

## Assignment 4 (Topic 5. Block Ciphers and Hash Functions)

1. For DES, explain DES decryption, what conclusion can you derive?
2. If you are approached by a company to design a cipher with low cost. Which type of cipher algorithms that you would like to recommend to them. Justify your answer.

The following two questions are optional.

3. Let  $A^c$  be the complement of  $A$  where  $A$  is a binary string (e.g. if  $A = 1000100$ , then  $A^c = 0111011$ .)
  - (a) Show that if  $Y = DES_k(X)$ , then  $Y^c = DES_{k^c}(X^c)$ .
  - (b) It has been said that a brute-force attack on DES requires searching a key space of  $2^{56}$  keys. Does the result of part (a) change that?
4. For RIJNDAEL,
  - (a) For 128-bit version of RIJNDAE, what is the complexity of placing a brute-force attack on it? Do you know any improvement for this complexity?
  - (b) In the description of RIJNDAEL, the order of performing three basic operators is illustrated in the slides. Explain that why we can change this order to the Word-Operation.
5. The core nonlinear part of the permutations in AES is the  $S$ -box, which is the 8-bit inverse function. Let a simplified AES 4-bit S-box, denoted by  $E(x)$  given as follows.

$x$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$E(x)$	0	1	9	14	13	11	7	6	15	2	12	5	10	4	3	8

(1)

Let  $k = 0011$  be the symmetric key shared by two communication entities, say Alice and Bob. (We assume that the right most bit is the least significant bit.) The encryption is defined as follows:

$$c = E(k + m)$$

where the addition is bitwise addition. For example, if the message  $m = 0101$ , since  $k + m = 0011 + 0101 = 0110$ , look at the table, for input  $x = 0110 = 2 + 2^2 = 6$ , then the cipher text is given by

$$c = E(k + m) = E(6) = 7 = 0111.$$

Find the cipher text for the plaintext  $m = 1100010111110011$ .