Cryptography Notes

Table of contents

Anish Goyal Schepens Period 1 01/25/2023

Introduction

Ciphers

- A generic way to refer to any system involving encrypting and decrypting data
- Can be monoalphabetic or polyalphabetic
- Encryption
  - The process of converting plaintext into ciphertext
- Decryption
  - The process of converting ciphertext into plaintext
- The ciphertext is unreadable to anyone who does not have the key
- Caesar Cipher
  - Shifts each letter by a certain number of places
  - A subset of a type of cipher called a substitution cipher
  - A drawback of this cipher is that the frequency of letters in the plaintext is preserved in the ciphertext
- Permutation Cipher
  - Take the letters, put them in a grid in order, and then read them off in a different order
  - As long as you know the shape of the grid and the way to read it, you can decrypt the ciphertext
  - ENIGMA (encryption technique by the Nazis) was a permutation cipher
    - Alan Turing
      - Instrumental in helping the Allies break the ENIGMA code
      - Helped create a machine to break the code
      - The machine was called the Bombe
    - Enigma rotor
      - A wheel that was used to scramble the letters within the machine using wires
    - The rotor could swap the order of the letters and rotate the rotors such that the ciphertext would have more permutations
    - Symmetric: both Enigma machines have the same starting rotor configuration

Digital Encryption

- Data Encryption Standard (DES)
  - One of the first widely used symmetric encryption algorithms

  - Used a 56-bit key
  - Developed by the NSA
  - Replaced later by the Advanced Encryption Standard (AES)
    * Increased the number of bits in the key to 128
    * Chops the number of bits in the key into blocks
    * Rounds are performed on each block
    * Used everywhere, from encrypting files to SSL
  - Deprecated because modern computers are fast enough to break the algorithm

- Secure Socket Layer (SSL)
  - A protocol that provides security for web browsers and web servers
  - Uses the Advanced Encryption Standard
  - Uses a public key infrastructure (PKI)
    * A system that uses a certificate authority (CA) to verify the identity of a user
    * The CA is a trusted third party
    * The CA signs the certificate of the user
    * The user can then use the certificate to prove their identity
    * The CA can revoke the certificate if the user is no longer trusted
  - Preceded by Transport Layer Security (TLS)
    * TLS is the successor to SSL
    * TLS is more secure than SSL
    * TLS is more widely used than SSL

- Symmetric encryption
  - The same key is used to encrypt and decrypt

- Asymmetric encryption
  - Two different keys are used to encrypt and decrypt
  - The public key is used to encrypt and the private key is used to decrypt

- Substitution cipher
  - A cipher that replaces each letter with another letter
  - Can be randomized or deterministic

- Key exchange
  - The process of exchanging keys between two parties
  - One way functions are used to generate keys, and they can only be used by the client but not the server
  - Diffie-Hellman key exchange
    * A method of exchanging keys between two parties
    * The two parties agree on a prime number and a base

    * The two parties then generate a random number
    * The two parties then calculate the public key
    * The two parties then calculate the shared secret
    * The shared secret is the same for both parties
    * The shared secret is used as the key for encryption
    * Uses modular exponentiation
        - $a^x \mod n$
        - a is the base
        - x is the exponent
        - n is the modulo, which is a prime number agreed on the client and server
        - Hard to calculate the exponent from the base, modulo, and the result given numbers containing more than 100 digits
- Hashing
    * Encryption using a one-way function that is not reversible
    * Used for password checking; if the hash value of the string you passes matches the hash value of the string in the database, then you are allowed to log in
    * The hash function is deterministic