

Homework #2
ISA 562 Information Security Theory & Practice
Fall 2007

This homework is due on 10/22 by 4:30 PM. This assignment is to be done by each student individually.

- Submit your solutions in either MS Word or in PDF format. Submit your solutions to the TA at gmuisa562@gmail.com with “ISA 562 HW#2” as the subject in your email. You will also need to submit a hard copy on the day the assignment is due as well.

- **Make sure to include your name and G-number at the beginning of your homework submission.**

1. (10 points) Are all the 56 bits of the DES key used an equal number of times in the K_i ? (explain)
2. (10 points) The Mangler function takes a 32-bit R and XORs it with a 48-bit subkey. How is this possible?
3. (20 points) Decode the following cipher-text, and write a detailed explanation of the process you went through to get the plaintext. If you ended up writing a program, submit it with your solution. (hint: scytale)

TETHIETLTHRRNOHCIYSRHEGOTIEIERSPOIOTOUASRTSETRNFUITAPOT

4. (60 points) Decode the following cipher-text, and write a detailed explanation of the process you went through to get the plaintext. If you ended up writing a program, submit it with your solution. You will receive partial credit even if you cannot decrypt the cipher-text, presuming that your answer includes a very descriptive and elaborate discussion on the approach and methodology you used to try to decrypt the cipher-text. Make sure you also include what you have learned or realized from this experience in your discussion.

Hints:

1. The encryption algorithm used is a classic symmetric cipher (not covered in the lecture) that has the following property:
 - a. Just as plaintext is entered into the cryptographic system to get the cipher-text, the cipher-text can be entered in the same place in the system, to retrieve the original plaintext.
2. The 5 character grouping of cipher-text is independent of the plaintext; meaning that the plain text is not composed of thirteen 5 character words.
3. The plaintext is a valid English sentence.

Z W E P F M Y X I F Y G I D Y Q I N X J M O C C G
U Q Y Q K C C N O C C G Q Y O C C G Y K C Q D N Q
Y O C C G Y K C Y J M U M D X