

CSCI 283 and CSCI 172- Graduate and Undergraduate Computer Security - Fall 2006
George Washington University

Homework 1

due 11 October, 6 pm.

100 points

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the test and final.

You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

You may not refer to solutions to previous years' problem sets, or ask for help students from previous years, except the TA.

Any violations will be treated as violations of the Code of Academic Integrity.

PLEASE submit all HW on Blackboard only. Name your files:
CS283_HW1_LASTNAME_FIRSTNAME.doc or .pdf or
CS172_HW1_LASTNAME_FIRSTNAME.doc or .pdf

1.

a. (2 points) Encrypt the following plaintext using the Caesar cipher with shift = 10:

HOW FAR IS IT?

b. Decrypt the following ciphertexts, encrypted using the Caesar cipher with unknown shift (in each message, a few symbols are in error):

i. (2 points) yjnfzscr omsn

ii. (2 points) xip ng

c. Provide the following (1 point each):

i. $4^{-1} \pmod{11}$

ii. $6^2 \pmod{19}$

iii. $5 \times 3^{-1} \pmod{7}$

iv. $3 \times 11 \pmod{17}$

2.

a. (3 points) Suppose $y = 3x + 5 \pmod{23}$ is the encryption function of an affine cipher. What is its decryption function?

b. (1 point) Encrypt $x = 8$ using the cipher of (a)

c. (1 point) Decrypt $y = 3$ using the cipher of (a)

d. (2 points) How many distinct affine ciphers are there over \mathbb{Z}_9 ? Count the identity as one cipher.

3. (10 points)

Let $y = DES(x, K)$ represent the encryption of plaintext x with key K using the DES cryptosystem. Suppose y' is the encryption of the bitwise complement of x with the bitwise complement of the key K . Show that y' is the complement of y , i.e. if the plaintext and the key are complemented, then so is the ciphertext.

More formally, if $y = DES(x, K)$ and $y' = DES(\bar{x}, \bar{K})$, where \bar{x} denotes the bitwise complement of x , prove that $y' = \bar{y}$. Note that this can be proved for any S-box structure. For this problem, note that the expansion function that acts on R (on Slide 4) consists of simply repeating some bits of R.

Is this a vulnerability? If so, what kinds of cryptanalysis does it make DES vulnerable to?

Make sure you provide all steps for full credit.

4. Shannon's condition for perfect secrecy is that, on receiving the ciphertext, the adversary should not be able to make a guess on the key or message that is better than random (or better than the guess they would have made before receiving the ciphertext). Are the following ciphers perfectly secret? Why or why not? All credit is reserved for the reasons you provide, no credit will be given for a correct answer that is not substantiated properly.

a. (2 points) The one-time pad, with a key as long as the message, where ones appear with probability 0.6.

b. (2 points) One round of the Feistel cipher, acting on two bytes, with a two byte key.

c. (3 points) A single SPN layer with message length = key length, and no reuse of the key.

d. (3 points) A single SPN layer with message length = key length, and key reused.

5. (20 points). Your teacher needs to create random IDs for each student in the class so as to be able to post grades in a public place yet maintain student privacy. Her goal is to ensure that the student can check his or her own grade, but that nobody may determine another persons grade. She decides to use encryption. She encrypts each students name in one of the following ways, and gives the student the ciphertext as his or her random ID. She then lists the students grade next to the ciphertext corresponding to the student.

For each of the following, state why or why not its use would be appropriate for the problem. In particular, describe vulnerabilities and attacks and their expense to the attacker, and the *expense of a secure method* to the professor. Assume that there are n students in the class, that the professors public key is known widely, that all private keys are well protected and revealed only to persons mentioned, that the list of students in the class is publicly available, and that, in accordance with good security practice, the professor makes known the method she uses.

a. Encrypting student names with her private key from her public/private key pair.

b. Encrypting student names with her public key.

c. Encrypting student names with a single shift cipher, key unknown to anyone but her.

d. Encrypting each student name with a different shift cipher, each key unknown to anyone but her.

e. Encrypting student names with a substitution cipher, key unknown to anyone but her.

f. Encrypting student names with a private key block-cipher, using a different private key for each student.

g. Rank the methods in order of security, from most to least secure. If two methods are equally secure, indicate this. Provide reasons for your ranking.

6. (10 points). Suppose there are n students in a class who want to send encrypted messages to one another.

a. Suppose they use private key encryption.

i How many keys would each student have to manage? Why?

ii. How many different keys would exist in the system? Why?

b. Suppose they use public key encryption. Answer i and ii above.

7. (10 points). Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice and Bob's public keys.

a. How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either?

b. How might Alice and/or Bob detect Eve's subversion?

8. (10 points).

a. Is the *complement-sum* function, which outputs the exclusive or of the complement of each byte in a file (to obtain a single byte), a good candidate for a secure hash function? Why or why not?

b. Is the *cherry-picking* function, which outputs the n^{th} bits of a file, a good candidate for a secure hash function? Why or why not? (For example, the function might output every 20th bit).

9a. (6 points) Assume a four-stage LFSR with $t=1011$ and the initial contents of the register $r=1010$. Generate the first four bits of the pseudo-random output of the LFSR, and determine the register content after the fourth bit is output. For full credit, show intermediate register contents and at least one example expression for a new register bit with 0's and 1's substituted into the expression for the new bit.

b. (4 points) How would one encrypt a message m given the output of an LFSR? What would the key for the encryption be? What are the advantages and disadvantages of the method?

c. (3 points) Suppose a pseudo-random string is such that its next bit can be determined from the previous n bits without knowing the seed. Describe a means of determining an entire plaintext encrypted by XORing with the pseudo-random string if the ciphertext is known, the key is not, and n consecutive bits of the plaintext are known.