Assignment #1:

Introduction, History, Network and Systems, Theory of Secure Communications

Total: 20 points

Q1. (5 points) For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. A student maintaining a blog to post public information.
b. An examination section of a university that manages sensitive information about exam papers.
c. An information system in a pathological laboratory maintains the patient's data.
d. A student information system used for maintaining student data in a university that contains both personal and academic information and routine administrative information (not privacy-related). Assess the impact for the two data sets separately and the information system as a whole.
e. A University library contains a library management system that controls the distribution of books amongst the students of various departments. The library management system contains both the student data and the book data. Assess the impact for the two data sets separately and the information system as a whole.

Q2. (2 points) A fundamental cryptographic principle states that all messages must have redundancy. But we also know that redundancy helps an intruder tell if a guessed key is correct. Consider two forms of redundancy. First, the initial n bits of the plaintext contain a *known pattern*. Second, the final n bits of the message contain a *hash over the message*. From a security point of view, are they equivalent? Discuss your answer.

Q3. (2 points) Suppose that a message has been encrypted using DES in ciphertext block chaining mode. One bit of ciphertext in block C_i is accidentally transformed from a 0 to a 1 during transmission. How much plaintext in block C_{i+1} received by the receiver will be garbled as a result?

Q4. (2 points) The following ciphertext was generated using a simple substitution algorithm. Find the key and the plaintext.

hzsrnqc klyy wqc flo mflwf ol zqdn nsoznj wskn lj xzsrbjnf,
wzsxz gqv zqhhnf ol ozn glco zlfnco hnlhrn; nsoznj jnrqosdnc
lj fnqj kjsnfbc, wzsxz sc xnjoqsfrv gljn efeceqr. zn rsdnb
qrlfn sf zsc zlecn sf cqdsrrn jlw, wzsoznj flfn hnfnojqonb.
q csfyrn blgncosx cekksxnb ol cnjdn zsg. zn pjnqmkqconb qfb
bsfnb qo ozn xrep, qo zlejc gqozngqosxqrrv ksanb, sf ozn cqgn
jllg, qo ozn cqgn oqprn, fndnj oqmsfy zsc gnqrc wsoz loznj
gngpnjc, gexz rncc pjsfysfy q yenco wsoz zsg; qfb wnfo zlgn
qo naqxorv gsbfsyzo, lfrv ol jnosjn qo lfxn ol pnb. zn fndnj
ecnb ozn xlcv xzqgpnjc wzsxz ozn jnkljg hjldsbnc klj soc
kqdlejnb gngpnjc. zn hqccnb onf zlejc leo lk ozn ownfov-klej
sf cqdsrrn jlw, nsoznj sf crnnhsfy lj gqmsfy zsc olsrno.

Hints:
1. As you know, the most frequently occurring letter in English is e. Therefore, the first or second (or perhaps third?) most common character in the message is likely to stand for e. Also, e is often seen in pairs (e.g., meet, fleet, speed, seen, been, agree, etc.). Try to find a character in the ciphertext that decodes to e.
2. The most common word in English is "the." Use this fact to guess the characters that stand for t and h.
3. Decipher the rest of the message by deducing additional words.
Warning: The resulting message is in English but may not make much sense on a first reading.

Q5. (2 points) Using the Vigenère cipher, encrypt the word “explanation” using the key “leg”.

Q6. (2 points) This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5..., then the first letter of the plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

(a) Encrypt the plaintext “send more money” with the keystream

(b) Using the ciphertext produced in part (a), find a key so that the ciphertext decrypts to the plaintext “cashnotneeded.”

Q7. (5 points) For the following ciphertext:

dhtcgmicskfstadpnixklsduryojqjlmdiflrbppfcdbcztdbczptpipnvlmydhdddihsmtltigabtplkicbwoojgmmdpgiuehhq
oexhqaacsguggxeotxcdyocimmmthnlazxlnwdgbzoulgzddbjltxizlltigabtacaiiqcseixrieatrptqtuoihecywdgbzoulgzd
dbjltxizlacsuoeciflbgdilnwtyyttsnloeacsikxlniciflwdgjkavgcltwtplwxajiepcyusltpseixrieudpahdjeotwtwtanqcwag
icktwtplihhrplapaoacrcahpiroenlgslhtcahtgcdiaazlacplzwtgjltxizlltigabtacaiiqcseixrieatrptqtwlawiflrtlgslqtyuach
ulratrptqtjltxizlltigabtacaiiqcseixrielwgzptguvrshmmwxhbvmatrptqtjltxizlltigabtacaiiqcfepwjltxizlwwxqweglmy
dhdddihsmtltigabtplkwwtlahtcgnhixqjldjbftwtplihhrplapjpgwiroaihfpnthmumthfpntjlaiaimtoggmdltigabtxuhktjn
aoiwczojcbvfbjqpcbdroegbyyyrdklsidklsetyricvuvrshmmwxhbvmatrptqtjltxizlltigabtacaiiqcfepwjltxizltwtplwxaj
iepcyusltpseixrieatrptqtjltxizlltigabtnchhatrptqtroegtuplaqchnpcqdegacaiiqcseixrieatrptqtjltxizlytpfseixrielwgzpt
guvrshmmwxhbvmatrptqt

(1) Analyze and identify the ciphering technique used (1 points)

(2) Identifying the correct key and the corresponding plaintext (1 point)

(3) Programming code for decryption (3 point): The fully automated code (which give output with analysis) is not necessary. However, the students need to implement codes that does the analysis for them. You cannot just simply guess or do it by trial and error. It is important that the code include the analysis code.