

# Cryptosystem App Documentation

## Overview

You can use the app to make your messages secret by changing them with a code. You can use either a code that uses the same key for both encryption and decryption (AES) or a code that uses different keys for encryption and decryption (RSA). The program has a user-friendly interface that's made using Swing, which makes it simple to do cryptographic stuff.

## Cryptographic Algorithms

**AES (Advanced Encryption Standard)** is a widely used encryption algorithm. Symmetric encryption is a type of encryption.

**Key sizes:** 128, 192, or 256 bits.

### Positive attributes:

- This is a very secure system with a key length that is appropriate for the level of security required.
- Quick and effective for extensive data.
- Accepted and commonly used.

### Weaknesses:

- Key management is super important, losing the key means you lose access to data.
- Everybody needs to keep the key safe and share it with each other.

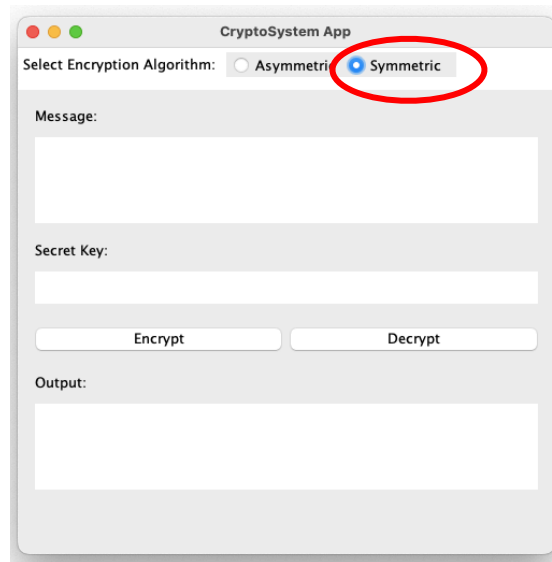
**RSA (Rivest-Shamir-Adleman)** is a widely used public-key encryption algorithm.

- Asymmetric encryption is a type of encryption.
- The length of a key is usually 2048 bits or more.
- Positive attributes:
  1. Ensure safety with extensive key lengths.
  2. The public key can be freely shared, but the private key is kept a secret. is a method of ensuring digital signatures and secure key exchange.
  3. The main drawbacks of asymmetric encryption are that its computationally expensive and slower than symmetric encryption.
  4. Generating and managing keys is more intricate.

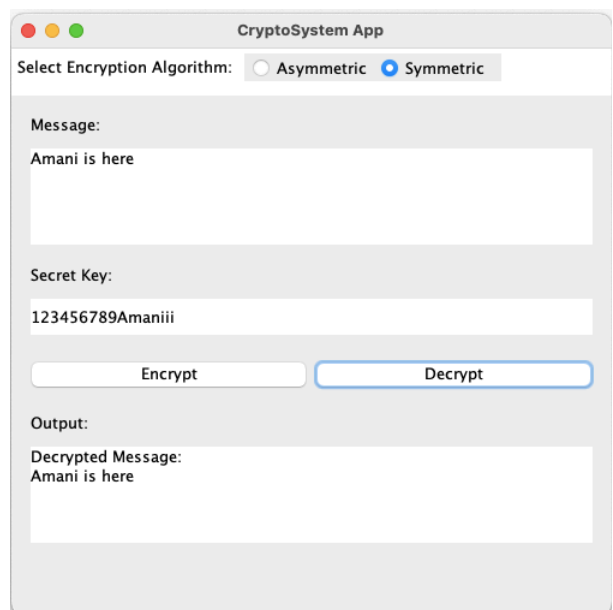
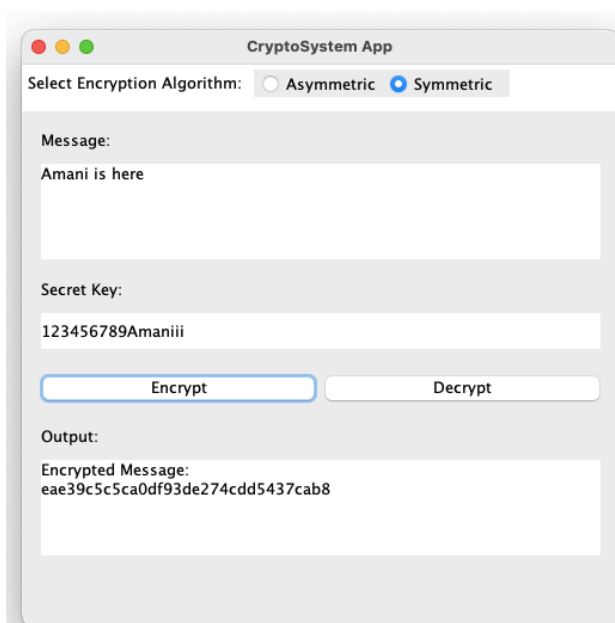
# How to Use cryptoSystem App

## Using Symmetric Encryption (AES)

1. Choose Encryption Method: Make sure the "Symmetric" option is selected.

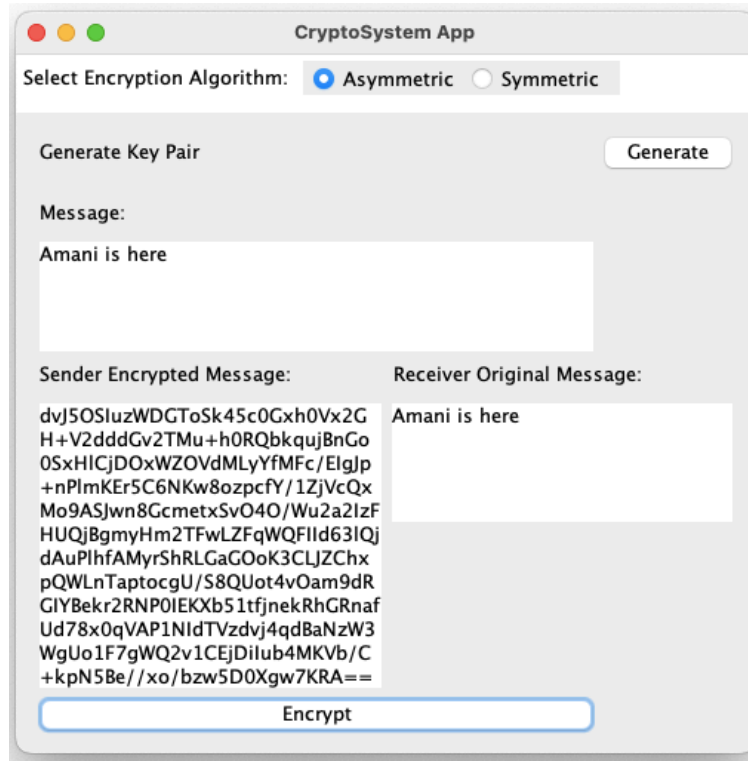


2. Enter Message: Put the message you want to encrypt in the "Message" box.
3. Enter Secret Key: Type in a secret key in the "Secret Key" field. The password should be 16, 24, or 32 characters long.
4. Encrypt: Click the "Encrypt" button. The encoded message will be shown in the "Output" section.
5. To decrypt an encrypted message, just put it in the "Output" area, make sure the right key is in the "Secret Key" field, and then click the "Decrypt" button. The decrypted message will be shown in the "Output" section.



## Using Asymmetric Encryption (RSA)

1. Choose Encryption Method: Make sure the "Asymmetric" option is selected.
2. Click the "Generate" button to make a new RSA key pair.
3. Enter Message: Put the message you want to encrypt in the "Message" text box.
4. Encrypt: Click the "Encrypt" button. The message will be shown in the "Sender Encrypted Message" section.
5. If you manage to decrypt the message, it will show up in the "Receiver Original Message" section.



The screenshot shows a macOS-style window titled "CryptoSystem App". At the top, there's a "Select Encryption Algorithm:" section with two radio buttons: "Asymmetric" (which is selected) and "Symmetric". Below this is a "Generate Key Pair" section with a "Generate" button. Underneath is a "Message:" label followed by a text input box containing "Amani is here". The bottom half of the window is divided into two columns. The left column is labeled "Sender Encrypted Message:" and contains a long, multi-line base64-encoded string. The right column is labeled "Receiver Original Message:" and contains the text "Amani is here". At the very bottom, there is a wide "Encrypt" button.

CryptoSystem App

Select Encryption Algorithm: ☒ Asymmetric ☐ Symmetric

Generate Key Pair Generate

Message:  
Amani is here

Sender Encrypted Message: Receiver Original Message:

dvj5OSIuzWDGToSk45c0Gxh0Vx2G  
H+V2dddGv2TMu+h0RQbkqujBnGo  
0SxHICjDOxWZOvMLyYfMFc/ElgJp  
+nPlmKEr5C6NKw8ozpcfY/1ZjVcQx  
Mo9ASJwn8GcmetxSvO4O/Wu2a2IzF  
HUQjBgmyHm2TFwLZFqWQFIld63IQj  
dAuPlhfAMyrShRLGaGOoK3CLJZChx  
pQWLnTaptocgU/S8QUot4vOam9dR  
GIYBekr2RNP0IEKXb51tfjnekrRhGRnaf  
Ud78x0qVAP1NIdTVzdvj4qdBaNzW3  
WgUo1F7gWQ2v1CEjDilub4MKVb/C  
+kpN5Be//xo/bzw5D0Xgw7KRA==

Encrypt

# Detailed Steps for Using the App

## Symmetric Encryption (AES)

- Choosing an Algorithm: Make sure the "Symmetric" radio button is chosen at the top of the window.
- Input Message: Please enter your plaintext message in the "Message" text field.
- Key Input: Enter a secret key in the "Secret Key" field. The key length can be one of these: 16, 24, or 32 characters.
- Encryption: Click the "Encrypt" button. The message will be shown in the "Output" area, with "Encrypted Message:" at the beginning.
- To decrypt, make sure the encrypted message is in the "Output" area, remove the "Encrypted Message:" prefix, enter the same key used for encryption in the "Secret Key" field, and click "Decrypt". The initial message will be shown.

## Asymmetric Encryption (RSA)

- Choosing an Algorithm: Make sure the "Asymmetric" radio button is chosen at the top of the window.
- Generating Key Pairs: Click the "Generate" button to make an RSA key pair. An acknowledgement message will be displayed.
- Input Message: Please enter your message in the "Message" text box.
- Encryption: Click the "Encrypt" button.
- The message will be shown in the "Sender Encrypted Message" section.
- Decryption: The decrypted message will show up in the "Receiver Original Message" area if you have the private key.

## Error Handling

- Key Length: If you enter the wrong key length, a message will pop up asking you to enter a key that's 16, 24, or 32 characters long.
- The message field is empty, so a message box will ask you to type a message.
- The message box will ask you to create an RSA key pair if you don't have one before encrypting.

## Summary

CryptoSystem App lets you encrypt and decrypt stuff using two different methods: one that uses the same key for both, and one that uses different keys for each. You can use it to keep your data safe from hackers. The user interface is easy to use, so you can manage your cryptographic operations easily. And the encryption and decryption processes are secure because of the strong AES and RSA implementation.