School of Digital Media and Infocomm Technology

### ST2504 Applied Cryptography

1. What is the difference between a block cipher and stream cipher?

Block ciphers encrypt fixed size blocks using either DES or AES encryption, but stream cipher uses a pseudo random keystream to process message and combined (XOR) with plaintext bit-by-bit.

**Model answer:**

**Block-cipher: Encodes blocks of several (typically 64) bits at the time.**

**Stream-cipher: Encodes one bit at a time.**

2. How can one make a block cipher act as a stream cipher?

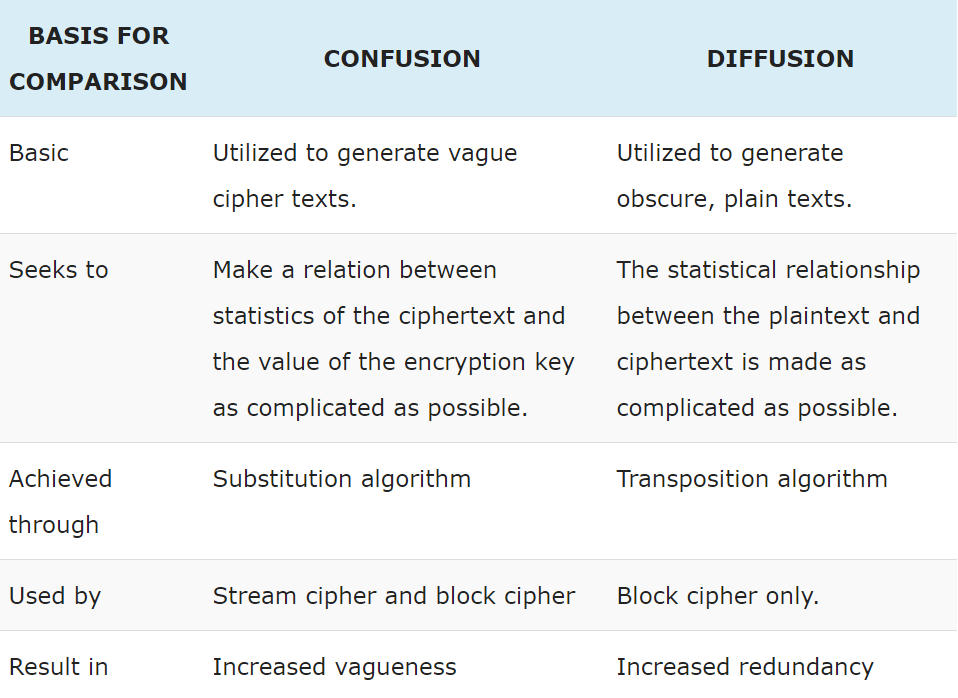
To make a block cipher act as a stream cipher, we could use Cipher Feedback mode (CFB) or Output Feedback mode (OFB). CFB adds a message stream to the output of the block cipher where each ciphertext block get ‘feedback’ into the encryption process to encrypt the next plaintext block. Whereas OFB uses unique IV to generate a sequence of output blocks that are XOR with the plaintext. Output of cipher is added to message stream then feedback to the next cycle of independent of message.

**Model answer:**

**One can convert a block cipher, DES, into a stream cipher by using the cipher feedback mode with n=1.**

3. What is the difference between confusion and diffusion?

Confusion refers to making the correlation between the key and the ciphertext as complex and intricate as possible. Whereas diffusion refers to the property that the redundancy in the statistics of the plaintext is “dissipated” in the statistics of ciphertext.



**Model answer:**

**Confusion: seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible.**

**Diffusion: the statistical structure of the plaintext is dissipated into long-range statistics of the ciphertext.**

4. What are the two general approaches to attacking a cipher?

The two general approaches are cryptanalysis and brute-force attack. As most of the DES mode of operation had a similar limitation which is they are unable to reuse the same key or the IV as this will cause a possibility of the output stream and messages to be recovered from attackers.

<https://study-for-exam.blogspot.com/2014/12/what-are-two-general-approaches-to.html>

5. What are the advantages of implementing encryption algorithms in **hardware** instead of software?

When large volumes of secure data need to be processed, high performance security can best be achieved in hardware. Only cryptographic hardware can transparently address such service, as it allows easy software porting and execution from an unsecure context to a very secure one without extra cost.

**Model answer:**

**Faster as hardware usually designed to do one specific task.**

**Energy efficient due to less CPU cycle, less power consumption.**

6. List four (4) attributes of a “good” cipher.

Size of the ciphered text should be no larger than the text of the plaintext.

The mode of operation should be as simple as possible.

Integrity and authenticity for encryption and decryption when using the cipher.

Keys and IV used in the cipher should be complex in nature but simple to use.

**Model answer:**

**Amount of secrecy needed should determine effort to encrypt and decrypt.**

**Key set and enciphering algorithm should not be complex.**

**Implementation should be as simple as possible.**

**Errors should not propagate.**

7. What are the advantages and disadvantages of the ECB and CBC modes?

The advantages of ECB are it has the simplest mode of operation, each block is encrypted independently with the same key and substituting with another value. Hence, securing transmission of single block of info that needs to be sent. Whereas the disadvantages of ECB are it can only send a few blocks of data to encrypt and the encrypted message blocks being independent.

The advantages of CBC are that the cipher blocks are linked together where each cipher blocks is chained with current plaintext block. Furthermore, it uses IV for each encryption operation to have a unique binary sequence. IV ensures security and authenticity by ensuring different ciphertext blocks will be generated. The disadvantage of CBC is the ciphertext block is dependent on all blocks before it hence any change to a block affects all following ciphertext blocks causing an avalanche effect.

**Model answer:**

**Advantage for ECB: Fast and efficient for short message**

**Disadvantage for ECB: Same input plaintext always gives the same output ciphertext. (leak information)**

**Advantage for CBC: Self synchronization (no synchronization between sender and receiver)**

**More secure than ECB mode (cannot deduce the plaintext by looking at the encrypted blocks separately)**

**Disadvantage for CBC: Parallel encryption is not possible as it need to encrypt block 1 before it can encrypt block 2.**

**Error extension: loss of one block results in loss of subsequent blocks**

8. Encryption of large blocks using DES (or any fixed size block cipher) can be achieved through the means of Electronic Code Book (ECB) mode and Cipher Block Chaining (CBC) modes. For the two modes, the encryption is depicted below. You are required to draw the decryption block diagram for each of these two modes, and also give the mathematical expression.

a) Electronic Code Book (ECB) mode



b) Cipher Block Chaining (CBC) mode



9. What are the advantages and disadvantages of the OFB and CFB modes?

**Advantages of OFB is its bit errors do not propagate where a single bit error in ciphertext will only affect one bit in a plaintext as such it makes it easy for recovery. The disadvantages of OFB is that it must never reuse the same key and IV to prevent a portion of the output stream to be recovered.**

**Advantages of CFB is each ciphertext block get ‘feedback’ into the encryption process in order to encrypt the next plaintext block. The disadvantage of CFB is it will stall during block encryption after every n-bits if cannot keep up with input data. And error propagate for several blocks when the network transmission data is noisy.**

10. Explain why the CFB mode does not have good error propagation property as compared to the OFB mode.

The reason why the OFB mode has a good error propagation property unlike the CFB mode is due to the bit errors in OFB as the bit errors do not propagate hence it will not spread thus resulting only a single bit error, allowing for easy recovery. However, for CFB the errors propagate for several blocks causing the effect of variable uncertainties.

**Model answer:**

**In CFB mode, if there is a transmission error in the ciphertext, it will not only affect the decrypted block, but also the subsequent blocks.**

**In OFB mode, only the bits with transmission error will be affected in the decrypted plaintext. Errors do not propagate.**

Optional question.

Consider a block cipher mode proposed as follows,

C0 = IV

Ci = Ek (Mi) XOR Ci-1

How can an attacker identify the plaintext message blocks that are the same, from the captured ciphertext?

**Assuming an attacker can sniff the ciphertext blocks,**

**Since Ci = Ek(Mi) XOR Ci-1**

**The attacker can perform Ci XOR Ci-1= Ek(Mi) XOR Ci-1 XOR Ci-1 = Ek(Mi), to obtain the ciphertext blocks that have been independently encrypted without chaining.**

**Ci XOR Ci-1= Ek(Mi) XOR Ci-1 XOR Ci-1 (Ci XOR Ci-1) = Ek(Mi) XOR Ci**

**If there are duplicated plaintext blocks from 2nd block onwards, the attacker can identify them from their repeated Ek(Mi) values.**