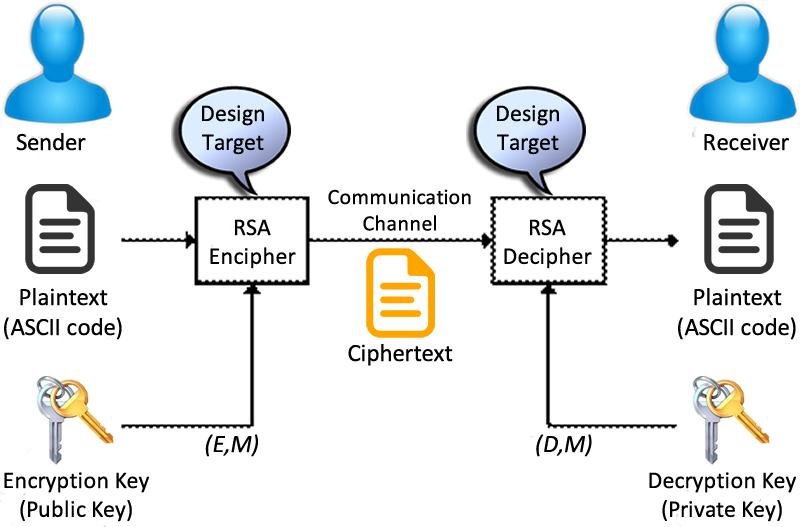
Question 1:

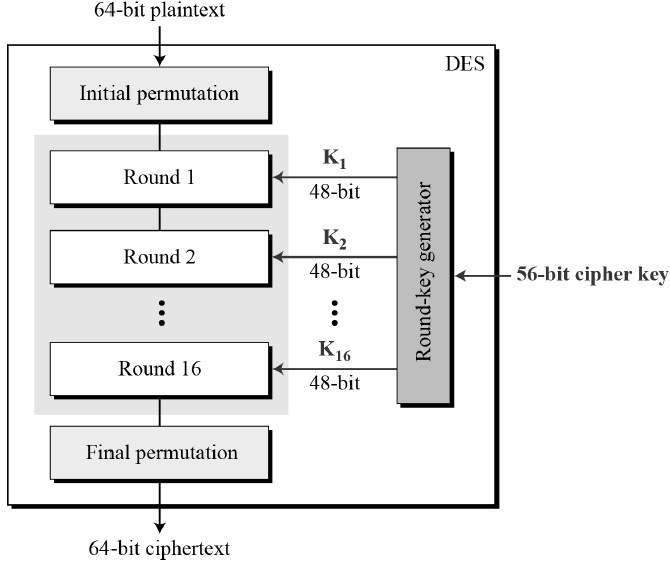
1.1Concept

Asymmetric and symmetric encryption are two fundamental techniques used in network security and cryptography.

-Symmetric encryption uses a single key for both encryption and decryption, making it faster and suitable for encrypting data at rest. Examples of symmetric encryption algorithms include AES (Advanced Encryption Standard).

-Asymmetric encryption uses a pair of keys, a public key for encryption and a private key for decryption. This method is suitable for securely exchanging keys or encrypting data for secure communication. Examples of asymmetric encryption algorithms include RSA and ECC (Elliptic Curve Cryptography).

1.2 Draw an encoding and decoding diagram:  




1.3 Compare:

-Symmetric encryption is faster and more efficient than asymmetric encryption.

-Asymmetric encryption provides better security for key exchange and secure communication.

-Symmetric encryption uses a single key for both encryption and decryption, while asymmetric encryption uses a pair of keys.

Question 2:

2.1 Security Vulnerability:

A security vulnerability is a weakness or flaw in a system, application, or network that can be exploited by attackers to compromise its security. Security vulnerabilities can lead to unauthorized access, data breaches, and other security threats.

2.2 SQL Injection and how to prevent it:

-SQL Injection (SQLi) is a type of an injection attack that makes it possible to execute malicious SQL statements. These statements control a database server behind a web application. Attackers can use SQL Injection vulnerabilities to bypass application security measures. They can go around authentication and authorization of a web page or web application and retrieve the content of the entire SQL database. They can also use SQL Injection to add, modify, and delete records in the database.

-An SQL Injection vulnerability may affect any website or web application that uses an SQL database such as MySQL, Oracle, SQL Server, or others. Criminals may use it to gain unauthorized access to your sensitive data: customer information, personal data, trade secrets, intellectual property, and more. SQL Injection attacks are one of the oldest, most prevalent, and most dangerous web application vulnerabilities

-SQL Injection is a type of security vulnerability that occurs when an attacker is able to manipulate SQL queries by injecting malicious SQL code into user inputs. To prevent SQL Injection, you can:

how to prevent SQL Injection:  
-Parameterize queries

-Validate user input data

-Conceal information in messages

-Restrict privileges

-Regularly back up data