A diagram of a computer

Description automatically generated

Encoding vs Encryption vs Tokenization.   
  
Encoding, encryption, and tokenization are three distinct processes that handle data in different ways for various purposes, including data transmission, security, and compliance.   
  
In system designs, we need to select the right approach for handling sensitive information.   
   
🔹 Encoding   
Encoding converts data into a different format using a scheme that can be easily reversed. Examples include Base64 encoding, which encodes binary data into ASCII characters, making it easier to transmit data over media that are designed to deal with textual data.   
   
Encoding is not meant for securing data. The encoded data can be easily decoded using the same scheme without the need for a key.   
   
🔹 Encryption   
Encryption involves complex algorithms that use keys for transforming data. Encryption can be symmetric (using the same key for encryption and decryption) or asymmetric (using a public key for encryption and a private key for decryption).   
   
Encryption is designed to protect data confidentiality by transforming readable data (plaintext) into an unreadable format (ciphertext) using an algorithm and a secret key. Only those with the correct key can decrypt and access the original data.   
   
🔹 Tokenization   
Tokenization is the process of substituting sensitive data with non-sensitive placeholders called tokens. The mapping between the original data and the token is stored securely in a token vault. These tokens can be used in various systems and processes without exposing the original data, reducing the risk of data breaches.