

AUTHENTICATION USING CAESAR CIPHER WITH RANDOMLY GENERATED KEY

MINI PROJECT: -
Department: -CSE(AI)

Under the guidance of :
Dr. M.Chandran
Dr.g.soniypriyatharshini

GROUP MEMBERS:-

201211101051 - Y. Rajesh
201211101027 - K. Bhaskar
201211101029 - K.Audi Dinakar

CONTENTS

☐ Introduction

☐ Abstract

☐ Literature survey

☐ Existing System

☐ Proposed System

☐ Conclusion

ABSTRACT

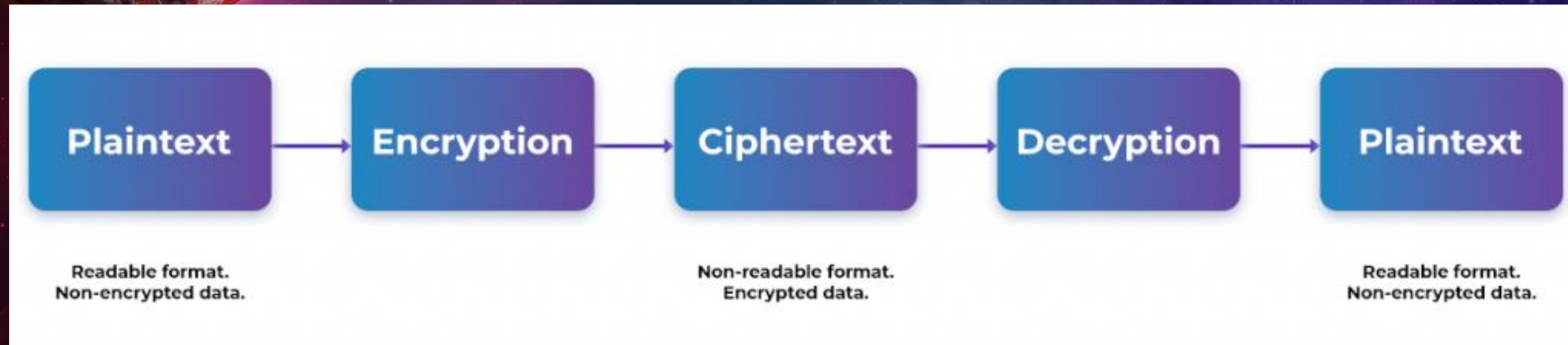
- ❖ Cryptography helps us to maintain the encryption of data.
- ❖ Fundamentally, there are two types of cryptographic techniques Symmetric and Asymmetric.
- ❖ This project gives us that what is symmetric and asymmetric cryptography and what are the benefits and Caesar cipher technique
- ❖ Caesar ciphers use a substitution method where letters in the alphabet are shifted by some fixed number of spaces to yield an encoding alphabet.

INTRODUCTION

- It is the art of secret writing Cryptography is the creativity of translating the original plain text in to cipher text and vice versa.
- Cryptography plays a vital role in security aspect. It provides many security goals to make sure the secrecy of data.
- The Caesar cipher is a historic encryption method that involves shifting each letter of a message a certain number of positions to the right or left of the alphabet.
- The key to the cipher is the number of positions that the letters are shifted.
- Encryption at the sending end and decryption at the receiving end of the communication system are required for secure communication.

CRYPTOGRAPHY:

Cryptography is the science of encrypting and decryption data to prevent unauthorized access. Encryption converts data from plaintext to Ciphertext. Decryption reverses the process of encryption to retrieve the original information.



It is of two types:

- Symmetric key cryptography.
- Asymmetric key cryptography.

Symmetric Key Cryptography:

Symmetric Key Cryptography relies on a single key for encryption and decryption of information. The key needs to be kept secret and be available with both the sender and receiver. Strength of encryption depends on the key size being used.

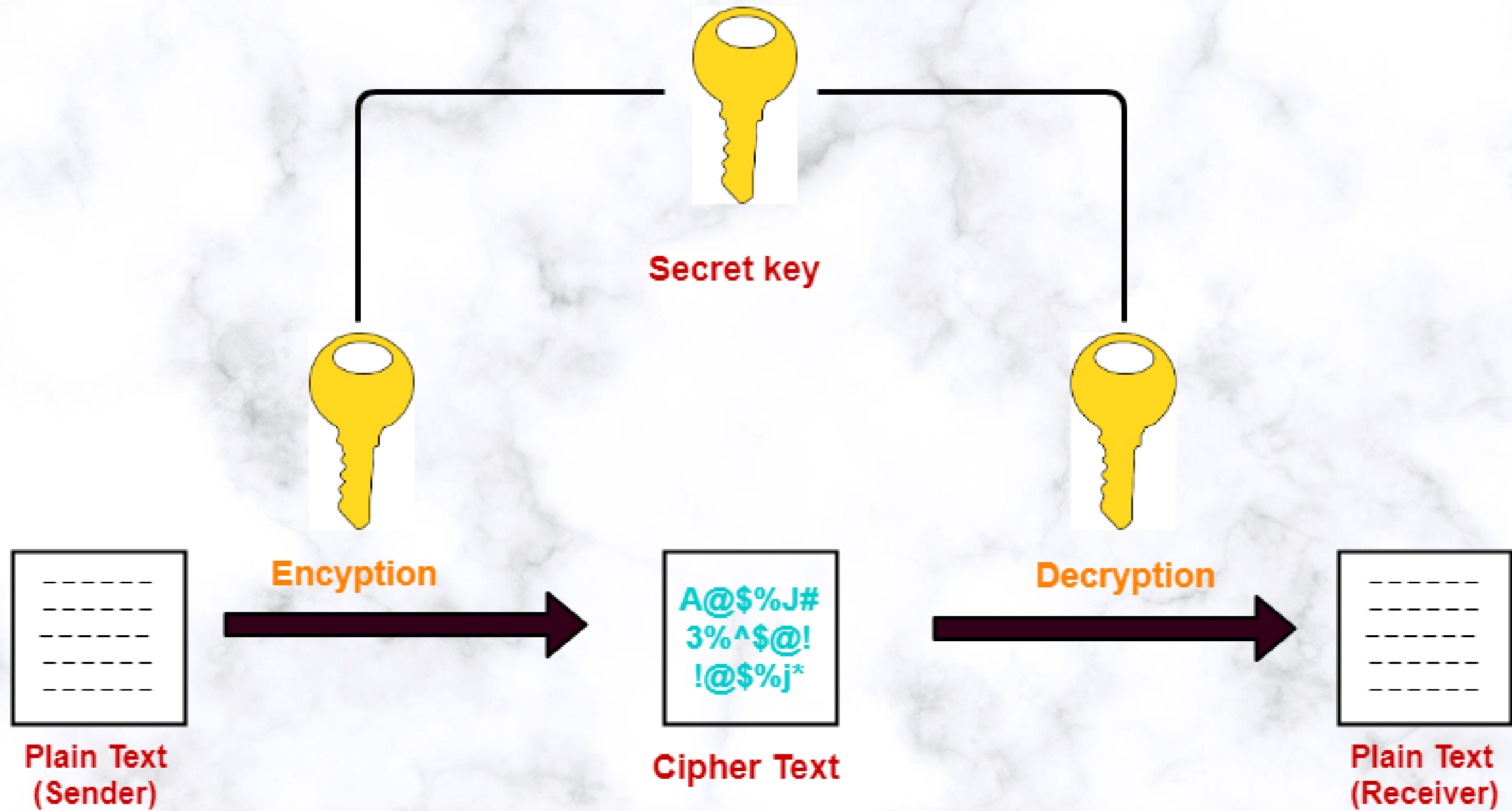
Types:

Stream Cipher:

- Encrypt information one bit/byte at time.
- Quicker format of encryption.
- Data is converted to binary digits and encrypted sequentially.
- Popular algorithms - RC4, Salsa20.

Block Cipher:

- Information broken down to chunks/blocks of fixed size.
- Size of block depends on key size.
- The chunks are encrypted and later chained together.
- Popular algorithms - AES, DES, 3DES.



Symmetric Key Cryptography

Asymmetric key cryptography.

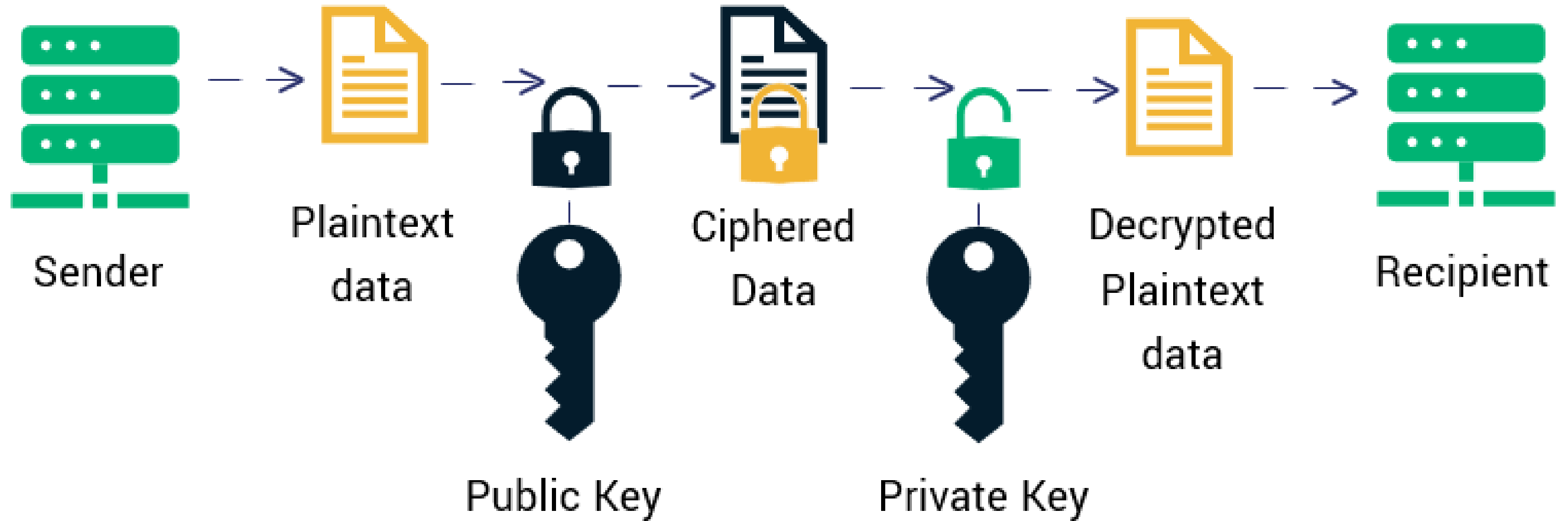
Asymmetric Key Cryptography uses two different keys for encryption and decryption. The key used for encryption is the public key, and the key used for decryption is the private key.

Applications:

- Digital Signatures to maintain authenticity of documents.
- Managing Crypto-currency transactions securely.
- Encrypted browsing sessions for better protection against hackers



Asymmetric Encryption



LITERATURE SURVEY

TITLE OF THE PAPER	AUTHOR NAME	OBJECTIVE	RESULTS	YEAR
A research Paper for Symmetric and Asymmetric Cryptography	Akshay Kekunnaya, Rajeshwari Gundla, Siddharth Nanda	what is use of cryptography and where and when to use cryptography.	We have learned the type of cryptography that is symmetric and asymmetric cryptography. Cryptography is used to ensure that the message sent by the people is secured or not.	2019
A study on symmetric and asymmetric key encryption algorithms.	S.Suguna, Dr.V.Dhanakoti, R. Manjupriya	study of symmetric and Asymmetric key encryption algorithm like AES, DES, TRIPLE DES,	This paper tells about the study of symmetric and Asymmetric key encryption algorithm like AES, DES, TRIPLE DES, RC4, Multiphase encryption, RSA, Elgamal cryptosystem, Digital signature and Diffie Hellman.	2020
Comparison study of symmetric key and asymmetric key algorithm	Priasnyomo Prima Santoso, Elkin Rilvani, Ahmad Budi Trisnawan , Krisna Adiyarta, Darmawan Napitupulu, Tata Sutabri , Robbi Rahim	This study aims to conduct a review literature on the development of cryptographic algorithms and its application so that it can be known comparison cryptographic algorithm	This section discusses various key symmetric cryptographic algorithms and asymmetric keys from several related literature review article	2022

EXISTING SYSTEM

- 1.Vulnerable to Brute Force Attack
- 2.Lack of Security
- 3.Limited Key Space
- 4.Not Suitable for Modern Communication
- 5.Inability to Encrypt Numbers and Symbols
- 6.Languages

PROPOSED SYSTEM

1. In proposed system increased number of possible keys more than 100 and it is secure against brute force attacks. As it is not possible to decode the message.
2. Now Caesar-cipher is very fast and efficient, both in terms of encryption and decryption.
3. Increased the key space of Caesar-cipher to large size with more than 100 possible shift values. Along with combination of alphabets, numbers, special characters and symbols as the shift values.
4. Include many different types of languages such as English, French, German, Italian, Portuguese, Spanish and Swedish used to encrypt and decrypt the message.
5. Increased more secure and reliable communication between sender and receiver

ALGORITHMS USED

- **Advanced Encryption Standard (AES):** AES is a symmetric encryption algorithm that is widely used for securing data. It is a block cipher algorithm that uses a 128-bit block size and key sizes of 128, 192, or 256 bits.
- **RSA:** RSA is an asymmetric encryption algorithm that is widely used for secure communication, digital signatures, and key exchange.
- **Vigenère cipher:** The Vigenère cipher is a polyalphabetic substitution cipher that involves shifting each character by a different amount, depending on a secret keyword.
- **Playfair cipher:** The Playfair cipher is a polygraphic substitution cipher that involves encrypting pairs of characters instead of single characters.
- **Diffie-Hellman algorithm:** it is a public-key cryptography algorithm used for secure key exchange between two parties over an insecure channel.

OUTPUT

#Encoding message


Caesar Cipher Tool


The current moon phase for today is the Waning Crescent phase. On this day, the moon is 24.11 days old and 36.67% illuminated with a tilt of -16.036°. The approximate distance from Earth to the moon is 369,405.40 km and the moon sign is Capricorn. The Moon phase for today is a Waning Crescent phase.

Copy

Paste

Text Options...

 8

 English

Decode

Encode

Auto Solve (without key)

Instructions

Auto Solve Options

Max Results

Spacing Mode

10

Automatic

Results

Encoded message

```
,pm!k.zzmV,!uwwv!xpi m!nwz!,wli`!q !,pm![ivqvo!Kzm kmv,!xpi m#!Wv!,pq !li`@!,pm!uwwv!q !0B#99!li`  
!wtl!ivl!AD#DE}!qtt.uqvi,mll[q,p!i!,qt,!wn!F9D#HAD°#!,pm!ixxzw]qui,m!lq ,ivkm!nzwu!Miz,p!,w!,pm!uwwv!q  
!ADG@BHC#BH!su!ivl!,pm!uwwv! qov!q !Kixzqkwzv#!,pm!Uwwv!xpi m!nwz!,wli`!q !i![ivqvo!Kzm kmv,!xpi m#
```

Copy

Text Options...

#Decoding Message


Caesar Cipher Tool


,pm!k.zzmV,!uwwv!xpi m!nwz!,wli`!q !,pm![ivqvo!Kzm kmv,!xpi m#!Wv!,pq !li`@!,pm!uwwv!q !0B#99!li`
!wtl!ivl!AD#DE}!qtt.uqvi,m!l[q,p!i!,qt,!wn!F9D#HAD°#!,pm!ixxzw]qui,m!lq ,ivkm!nzwu!Miz,p!,w!,pm!uwwv!q
!ADG@BHC#BH!su!ivl!,pm!uwwv! qov!q !Kixzqkwzv#!,pm!Uwwv!xpi m!nwz!,wli`!q !i![ivqvo!Kzm kmv,!xpi m#

Copy

Paste

Text Options...

 8

 English

Decode

Encode

Auto Solve (without key)

Instructions

Auto Solve Options

Max Results

Spacing Mode

10

Automatic

Results

Decoded message.

The cUrrEnT moon phaSe for TodaY iS The Waning CreScenT phaSe. On ThiS daY, The moon iS 24.11 daYS old and 36.67% illUminatEd WiTh a Tilt of 816.036°. The appRoXimaTe diStance from EarTh To The moon iS 369,405.40 km and The moon Sign iS Capricorn. The Moon phaSe for TodaY iS a Waning CreScenT phaSe.

Copy

Text Options...

CONCLUSION

- Security plays a major role in wireless type of medium because when we transmit our data wirelessly, it can be access by the third party or an outsider. Cryptography plays an important role for safe transmission of data. Data is encrypted and decrypted by many techniques. Caesar cipher is important technique which has less complex, limited power consumption and less memory consumption. Many advancement is done in Caesar cipher to make it more secure. Delta formation Caesar cipher and XOR Caesar cipher are the example of advanced Caesar cipher. Main factor which effect the Caesar cipher is brute force attack. Attacker tries all the possible set of key to recover the data. But the new techniques have substitution in key which make the Caesar cipher more secure.

