[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024
Scribed by: Manas Jitendrakumar Ingle (202151086) — Lecture 1,2 (Weak 1)

Introduction to Cryptography

Cryptography: The part where we develop algorithms for security designing and analysis of such algorithms.

Cryptanalysis: The part where we break the algorithm to get security designing and analysis of such algorithms.

Cryptology: The part where we develop and break the algorithm to get security designing and analysis of such algorithms.

Cryptology = Cryptography + Cryptanalysis

NIST Standards

NIST, the National Institute of Standards and Technology, plays a crucial role in standardizing cryptographic algorithms. NIST has published several standards and guidelines for cryptographic algorithms, key management, and security protocols.

Example

Consider the following examples to grasp the basics of cryptography:

- For Example:
  ATM 1: $\text{PIN}_1 + X = Y_1$
  ATM 2: $\text{PIN}_2 + X = Y_2$
  ATM 3: $\text{PIN}_3 + X = Y_3$
- Plain Text (PIN): The original message or data that needs to be protected.
- Secret Key (X): A piece of information used in encryption and decryption algorithms. It is known only to the sender and the intended recipient.
- Cipher Text (Y): The encrypted form of the plain text, obtained by applying encryption algorithms using the secret key.
- E(P, K) = C
  In this formula, E signifies the encryption function, P represents the plaintext, K is the secret key,and C is the resulting ciphertext.
- D(C, K) = P
  Here, D represents the decryption function, C is the ciphertext, K is the secret key, and P is the decrypted plaintext.

Symmetric Key Cryptography

Symmetric key cryptography, also known as secret key cryptography, employs a single key for both encryption and decryption. The same secret key is used by both communicating parties, making it crucial to keep the key secure.

- Encryption: $Y = E(X, \text{PIN})$
- Decryption: $\text{PIN} = D(X, Y)$

Public Key Cryptography

Public key cryptography is a type of encryption that uses a pair of keys: a public key and a secret key. The public key is used to encrypt data, and the secret key is used to decrypt data.

- Encryption: $Y = E(X, \text{PK})$
- Decryption: $\text{PIN} = D(X, \text{SK})$
- PK is the public key and SK is the secret key.

My Inferences

One of the significant advantages of public key cryptography is that there is no need for the secure distribution of keys. Users can freely share their public keys without compromising the security of the system. The use of two keys in public key cryptography provides a solution to the key distribution problem present in symmetric key cryptography.

I also Remembered the concept of zero knowledge proofs that was told to us by an IIT Bombay Faculty during our Orientation Programme.The Zero Knowledge Proof stuck me in the class and I felt it was related to public key cryptography but upon searching on internet after lecture I found out that it had different purposes i.e Zero Knowledge Proofs are used to just prove the validity of statement without revealing any information about the statement itself where as public key cryptography is used for secure communication and public key encryption.

Types of Services Provided by Cryptography

1. Confidentiality

Ensuring that no one can read the message except the intended receiver. The original data can't be recovered without the proper credentials even if the data is transferred via an insecure channel.

2. Integrity

Assuring the receiver that the received message has not been altered in any way from the original message.

3. Authentication

Verification of one's identity like the receiver that the receiver verifying that the sender/message is from the correct/intended source.

4. Non-Repudiation

Non-repudiation Algorithms ensures that the party cannot refute or deny the authenticity of the message or transaction.

Caesar Cipher

The Caesar Cipher is a basic and ancient encryption technique that involves shifting the letters of the alphabet by a fixed number of positions. Named after Julius Caesar, who is reputed to have used it, the Caesar Cipher is a type of substitution cipher.

1. Encryption

Replace each letter in the plaintext with the letter 3 positions ahead in the alphabet.

$$E(x) = (x + 3) \mod 26$$

2. Decryption

To decrypt, shift each letter in the ciphertext backward by 3 positions.

$$D(x) = (x - 3 + 26) \mod 26$$

Example:

Let's encrypt the message "SWAMI VIVEKANANDA" using the Caesar Cipher with a shift of 3.

Original Message

```
SWAMI VIVEKANANDA
```

Encryption

```
S → V  W → Z  A → D  M → P  I → L
V → Y  I → L  V → Y  E → B  K → H  A → D  N → K  A → D
```

Encrypted Message

```
VZDPL YLYBHKDK
```

One-way Function

A one-way function is a mathematical function that is easy to compute in one direction but computationally difficult to reverse. In other words, it is easy to calculate the function's output given an input, but it is difficult (infeasible) to determine the input given its output.
For Example: Prime number multiplication is easy but prime number factorization is hard.

Substitution Box

A substitution box is a function that maps a block of n-bits to another block of n-bits.
$S : A \to B$ with $|B| \leq |A|$
Example
$S : \{1, 2, 3, 4\} \to \{1, 2, 3\}$
$S(1) = 1, S(2) = 3, S(3) = 2$

Transposition Cipher

A transposition cipher is a method of encryption by which the positions held by units of plaintext(which are commonly characters or groups of characters) are shifted according to a regular system,so that the ciphertext constitutes a permutation of the plaintext.

$M = m_1 m_2 \ldots m_t$ (Plain text)
e: Permutation on t elements $1, 2, 3, \ldots, t$ $[\pi]$[Secret Keys]

Encryption: $C = C_1 C_2 \ldots C_t$
Decryption: $M = m_{e(1)}\, m_{e(2)}\, \ldots\, m_{e(t)}$

Substitution Cipher

A substitution cipher is a type of encryption algorithm where each letter in the plaintext is replaced with another letter based on a predefined rule or key.The receiver deciphers the text by performing the inverse substitution.
$S : A \to B$ with $|B| \leq |A|$
if $|B| < |A|$, then there exists multiple plaintext on decryption.

Mathematical Representation

Mathematically:

$$E(x) = f(x)$$

where f is a permutation.

For a substitution cipher with shift n:

$$E(x) = (x + n) \mod 26$$

$$D(x) = (x - n) \mod 26$$

Example:
Encryption
Plaintext: SHARDA MAA
Shift (Key): 4
Ciphertext: WLEVHE QEE

Decryption
Ciphertext: WLEVHE QEE
Shift (Key): 5
Plaintext: SHARDA MAA

Affine Cipher

The Affine Cipher is a type of monoalphabetic substitution cipher, where each letter in the plaintext is mapped to its numeric equivalent. It involves both multiplication and addition operations on each letter's numeric equivalent, providing a higher degree of security than traditional substitution ciphers.

For Encryption:

$$E(x) = (ax + b) \mod 26$$

where a and b are the key parameters, and x is the position of the letter in the alphabet.

For Decryption:

$$D(y) = a^{-1}(y - b) \mod 26$$

where a^{-1} is the modular multiplicative inverse of a (if it exists), and y is the numeric equivalent of the letter in the ciphertext.
Example(Encryption):
Plaintext: MANAS
Agreed Key: $a = 7$, $b = 4$
Ciphertext:

$$E(x) = (ax + b) \mod 26$$

Calculations:

$$\begin{aligned} E(M) &= (7 \times 12 + 4) \mod 26 = 10\,(\text{K}) \\ E(A) &= (7 \times 0 + 4) \mod 26 = 4\,(\text{E}) \\ E(N) &= (7 \times 13 + 4) \mod 26 = 17\,(\text{R}) \\ E(A) &= (7 \times 0 + 4) \mod 26 = 4\,(\text{E}) \\ E(S) &= (7 \times 18 + 4) \mod 26 = 0\,(\text{A}) \end{aligned}$$

So, the ciphertext is **KEREA**.

Playfair Cipher

The Playfair Cipher is a digraphic substitution cipher that encrypts pairs of letters (digraphs), replacing them with other pairs of letters based on a key table.

Rules for Encryption

- If the letters are in the same row, replace each with the letter to its right.
- If the letters are in the same column, replace each with the letter below.
- If the letters are not in the same row or column, form a rectangle and replace each letter with the letter in the same row at the other corner of the rectangle.
- If a letter is repeated or a pair of letters is the same, insert an extra letter (commonly ’X’) between them and apply the rules.

Construction of Key Table

1. Construct a 5x5 key table using a keyword (excluding duplicate letters) and the remaining letters of the alphabet.
2. Fill the table row-wise, avoiding repeated letters.

Playfair Keyword: SHREE SARASWATI

S	H	R	E	A
W	T	I	B	C
D	F	G	K	L
M	N	O	P	Q
U	V	X	Y	Z

Example

Using the above table Encrypting ”MANAS”
Encryption Process:

1. M → (3,1) → Q
2. A → (1,2) → S
3. N → (3,2) → Q
4. A → (1,2) → H
5. S → (4,2) → R

Ciphertext: QSQHRU
