1. **What is symmetric encryption?**

Symmetric encryption is a cryptographic method where the same key is used for both encrypting plaintext and decrypting ciphertext. This approach requires that both the sender and receiver share a secret key, ensuring that only authorized parties can access the information. While symmetric encryption is generally faster and more efficient for processing large amounts of data compared to asymmetric encryption, it necessitates secure key distribution and management.

2. **What does the AES standard include (key length, input block size, number of rounds)?**

The Advanced Encryption Standard (AES) specifies the following parameters:

- **Key Lengths:** AES supports key sizes of 128, 192, and 256 bits.
- **Input Block Size:** AES operates on fixed block sizes of 128 bits (16 bytes).
- **Number of Rounds:** The number of transformation rounds depends on the key length:
    - 10 rounds for 128-bit keys
    - 12 rounds for 192-bit keys
    - 14 rounds for 256-bit keys

Each round consists of several processing steps, including substitution, permutation, and mixing of the input data, to ensure security.

3. **Which algorithm was chosen as the AES standard?**

The Rijndael algorithm was selected as the Advanced Encryption Standard (AES) by the National Institute of Standards and Technology (NIST) in October 2000. Developed by Belgian cryptographers Joan Daemen and Vincent Rijmen, Rijndael was chosen for its combination of security, performance, efficiency, and flexibility. It officially became the AES standard in November 2001.

4. **What is the architecture of this standard?**

AES is based on a design principle known as a substitution-permutation network. It operates on a 4×4 column-major order matrix of bytes, termed the "state." The algorithm consists of a series of transformation rounds that include the following steps:

- **SubBytes:** A non-linear substitution step where each byte is replaced with another according to a lookup table (S-box).

- **ShiftRows:** A transposition step where each row of the state is shifted cyclically by a certain number of bytes.
- **MixColumns:** A mixing operation that operates on the columns of the state, combining the four bytes in each column.
- **AddRoundKey:** Each byte of the state is combined with a byte of the round key using bitwise XOR.

The number of rounds performed depends on the key length, as previously mentioned.

5. **What does a single round consist of?**

In AES, a single round (excluding the final round) comprises the following steps:

1. **SubBytes:** Each byte in the state matrix is substituted with a corresponding byte from the S-box, providing non-linearity.
2. **ShiftRows:** The rows of the state matrix are shifted cyclically to the left by a certain number of positions, ensuring diffusion.
3. **MixColumns:** Each column of the state matrix is transformed using a linear mixing operation, further enhancing diffusion.
4. **AddRoundKey:** The current state matrix is combined with a portion of the expanded key (round key) using bitwise XOR.

The final round omits the MixColumns step.

6. **Which process is faster: encryption or decryption? Why?**

In AES, encryption and decryption processes are designed to be efficient; however, encryption is generally faster, especially in hardware implementations. This is because decryption requires the inverse operations of those used in encryption, which can be more complex to implement. For instance, the MixColumns step in encryption has a straightforward inverse operation in decryption, but implementing this inverse can be computationally more intensive. Additionally, the key schedule for decryption involves reversing the order of the round keys, adding to the complexity. Therefore, while both processes are efficient, encryption tends to be faster due to the relative simplicity of its operations.

7. **What encryption modes are used in the AES standard?**

AES can operate in various modes of operation to encrypt data securely. Some of the commonly used modes include:

- **Electronic Codebook (ECB):** Each block of plaintext is encrypted independently.
- **Cipher Block Chaining (CBC):** Each block of plaintext is XORed with the previous ciphertext block before being encrypted.
- **Counter (CTR):** A counter is combined with a nonce to create a unique input for each block encryption.
- **Galois/Counter Mode (GCM):** Combines CTR mode encryption with Galois mode authentication for both confidentiality and integrity.

These modes offer different advantages and are chosen based on specific application requirements.

8. **Which modes are faster for decryption? Why?**

Modes like Counter (CTR) and Galois/Counter Mode (GCM) are generally faster for decryption because they allow for parallel processing. In CTR mode, both encryption and decryption involve the same operation: generating a keystream by encrypting counter values and then XORing it with the data. This symmetry and the ability to process multiple blocks simultaneously enhance decryption speed.

In contrast, modes like Cipher Block Chaining (CBC) require the decryption of each block to depend on the previous ciphertext block, making parallel processing challenging and potentially slowing down the decryption process.