George Jone

913177426

Due: 7:00PM, Tuesday, 02/23/2016

CSC650 Secured Network Systems

Homework 1

1. Five elements of a cryptosystem. 5-tuple. Plaintext, Ciphertext, Key, Encryption Algorithm, Decryption algorithm
2. This problem explores the use of a variation of the Vigenere cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5..., then the first letter of plaintext is encrypted with a circular shift of 3 letters to the right, the second with a circular shift of 19 letters to the right, the third with a circular shift of 5 letters to the right, and so on.
    a. Encrypt the plaintext sendmoremoney with the key stream 9 0 1 7 23 15 21 14 11 11 2 8 9. (5 Points)

i.	Plaintext	s e n d m o r e m o n e y
ii.	Index	19 5 14 4 13 15 18 5 13 15 14 5 25
iii.	Key	9 0 1 7 23 15 21 14 11 11 2 8 9
iv.	(index+key)mod26	2 5 15 11 10 4 13 19 24 26 16 13 8
v.	Ciphertext	b e o k j d m s x z p m h

    b. Find a key so that the plaintext cashnotneeded is encrypted to the same ciphertext as produced in part a. (5 Points)

i.	Plaintext	c a s h n o t n e e d e d
ii.	Index	3 1 19 8 14 15 20 14 5 5 4 5 4
iii.	Key	25 4 22 3 22 15 19 5 11 21 12 8 4
iv.	(index+key)mod26	2 5 15 11 10 4 13 19 24 26 16 13 8
v.	Ciphertext	b e o k j d m s x z p m h

3. Consider the brute-force attack.
    a. 2^(10 bits) * 1 second/key = 2^10 = 1024 seconds
    b. 2^10 * 0.001 = 1.024 seconds

c. 2^(20) * 0.001 = 1048.576 seconds

d. With each added bit, the time it takes for a worst-case brute force attack to succeed is exponentially longer. This means that, generally, having a longer key-space will make your system more secure.

4. Consider Data Encryption Standard (DES).

   a. What is the length of a plaintext, a ciphertext, and a key in DES? (10 Points)

      i. Plaintext length: 64 bits

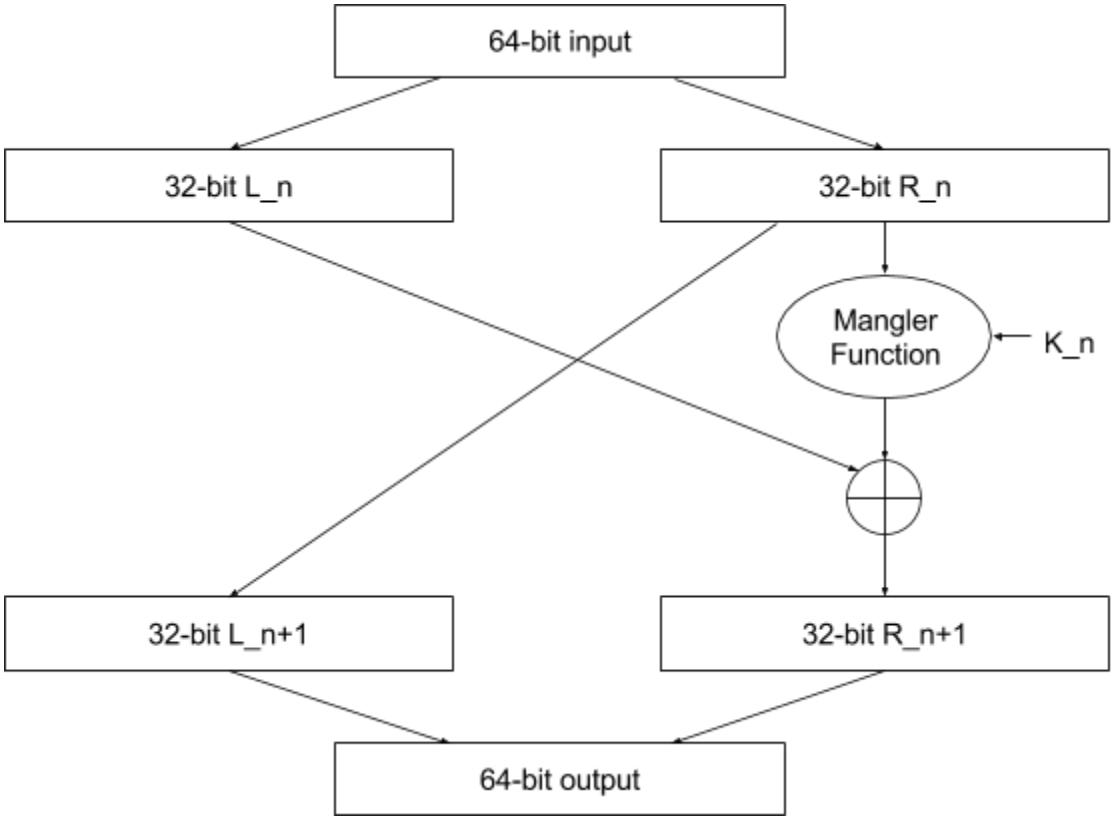
      ii. Ciphertext length: 64 bits

      iii. Key length: 64 bits

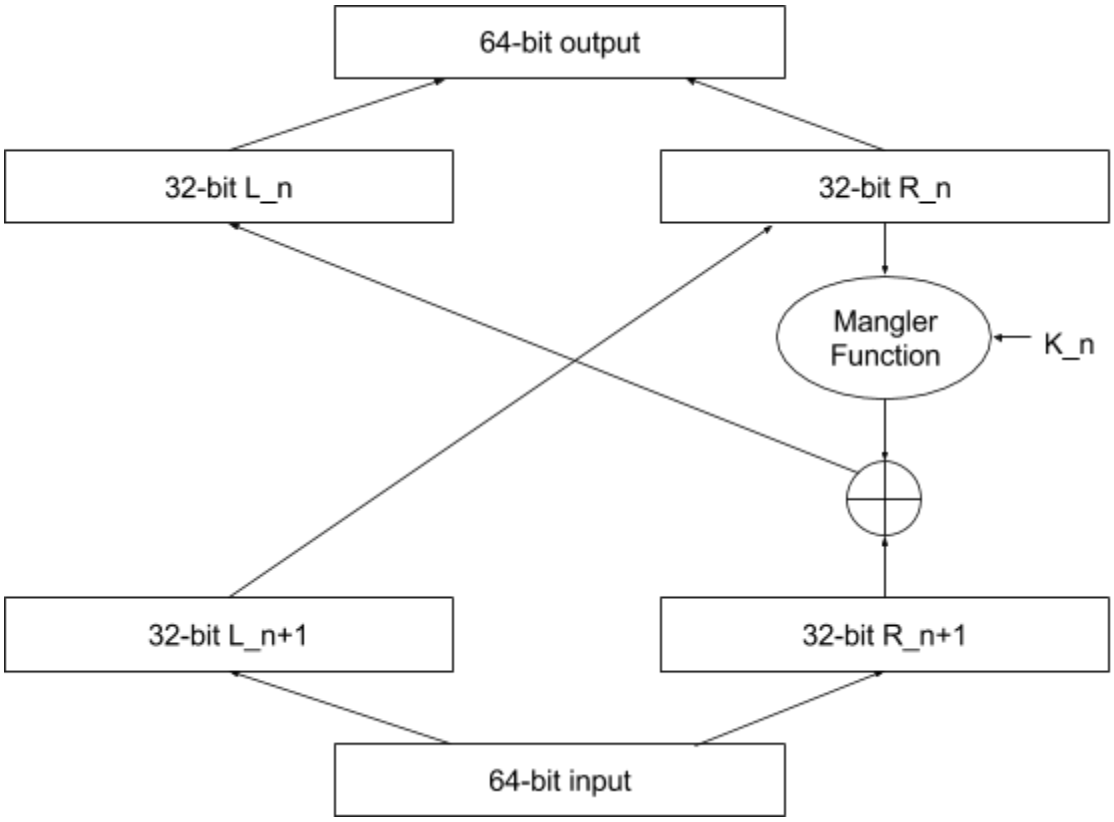
   b. 16 48 bit per-round keys

   c. Drawtheflowchartsfortheencryptionanddecryptionalgorithmsof DES. (10 Points)

      i. Encryption

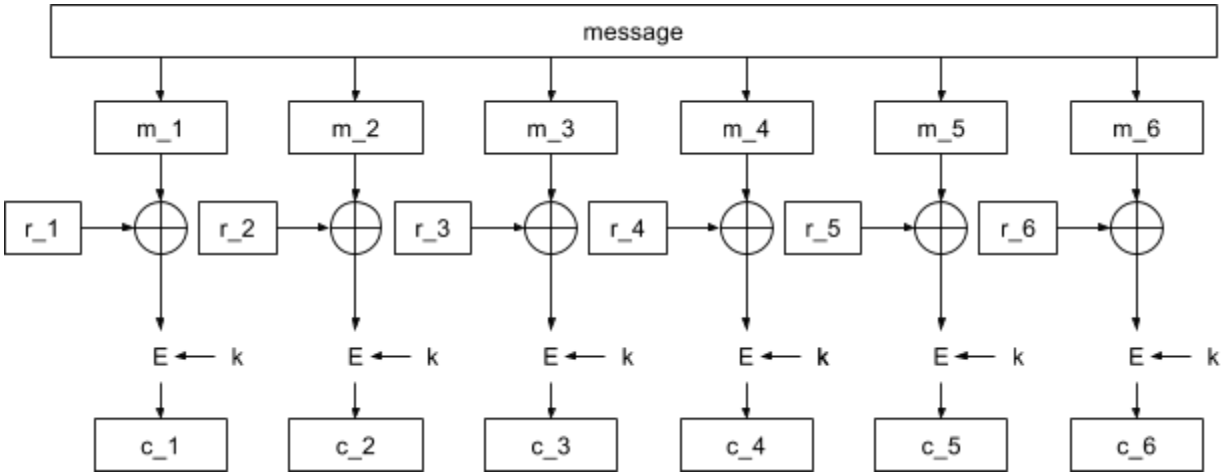


ii. Decryption



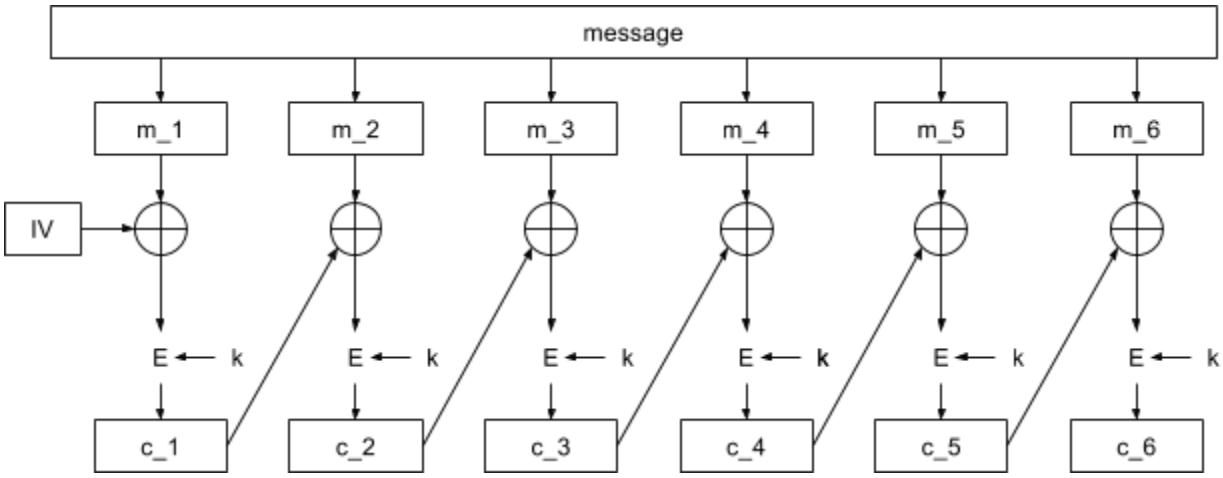
5. Consider Cipher Block Chaining (CBC).

a. Draw the diagram to show the encryption algorithm of CBC. (5 Points)



b. With ECB, you can manage partial decryption and fill in blanks. With CBC, you can't encrypt if there are missing pieces in a sequence.

c. Draw the diagram to show the decryption algorithm of CBC. (5 Points)



d. Any subsequent block will have corrupt data.

6. No, this 128 bit result is not unique.

7. Create file digest and securely store the files. Occasionally generate and compare the new digest with the old to see if the files have been tampered with.