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

Cryptography and Network Security
Lab 2

Hieu Nguyen

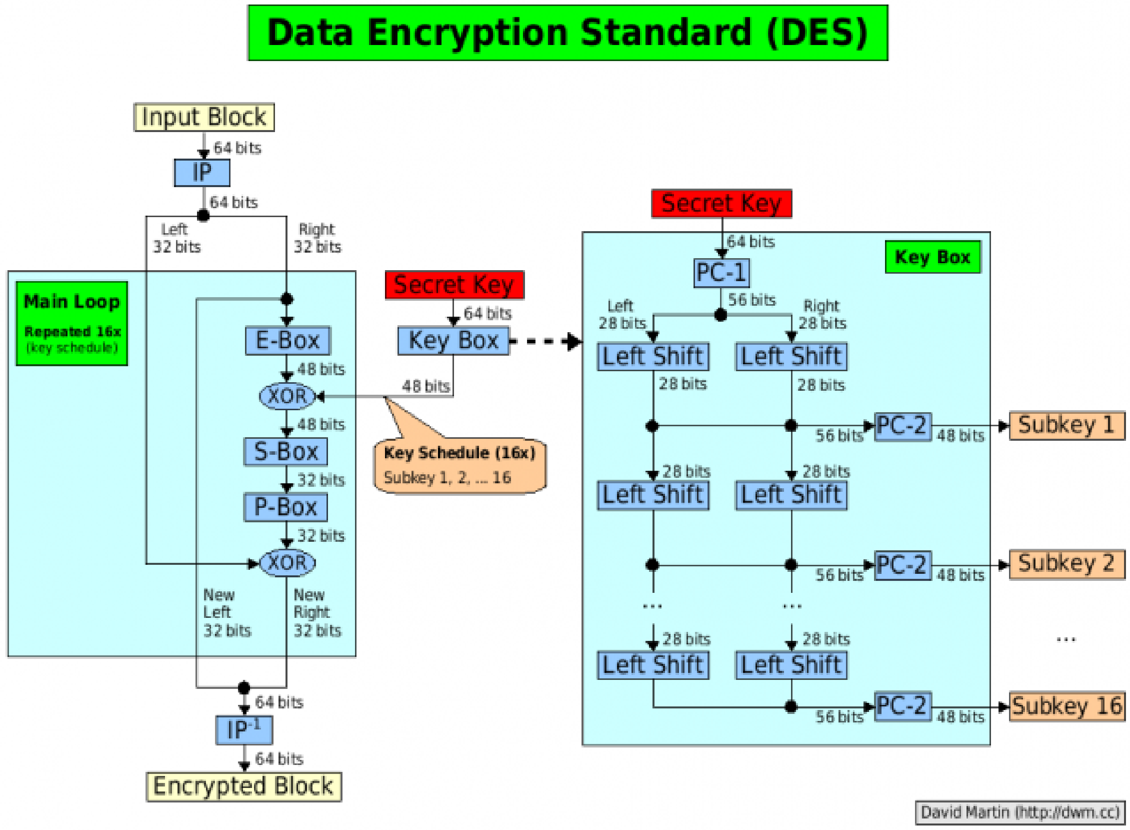
January 21, 2019

INTRODUCTION

In this exercise we will focus on modern ciphers, primarily on the most prominent block cipher DES. The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. Although now considered insecure, it was highly influential in the advancement of modern cryptography.

EXPERIENCE

How does DES work? This paper explains the various steps involved in DES-encryption, illustrating each step by means of a simple example. Since the creation of DES, many other algorithms (recipes for changing data) have emerged which are based on design principles similar to DES. Once you understand the basic transformations that take place in DES, you will find it easy to follow the steps involved in these more recent algorithms.



David Martin (http://dwm.cc)

HOMEWORK

Exercise 1.

Briefly define a nonsingular transformation.

Exercise 2.

What is the difference between a block cipher and a stream cipher?

Exercise 3.

Suppose the DES F function mapped every 32-bit input R, regardless of the value of the input K, to;

a. 32-bit string of zero

b. R

Then

1. What function would DES then compute?
2. What would the decryption look like?

Hint: Use the following properties of the XOR operation:

$(A \oplus B) \oplus C = A \oplus (B \oplus C)$

$(A \oplus A) = 0$

$(A \oplus 0\ ) = A$

$A \oplus 1 =$ bitwise complement of A

where
A,B,C are n-bit strings of bits 0 is an n-bit string of zeros
1 is an n-bit string of one

Exercise 4 (5pt).

This problem provides a numerical example of encryption using a one round version of DES. We start with the same bit pattern for the key and the plaintext, namely:
In hexadecimal notation:

```
0 1 2 3 4 5 6 7 8 9 A B C D E F
```

In binary:

```
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 SEPERATORS (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.

Exercise 5 (3pt).

Using S-DES, decrypt the string (10100010) using the key (0111111101) by hand. Show intermediate results after each function (IP, FK, SW, FK, IP-1). Then decode the first 4 bits of the plaintext string to a letter and the second 4 bits to another letter where we encode A through P in base 2 (i.e., A = 0000, B = 0001, ..., P = 1111). Hint: As a midway check, after the application of SW, the string should be (00010011).