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

COE 451 – Computer and Network Security (T151)

Homework # 02 (due date & time: Tuesday 15/09/2015 during class period)

Problem # 1: Suppose that we have a computer that can test 2^{50} keys each second.

a. What is the average time (in years) to find a key by exhaustive search if the key size is 112 bits?
b. What is the average time (in years) to find a key by exhaustive search if the key size is 256 bits?

Problem # 2: Decrypt the ciphertext

RENEINGERITYIETHSBESNGDRPAETMENTANK
ITGFAHDUEIVNRSITHEPOMCUTETINGHETULF

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 last word is "GULF")

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 "**killer**"?
b. What is the key if the plaintext is "**kettle**"?

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

123	kindness becomes part of
199	it leaves it tarnished
202	be kind for
221	it beautifies it and
233	it is taken from
332	something
451	whenever

Assume that the following additive sequence was used to encrypt the message: 199, 222, 119, 231, 202, 547, 346, 221, 547. Decrypt the following ciphertext: 401, 673, 242, 563, 423, 998, 579, 553, 746.