Ethics Report

Name: Salma Wagdy Abdulmoniem Abdelaal

ID:20210418

Cryptography

Introduction:

Cryptography is the science of protecting information by transforming it into a secure format that can only be read by authorized individuals or systems. In an increasingly digital world, where sensitive data is exchanged globally, cryptography ensures privacy, confidentiality, integrity, and authenticity. Whether it's securing online transactions, protecting personal messages, or safeguarding governmental secrets, cryptography plays an essential role in defending against cyber threats. This report explores the different types of cryptographic techniques and their applications in modern society.

Types of Cryptography:

2.1 Symmetric-Key Cryptography:

- **Definition**: Symmetric-key cryptography involves using the same key for both encryption and decryption.
- **Working Principle**: The sender and receiver share a secret key. The sender encrypts the data using the key, and the receiver decrypts it using the same key.

- **Examples**:
  - AES (Advanced Encryption Standard): Widely used in securing data and communication.
  - DES (Data Encryption Standard): An older encryption standard, largely replaced by AES due to vulnerabilities.

2.2 Asymmetric-Key Cryptography (Public-Key Cryptography):

- **Definition**: In asymmetric-key cryptography, two keys are used: a public key and a private key. The public key is used for encryption, and the private key is used for decryption.
- **Working Principle**: The sender encrypts the data using the recipient's public key. Only the recipient, with their private key, can decrypt the message.

- **Examples**:
  - **RSA (Rivest–Shamir–Adleman)**: One of the most common public-key cryptographic systems.
  - **ECC (Elliptic Curve Cryptography)**: A more efficient alternative to RSA with shorter key sizes.

2.3 Hash Functions

- **Definition**: A hash function takes an input and returns a fixed-size string, typically a "digest" or "hash value," that uniquely represents the input data.
- **Working Principle**: Hash functions are used to ensure data integrity by producing a unique hash value. Any modification to the input will result in a different hash.
- **Examples**:
  - **SHA (Secure Hash Algorithm)**: SHA-256 is commonly used in blockchain and certificate generation.
  - **MD5 (Message Digest Algorithm 5)**: Once widely used but now considered weak due to vulnerabilities.

2.4 Digital Signatures

- **Definition**: A digital signature is a mathematical scheme for verifying the authenticity and integrity of digital messages or documents.
- **Working Principle**: Digital signatures use asymmetric cryptography to generate a unique signature for a message. The sender signs the message with their private key, and the recipient can verify it using the sender's public key.
- **Examples**:
  - **RSA-based Digital Signatures**: Commonly used for email encryption and software distribution.

2.5 Cryptographic Protocols:

- **Definition**: Cryptographic protocols define the rules and methods for securely exchanging information over networks.
- **Examples**:
  - **TLS (Transport Layer Security)**: Used to secure communication over the internet (e.g., HTTPS).
  - **IPsec (Internet Protocol Security)**: Secures network communications at the IP level.

Conclusion:

Cryptography is a fundamental technology that protects information in an era of growing digital threats. From encrypting emails and securing financial transactions to ensuring privacy in cloud computing, cryptographic techniques are central to digital security. By understanding the different types of cryptography—symmetric-key, asymmetric-key, hash functions, digital signatures, and cryptographic protocols—we can appreciate their roles in ensuring confidentiality, integrity, and authenticity. As technology advances, so will the sophistication of cryptographic methods, making it an ongoing field of research and development in the fight against cybercrime.

Resources:

1. **Books**:
   - "Cryptography and Network Security" by William Stallings
   - "Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier
2. **Websites**:
   - Cryptography - Wikipedia
   - Khan Academy: Cryptography