CSC650 SECURE NETWORKED SYSTEMS

Homework 1

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

1. What are the five elements in a cryptosystem? (10 Points)

Sol:

A cryptosystem is a 5-tuple (E, D, M, K, C), where E is encryption algorithm, D is decryption algorithm, M is the set of plaintext, K is the set of keys, and C is the set of ciphertext

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

Sol:

a.

s	e	n	d	m	o	r	e	m	o	n	e	y
18	4	13	3	12	14	17	4	12	14	13	4	24
9	0	1	7	23	15	21	14	11	11	2	8	9
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	O	K	J	D	M	S	X	Z	P	M	H

b.

c	a	s	h	n	o	t	n	e	e	d	e	d
2	0	18	7	13	14	19	13	4	4	3	4	3
25	4	22	3	22	15	19	5	19	21	12	8	4
1	4	14	10	9	3	12	18	23	25	15	12	7
B	E	O	K	J	D	M	S	X	Z	P	M	H

3. Consider the brute-force attack.
    a. Assume the keys used in a cryptosystem are 10 bits long and it needs 1 second to test an individual key by using the brute-force attack. In the worst case, how much time would it take for the attacker to determine a particular key? (5 Points)
    b. If the time needed to test an individual key reduces to 0.001 second, how much time would it take now to determine a particular key by using the brute-force attack in the worst case? (5 Points)
    c. If we increase the length of the keys to 20 bits and the time needed to test an individual key is still 0.001 second. How much time would it take now to determine a particular key by using the brute-force attack in the worst case? (5 Points)
    d. What can you observe from Questions a-c? (5 Bonus Points)

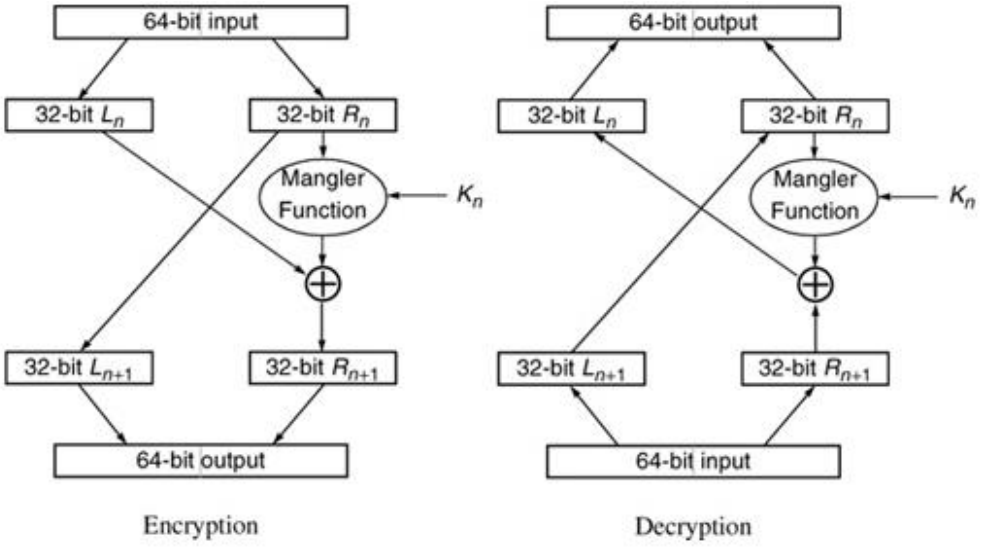
Sol:

a. $2^{10} \times 1 = 1024$ sec
b. $2^{10} \times 0.001 = 1.024$ sec
c. $2^{20} \times 0.001 = 1048.576$ sec
d. We can enhance the security of a cryptosystem in terms of resisting brute-force attack by increasing the key length

4. Consider Data Encryption Standard (DES).
    a. What is the length of a plaintext, a ciphertext, and a key in DES? (10 Points)
    b. What is the length of a per-round key? How many per-round keys are used in DES? (5 Points)
    c. Draw the flowcharts for the encryption and decryption algorithms used in each round in DES. (10 Points)

Sol:

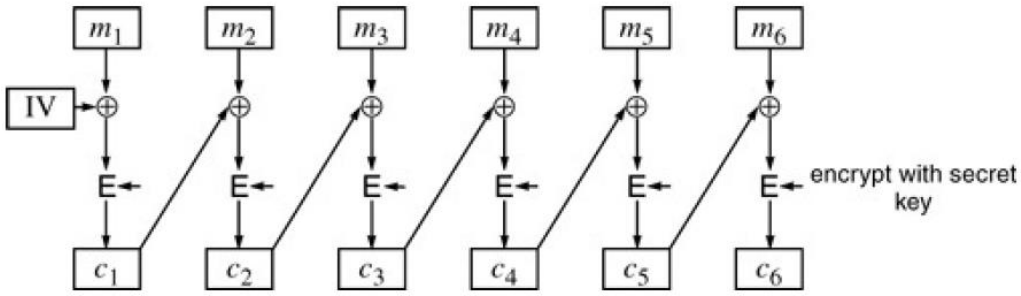
a. 64 bits; 64 bits; 64 bits
b. 48 bits; 16
c.



5. Consider Cipher Block Chaining (CBC).
   a. Draw the diagram to show the encryption algorithm of CBC. (5 Points)
   b. What is the advantage of CBC as compared with Electronic Code Book (ECB)? (5 Points)
   c. Draw the diagram to show the decryption algorithm of CBC. (5 Points)
   d. What is the effect to the decrypted plaintext blocks if a random error happens in one block of ciphertext, say the *i*th ciphertext block c_i? (5 Points)

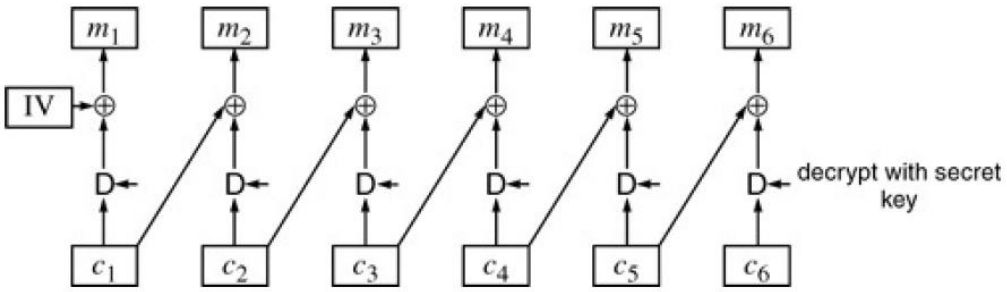
Sol:

a.



b. Identical plaintext blocks will not cause repeats in the ciphertext

c.



d. The *i*th plaintext block m_i and (*i+1*)th plaintext block m_{i+1} will be corrupted.

6. Existing hash functions are reasonably fast, but here is a much faster function: take your message, divide it into 128-bit chunks, and XOR all the chunks together to get a 128-bit result. Then, perform the standard hash function on the result. Is this a good hash function? (5 Points)

Sol:

No. It is fairly easy to generate another message with the same 128-bit result.

7. Most viruses infect your system by implanting themselves into the existing executable files on the disk. Explain how to use a hash algorithm to design a virus detector which identifies the files that may be infected by viruses (10 Points)

Sol:

A virus detector may generate the file digests by applying a hash algorithm on the files and then stores the file digests securely. Then the virus detector periodically computes the file digests and compares them with the stored version. If a virus changes the content of a file, the new digest will be different from the original digest. In this way, a virus detector can detect the modification of a file by a virus.