# Self Assignment

2024

## 1 Introduction to Cryptography and Algorithms

Cryptography is the study of techniques for secure communication in the presence of third parties. The primary goal of cryptography is to ensure confidentiality, integrity, authenticity, and non-repudiation of data.

Algorithms, on the other hand, are step-by-step procedures or formulas for solving problems. In the context of cryptography, algorithms are used to encrypt and decrypt data, generate cryptographic keys, and more.

In this lecture, we will cover fundamental cryptographic algorithms, their applications in modern computer science, and basic examples to help you get started.

## 2 Basic Concepts of Cryptography

### 2.1 Symmetric Key Cryptography

Symmetric key cryptography is a type of cryptography where the same key is used for both encryption and decryption. Common examples include:

- **AES (Advanced Encryption Standard)**: A widely used encryption algorithm.
- **DES (Data Encryption Standard)**: An older, but still historically significant encryption algorithm.

#### 2.1.1 Example of Symmetric Key Encryption

Assume Alice wants to send a message "HELLO" to Bob securely. Both Alice and Bob share a secret key, say $K = 3$. Using a simple Caesar Cipher, they can encrypt the message by shifting each letter by 3 positions.

$$\begin{aligned} \text{Original Message}: &\quad H\ E\ L\ L\ O \\ \text{Encrypted Message}: &\quad K\ H\ O\ O\ R \end{aligned}$$

Bob, knowing the key $K = 3$, can decrypt the message by shifting back by 3 positions.

## 2.2 Public Key Cryptography

Public key cryptography involves the use of two keys: a public key for encryption and a private key for decryption. The most common example is:

- **RSA Algorithm**: Named after its inventors Rivest, Shamir, and Adleman.

### 2.2.1 RSA Example

In RSA, the security comes from the difficulty of factoring large prime numbers. Here's a simplified version of the steps involved:

1. Choose two prime numbers $p = 3$ and $q = 11$. 2. Compute $n = p \times q = 33$. 3. Compute $\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$. 4. Choose $e = 3$, such that $1 < e < \phi(n)$ and $gcd(e, \phi(n)) = 1$. 5. Compute $d$ such that $e \times d \equiv 1 \pmod{\phi(n)}$. In this case, $d = 7$.

Thus, the public key is $(e, n) = (3, 33)$ and the private key is $d = 7$.

Now, let's encrypt the message $m = 2$:

$$c = m^e \mod n = 2^3 \mod 33 = 8$$

To decrypt:

$$m = c^d \mod n = 8^7 \mod 33 = 2$$

# 3 Algorithms in Cryptography

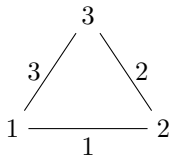
Algorithms play a crucial role in cryptography. Here are some of the most important algorithms used:

## 3.1 Kruskal's Algorithm (for Minimum Spanning Tree)

Kruskal's algorithm is used to find the minimum spanning tree (MST) of a connected graph, ensuring that all vertices are connected with the minimum possible total edge weight. The algorithm sorts all the edges in increasing order of their weight and adds edges one by one to the growing spanning tree, ensuring no cycles are formed.

- **Step 1**: Sort all edges in increasing order of their weight.
- **Step 2**: Pick the smallest edge. Check if it forms a cycle with the spanning tree formed so far. If no cycle is formed, include this edge.
- **Step 3**: Repeat Step 2 until there are $V - 1$ edges in the spanning tree.

**Example:** Consider the graph:




The minimum spanning tree would include edges with weights 1 and 2.

### 3.2 Prim's Algorithm (for Minimum Spanning Tree)

Prim's algorithm also finds a minimum spanning tree but starts from a single vertex and expands the tree one edge at a time.

#### 3.2.1 Steps in Prim's Algorithm

- **Step 1**: Start with any node.
- **Step 2**: Add the smallest edge that connects the tree to a new vertex.
- **Step 3**: Repeat until all vertices are included.

## 4 Applications in Modern Cryptography

### 4.1 Digital Signatures

A digital signature ensures that the data is authentic and has not been altered. This is critical for verifying the integrity of communications. Digital signatures rely on cryptographic algorithms like RSA.

### 4.2 Blockchains and Cryptography

Blockchain technology, widely known due to cryptocurrencies like Bitcoin, uses cryptographic hashing and public key cryptography to secure transactions. Each block in a blockchain contains a cryptographic hash of the previous block, ensuring that data cannot be altered without detection.

## 5 Conclusion

Cryptography is essential in modern computing, providing security for communications, financial transactions, and much more. Understanding how algorithms like RSA, Kruskal's, and Prim's work is a crucial part of computer science, especially when applying cryptography to secure data.