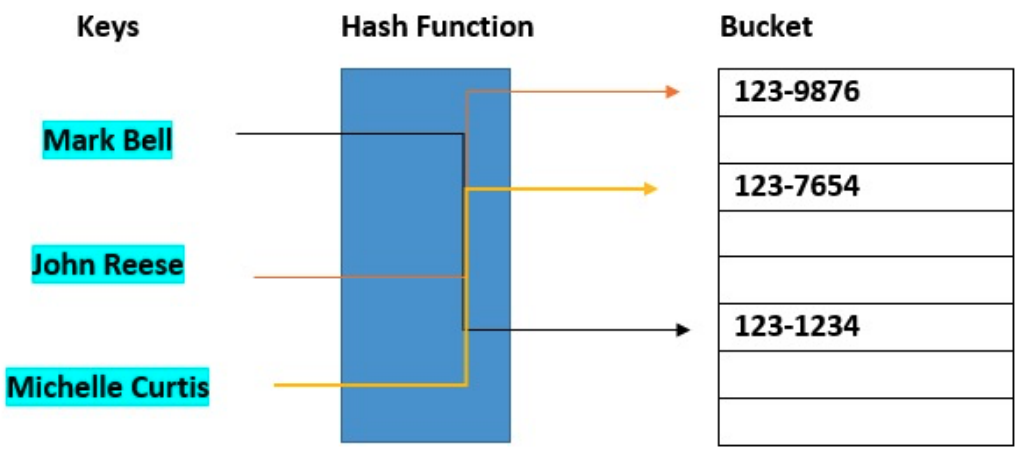
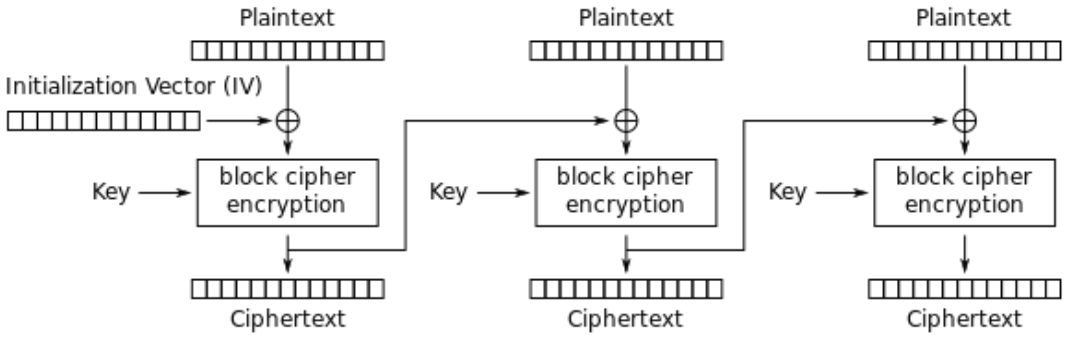
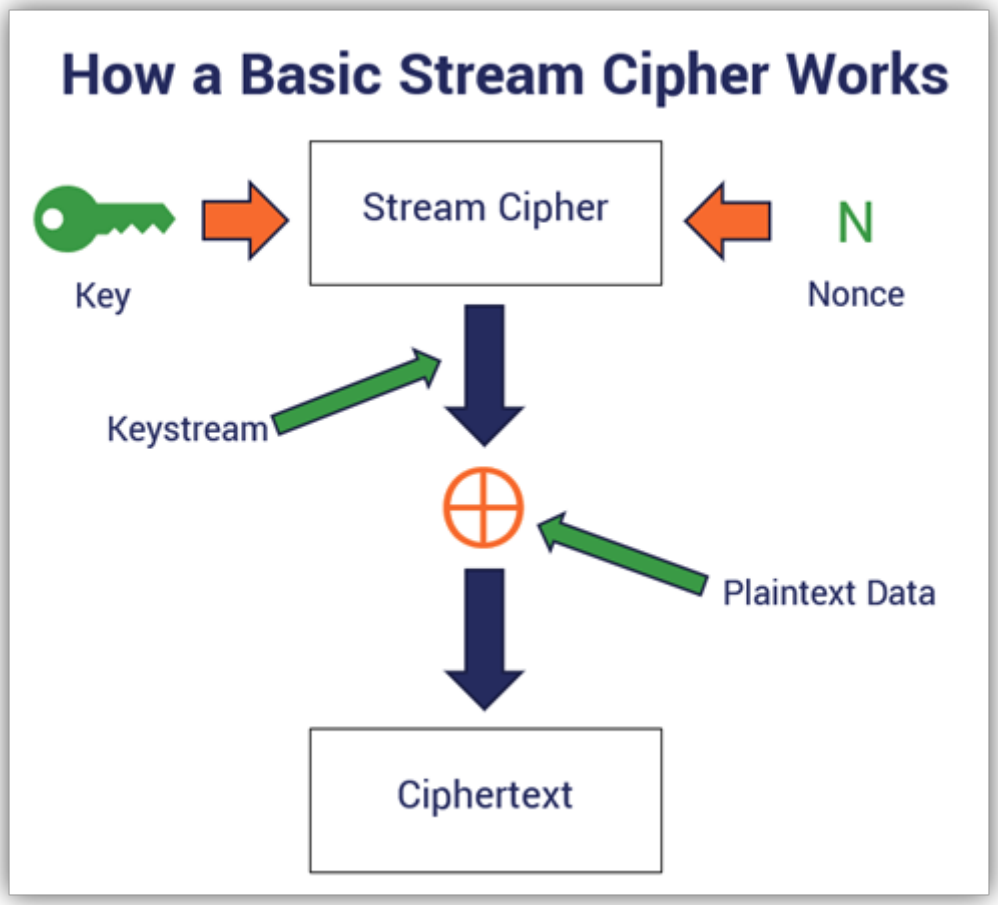
10/22

- Intro to crypto
  - hashing
    - Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string
    - one way
    - 

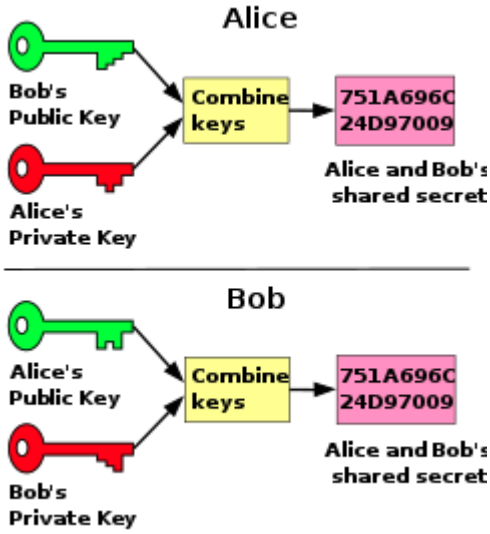
  - encoding
    - process of putting a sequence of characters (letters, numbers, punctuation, and certain symbols) into a specialized format for efficient transmission or storage
    - HTML encoding, URL encoding
  - cryptographic hash
    - MD5 (outdated)
    - Sha-256
    - Sha-1
  - symmetric crypto
    - same key encrypt and decrypt
    - block
      -



Cipher Block Chaining (CBC) mode encryption

- stream
  - 

- assymetric crypto
  - two different keys encrypt and decrypt
  - used for signing and encryption
    - Encryption uses a key to ensure the ciphertext cannot be deciphered by anyone but the authorized recipient. Signing of data works to authenticate the sender of the data and tends to implement a form of encryption in its process.
  - Encrypt and Decrypt
    - public key given out to all
    - private key kept safe

    - encrypt with your private and receipients public
    - decrypt with your private key
    - can authenticate sender based on private key used to encrypt message
    - 

- signing
    - only sign using your private key
    - anyone can use your publically available public key to validate you signed the message
    -