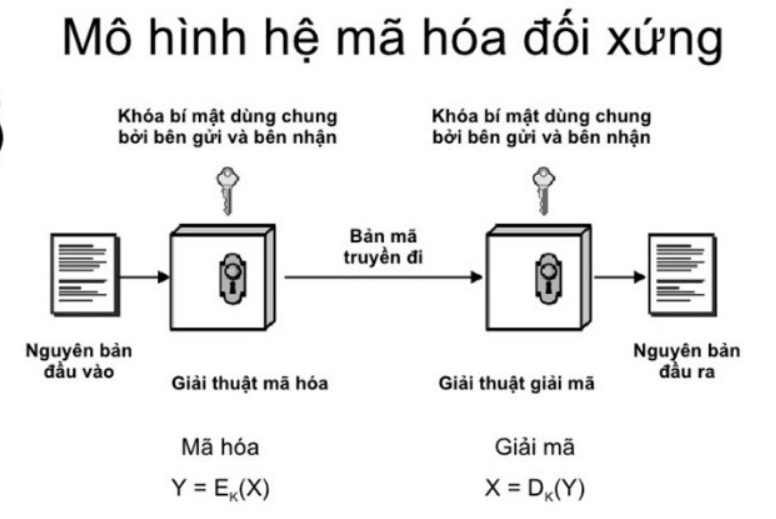
Questions1:

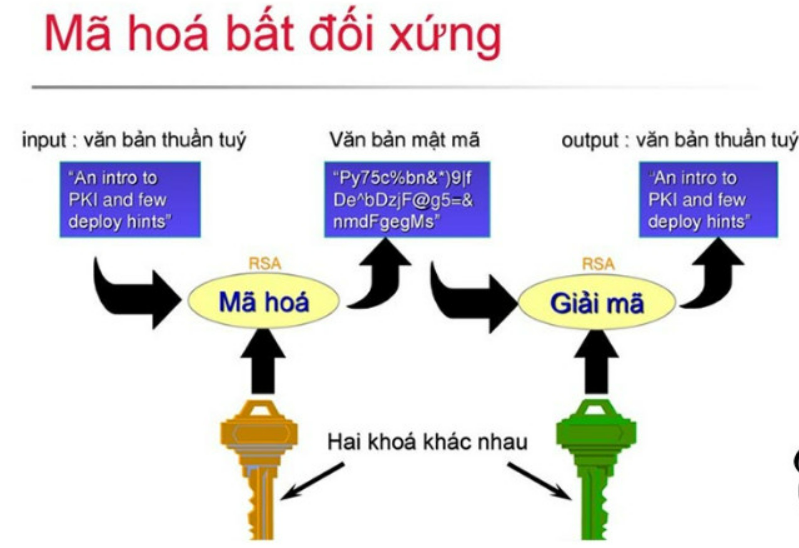
1.1

-Symmetric encryption, also known as private-key encryption, involves using the same key for both the encryption and decryption processes. In other words, the sender and the receiver share a secret key. This key is used to transform plaintext into ciphertext during encryption and then reverse the process to decrypt the ciphertext back into plaintext.

-Asymmetric encryption, also known as public-key encryption, involves the use of a pair of keys: a public key and a private key. The public key is used for encryption, and the private key is used for decryption. Unlike symmetric encryption, the public key can be freely shared, while the private key is kept secret.

1.2





1.3

\*Symmetric encryption:

– Key: Symmetric encryption uses the same key to perform both encryption and decryption. This key needs to be shared between the sender and receiver, which requires secure and efficient key management.

– Symmetry: The encryption and decryption processes both use the same key, creating symmetry in implementation. This means that if someone knows the encryption key, they also have the ability to decrypt the data.

– Speed: Symmetric encryption is often faster than asymmetric encryption because it only requires a series of simple transformations.

\* Asymmetric encryption:

– Key: Asymmetric encryption uses a pair of keys, including a public key and a private key. The public key is shared publicly and used to encrypt data, while the private key is kept secret and used to decrypt data. No need to share private keys.

– Asymmetry: The public key and private key play an asymmetric role, which means that data encrypted with the public key can only be decrypted with the private key, and vice versa.

– Security: Asymmetric encryption often ensures higher security because there is no need to share private keys. The sender only needs to know the receiver's public key to encrypt the data, and the receiver keeps the private key to decrypt.

Question 2:

1.

A security vulnerability, also known as a security flaw or security issue, is a weakness or gap in the security measures of a system, application, or network that can be exploited by malicious actors to compromise the confidentiality, integrity, or availability of data or systems. These vulnerabilities can exist at various levels of an IT environment, including software, hardware, and human processes.

Security vulnerabilities can take many forms, such as software bugs, misconfigurations, design flaws, or human errors, and they can lead to security breaches, data leaks, unauthorized access, and other security incidents. It is essential to identify and remediate vulnerabilities proactively to enhance the overall security posture.

2.