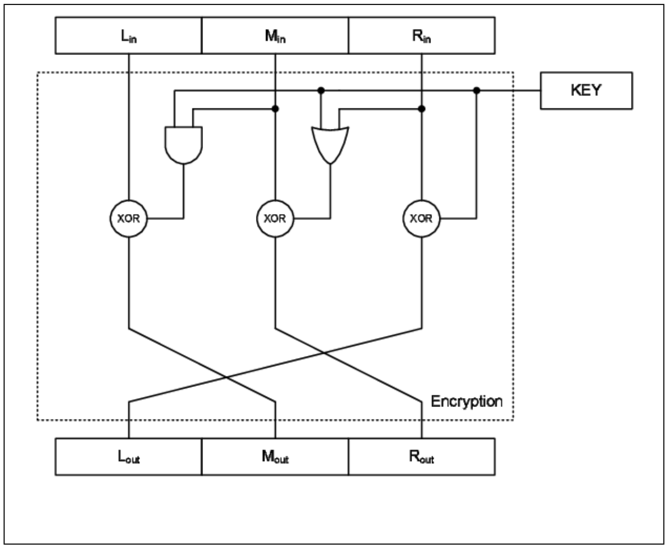
Assignment II - B.Tech VIIth Semester
Cryptography
last date for submission - will be announced in class

Five students can submit one assignment

1. Consider the follwing block structure encryption.The input blocks is divided into 3 sub-blocks:L_{in} (Left sub-block), M_{in} (Middle sub-block), R_{in} (Right sub-block). The encrypted output block is composed of L_{out},M_{out},R_{out} as in the input block.Design the decryption structure.



2.
   - Show that in DES Decryption is similar to Encryption.
   - Draw the diagram for single round of DES Algorithm (with diagram of F-function). Let X' be the bitwise complement of X. Prove that if the complement of the plaintext block is taken and the complement of an encryption key is taken, then the result of DES encryption with these values is the complement of the original ciphertext. That is,
     If Y = E(K,X)
     Then Y' = E(K',X')
     (you can use the results: $(A \otimes B)' = A' \otimes B$ and $A \otimes B = A' \otimes B'$)
   - How many key space searching is required to make brute-force attack on DES. Does the result of part(a) change that under chosen plaintext attack? How?

3. Explain the meet in middle attack on 3-DES. Find the mempory and time complexity of this attack.

4. Briefly explain an ideal block cipher. In this ideal block cipher, what is the probability that two keys (k_1, k_2) will give the same pair of plaintext and ciphertext.

5. $Z_7 = (1, 2, 3, 4, 5, 6), * \, mod \, 7$ is a group. Write all cyclic subgroups (different order) of Z_7.Is Z_7 cyclic group.

6. $H = (0, 1, 2, 3, 4, 5, 6, 7), + \, mod \, 8$ is a group. Write all cyclic subgroups (different order) of H. Is H cyclic group.

7. Find generator of Schnorr group for following prime $p = 11$. Also find other elements of the Schnorr group.
(i) $p = 11 = 2 * 5 + 1$

8. Consider $R = Z_{18}[x]/(x^4 + 1)$, the ring of polynomials with coefficients from Z_{18}, with operations defined modulo $x^4 + 1$. It is known that R is a commutative ring with unity. Is it a field.

9. Consider $R = Z_{11}[x]/(x^4 + 1)$, the ring of polynomials with coefficients from Z_{11}, with operations defined modulo $x^4 + 1$. It is known that that R is a commutative ring with unity. Is it a field.

10. How will create field of size (3^2). Write all the elements of field of size (3^2). Assume that prime(irreducible) polynomial exist in every degree.

11. Find the additive and the multiplicative inverse of $x^3 + x + 1$ in GF(2^4), with prime polynomial $= x^4 + x + 1$.

12. Find the multiplicative inverse of the following in GF(3^3) with respect to the prime polynomial $= x^3 + x + 1$.
(i) $x^2 + 2x + 1$ (ii) $2x + 2$

13. Suppose that using commodity hardware it is possible to build a computer for about 200 that can brute force about 1 billion AES keys per second. Suppose an organization wants to run an exhaustive search for a single 128-bit AES key and was willing to spend 4 trillion dollars to buy these machines (this is more than the annual US federal budget). How long would it take the organization to brute force this single 128-bit AES key with these machines? Ignore additional costs such as power and maintenance.

14. Let m be a message consisting of l AES blocks (say $l = 100$). Alice encrypts using randomized counter mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number $l/2$ is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

15. Let m be a message consisting of l AES blocks (say $l = 100$). Alice encrypts using CBC mode and transmits the resulting ciphertext to Bob. Due to a network error, ciphertext block number 15 is corrupted during transmission. All other ciphertext blocks are transmitted and received correctly. Once Bob decrypts the received ciphertext, how many plaintext blocks will be corrupted?

16. Prove that block cipher with ECB mode is not semantically secure.

17. Find the minimum value of k (minimum no. of students) such that probability is greater than 0.5 that at least two people in a group of k-people have the same birthday? How it improves the attack on collision resistant property of the hash function.

18. Alice and Bob share a secret key of some private key system. Bob has a message he claims came from Alice and to prove this he produces a plaintext message and a ciphertext. The ciphertext decrypts to the plaintext under the secret key which Alice and Bob share. Please explain why this does not satisfy the requirements of non-repudiation of origin.

19. Show that 64-bit message digest is vulnerable to collision attack. Assuming that adversary can perform 2^{20} tests(hash values) per second.

20. What is the minimum and maximum number of padding bits that can be added to a message in SHA-512.

21. Let $E : \{0,1\}^k \otimes B^n \longrightarrow B^n$ be a block cipher, where $B = 0, 1^n$. View a message $M \in B*$ as a sequence of $l-$ bit blocks, $M = M[1] \ldots M[m]$. Consider $MAC : \{0,1\}^k \otimes B^* \longrightarrow B$. Show that following MAC are forgeable under chosen message attack.

    - Function MAC is defined by $MAC_k(M[1] \ldots M[m]) = E_k(M[1]) \oplus \ldots \oplus E_k(M[m])$.
    - Here $l = n - 32$. Function MAC is defined by $MAC_k(M[1] \ldots M[m]) = E_k(< 1 > ||M[1]) \oplus \ldots \oplus E_k(< m > ||M[m])$. $< i >$: is the $32-$ bit binary representation of the block index i.

22. To make the message multiple of block length n, padding is required. If padding is $00 \ldots 00$ then show that it may lead to some kind of forgery under CMA.

23. If basic $CBC - MAC$ is used for variable number of blocks then show that basic $CBC - MAC$ is vulnerable for some kind of attack.