CRYPTOGRAPHY 1

First Lecture - Introduction

Assistant Professor Dr.

Sufyan Salim Mahmood

2024 - 2025

What is Cryptography

- Cryptography is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.

BASIC TERMINOLOGY

- Plaintext: Original message to be encrypted
- Ciphertext: The encrypted message
- Enciphering or encryption: The process of converting plaintext into ciphertext
- Encryption algorithm: Performs encryption
  - Two inputs: a plaintext and a secret key

- Deciphering or decryption: Recovering plaintext from ciphertext
- Decryption algorithm: Performs decryption
  - Two inputs: ciphertext and secret key
- Secret key: Same key used for encryption and decryption
  - Also referred to as a symmetric key

- Cipher or cryptographic system : A scheme for encryption and decryption

- Cryptography: Science of studying ciphers

- Cryptanalysis: Science of studying attacks against cryptographic systems

- Cryptology: Cryptography + cryptanalysis

How does Cryptography work?

- A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key—a word, number, or phrase—to encrypt the plaintext.

How does Cryptography work?

- The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

Why the Cryptography ?

- Cryptography is essential for maintaining the confidentiality, authenticity, and integrity of messages that are communicated over untrustworthy channels.

Why the Cryptography ?

- Confidentiality is the assurance that only the owners of the keys can access the data. Authenticity is the assurance that the originator of the message is not an imposter. Integrity is the assurance that data has not been altered while in transit.

Diffusion and Confusion

- All ciphering methods are based on the principles of diffusion and confusion, which are terms coined by Claude Shannon. Diffusion is the technique of transposing and substituting characters or bits. The intent is to disperse the statistical nature of the encrypted message or cipher text, and thereby hide its relationship with the plain text.

Diffusion and Confusion

- Alternatively, confusion is the cryptographic principle of hiding the relationship between the cipher text and the secret key.

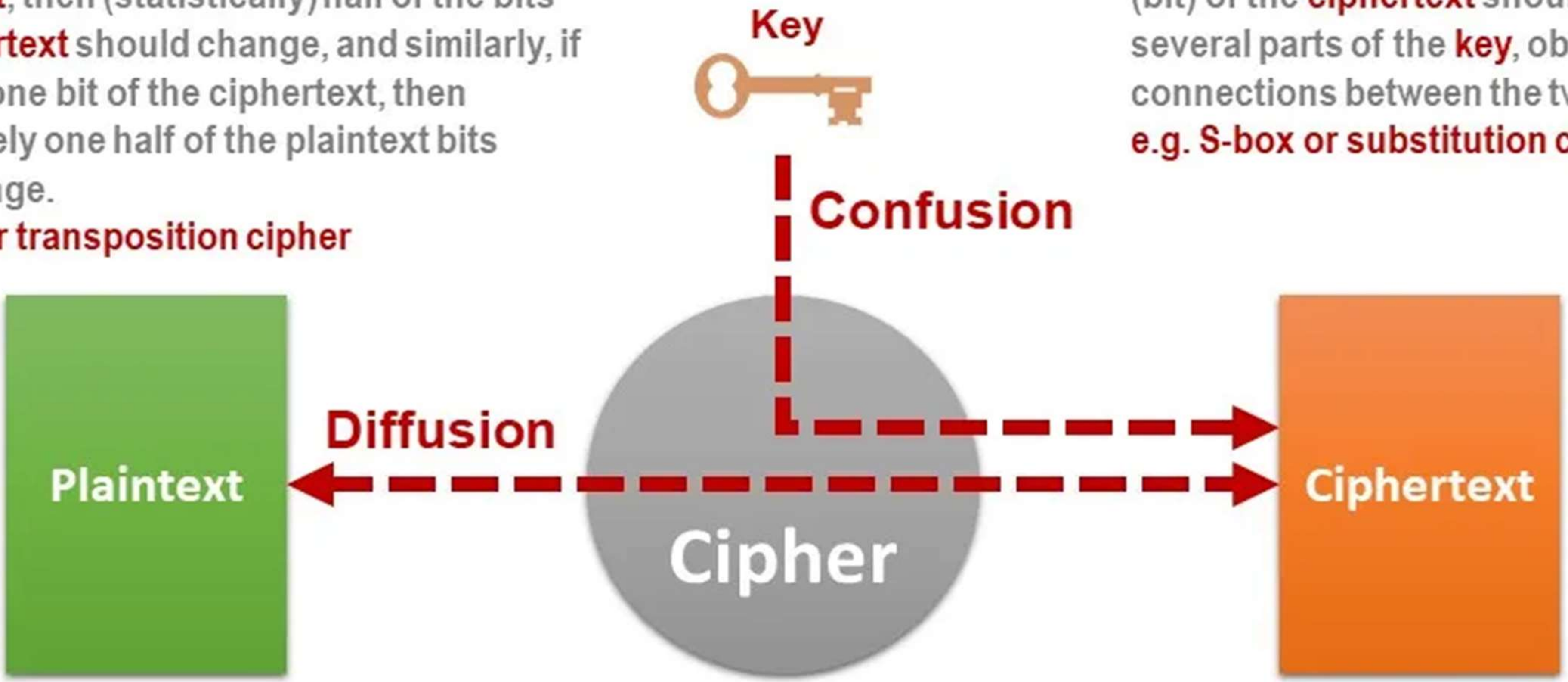
onfusion and Diffusion

fusion means that if we change a single bit of e **plaintext**, then (statistically) half of the bits the **ciphertext** should change, and similarly, if change one bit of the ciphertext, then proximately one half of the plaintext bits ould change.

g. P-box or transposition cipher

Confusion means that each binar (bit) of the **ciphertext** should dep several parts of the **key**, obscurin connections between the two.

e.g. S-box or substitution cipher



wikipedia.org/wiki/Confusion_and_diffusion

Types of Cryptography

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hash Functions

Symmetric Key Cryptography

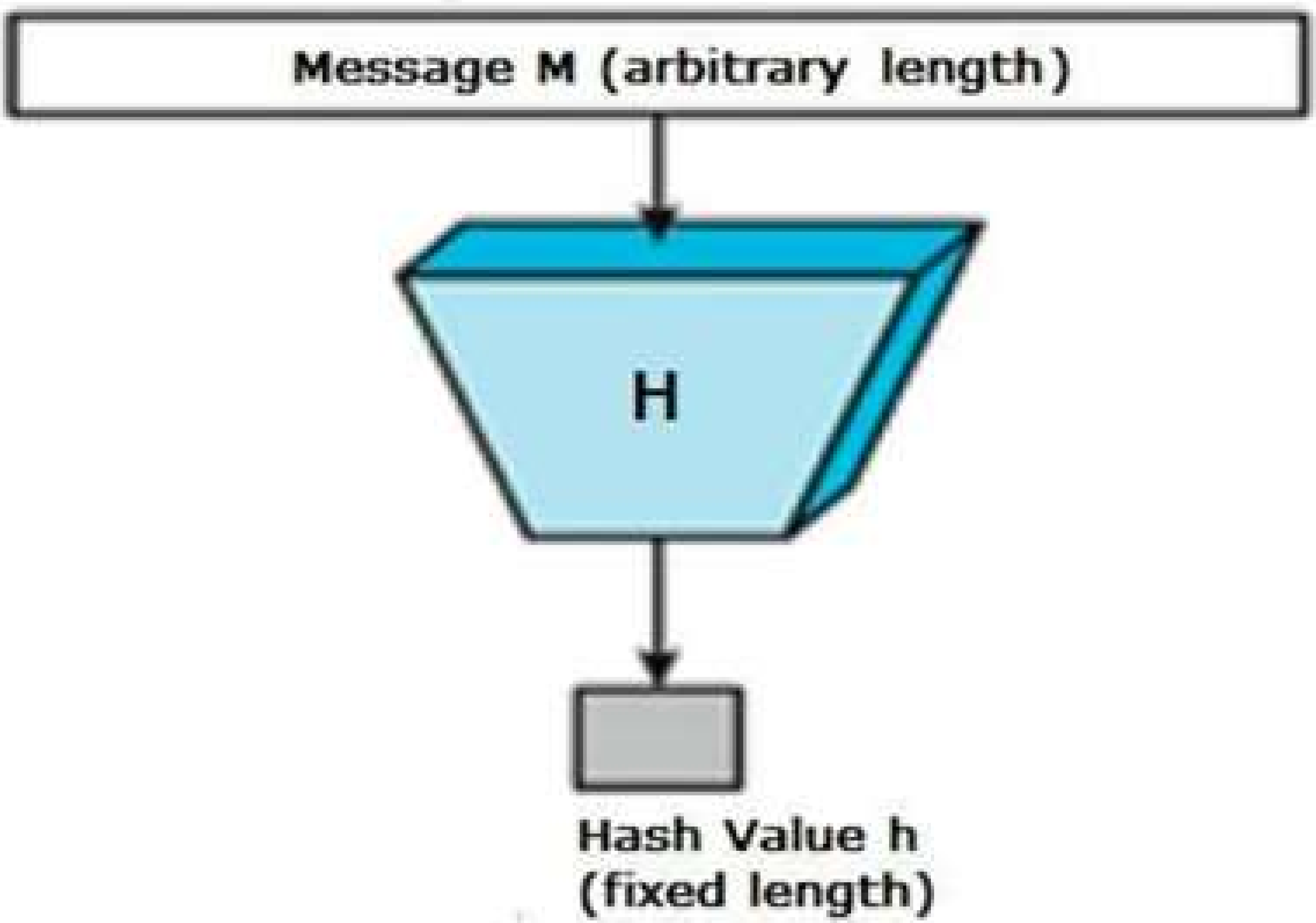
- Also known as Secret Key Cryptography or Conventional Cryptography, Symmetric Key Cryptography is an encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.

Asymmetric Key Cryptography

- Asymmetric cryptography , also known as Public-key cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is private and one of which is public. The public key is used to encrypt the message and the private one is used to decrypt the message.

Hash Functions

- A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value, such that any change to the data will change the hash value. The data to be encoded are often called the message, and the hash value is sometimes called the message digest or simply digest.



Message M (arbitrary length)
H
Hash Value h
(fixed length)

Ideal cryptographic hash function

It has four main properties:

- It is easy to compute the hash value for any given message.
- It is infeasible to generate a message that has a given hash.
- It is infeasible to modify a message without changing the hash.
- It is infeasible to find two different messages with the same hash.

Randomness

- ensures that encryption keys and other critical parameters are truly random, making it difficult for adversaries to crack the encryption or predict the output. Without proper randomness, cryptographic systems may become vulnerable to attacks, compromising the security of sensitive data.

Why is randomness important in security

- Security fundamentally depends on secret information, such as passwords and encryption keys. These passwords and keys are used to protect access to data and systems, but they can only serve that purpose if they're kept secret. To stay secret, they must be random enough to be unguessable even to hackers and sophisticated computer programs.

- A password that isn’t random, like “LetMeIn2023”, can be easily guessed by someone trying to break into an account. A password that’s long and random, like “z5W!j%5FySnnHK”, will be impossible for a hacker to guess within a person’s lifetime, even if they could try thousands of passwords every second.

Cryptographic Attack

- A cryptographic attack permits threat actors to bypass the security of a cryptographic system by finding weaknesses in its code, cipher, cryptographic protocol, or key management scheme. This circumvention is also called “cryptanalysis.”

Cryptographic Attack

- Depending on the type of cryptographic system in place and the information available to the attacker, these attacks can be broadly classified into six types:

Cryptographic Attack

- **Brute force attacks:** In a brute force attack, the threat actor in question will attempt a variety of keys in order to decipher an encrypted message or data. If the key size is 8-bit, the possible keys will be 256 (i.e., 2^8). In order for this to be successful, the threat actor must know the algorithm (generally found as open-source programs) to try all the 256 possible keys in this attack technique.

Cryptographic Attack

- **Ciphertext-only attack:** In this attack vector, the threat actor will gain access to a collection of ciphertext. Although the threat actor can't access the plaintext directly, they can successfully determine the ciphertext from the collection. This vector is generally less effective than its brute-force counterpart

Cryptographic Attack

- **Chosen plaintext attack:** Via a chosen plaintext attack, a threat actor cybercriminal can select plaintext data to obtain the ciphertext, which in turn simplifies their task of resolving the encryption key

Cryptographic Attack

- **Chosen ciphertext attack:** In this method, the threat actor will attempt to obtain a secret key or the details about the system. By analyzing the chosen ciphertext and relating it to the plaintext, the threat actor will try to guess the key

Cryptographic Attack

- **Known plaintext attack:** This technique can occur when a threat actor already knows the plaintext of some portions of the ciphertext using information-gathering techniques

Cryptographic Attack

- **Dual key and algorithm attack:** The threat actor will attempt to recover the key used to encrypt or decrypt the data by analyzing the cryptographic algorithm

Cryptographic Attack

- Alongside these six main types of cryptographic attacks, a cryptography attack can be either passive or active.

Cryptographic Attack

- **Passive attacks:** Passive cryptography attacks are launched with the intent to gather unauthorized access to sensitive data or information by intercepting or eavesdropping on general communication. In this situation, the data and the communication remain intact and are not tampered with

Cryptographic Attack

- **Active attacks:** As a direct comparison, active cryptography attacks hinge on the modification of the data or the communication. In this case, the attacker not only gains access to the data but also tampers with it

CRYPTOGRAPHY 1

Second Lecture –

Introduction to Numbers

Assistant Professor Dr.

Sufyan Salim Mahmood

2024 - 2025

- Primes Numbers
- Greatest Common Divisor GCD
- Euler Totient Function ø(n)
- Finding inverses in finite fields

The Prime Theorem

- A prime is a number divisible only by itself and one.
- Example :

- 2,3,5,7 are prime
- 4,6,8,9,10 are not prime
- list of prime number less than 200 is:

  2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

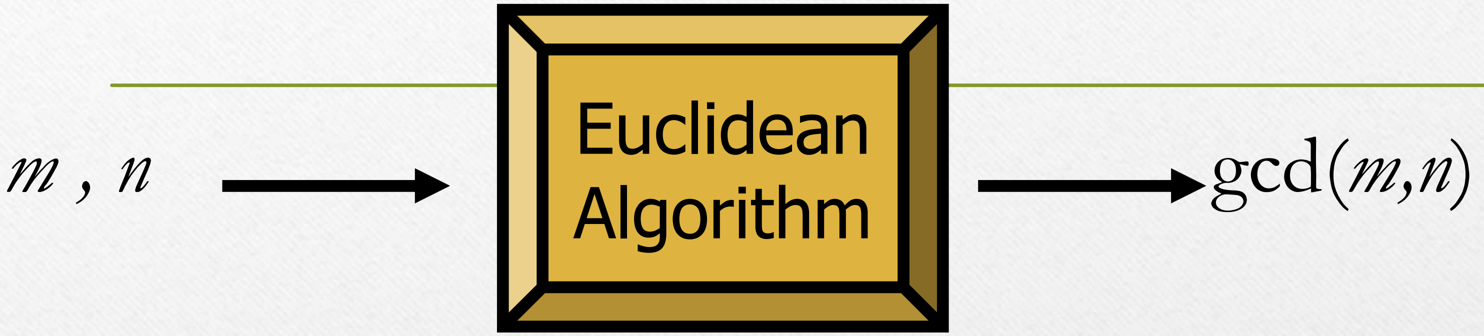
Greatest Common Divisor (GCD)

- GCD (a,b) of a and b is the largest number that divides evenly into both a and b
  - GCD(60,24) = 12

The factors of 24 are: 1, 2, 3, 4, 6, 8, **12**, 24

The factors of 60 are: 1, 2, 3, 4, 5, 6, 10, **12**, 15, 20, 30, 60

Euclidean Algorithm



m , n

Euclidean Algorithm

gcd(m,n)

```
integer euclid(pos. integer $m$, pos. integer $n$)
    $x = m, y = n$
    while($y > 0$)
        $r = x \mod y$
        $x = y$
        $y = \mathrm{r}$
return $x$
```

Euclidean Algorithm. Example

gcd(x,y) = gcd(33,77):

Step	$r = x$ **mod** y	x	y
0	–	33	77

Euclidean Algorithm. Example

gcd(33,77):

Step	$r = x$ **mod** y	x	y
0	–	33	77
1	33 **mod** 77 = 33	77	33

Euclidean Algorithm. Example

gcd(33,77):

Step	$r = x$ **mod** y	x	y
0	–	33	77
1	33 **mod** 77 = 33	77	33
2	77 **mod** 33 = 11	33	11

Euclidean Algorithm. Example

gcd(33,77):

Step	$r = x$ **mod** y	x	y
0	–	33	77
1	33 **mod** 77 = 33	77	33
2	77 **mod** 33 = 11	33	11
3	33 **mod** 11 = 0	11	0

Euclidean Algorithm. Example

gcd(244,117):

Step	$r = x$ **mod** y	x	y
0	–	244	117

Euclidean Algorithm. Example

gcd(244,117):

Step	$r = x$ **mod** y	x	y
0	–	244	117
1	244 **mod** 117 = 10	117	10

Euclidean Algorithm. Example

gcd(244,117):

Step	$r = x$ **mod** y	x	y
0	–	244	117
1	244 **mod** 117 = 10	117	10
2	117 **mod** 10 = 7	10	7

Euclidean Algorithm. Example

gcd(244,117):

Step	$r = x$ **mod** y	x	y
0	–	244	117
1	244 **mod** 117 = 10	117	10
2	117 **mod** 10 = 7	10	7
3	10 **mod** 7 = 3	7	3

Euclidean Algorithm. Example

gcd(244,117):

Step	r = x **mod** y	x	y
0	–	244	117
1	244 **mod** 117 = 10	117	10
2	117 **mod** 10 = 7	10	7
3	10 **mod** 7 = 3	7	3
4	7 **mod** 3 = 1	3	1

Euclidean Algorithm. Example

gcd(244,117):

Step	$r = x$ **mod** y	x	y
0	–	244	117
1	244 **mod** 117 = 10	117	10
2	117 **mod** 10 = 7	10	7
3	10 **mod** 7 = 3	7	3
4	7 **mod** 3 = 1	3	1
5	3 **mod** 1=0	1	0

By definition ➔ 244 and 117 are rel. prime.

Euler Totient Function ø(n)

- Euler's Totient function ø(n) for an input n is the count of numbers in {1, 2, 3, …, n} that are relatively prime to n, i.e., the numbers whose GCD (Greatest Common Divisor) with n is 1.

Euler Totient Function ø(n)

n	ø(n)
n (n prime)	n-1
n^r (n prime)	n^{r-1} *(n-1)
p*q (p & q primes)	(p-1)*(q-1)
$\prod^t_{i=1} p_i^{ei}$ (p_i primes)	$\prod^t_{i=1} p_i^{ei-1} * (p_i-1)$

Euler Totient Function ø(n)

- eg.

ø(37) = (n-1) = (37-1) = 36

ø(11) =

ø(9) = $(n^{r-1} * (n-1)) = 3^{2-1}*(3-1) = 3*2 = 6$

ø(25) =

ø(21) = (p-1)*(q-1) = (7–1)x(3–1) = 6*2 = 12

ø(55) =

ø(20) = $(\prod^{t}_{i=1} p_i^{ei-1} * (p_i-1)) = 4*5 = 2^2*5^1$

$= 2^{2-1}*(2-1) * 5^{1-1}*(5-1) = 2 * 4 = 8$

ø(100) =

Inverse

Fermat's theorem

- If (**n** is prime) and (GCD(n , a)=1) then the Inverse X is

$$\boxed{\mathbf{X = a^{n-2} \bmod n}}$$

- eg.
- If n=5, a=3, find the Inverse?
- $X = a^{n-2} \bmod n$
- $X = 3^{5-2} \bmod 5$
- $X = 27 \bmod 5$
- $X = 2$

$a * X \bmod n = 1$

$3 * 2 \bmod 5 = 1$

$6 \bmod 5 = 1$

Inverse

General Method

- If (**n** is prime or not prime) and (GCD(n , a)=1) then the Inverse X is

$$\boxed{X = a^{ø(n)-1} \bmod n}$$

Inverse

General Method

- If (**n** is prime) and (GCD(n , a)=1)
- then the Inverse X is

$$\boxed{\mathbf{X = a^{ø(n)-1}\ mod\ n}}$$

- eg.
- If n=3, a=4, find the Inverse?
- $X = 4^{ø(3)-1} \bmod 3$
- $X = 4^{2-1} \bmod 3$
- $X = 4 \quad \bmod 3$
- $X = 1$

$a * X \bmod n = 1$

$4 * 1 \bmod 3 = 1$

$4 \bmod 3 = 1$

Inverse

General Method

- If (**n is even**) and (GCD(n,a)=1) then the Inverse X is

$$\boxed{\mathbf{X = a^{\text{ø}(n)-1} \bmod n}}$$

- eg.
- If n=4, a=3, find the Inverse?
- $X = 3^{\text{ø}(2)-1} \bmod 4$
- $X = 3^{2-1} \bmod 4$
- $X = 3 \bmod 4$
- $X = 3$

$a * X \bmod n = 1$

$3 * 3 \bmod 4 = 1$

$9 \bmod 4 =1$

Inverse

General Method

- If (**n is odd and** is not prime) and (GCD(n,a)=1) then the Inverse X is

$$\boxed{\mathbf{X = a^{\text{ø}(n)-1} \bmod n}}$$

- eg.
- If n=9, a=4, find the Inverse?
- $X = 4^{\text{ø}(9)-1} \bmod 9$
- $X = 4^{6-1} \bmod 9$
- $X = 1024 \bmod 9$
- $X = 7$

$a * X \bmod n = 1$

$4 * 7 \bmod 9 = 1$

$28 \bmod 9=1$

CRYPTOGRAPHY 1

Third Lecture – Traditional Cryptography

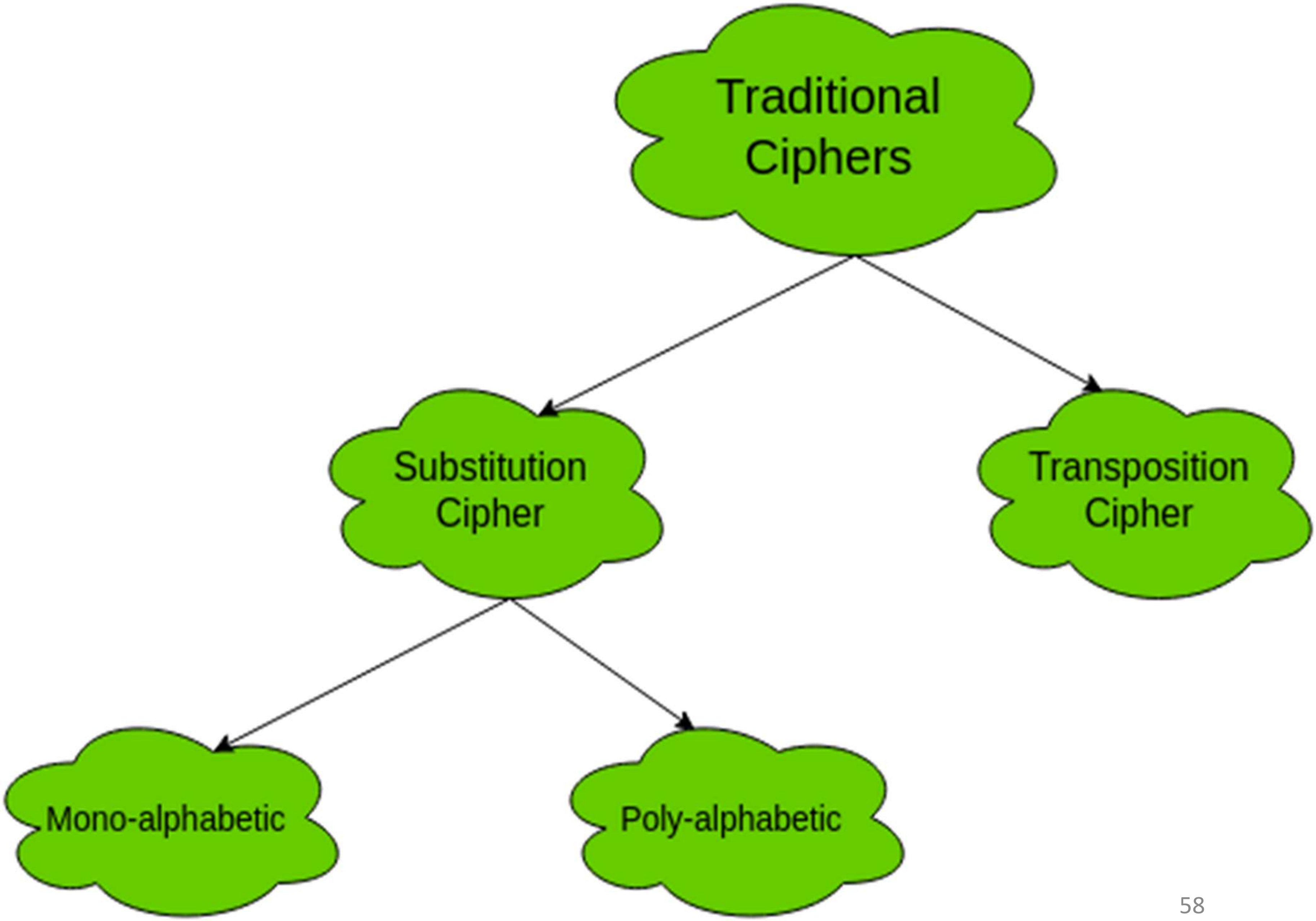
Assistant Professor Dr.

Sufyan Salim Mahmood

2024 - 2025

Traditional Cryptography

- The two types of traditional symmetric ciphers are **Substitution Cipher** and **Transposition Cipher**.



Traditional Ciphers

Substitution Cipher

Transposition Cipher

Mono-alphabetic

Poly-alphabetic

Substitution Cipher:

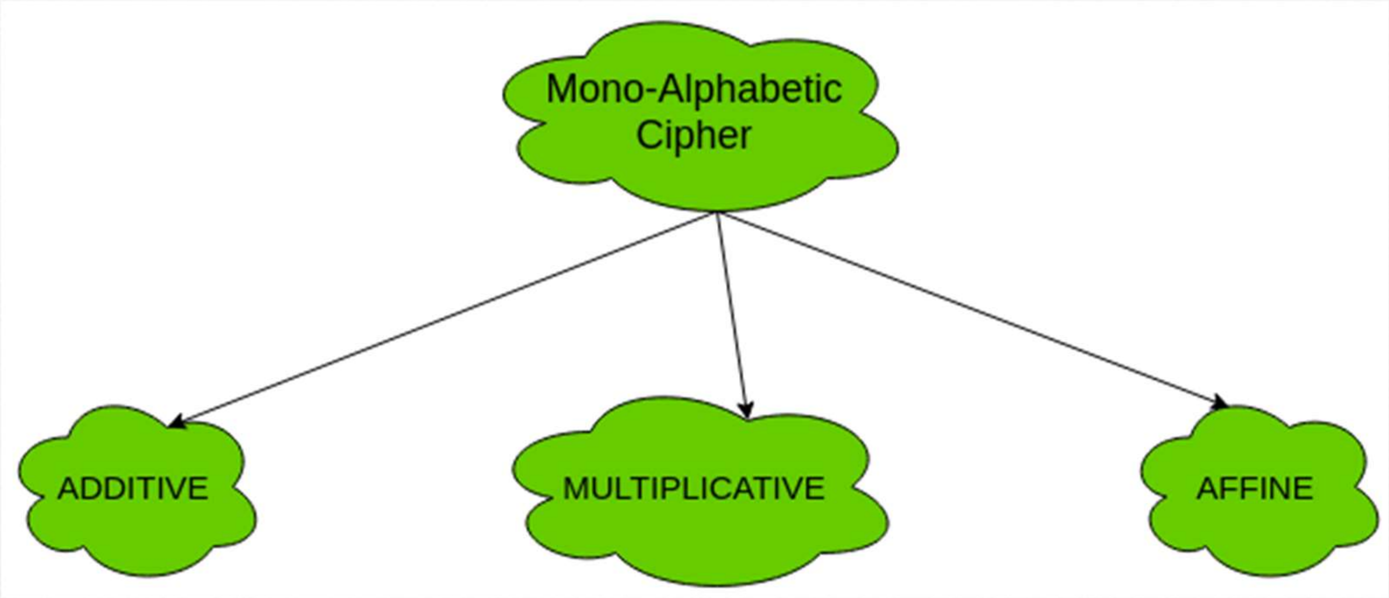
- Mono-alphabetic Cipher
- Poly-alphabetic Cipher.

Mono Alphabetic Cipher

- In mono-alphabetic ciphers, each symbol in plain-text (eg; ‘o’ in ‘follow’) is mapped to one cipher-text symbol. No matter how many times a symbol occurs in the plain-text, it will correspond to the same cipher-text symbol.

- For example, if the plain-text is ‘follow’ and the mapping is :f -> g
- o -> p
- l -> m
- w -> x
- The cipher-text is ‘gpmmpx’.

Types of mono-alphabetic ciphers are:



Additive Cipher
(Shift Cipher / Caesar Cipher)

The simplest mono-alphabetic cipher is additive cipher. It is also referred to as ‘Shift Cipher’ or ‘Caesar Cipher’. As the name suggests, ‘addition modulus 2’ operation is performed on the plain-text to obtain a cipher-text.

Additive Cipher
(Shift Cipher / Caesar Cipher)

- $C = (M + k) \bmod n$
- where,
  C -> cipher-text
  M -> message/plain-text
  k -> key
- The key space is 26. Thus, it is not secure. It can be broken by brute-force attack.

Multiplicative Cipher

- The multiplicative cipher is similar to additive cipher except the fact that the key bit is multiplied to the plain-text symbol during encryption. Likewise, the cipher-text is multiplied by the multiplicative inverse of key for decryption to obtain back the plain-text.

Multiplicative Cipher

- C = (M * k) mod n

  The key space of multiplicative cipher is 12.

  Thus, it is also not secure.

- Note : The key should be coprime with n

Affine Cipher

- The affine cipher is a combination of additive cipher and multiplicative cipher. The key space is 26 * 12 (key space of additive * key space of multiplicative) i.e. 312. It is relatively secure than the above two as the key space is larger.

Affine Cipher

Here two keys k_1 and k_2 are used.

- $C = [(M * k_1) + k_2] \bmod n$

Poly-alphabetic Ciphers

- Every symbol in plain-text is mapped to a different cipher-text symbol regardless of its occurrence. Every different occurrence of a symbol has different mapping to a cipher-text.

- For example, in the plain-text ‘follow’, the mapping is :f -> q

  o -> w

  l -> e

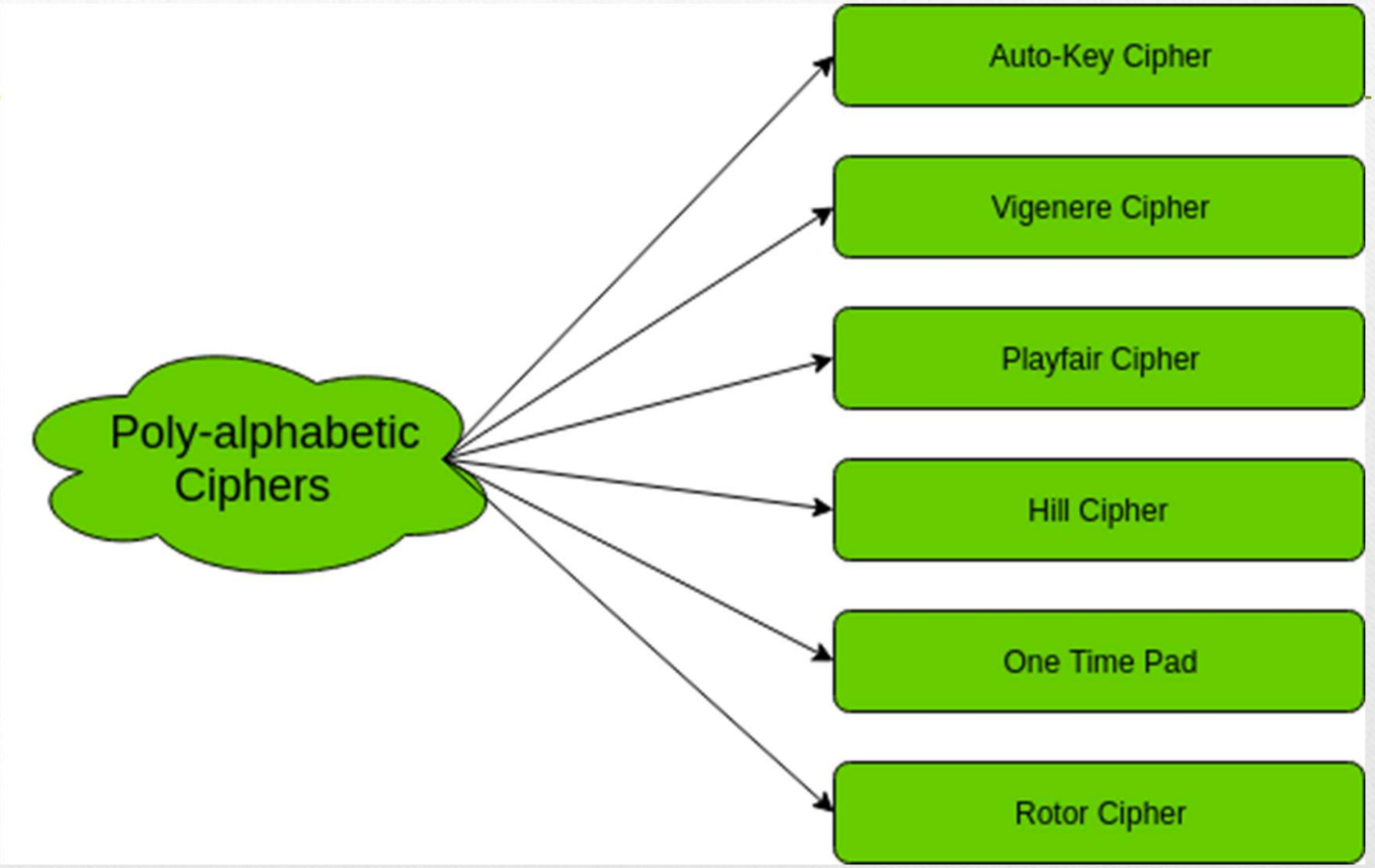
  l -> r

  o -> t

  w -> y

- Thus, the cipher text is ‘qwerty’.

Types of poly-alphabetic ciphers



Poly-alphabetic Ciphers

Auto-Key Cipher

Vigenere Cipher

Playfair Cipher

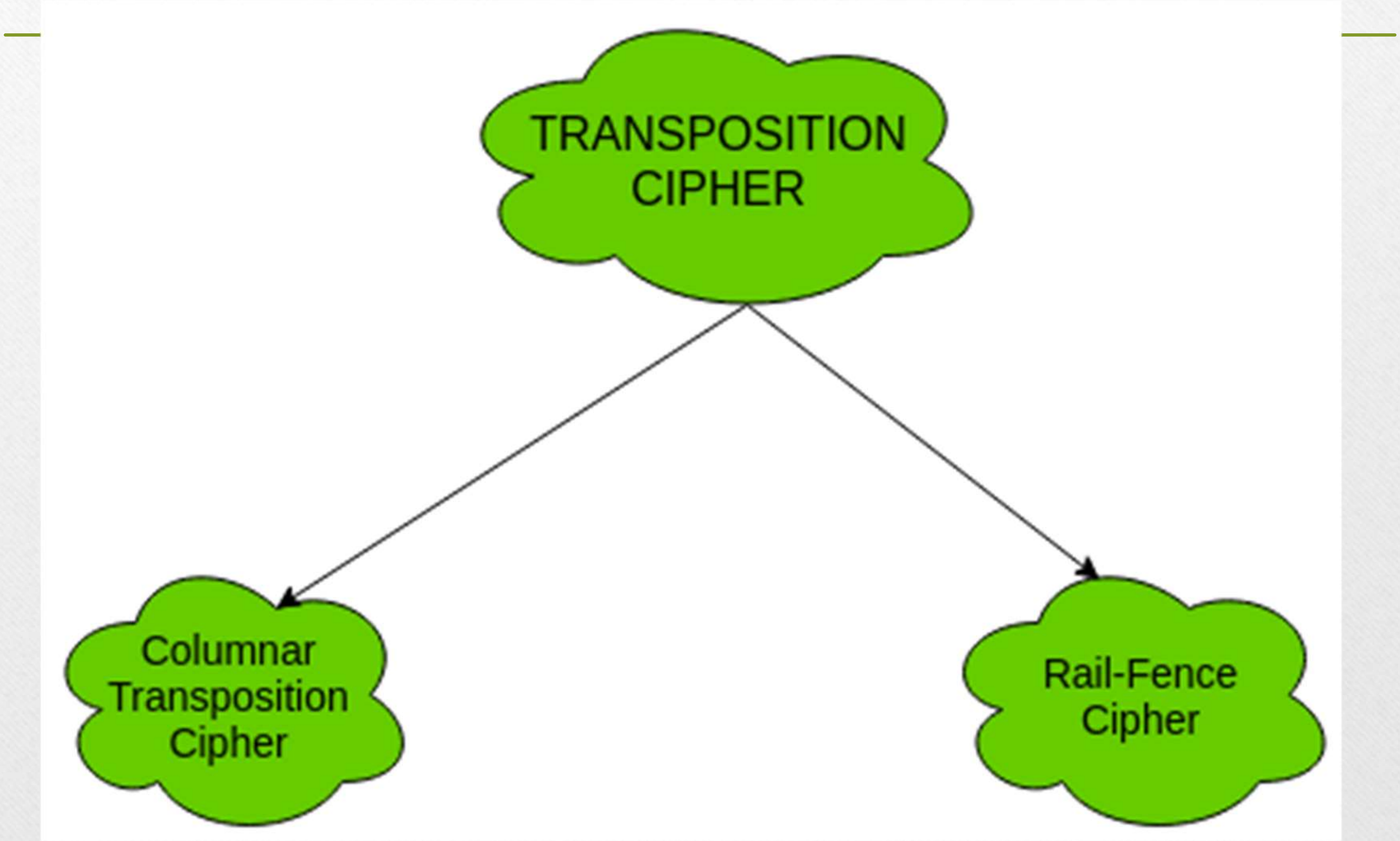
Hill Cipher

One Time Pad

Rotor Cipher

Transposition Cipher

The transposition cipher does not deal with substitution of one symbol with another. It focuses on changing the position of the symbol in the plain-text. A symbol in the first position in plain-text may occur in fifth position in cipher-text.


TRANSPOSITION CIPHER

Columnar Transposition Cipher

Rail-Fence Cipher

CRYPTOGRAPHY 1

Fourth Lecture –

Modern Cryptography

Assistant Professor Dr.

Sufyan Salim Mahmood

2024 - 2025

Introduction

- The most common method for securing data transmissions in web applications or computer science projects is modern Cryptography.
- It is like a secret code language that helps to keep information safe.

Cryptography Algorithms

- Cryptographic algorithms are classified in various respects. For the basis of the current review, the keys used for encryption and decryption will be classified :
- Symmetric cryptography
- Asymmetric cryptography

Symmetric Cryptography

Symmetrical encryption allows the content of material to be encrypted where the recipient and sender both use the same secret key.

Symmetric cryptography

This type of algorithms uses the same key for encryption and decryption process. The sender has a specific key to encrypt the plain-text and the receiver relates the same key to decrypt the message.

This key must save secretly

Symmetric cryptography

A symmetric key encryption scheme ensures confidentiality when two sides communicate, sending and receiving. They meet on a specific key to establish a safe communication.

Encrypted of a plain-text is performed by the sender to compute ciphertext that is sent to the receiver.

Symmetric cryptography

By using the symmetric key encryption, each pair of the users who need to exchange the data must have two instances of the identical key.

Symmetric cryptography

If 10 people expect the symmetrical keys to be used to interact safely, 45 keys should be kept informed.

Then, there will be 4,950 keys if 100 persons are to interact.

Symmetric cryptography

In order to verify the number of the symmetric keys required, the mathematical statement is n (n–1)/2.

The safeguard key is the basis for the symmetrical encryption technique

Symmetric cryptography

Stream and block ciphers can be classified as the main parts of the symmetric algorithms.

Stream ciphers encode one bit of plain-text at a moment. Block ciphers encrypt amount of bits in one piece(such as 64 bit).

Symmetric cryptography

The symmetrical encoding algorithms Blowfish, AES, DES, RC5, and RC6 are popular examples

Symmetric cryptography

- Symmetric encryption provides several benefits, including:
- Security: Symmetric encryption provides strong security for data, as the same key is used for both encryption and decryption.
- This makes it difficult for unauthorised users to access the data.

Symmetric cryptography

- Speed: Symmetric encryption is generally faster than other types of encryption, as the same key is used for both encryption and decryption. This makes it a good choice for applications that require fast data encryption and decryption.

Symmetric cryptography

- Efficiency: Symmetric encryption requires less processing power and resources to encrypt and decrypt data, which can save time and money.

Symmetric cryptography

- Simplicity: Symmetric encryption is easy to implement and use, as it only requires a single key for both encryption and decryption.
- This makes it a popular choice for applications that require simple and straightforward encryption.

Symmetric cryptography

- Compatibility: Symmetric encryption is widely used and supported by most software and hardware platforms, making it compatible with a wide range of systems and devices.
- This means that it can be easily integrated into existing applications and systems without requiring major modifications.

Symmetric cryptography

- However, the downside of symmetric encryption is that it can be less secure than asymmetric encryption. If the key falls into the wrong hands, the data can be compromised.
- Therefore, it is important to ensure that the key is kept secure and only shared with authorised users.