Hari Manivannan

915526422

CSC 650

2/16/2016

1. The 5 elements of a cryptosystem are:

Plaintext: a message in its original form

Ciphertext: the encrypted message

Key: an input to a cryptographic algorithm

Encryption Algorithm: algorithm used to make messages unreadable by all but the intended receivers. E(m, ke ) = c

Decryption Algorithm: the reverse of encryption algorithm. D(c, kd ) = m

2.

a) beokjdmsxzpmh

b) 25 4 22 3 22 15 19 5 19 21 12 8 4

3.

a) 2^10 \* 1 second = 1024 seconds

b) 2^10 \* 0.001 second = 1.024 seconds

c) 2^20 \* 0.001 second= 1048.576 seconds

d) The observation made from questions a-c is that if you increase the key length, the worst case time increases by around a 1000%

4.

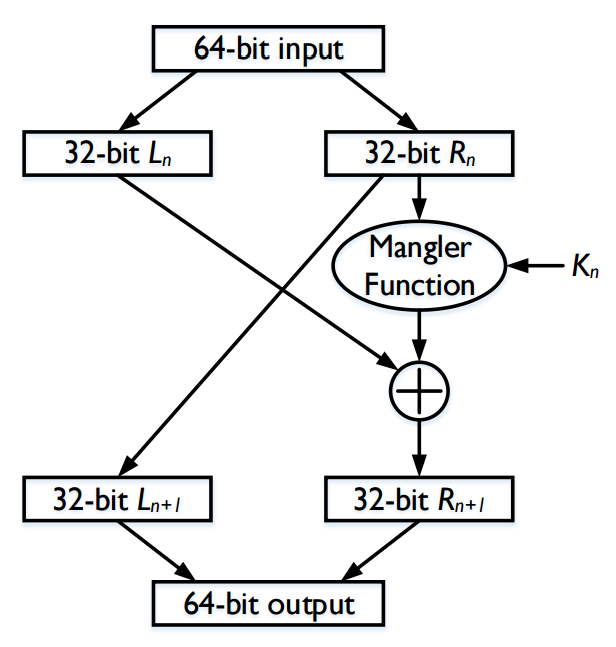
e) length of plaintext: 64 bits

length of ciphertext: 64 bits

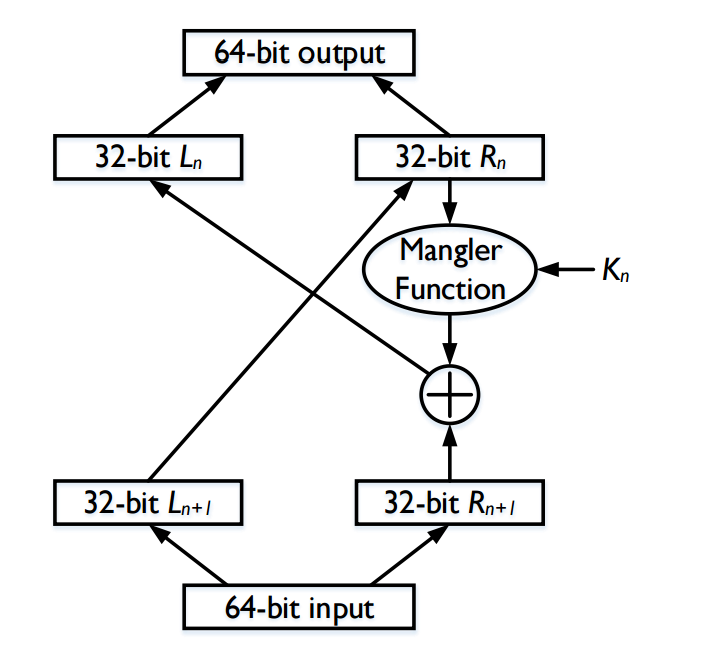
length of key: 64 bits

f) There are 16 48-bit per-round keys

g) **Encryption algorithm**

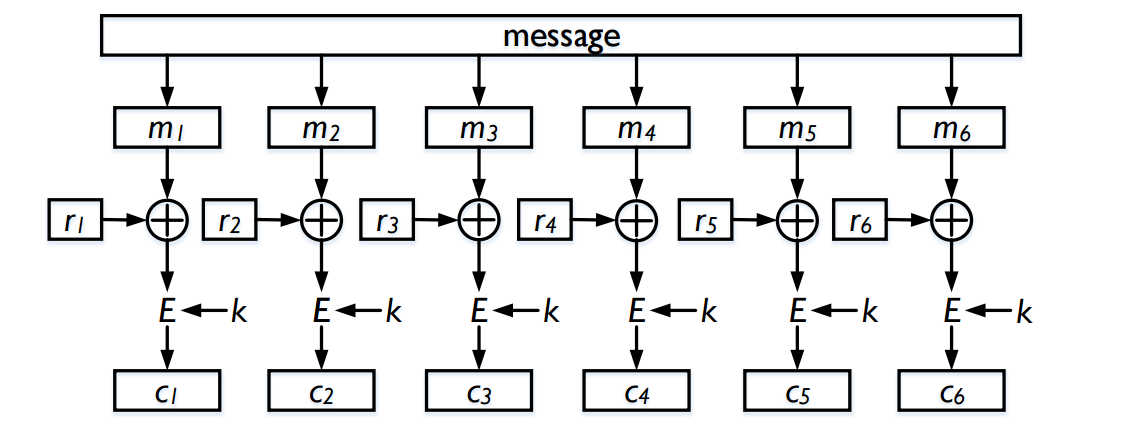


**Decryption Algorithm**



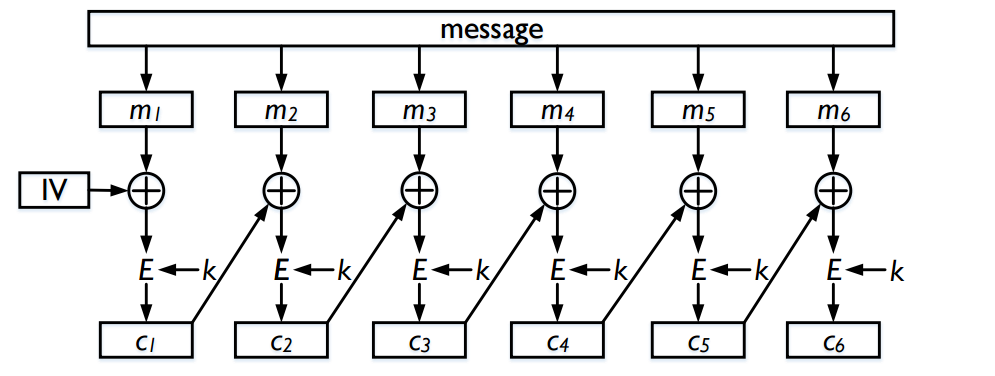
5.

a) **Encryption algorithm of CBC**



b) One of the advantages of CBC as compared with ECB is that you could manage a partial decryption and fill in the blanks. With CBC, if a few blocks are missing in the sequence, encryption becomes impossible.

c) **Decryption algorithm of CBC**



6. No, because it is very easy to generate another message with the same 128 bit

7. A virus detector may create the file digests by applying hash algorithm on the files and then stores the file digests securely. After that, the virus detector occasionally calculates the file digests and compares them with the already stored version. If the contents of file are changed by a virus, the new digest will be different from the original digest. This way a virus detector can detect the modification of a file by a virus.

8. Given hash function h(), key k, and message m MAC(k,m)= h(m|k). So without using any key k, we cannot generate MAC(k,m). This is why the problem is not solved.