[CS309] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Autumn 2024-2025
Scribed by: Tanuj Saini (202251141) — Lecture (Week 3)

Extended Euclidean Algorithm

The Extended Euclidean Algorithm (Extended GCD) is an extension of the Euclidean algorithm that not only computes the greatest common divisor (GCD) of two integers a and b, but also finds integers x and y such that:

$$\gcd(a, b) = ax + by$$

These integers x and y, called Bézout coefficients, express the GCD as a linear combination of a and b.

Algorithm Steps

1. Use the Euclidean algorithm to compute the GCD of a and b.
2. Backtrack through the steps to express the GCD as a linear combination of a and b.

Pseudocode

```
function extended_gcd(a, b):
    if b == 0:
        return (a, 1, 0)
    else:
        gcd, x1, y1 = extended_gcd(b, a % b)
        x = y1
        y = x1 - (a // b) * y1
        return (gcd, x, y)
```

Application in Cryptography: Affine Cipher

The Affine Cipher is a type of monoalphabetic substitution cipher, where each letter in the alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and then converted back to a letter.

Encryption Function

The encryption function for a letter x is:

$$E(x) = (ax + b) \mod m$$

Where:

- m is the size of the alphabet (for English, $m = 26$).
- a and b are the keys of the cipher, with a being coprime with m (i.e., $\gcd(a, m) = 1$).

Decryption Function

The decryption function is:

$$D(y) = a^{-1} \cdot (y - b) \mod m$$

Where a^{-1} is the modular multiplicative inverse of a modulo m.

Role of Extended GCD

The Extended GCD algorithm is used to compute the modular multiplicative inverse a^{-1}. Specifically, it finds x such that:

$$ax \equiv 1 \pmod{m}$$

This x is the value of a^{-1}, which is necessary for the decryption process.

Playfair Cipher

The Playfair Cipher is a manual symmetric encryption technique and was the first digraph substitution cipher. Introduced by Charles Wheatstone in 1854 but popularized by Lord Playfair, it encrypts pairs of letters (digraphs) instead of single letters, making it significantly harder to break using frequency analysis compared to simple substitution ciphers.

How the Playfair Cipher Works

The Playfair cipher involves the following steps:

1. Key Matrix Creation
2. Preparation of the Plaintext
3. Encryption Process
4. Decryption Process

Let's delve into each step in detail.

1. Key Matrix Creation

The Playfair cipher uses a 5x5 matrix containing a keyword or phrase. Since the English alphabet has 26 letters, typically 'J' is merged with 'I', reducing the alphabet to 25 letters.

Example Key Matrix

$$\begin{array}{ccccc} P & L & A & Y & F \\ I & R & E & X & M \\ B & C & D & G & H \\ K & N & O & Q & S \\ T & U & V & W & Z \end{array}$$

2. Preparation of the Plaintext

The plaintext is prepared by:

1. Removing non-letter characters.
2. Converting the text to uppercase.
3. Replacing ‘J’ with ‘I’.
4. Splitting the text into digraphs (pairs of letters).
5. Handling duplicate letters by inserting an ‘X’.
6. Ensuring the number of letters is even by adding an ‘X’ at the end if needed.

Example Plaintext: HELLO WORLD
Prepared Digraphs: HE LX LO WO RL DX

Iterated Block Cipher

Iterated block ciphers operate on blocks of data in sequential rounds. Each round applies a round function and uses round keys derived from the master key.

Example: Data Encryption Standard (DES)

- Designed by IBM.
- Secret Key: 64-bit (56 bits used for encryption, 8 parity bits).
- Block size: 64-bit plaintext.

Encryption: DES(K, P) = C
Decryption: DES^{-1}(K, C) = P