King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Department of Computer Engineering

COE 451 – Computer and Network Security (T142)

Homework # 02 ***(due date & time: Tuesday 24/02/2015 during class period)***

Problem # 1: Suppose that we have a computer that can test 2^{40} keys each second.

a. What is the expected time (in years) to find a key by exhaustive search if the key size is 64 bits?
b. What is the expected time (in years) to find a key by exhaustive search if the key size is 128 bits?

Problem # 2: Decrypt the ciphertext

TDEUNOTFTHAKITNFGAHDEOMCPTUEREIMAAP
ORUDSNINGEREINGUIVNESRITYDPAERMTENT

This message was encrypted with a double transposition (of the type discussed in the text) using a matrix of 7 rows and 10 columns. (Hint: The first 2 words are "I am")

Problem # 3: Using the letter encodings in Table 2.1, the following ciphertext message was encrypted with a one-time pad:

KITLKE

a. What is the key if the plaintext is "**thirst**"?
b. What is the key if the plaintext is "**hikers**"?

Problem # 4: Suppose that the following is an excerpt from the decryption codebook for a classic codebook cipher.

123	in the long
199	nothing but
202	spoon
221	us
233	the shape of the
332	run teaches
451	feeding

Assume that the following additive sequence was used to encrypt the message: 119, 222, 199, 231, 202, 547, 547, 221. Decrypt the following ciphertext: 321, 673, 322, 563, 423, 746, 780, 423.