

User Manual for Encryption and Decryption Application

Introduction

This application allows users to encrypt and decrypt messages using four encryption algorithms: AES 256 CBC, AES 256 GCM, One Time Pad, and ChaCha20-Poly1305. It accepts two 256-bit keys in base64 format and provides an interface for users to enter plaintext messages, encrypt them, and decrypt encrypted messages.

Getting Started

The screenshot shows a window titled "Encryption Methods" with a standard Windows title bar (minimize, maximize, close buttons). The window contains several input fields and buttons. At the top, there are two text boxes for "QKD Keys (Base64)". The first is labeled "QKD Key 1(Base64)" and contains the text "k5ifalkYINhtnZV/ailYy6konhEcK18/YOh7hgT9YHg=". The second is labeled "QKD Key 2(Base64)" and contains "wBEvA+Zn6chnngfnkdAYc0By7seBGRgDFxFmF07qRkfw=". Below these is a "Plain Tex" label followed by a text area containing "Antonis". Underneath is a section titled "Encryption Algorithms" which contains four rows, each with a label, a "Clear" button, and a text area. The first row is "AES-256 CBC Encrypted (Base64)" with the text "0uEgEKaFKW2VldptmEI16g==". The second row is "AES-GCM Encrypted (Base64)" with the text "wBEvA+Zn6chnngfnko02pJQypIfp7OorQjQbZVtmihAlQZ9o=". The third row is "One Time Pad Encrypted (Hex)" with the text "DC-AA-75-0B-51-05-55". The fourth row is "ChaCha20-Poly1305 (Base64)" with the text "mLrKZyFNFOV9LdQr4sCoYvZfYAGSZIM=". At the bottom of the window are three buttons: "Encrypt", "Decrypt", and "Exit". The "Encrypt" button is highlighted with a blue border.

Inputs

1. **Keys:** The application requires two 256-bit keys in base64 format. These keys are referred to as QKD Key 1 and QKD Key 2.
2. **Message:** Users can enter a message they wish to encrypt in the provided plaintext textarea.

Interface

- **Plaintext Textarea:** Enter the message you want to encrypt here.
- **Encrypt Button:** Press this button to encrypt your message.
- **Decrypt Button:** If you have an encrypted message and the corresponding keys, use this button to decrypt the message.

Encryption Process

1. Entering Keys and Message:

- Enter the two 256-bit keys in base64 format (QKD Key 1 and QKD Key 2).
- Type your message into the plaintext textarea.

2. Encrypting the Message:

- After entering the keys and message, press the **Encrypt** button.
- The application will encrypt the message using the following four algorithms:
 - AES 256 CBC
 - AES 256 GCM
 - One Time Pad
 - ChaCha20-Poly1305

3. Viewing Encrypted Message:

- The encrypted message will be displayed in the designated area for each encryption algorithm.

Decryption Process

The screenshot shows a window titled "Encryption Methods" with a standard Windows title bar (minimize, maximize, close buttons). The window contains several input fields and buttons. At the top, there are two text boxes for "QKD Keys (Base64)": "QKD Key 1(Base64)" contains "k5ifalkYINhtnZV/ailYy6konhEck18/YOh7hgT9YHg=" and "QKD Key 2(Base64)" contains "wBEvA+Zn6chnngfnkdAYc0By7seBGRgDFxFmF07qRkfw=". Below these is a "Plain Tex" label and a text area containing "Antonis". Underneath is a section titled "Encryption Algorithms" with four rows, each containing a label, a "Clear" button, and a text area. The first row is "AES-256 CBC Encrypted (Base64)" with an empty text area. The second row is "AES-GCM Encrypted (Base64)" with an empty text area. The third row is "One Time Pad Encrypted (Hex)" with the text "DC-AA-75-0B-51-05-55". The fourth row is "ChaCha20-Poly1305 (Base64)" with an empty text area. At the bottom of the window are three buttons: "Encrypt", "Decrypt" (which is highlighted with a blue border), and "Exit".

1. Entering Encrypted Message and Keys:

- If you have an encrypted message and the corresponding encryption keys, enter them into the respective fields.

2. Decrypting the Message:

- Press the **Decrypt** button.
- The application will decrypt the message and display the plaintext.