[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy
Scribed by: Khushi Saxena (202151078)

Winter 2023-2024
Lecture (Weak 1)

Introduction

Cryptography is the science and practice of secure communication. It involves the use of mathematical techniques and algorithms to encrypt and decrypt information, ensuring confidentiality, integrity, and authenticity.

- **Cryptography**
  In cryptography, we formulate algorithms to enhance security.
- **Cryptanalysis**
  This is the part, where we endeavor to test the robustness of the designed algorithm by attempting to uncover potential security vulnerabilities.

Cryptology = Cryptography + Cryptoanalysis

The National Institute of Standards and Technology (NIST) is responsible for establishing standards for cryptographic algorithms and conducting thorough evaluations of both their design and implementation.

- **For Example:**
  ATM1 $\rightarrow$ pin1 + x = y1
  ATM2 $\rightarrow$ pin2 + x = y2

In this scenario, 'x' serves as the secret element. By inscribing 'y1' on our ATM card, we can easily retrieve the actual pin by subtracting 'x' when needed.

- **Encryption:** Converting readable text into unreadable text
  $E(P, K) = C$
- **Decryption:** Converting unreadable text into meaningful, readable text
  $D(C, K) = P$

In the above example, *pin1* is the plain text, x is the secret key, and *y1* is the cipher text. The encryption and decryption functions are always public; the only hidden element is the secret key.

Types of Cryptography

Cryptography can be broadly categorized into two main types:

- **Symmetric Key Cryptography:** Utilizing a single secret key for both encryption and decryption operations.
- **Public Key Cryptography:** Employing two distinct keys, one for encryption (public key) and another for decryption (secret key). While these keys are related, they are distinct from each other.

Security Services

1. **Confidentiality:** Securing information from unwanted and unauthorized individuals.Confidentiality can be achieved by encryption and decryption.
2. **Integrity:** Guaranteeing that the information remains unchanged, and in the event of any modification, appropriate notification is given, permitting only specified and authorized alterations.
3. **Authentication:** Confirming that the information originates from the intended source.
4. **Non-repudiation:** Creating a system to demonstrate that the sender has genuinely dispatched a specific message, with the ability to uniquely trace the actions.

- **Plain Text:** Original message.
- **Encryption Algorithm:** A function.
- **Cipher Text:** Unreadable form of plain text.
- **Decryption Algorithm:** A function.

Encryption function $(M, \text{Encryption key}) = \text{Cipher text}$
$(P \times \text{Encryption key} \to C)$
Decryption function $(C, \text{Decryption key}) = \text{Plain text}$
$(C \times \text{Decryption key} \to P)$

Definitions

- **Function:** $f : A \to B$ is a relation between the elements of A and B such that if $a, b \in A$ and $a = b$, then the corresponding function values $f(a) = f(b)$.
- **One-to-One Function:** If $f(a) = f(b)$, then it implies that a must be equal to b.
  $f(a) = f(b) \Rightarrow a = b$
- **Onto Function:** For a function $f : A \to B$, it holds true that for every element b in set B, there exists an element a in set such that $f(a) = b$
- **Bijective Function:** $f : A \to B$ is considered bijective if and only if it is both one-to-one and onto.
- **Permutation:** Let π be a permutation on a set S, then $\pi : S \to S$ is a bijection from S to S
- **One-way Function:** $f : x \to y$ is one-way if it is easy to compute $f(x)$ (in polynomial time) but difficult to find x if $f(x)$ is given. For instance, the ease of finding the product of two prime numbers contrasts with the difficulty of factorizing the product back into its prime components.
- **Substitution Box:** A substitution box is a cryptographic component that performs substitution of elements, typically bits or bytes, to enhance the security of a cryptographic algorithm.
  $S : A \to B$, $|B| \leq |A|$

Classical Ciphering Techniques

Caesar Cipher

The Caesar Cipher, named after Julius Caesar, involves shifting the letters of a message by a predetermined number.
Agreed number = 3(for Caesar Cipher)
E(x,3) = (x+3)
D(c,3) = (c+26-3)

Encryption: $E(x, 3) = (x + 3) \mod 26$
Decryption: $D(c, 3) = (c + 26 - 3) \mod 26$

Example:

- Plain text: INTERNET
- Key: 3
- Encryption: Cipher text $\rightarrow$ LQWHUQHW
- Decryption: Plain text $\rightarrow$ INTERNET

Transposition Cipher

This encryption method alters the sequence of alphabets in the plaintext to generate the ciphertext.
M = m1m2m3m4....mt
Now we do a permutation on t elements.

Encryption: $C = m_{e(1)}m_{e(2)}m_{e(3)} \dots m_{e(t)}$
Decryption: $M = c_{e^{-1}(1)}c_{e^{-1}(2)}c_{e^{-1}(3)} \dots c_{e^{-1}(t)}$

Example:

- Plain Text: CAESAR
- Secret Key (e): 641352
- Cipher Text: RSCEAA

The secret key implies that the character at the e_i position in the plaintext should be shifted to the i-th position to produce the ciphertext.

- Cipher Text: RSCEAA
- Secret Key (e^{-1}): 641352
- Plain Text: CAESAR

It is a symmetric cryptographic technique.

Substitution Cipher

This technique produces ciphertext by replacing the letters of plaintext with alternative alphabets or symbols.

Encryption:

$$C = e_{(m_1)} \cdot e_{(m_2)} \cdot \ldots \cdot e_{(m_t)}$$

where e is the secret key.

Affine Cipher

An extended form of the shift cipher (substitution cipher), the affine cipher utilizes an encryption key represented by an ordered pair of integers from a specified set. $\{0, \ldots, n-1\}$ where n is the size of the character set being used(Here it is the alphabets so range is from 0 to 25).
The secret key for affine cipher is :

$$k = (a, b) belongsto Z_{26} \cdot Z_{26}$$

Encryption: $e(x, k) = (ax + b) \mod 26$

Decryption: $d(c, k) = ((c - b) \cdot a^{-1}) \mod 26$
Here, (a^1) is multiplicative inverse of a modulo m. We will be able to decrypt a message only if we are able to find (a^1).

Multiplicative Inverse:
The multiplicative inverse of an integer x under modulo m is an integer x^{-1} such that:

$$x \cdot x^{-1} \equiv 1 \pmod{m}$$

The multiplicative inverse of x under modulo m exists if and only if $\gcd(x, m) = 1$. Let y be the multiplicative inverse of x modulo m. Hence,

$$x \cdot y \equiv 1 \pmod{m}$$

$$\Rightarrow m \mid (x \cdot y - 1)$$

$$\Rightarrow \exists\, t \in \mathbb{Z} \text{ such that } (x \cdot y - 1) = t \cdot m$$

$$\Rightarrow 1 = t \cdot m + x \cdot y$$

The Bézout's Identity states that there always exist integers a and b such that:

$$\gcd(x, y) = a \cdot x + b \cdot y$$

The integers a and b can be found using the Extended Euclidean Algorithm. Equation 1 can be written as:

$$\gcd(x, m) = 1 = t \cdot m + x \cdot y$$

Therefore, t and y are the integers that can be found using the Extended Euclidean Algorithm, of which y will be the multiplicative inverse of x under modulo m.

Playfair Cipher

It is a method of encryption that involves encrypting pairs of letters instead of individual letters.

Encryption: We create a matrix with dimensions 5×5. Each of the 25 letters must be distinct, and typically, one letter (often J) is excluded to limit the set to 25 alphabets instead of 26. If the plaintext includes J, it is substituted with I. Let's explore how to construct this key table using the secret key.

In the key table, the initial characters (left to right) form the phrase, removing any duplicate letters. The remaining table entries are then filled with the remaining letters of the alphabet in their natural order. If the number of letters is odd, an X is appended to the last letter.

Now, let's create the key table for the provided example.

Example: Secret Key : PLAYFAIR EXAMPLE

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

- If both letters reside in the same column, select the letter below each one, wrapping around to the top if at the bottom.
- If both letters are positioned in the same row, choose the letter to the right of each one, looping back to the left if they are at the farthest right.
- If neither of the previous two rules applies, create a rectangle with the two letters and select the letters at the horizontal opposite corners of the rectangle.

Plain text: HIDE $\Rightarrow HIDE$

Cipher text: BM OD $\Rightarrow BMOD$

Plain text: SACHIN $\Rightarrow SACHIN$

Cipher text: OF DB RK $\Rightarrow OFDBRK$