Faculty of Computer Science and Engineering
Ho Chi Minh City University of Technology

Cryptography and Network Security
Tutorial 2

Nhat Nam Nguyen
nhatnamcse@gmail.com

20/02/2016

Basic Exercises (7pts)

Exercise 1. (1pts)
What is the difference between diffusion and confusion?

Exercise 2. (1pts) What is the avalanche effect?

Exercise 3. (1pts) How many keys are used in triple encryption?

Exercise 4. (4pts)
This problem provides a numerical example of encryption using a one round version of DES. With the the key and the plaintext following:

```
PLAINTEXT:
0001 0001 0110 0011 0100 0101 0110 0111
0000 1001 1110 1011 1100 1101 1110 1111

KEY:
0000 0001 0010 0011 0100 0101 0110 0111
1000 1001 1010 1011 1100 1101 1110 1111
```

EXPRESS YOUR ANSWERS IN BINARY NOTATION IN 4-BIT GROUPS WITH SPACE SEPARATORS (I.E., 0010 1100 1110, ETC.)!

Part a. Derive K_1, the first round key.
Part b. Derive L_0, R_0
Part c. Expand R_0 to get $E[R_0]$, where E is the expansion function of Table 3.2.
Part d. Calculate $A = E[R_0] \oplus K_1$
Part e. Group the 48-bit result of part d into sets of 6 bits and evaluate the coresponding S-box substitutions. Express your answers in decimal and binary.
Hint: Be sure you count 0, 1, 2, 3, etc for row and column position when doing the S-box lookup.
Part f. Concatenate the results of part e to get a 32-bit result, B. Express the answer in binary.
Part g. Apply the permutation to get P(B).
Part h. Calculate $R_1 = P(B) \oplus L_0$
Part i. Write down the cipher text.

Advanced Exercises (3pts)

Exercise 5. (3pts)
(a) Suppose that we have a network with 10 nodes. How many different keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way using classical cryptosystem?
(b) We replace classical system with a public key system. How many dif- ferent keys do we have to generate such that every pair of nodes can communicate in a bi-directional secure way?
(c) Suppose that we extend the network with one more node. How many new extra keys do we need to generate such that every pair of nodes can communicate in a bi-directional secure way? (Calculate for classical and public cryptosystems).
(d) What is your short conclusion or the interpretation of the results found above?

THE END