[CS304] Introduction to Cryptography and Network Security

Course Instructor: Dr. Dibyendu Roy — Winter 2023-2024
Scribed by: Dipean Dasgupta (202151188) — Lecture (Week 1)

1 Introduction

- **Cryptography:**
  Cryptography refers to the study and application of methods for protecting data and communication from unauthorized access. Using cryptography, Information is encoded using specific mathematical algorithms so that only authorized parties will be able to decode and comprehend it.
  Fundamental topics in cryptography include Cryptographic algorithms, keys (secret values used in encryption and decryption procedures), encryption (converting plaintext into ciphertext), decryption (converting ciphertext back into plaintext), and protocols (systems of rules governing safe communication). In the digital age, cryptography is a vital instrument for protecting the privacy and security of data.

- **Cryptanalysis:**
  The science and practice of analysing and decoding cryptographic systems are known as cryptanalysis. It is used to find the security measurement types and levels and tries to break the security of designed algorithms to find secret information without the right key. Using a variety of approaches and strategies, cryptanalysis also seeks to take advantage of defects or weaknesses in the methods, protocols, or applications used for encryption.

- **Cryptology:**
  The broad term ”cryptology” includes both cryptanalysis and cryptography. It is the study of secure communication methods, which includes the development of ciphers and codes to protect data (cryptography) and the deciphering of those codes to uncover the data that is hidden (cryptanalysis). In the context of cryptography,**NIST(National Institute of Standards and Technology)** plays a significant role in the development and standardization of cryptographic algorithms and protocols.Essentially, cryptology is a broad topic that includes techniques for breaking or compromising secure communication systems as well as its design and implementation. So, it can be said that:

  $$\textbf{Cryptology} = \textbf{Cryptography} + \textbf{Cryptanalysis}$$

2 Cryptography workflow

Let’s use the example of an ATM PIN to demonstrate how cryptography functions:

$$\textbf{ATM Card1} \rightarrow \textbf{PIN1} + \textbf{A} = \textbf{X}$$

$$\textbf{ATM Card2} \rightarrow \textbf{PIN2} + \textbf{A} = \textbf{Y}$$

Plaintext(P): ATM PIN is the original, easily accessible information. Here **PIN1 and PIN2** are plaintexts.
Encryption(E): Entered PIN is changed into a separate, seemingly random string of numbers using an encryption technique, which functions similarly to a mathematical formula. Here **'+'** is the encryption function.
Ciphertext(C): The original PIN is represented by a jumbled string of integers that is the result of encryption. Here **'X'** and **'Y'** are the ciphertexts. The ATM system stores this ciphertext, or it can be securely transferred for validation.
Key(K): The key is a confidential parameter or code that only the specific bank and its ATM system are aware of. 'A' is the Secret Key here.
Decryption(D): The ATM utilizes the secret key to decrypt the ciphertext when one enters his/her PIN. The ciphertext is converted back into the original plaintext PIN through decryption.

Encryption: E(P,K) = C
Decryption: D(C,K) = P

3 Types of Cryptography

Symmetric key cryptography and asymmetric key cryptography are the two fundamental types of cryptography. Both employ distinct techniques to ensure secrecy and integrity when transferring sensitive information.

- **Symmetric key cryptography**
  In symmetric key cryptography, the encryption and decryption processes employ the same secret key. The challenge lies in securely passing the key between people who are in communication, even if it's a quick and simple process.

ENCRYPT("HELLO", "KEY123") = "XKJSF."
DECRYPT("XKJSF", "KEY123") = "HELLO."

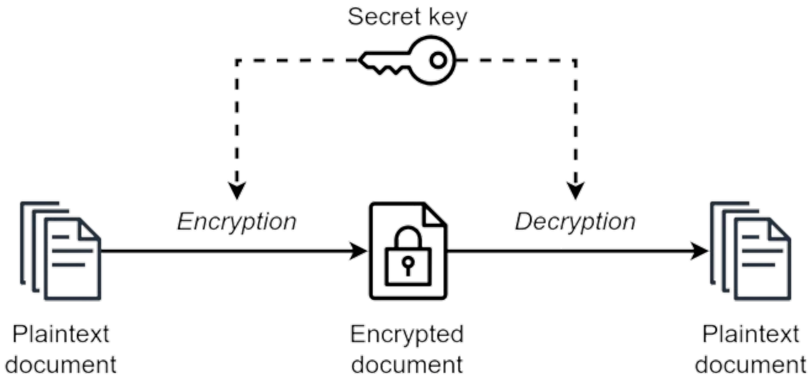


Figure1: Symmetric key cryptography
Source: Wikipedia

- **Assymmetric key cryptography** A public key is used for encryption in asymmetric key cryptography, while a private key is used for decryption. Securely sharing information is made possible by the fact that messages encrypted with the public key can only be unlocked with the matching private key.

ENCRYPT(”HELLO”,Public Key) = ”XWPGT.”
DECRYPT(”XWPGT”,Private Key) = ”HELLO.”

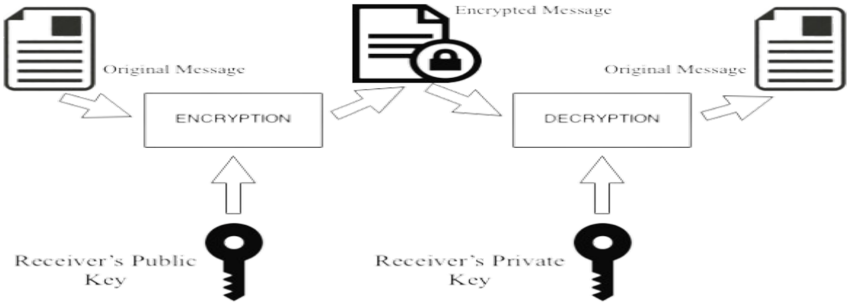


Figure1: Asymmetric key cryptography
Source: Wikipedia

4 Security Services:

- **Confidentiality:** Confidentiality in cryptographic security services guarantees that data is not accessible to unauthorized parties. Data is converted from plaintext into ciphertext using encryption techniques, which only authorized parties with the right keys may decode.
- **Integrity:** In cryptography, integrity ensures that information is preserved and does not change while being sent or stored. Unauthorized changes or tampering can be identified via comparison at the sender and recipient ends.
- **Authentication:** Authentication makes sure that the individuals involved in communication may be identified. In secure communications, this procedure aids in preventing impersonation and unwanted access.
- **Non-repudiation:** This is a security measure that keeps someone from retracting or denying what they have done. It guarantees that a sender cannot subsequently deny sending a message and that a recipient cannot dispute receiving it in cryptography.

5 Function

$$f : A \to B$$

A function f maps elements from set A to set B.

$$f : \mathbb{N} \to \mathbb{N}, \quad f(x) = 2x$$

A function f that maps natural numbers to their doubles.

- **One-to-One/Injective Function:**

$$f : A \to B \text{ is injective if } f(x_1) \neq f(x_2) \text{ whenever } x_1 \neq x_2$$

  A one to one function ensures that each element in the domain maps to a unique element in the codomain.

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = 3x$$

  This function is injective because different inputs always produce different outputs.

- **Onto/Surjective function:**
  A function is a surjection iff each element in its co-domain is mapped to some element in the domain.

$$\text{f: A} \to B, \text{then } \forall b \in B \exists a \in A \text{ such that } f(a) = b$$

- **Bijective Function:**
  A function f is bijective if, for every element in the domain ($\forall$), there exists a unique element in the codomain ($\exists$), and vice versa. In other words, each element in the domain maps to a unique element in the codomain, and the codomain is fully covered.
  A bijective function mapping integers to themselves, $f(x) = x$, is both injective and surjective.

- **Permutation (π):**

$$\pi : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$$

  A bijective function that rearranges items is called a permutation. In cryptography, permutations are often represented by the symbol π.

$$\pi : \{1, 2, 3\} \to \{1, 2, 3\}, \quad \pi(1) = 2, \pi(2) = 3, \pi(3) = 1$$

  A permutation that cyclically shifts elements.

- **Substitution Box**:
  It is a mapping from set A → B such that the $|B| \leq |A|$.

6 Classical Cipher Techniques:

6.1 Transposition Cipher:

A transposition cipher is a kind of encryption procedure in which the ciphertext is created by rearranging the plaintext's character locations.
Here, $M = M_1 M_2 \dots M_t \to$ plaintext
Encryption algorithm(e): permutation on t elements $\to 1, 2 \dots t$

Encryption: $C = M_e(1), M_e(2), \ldots, M_e(t) = C_1C_2\ldots C_t$
Decryption: $M = C_e^{-1}(1)\ldots C_e^{-1}(t)$
For example:

$$\text{CAESER} = \text{M}_1 .... M_6$$
$$\text{Secret Key: E}(1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \rightarrow \; 6\,4\,1\,3\,5\,2)$$

$$\text{Cipher: RSCEAA}$$
$$= \text{C}_1C_2C_3C_4C_5C_6$$
$$\text{M}_6M_4M_1M_3M_5M_2$$
$$D = E^{-1} = (1\,2\,3\,4\,5\,6 \rightarrow \; 3\,6\,4\,2\,5\,1)$$

$$\text{Cipher: RSCEAA}$$
$$\text{Secret Key: } (1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \rightarrow \; 3\,6\,4\,2\,5\,1)$$
$$\text{plainText: CAESER}$$

6.2 Substitution Cipher:

In substitution, a cipher replaces letters in regular text with other letters or symbols to create cipher text. The cipher text may contain new characters or symbols since the letters are changed. The substitution of itself for a set of alphabets is the secret key involved.

$$M = m_1m_2...m_y \quad \text{(plaintext)}$$

Encryption: $C = C_1C_2.....C_m$, where e is a function from the set S to itself.

Here, $S = \{A, B, C, ..., Z\}$ represents a set of symbols used in the entire encryption process.

For example, $e(A) = Z, e(B) = D$ can be the substitutions. **Note: The same element can be used to replace more than one character. In this scenario, determining the proper combination of these characters is necessary for decryption.**

Decryption: To obtain the plaintext, all that has to be done is flip the replacements.

6.3 Caeser Cipher:

Roman General Julius Caesar created the Caesar cipher to transmit encoded messages. It is one of the earliest and simplest methods of encryption techniques. This technique involves shifting each letter in the plaintext by a fixed number of positions(mainly 3), known as the ”key” or ”shift.”

E: E(x) = (x + 3) mod 26
D: D(x) = (x - 3) mod 26

Let us consider the plaintext "CRYPTO".
Encryption:

$$\begin{aligned} C &\rightarrow (2+3) \mod 26 = 5 \rightarrow F \\ R &\rightarrow (17+3) \mod 26 = 20 \rightarrow U \\ Y &\rightarrow (24+3) \mod 26 = 1 \rightarrow B \\ P &\rightarrow (15+3) \mod 26 = 18 \rightarrow S \\ T &\rightarrow (19+3) \mod 26 = 22 \rightarrow W \\ O &\rightarrow (14+3) \mod 26 = 17 \rightarrow R \end{aligned}$$

So, "CRYPTO" is encrypted to "FUBSWR" with a key of 3.
Decryption:

$$\begin{aligned} F &\rightarrow (5-3) \mod 26 = 2 \rightarrow C \\ U &\rightarrow (20-3) \mod 26 = 17 \rightarrow R \\ B &\rightarrow (1-3) \mod 26 = 24 \rightarrow Y \\ S &\rightarrow (18-3) \mod 26 = 15 \rightarrow P \\ W &\rightarrow (22-3) \mod 26 = 19 \rightarrow T \\ R &\rightarrow (17-3) \mod 26 = 14 \rightarrow O \end{aligned}$$

So, "FUBSWR" is decrypted back to "CRYPTO" using the key 3.

6.4 Affine Cipher:

Let A be the set of alphabets and Z_{26} be the integer set from 0 to 25. The secret key for the Affine Cipher is given below:

$$k = (a, b) \in Z_{26} \times Z_{26}$$

Encryption:

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

Decryption:

$$d(c, k) = ((c - b)a^{-1}) \mod 26$$

where $k = (a, b)$ is the key, x =PT(plain text), c = CT(cipher text), and $a^{-1} \in Z_{26}$ is the multiplicative inverse of a modulo 26. The message can be decrypted only after a^{-1} is found.
Condition:

$$gcd(a, 26) = 1$$

6.4.1 Multiplicative Inverse:

An x inverse such that is the multiplicative inverse of an integer x under modulo m is:

$$x \cdot x^{-1} \equiv 1 \; mod \; m$$

Prior to deciphering the meaning of multiplicative inverse, we must comprehend its necessity. In short, $(c - b)/a)mod26$ wouldn't work as division could result in a fraction, and it wouldn't be able to transfer a fraction to an alphabet. Therefore, multiplicative inverse became crucial.

The multiplicative inverse of x under modulo m exists iff ged(x, m) equals 1. Let y be the multiplicative inverse of x modulo m. Hence, $x \cdot y \equiv 1$ mod m m divides $((x \cdot y) - 1) \Rightarrow \exists t \in Z$ such that $(x \cdot y) - 1 = t \cdot m$

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

According to Bezout's Identity, there are always two integers, a and b, such that: ged(x, y) = ax+by The final equation can be written as:

$$gcd(x, m) = 1 = t.m + xy \tag{1}$$

6.4.2 Extended Euclidian Algorithm:

The extended Euclidean algorithm extends the Euclidean method for finding the greatest common divisor (GCD) of two numbers. The coefficients for Bezout's Identity, which is gcd(x, y)=a.x+b.y, are likewise determined by it. This is often used in modular arithmetic and number theory, especially when discussing modular inverses. The values of a and b can be found using the Extended Euclidean Algorithm. The Extended Euclidean Algorithm can be used to find the numbers a and b.
Now, Let us first compute the GCD of $x = 3$ and $y = 17$ using Euclid's Division Algorithm.

$$\begin{aligned} 17 &= 3 \cdot 5 + 2 \quad \text{(Eq. 1)} \\ 3 &= 2 \cdot 1 + 1 \quad \text{(Eq. 2)} \\ 2 &= 1 \cdot 2 + 0 \quad \text{(Eq. 3)} \end{aligned}$$

Hence,GCD(3, 17) = 1.Now, going in reverse direction of this will lead us to the values of a and b.

$$\begin{aligned} 1 &= 1 \cdot 3 - 1 \cdot 2 \quad \text{(from Eq. 2)} \\ &= 1 \cdot 3 - 1(17 - 3 \cdot 5) \quad \text{(from Eq. 1)} \\ &= 6 \cdot 3 - 1 \cdot 17 \quad \text{(from Eq. 1)} \end{aligned}$$

Hence, $a = 6$ and $b = -1$.

6.4.3 Euler's Totient Function:

The number theory function known as Euler's Totient Function, sometimes represented by $\phi(n)$,, counts the positive integers that are relatively prime to a given integer n up to that point. The count of numbers in the range of 1 to n that, except from 1, have no common factor with n is provided by $\phi(n)$.

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k})$$

where $p_1, p_2, ..., p_k$ are the distinct prime factors of n.

n	$\phi(n)$
n	$n - 1$
$n = p \cdot q$, p and q are primes	$(p - 1)(q - 1)$
n is prime	$n - 1$

Table: Euler's Totient Function.

6.4.4 Number of Keys for Affine Cipher:

We’ve seen that decrypting Affine encryption is only feasible in cases where there is a multiplicative inverse of a mod 26, where a Z26. From Euler’s Totient Function as well:

$$\phi(26) = (2 - 1)(13 - 1) = 12 \tag{2}$$

since 26 = 2 * 13, and 2 and 13 are prime. As a result, there are 12 possible values for an in the key and 26 possible values for b. As a result, the Affine Cypher can have a total of 12 • 26 312 keys. This restriction results from the need that have a multiplicative inverse modulo 26 to guarantee the decryption’s viability.

6.5 Playfair Cipher

Playfair cyphers are a type of block cypher in which a character that is substituted during encryption from a plaintext character to a ciphertext character depends in part on a character that is nearby. They were designed by Charles Wheatstone in 1854, but Lyon Playfair, an English lord who encouraged their use, is credited with giving them their name.

The Playfair Cypher encrypts and decrypts data using a 5 X 5 matrix created with the secret key.

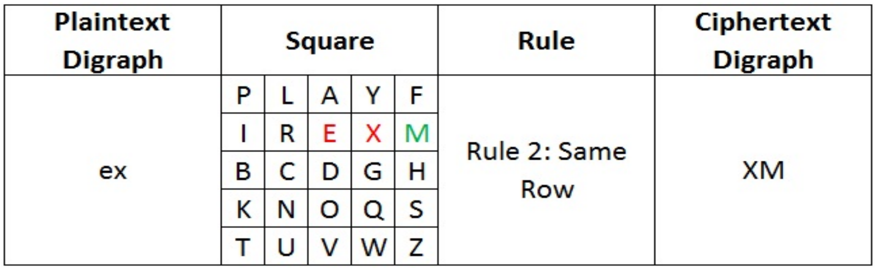
Encryption: The following rules are followed for encryption:

1. Create the 5×5 matrix using secret key. Rules for creating the matrix are mentioned below:
   - A Secret key is adopted, for example a standard secret key is ”PLAYFAIR EXAMPLE”
   - Characters I and J are considered as same. This is done because a 5×5 matrix can hold 25 characters, and the English Alphabet system has 26. So one alphabet is merged with another. I and J look similar, so they have been put into once cell.

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

   - Now fill in the characters in the matrix row-by-row using the secret key. Go on to the next character and skip any that have already made an appearance.
   - Once every character in the secret key has been used, lexicographically fill the remaining alphabets.
2. Divide the plain text message into groups of two characters. This is fundamentally required because a character’s ability to transform into its cypher form is dependent upon the character with which it is linked. Later on, we will see the same thing through an example.
3. If the characters cannot be divided into groups of two or if there are repeated characters in a row, fillers must be inserted.
4. The characters’ locations in the matrix must be determined for every pair. There are several guidelines that must be followed after it.
   - **Rule1:** If length of message is odd, add X as a filler at the end of message.Suppose the plaintext is CALL” , in that case it needs to be converted to CALXLX”.The first X to separate the two L’s, and the last X to make the text even numbered.

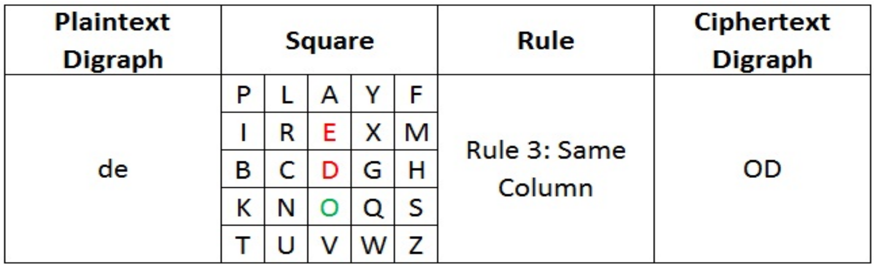
- **Rule2:**If two letters are found in the square on the same row, swap out each letter for the letter that appears exactly next to it, going around to the left if needed.



Plaintext Digraph	Square	Rule	Ciphertext Digraph
ex	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	Rule 2: Same Row	XM

Figure: Rule 2: Same Row
Source: crypto corner

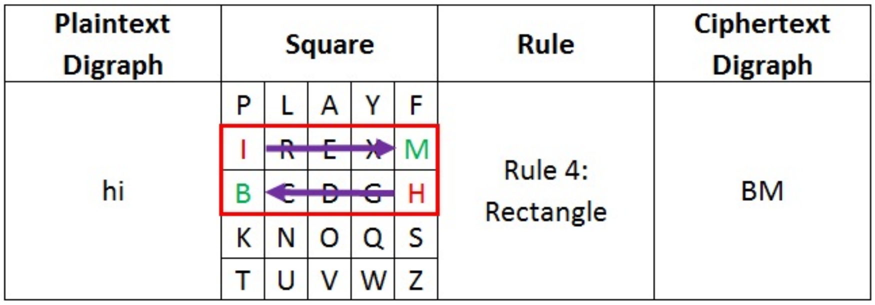
- **Rule3:** Replace each letter in the square with the one just below it if the two letters are present in the same column. If needed, continue to cycle all the way to the top of the square.



Plaintext Digraph	Square	Rule	Ciphertext Digraph
de	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	Rule 3: Same Column	OD

Figure: Rule 3: Same Column
Source: crypto corner

- **Rule4:** If not, create the rectangle whose two opposite corners are the plaintext letters. Next, (taking cautious to retain the sequence) replace each plaintext letter with the letter that forms the other corner of the rectangle that lies on the same row as that plaintext letter.



Plaintext Digraph	Square	Rule	Ciphertext Digraph
hi	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	Rule 4: Rectangle	BM

Figure: Rule 4: corner
Source: crypto corner

Example 1:

Secret Key: PLAYFAIR EXAMPLE
Plain Text: HIDE

The encryption matrix:

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

Breaking the plain text into groups of 2:

Plain Text: HI DE

Encryption steps:

1. For the first group (HI), the characters H and I form a rectangle in the matrix. Swap the corners to get BM.

2. For the second group (DE), the characters D and E are in the same column. Take the next character down in each column to get OD.

Plain Text: HI DE
Cipher Text: BM OD