CryptoLib

Encryption and Decryption in JavaScript. : Base64,AES and RSA

PROJECT 4B

Team Members

Lahasya Kakkadde Rajanna

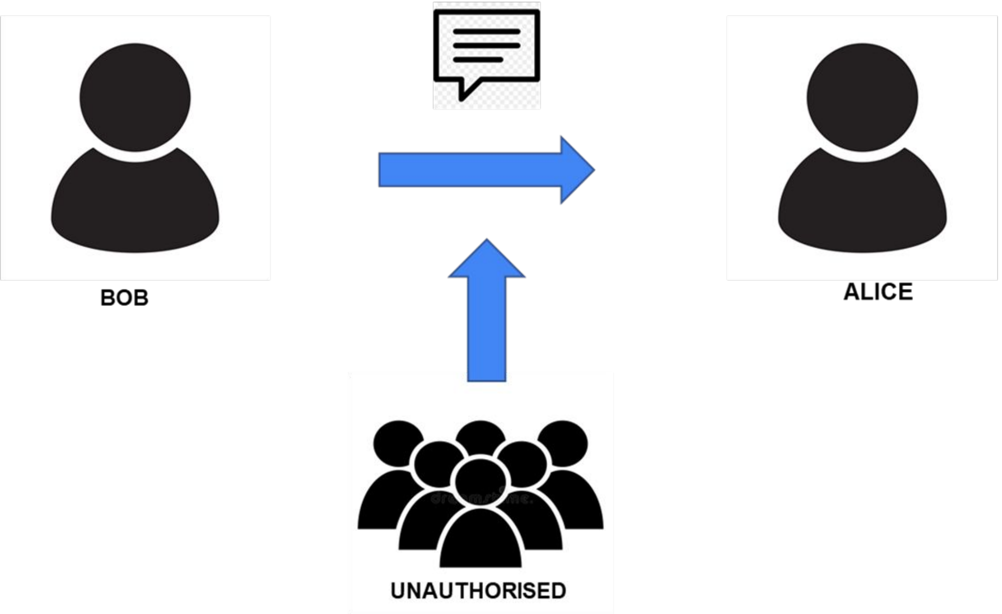
Samyak Gangwal

Sneha Babuji

Introduction

- Project is a standalone JavaScript library that can be used in a JavaScript SDK of Atsign.
- Main function of this library is to encrypt and decrypt the string.
- Algorithms used:
  - Base64 Encode and Decode
  - AES Encryption and Decryption
  - RSA Encryption and Decryption
- Unit Test Cases are also included for each of the functions.
- Link to project repository - https://github.com/Lahasyakr/CS682-Project4b

Data Security Breach



BOB

ALICE

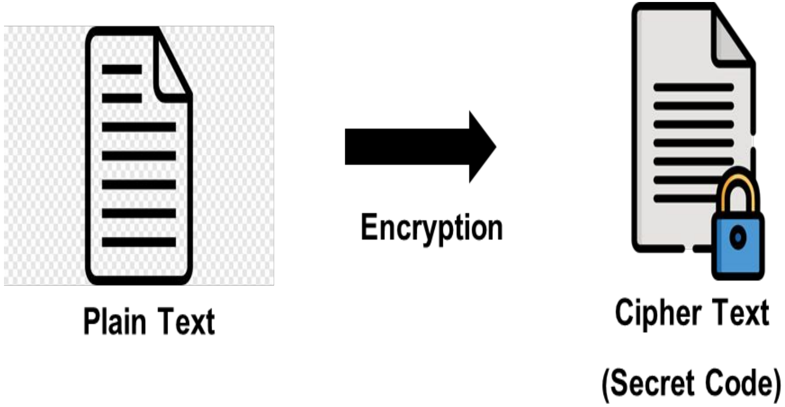
UNAUTHORISED

How do we protect sensitive information from unauthorized access?

What is Encryption and Decryption?

Encryption and Decryption

- **Encryption** is the process of converting the plain text to cipher text in order to prevent unauthorized access



Plain Text

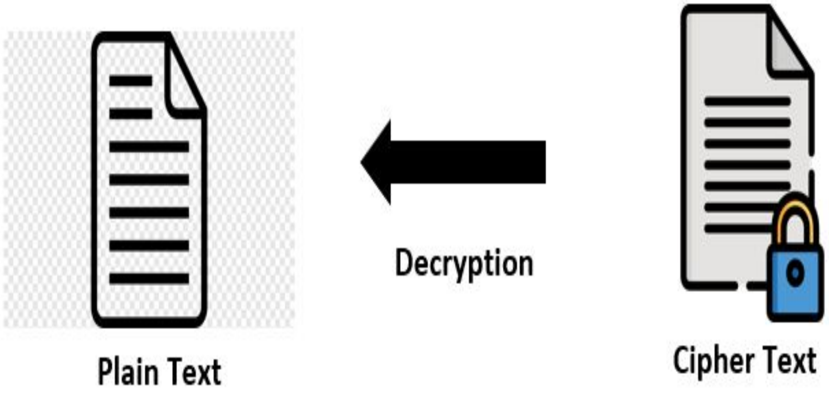
Encryption

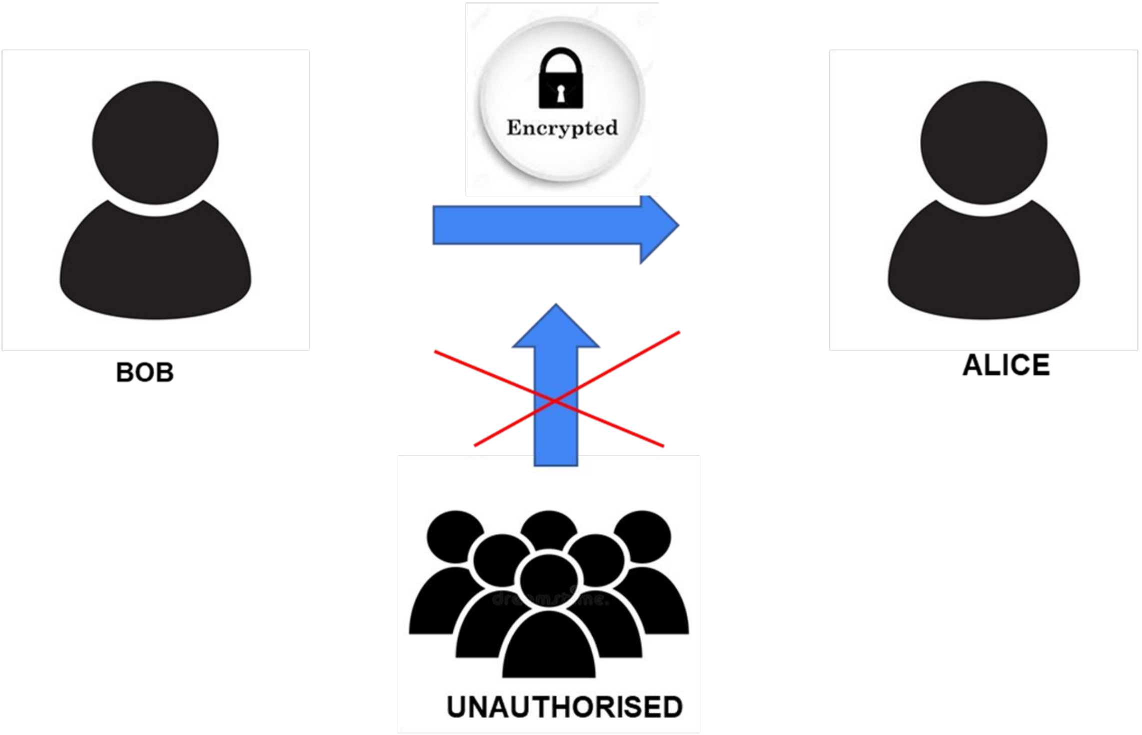
Cipher Text

(Secret Code)

Encryption and Decryption

- **Decryption** is a process of converting ciphertext back to the plaintext.





Encrypted

BOB

ALICE

UNAUTHORISED

Types of Encryption

Public Key

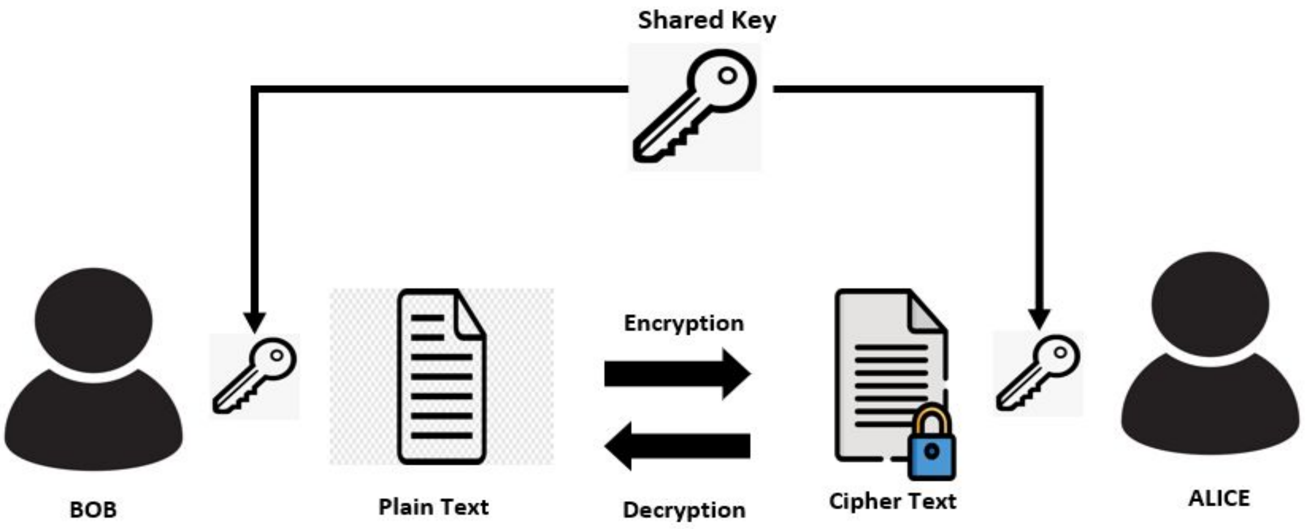
Shared Key

Private Key

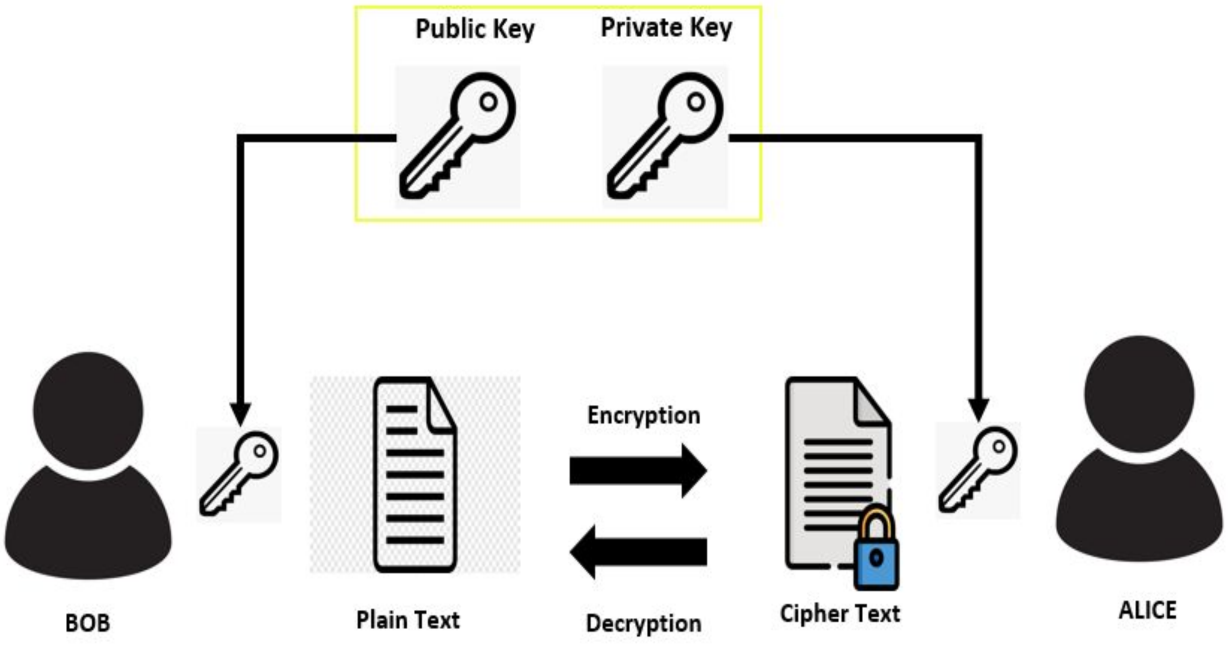
Symmetric Encryption

Asymmetric Encryption

Symmetric Encryption

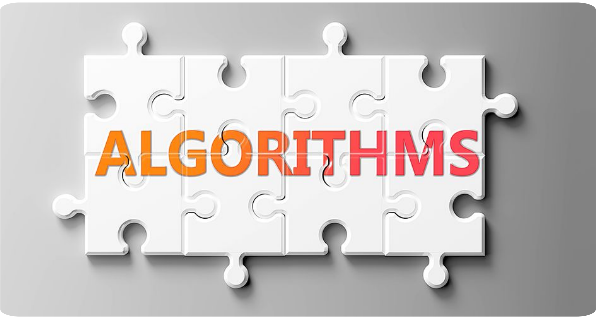


Asymmetric Encryption



Algorithms used

- We worked with RSA, AES-CTR, Base64.
- RSA: Asymmetric algorithm used for encrypting messages for communication.
- AES: Symmetric algorithm used for encrypting objects.
- Base64: A binary to text encoding scheme used to transfer data over the internet.



Use in Atsign

- Atsign’s protocol uses RSA keys as its main keys for generating atSigns and other communication.
- The public key and private keys are all encrypted using AES algorithm.
- The AES key and the other keys are all Base64 encoded.

Challenges we faced.

- Task decomposition
- Environment setups.
- First time working with mocha and chai
- Writing test cases for RSA Encryption can be challenging due to the variability of the encrypted data output.

Lessons Learned.

- Our exposure to Node.js gave us valuable experience in this technology.
- Effective Collaboration.
- Testing is critical.
- Encryption is a crucial aspect of securing data.

Thank you