denotes the bitwise complementation of $X$. Show all steps.

[Hint: Consider the operations that take place in each round of DES encryption; focus on say the i-th round, and carefully analyze how the input changes after each step]

Problem 4 [10pts]

1) [5pts] [5pts] A 7-bit long message (assume that the message space size is $2^7$) was encrypted using one-time pad to yield a cipher-text “0110011”. What is the probability that the corresponding plain-text was “1001001”. *Explain your answer.*
2) [5pts] A message m1 was encrypted with a key K using one-time pad and the ciphertext was transmitted. The encryptor became lazy and encrypted another message m2 with the same key K using one-time pad, and the ciphertext was transmitted. Is this a secure way of encryption? Why/why not?

Problem 5 [30pts]: Option A

The reading assignment in the last lecture covered how AES (Rjindael) works. This problem will give you an idea as to how much processing time AES requires to perform key generation, encryption and decryption.

Download the AES implementation source code from: http://www.cis.uab.edu/saxena/teaching/csx36-s14/labs/aes-src-modified.zip. The folder contains a README file for instructions, and a Makefile is also provided.

First, familiarize yourself with the AES key generation, encryption and decryption functions in this source code. Choose a key and block size of 128 bits. Choose any plaintext M 128*5 bit long. Then, perform the following:
   1) Execute the key generation function to get a key K.
      • Compute the execution time.
   2) Execute the encryption function to encrypt M using K and obtain the ciphertext.
      • Compute the execution time.
   3) Execute the decryption function to decrypt C using K and once again obtain M.
      • Compute the execution time.

Repeat each of the above steps 100 times and give the average execution time for each of the three functions. List the type and speed of the processor, and the memory (RAM) of the machine you execute the code on.

I hope you know how to measure execution time! If not, please try to figure it out yourself before asking for help. Please include a description (such as in the form of a README file) of how you measured the timing, such as what functions you measured the execution time of. **Submit your modified code along with the homework submission.**

Problem 5 [30pts]: Option B

1) [15pts] Is the following statement True or False:
   “4-DES uses four (single) DES encryption operations in series and four independent keys – C = Enc(K4,(Enc(K3, Enc(K2, (Enc(K1, P))))) – has an effective keyspace size of 2^{224} under the known-plaintext attack”?’

Argue your answer in details.

2) [15pts] Demonstrate a chosen-ciphertext attack (CCA) against the CFB mode of encryption with Triple-DES as the building block. **Discuss all details.**