Malaviya National Institute of Technology Jaipur	2019-20
Department of Computer Science and Engineering	M-Tech
CST-618 : Security In Computing	Semester - I
Assignment-II	**Due on: 23/09/2019**

Name: _____ **ID:** _____

Problem 1: Answer all the following questions.

1 In AES

a The so called S-box (Substitution box) is widely used cryptographic primitive in symmetric key cryptosystems. In AES (Advanced Encryption Standard) the 16 S-boxes in each round are identical. All these S-boxes implement the inverse function in the Galois Field GF(2^8), which can also be seen as a mapping, $S : \{0,1\}^8 \rightarrow \{0,1\}^8$ so that

$$x \in GF(2^8) \rightarrow sx^{-1} \in GF(2^8)$$

that is 8 input bits are mapped to 8 output bits. What is the total number of possible mappings one can specify for function S ?

that is 8 input bits are mapped to 8 output bits. What is the total number of possible mappings one can specify for function S ? Hint: Any function $f : GF(2^n) \rightarrow GF(2^n)$ can be represented as a polynomial, $f(x) = a_0 + a_1(x) + a_2(x^2) + ... + a_{2^n-2}(x^{2^n-2}) + a_{2^n-1}(x^{2^n-1}, \ a_i \in GF(2^n)$

b Construct the Galois

field of 16 elements, $GF(2^4)$, using a primitive polynomial $f(x) = x^4 + x + 1$. Compute the powers x_i, $0 \leq i \leq 14$ and represent these powers (multiplcative group) as polynomials of the form $a_0 + a_1x + a_2x^2 + a_3x^3$:

c Assume we want to implement an S-box using the Galois field from b). If we would like that our S-box is bijective is it a good choice to use function $S : GF(2^4) \rightarrow GF(2^4)$ specified by,

$$x \in GF(2^4) \rightarrow sx^3 \in GF(2^4)$$

Motivate your answer !

2 Consider a modified substitution-permutation network where instead of carrying out the key-mixing, substitution, and permutation steps in alternating order for r rounds, the cipher instead first applies r rounds of key-mixing, then carries out r rounds of substitution, and finally applies . r permutations. Analyze the security of this construction.

3 In the actual construction of DES, the two halves of the output of the final round of the Feistel network are swapped. That is, if the output of the final round is (L_{16}, R_{16}) then the output of the cipher is in fact (R_16, L_16). Show that the only difference between the computation of DES_k and DES^{-1} (given the swapping of halves) is the order of subkeys.

4 (This problem assumes the results of the previous exercise.)

(a) (a) Show that for $k = 0^{56}$ it holds that $DES_k(DES_k(x)) = x$. Why does the use of such a key pose a security threat?

(b) (b) Find three other DES keys with the same property. These keys are known as weak keys for DES.

(c) (c) Does the existence of these 4 weak keys represent a serious vulnerability in DES? Explain your answer.

5 Say the key schedule of DES is modified as follows: the left half of the master key is used to derive all the sub-keys in rounds 1-8, while the right half of the master key is used to derive all the sub-keys in rounds 9-16. Show an attack on this modified scheme that recovers the entire key in time roughly 2^{28} .

6 As you know, DES is insecure because of its short key length (56 bits). An improvement, proposed by Rivest, is $DESX$. $DESX$ has key length 120 bits, seen as a pair (k_1, k_2), where k_1 is 56 bits and k_2 64 bits. The encryption of a one-block message m is

$$DESX_{(k_1,k_2)}(m) = DES_{k_1}(m \oplus k_2) \oplus k_2$$

(a) Explain how decryption is done.

(b) Explain why the inner xor is necessary, i.e. explain an attack against

$$DESX'_{(k_1,k_2)}(m) = DES_{k_1}(m) \oplus k_2$$

that is much better than brute force.

"Good friends, good books, and a sleepy conscience: this is the ideal life. " **- Mark Twain**