T2 Solutions

Q1. [C330-2.2: 4 Marks] Describe the working procedure of Stream and Block Ciphers. Also list at least two advantages and disadvantages of them.

2 categories on the basis of type of data encrypted

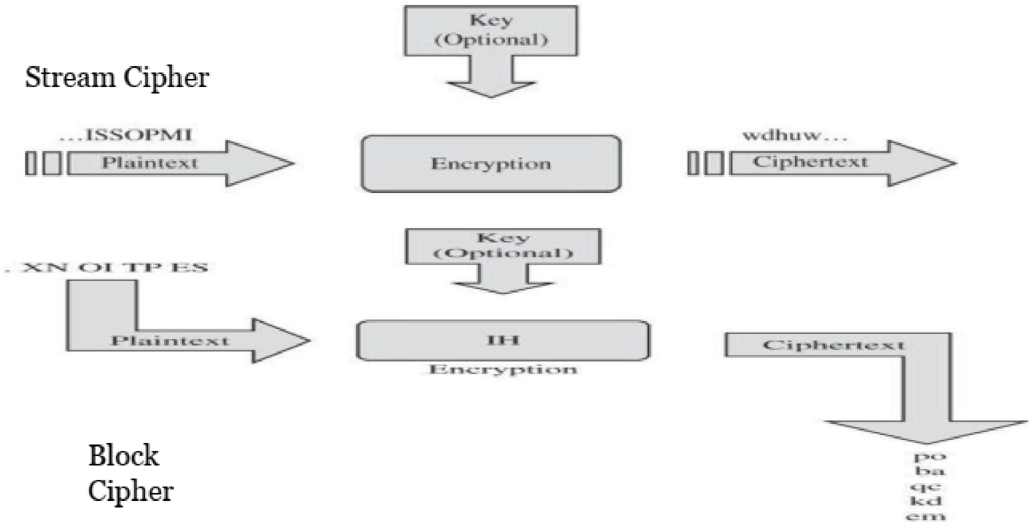
1. Block encryption
2. Stream encryption

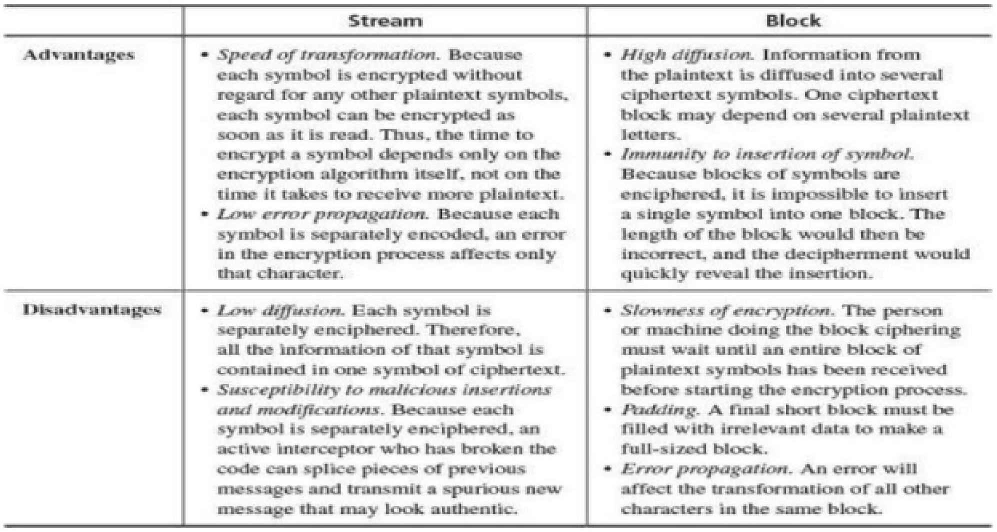
In **stream encryption**, each bit, or perhaps each byte, of the data stream is encrypted separately.

- Can be applied immediately to whatever data items are ready to transmit.
- For example, streaming video, perhaps a movie, from a satellite. The stream comes in bursts, depends on the satellite load and the speed at operation speed of the sender and receiver.

A **block cipher** encrypts a group of plaintext symbols as a single block. It works on a quantity of plaintext data all at once.

- Block ciphers work on blocks of plaintext and produce blocks of ciphertext,
- Blocks are typically 64, 128, 256 bits or more and the block size need not have any particular relationship to the size of a character.





	Stream	Block
Advantages	• *Speed of transformation.* Because each symbol is encrypted without regard for any other plaintext symbols, each symbol can be encrypted as soon as it is read. Thus, the time to encrypt a symbol depends only on the encryption algorithm itself, not on the time it takes to receive more plaintext. • *Low error propagation.* Because each symbol is separately encoded, an error in the encryption process affects only that character.	• *High diffusion.* Information from the plaintext is diffused into several ciphertext symbols. One ciphertext block may depend on several plaintext letters. • *Immunity to insertion of symbol.* Because blocks of symbols are enciphered, it is impossible to insert a single symbol into one block. The length of the block would then be incorrect, and the decipherment would quickly reveal the insertion.
Disadvantages	• *Low diffusion.* Each symbol is separately enciphered. Therefore, all the information of that symbol is contained in one symbol of ciphertext. • *Susceptibility to malicious insertions and modifications.* Because each symbol is separately enciphered, an active interceptor who has broken the code can splice pieces of previous messages and transmit a spurious new message that may look authentic.	• *Slowness of encryption.* The person or machine doing the block ciphering must wait until an entire block of plaintext symbols has been received before starting the encryption process. • *Padding.* A final short block must be filled with irrelevant data to make a full-sized block. • *Error propagation.* An error will affect the transformation of all other characters in the same block.

Q2. [C330-2.2]Discuss how the public key cryptography overcomes the limitation of symmetric key cryptography. Describe how a one-way hash function may be used for message authenticating in both asymmetric and symmetric cryptography.

[2 marks]
The advantages of public key cryptography are:

- No need to exchange the keys
- Another key cannot be derived from one key
- The confidentiality of the message can be ensured by using the public key cryptography
- It is possible to establish authentication of the sender by using public key cryptography (digital signature)
- It is possible to ensure the confidentiality and authentication of the message at the same time
- It is possible to use public key cryptography for session key exchange

Applications of PKC

Public Key Cryptography is used in a number of applications and systems software. Some examples of application of cryptography are:

- Digitally signed document
- E-mail encryption software such as PGP and MIME
- RFC 3161 authenticated timestamps
- Digital signatures in the Operating System software such as Ubuntu, Red Hat Linux packages distribution
- SSL protocol
- SSH protocol

Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) enables users to securely transact through the use of public key cryptography.

A public key infrastructure consists of:

- A Certificate Authority (CA) that issues and verifies digital certificates. A certificate includes the public key or information about public key
- A registration Authority (RA) which verifies the user's authenticity for CA before CA issues a digital certificate
- A secured storage place to hold the certificates and public keys
- A certificate management system
- Hardware, software, policies, procedures, and people used to create, manage, and revoke digital certificates along with the distribution and storage of the digital certificates

Hash based message authentication [2 marks]

In a symmetric key system, a one-way hash function is used as the fundamental component of a key dependent Hash-Based Message Authentication Code that takes as its input the whole message and outputs a message authentication code that is appended to the message. Only those with knowledge of the key may generate or check the message authentication code. In a public key system the message is input into a one way hash function the output of which is a message digest. A private key is used to encrypt the message digest to give digital signature which is attached to the message. The corresponding public key may be used to check the signature. An adversary will be unable to create a valid signature.

Q3. [C330-2.3] Calculate the timings of password guessing attacks:

a) **If password is three uppercase alphabetic characters long, how much time would it take to determine a particular password, assuming that testing an individual password requires 5 seconds?**
Ans: No of upper case letters = 3
Time to test single password = 5 secs
No. of alphabets in English= 26
So, Time taken to test a 26^3 = 5 *26^3 = 87880 secs = 24.41 hours. **[2 marks]**

b) Suggest ways to improve password so that to increase password guessing time.
Ans: Use characters other than just a-z. Choose long passwords. Avoid actual names or words. Use variants for multiple passwords. Change password regularly **[2 marks]**

Q4. [C330-2.3]In almost all systems, when a user needs to sign in there is an authentication mechanism to establish identity. Analyze the need for access controls, when we already have such authentication mechanism in every system. Elaborate using suitable use-cases.

Ans: Authentication is any process by which a system verifies the identity of a user who wishes to access the system. Because access control is typically based on the identity of the user who requests access to a resource, authentication is essential to effective security. User authentication is implemented through credentials which, at a minimum, consist of a user ID and password. Authorization is any mechanism by which a system grants or revokes the right to access some data or perform some action. Often, a user must log in to a system by using some form of authentication. Access control mechanisms determine which operations the user can or cannot do by comparing the user's identity to an access control list (ACL). **[2 marks]**

If student mentioned Use-Case only with detailed explanation **[1 mark]**

If Detailed Explanation of use case in context also written**[1 mark]**

Q5. [C330-2.3]Compare and illustrate the major points of differences between Role-based access control and Capabilities. Explain all your points using a sample scenario or a case study.

Ans: role-based access control is an approach to restricting system access to authorized users. Role-based access control is a policy-neutral access-control mechanism defined around roles and privileges. The components of RBAC such as role-permissions, user-role and role-role relationships make it simple to perform user assignments. Role-based access control lets us associate privileges with groups Role-based access control can model the separation of duty rule For example, some users (such as administrators) to have significant privileges, and we want others (such as regular users or guests) to have lower privileges. Access control keeps up with a person who changes responsibilities, and the system administrator does not have to choose the appropriate access control settings for someone

A capability is a communicable, unforgeable token of authority. It refers to a value that references an object along with an associated set of access rights. A user program on a capability-based operating system must use a capability to access an object. Capability-based security refers to the principle of designing user programs such that they directly share capabilities with each other according to the principle of least privilege

A capability can be thought of as a pair (x, r) where x is the name of an object and r is a set of privileges or rights. With each subject we can store that subject's capabilities. And, the subject presents to the guard a capability in order to get access to an object. Note that a capability is completely transferable; it doesn't matter who presents the capability. This framework completely eliminates the need for authentication.

Any other relevant point of comparison.