Number Theory and Cryptography Final Project

Perform AES Encryption and Decryption on Website

Dachuan Chen 10828241

Department of Electrical Engineering Chung Yuan Christian University January 4, 2023

Contents

1	Development Environment	3
2	Develop Process	4
3	Website Introduction	5
	3.1 Functionality	5
	3.2 How to Use	5

List of Figures

2.1	VScode Screenshot
3.1	Website Screenshot
3.2	Key Expansion Section Screenshot
3.3	Encryption Section Screenshot
3.4	Decryption Section Screenshot
3.5	Key Expansion Result Screenshot
3.6	Encryption Result Screenshot 1
3.7	Encryption Result Screenshot 2
	Decryption Result Screenshot 1
3.9	Decryption Result Screenshot 2

Chapter 1

Development Environment

• Operating System: Windows 11

• Web Server: Firebase Hosting

• Web Browser: Firefox 108.0.1

• IDE: Visual Studio Code 1.74.2

• Code Management: Git 2.39.0

• Programming Language: Node.js v18.12.1, HTML, CSS, JavaScript

• JS Library: Firebase v9.2.0

Chapter 2

Develop Process

- Step 1: Test AES Encryption and Decryption on Node.js (Figure 2.1).
- Step 2: Migrate the code to Firebase Hosting files.
- Step 3: Adjust HTML, CSS and test the website functionalities.

All the source code can be found in my GitHub Repository. The source code is written in Node.js and the website is hosted on Firebase Hosting.

Link to the source code: https://github.com/belongtothenight/NTC_Code

Figure 2.1: VScode Screenshot

Chapter 3

Website Introduction

Link to the website: https://ntc-demo-296be.web.app/

3.1 Functionality

- **Key Expansion:** Generate the round keys from the original key.
- Encryption: Encrypt the plaintext with the round keys.
- Decryption: Decrypt the ciphertext with the round keys.

3.2 How to Use

- **Key Expansion:** Input the original key (Figure 3.2) and click the button "Generate Expanded Key" to generate the round keys (Figure 3.5).
- Encryption: Input the plaintext (Figure 3.3) and click the button "Encrypt" to encrypt the plaintext (Figure 3.6 3.7).
- **Decryption:** Input the ciphertext (Figure 3.4) and click the button "Decrypt" to decrypt the ciphertext (Figure 3.8 -3.9).

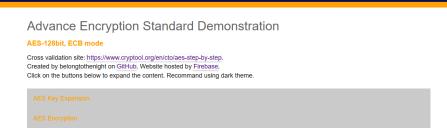


Figure 3.1: Website Screenshot



Figure 3.2: Key Expansion Section Screenshot



Figure 3.3: Encryption Section Screenshot



Figure 3.4: Decryption Section Screenshot

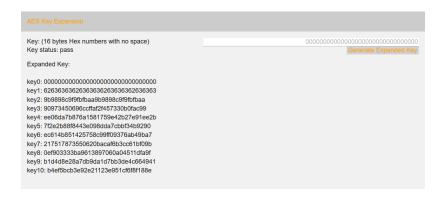


Figure 3.5: Key Expansion Result Screenshot

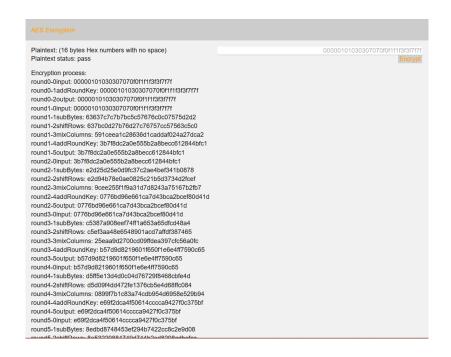


Figure 3.6: Encryption Result Screenshot 1

```
round5-0input: e69f2dca4f50614cccca9427f0c375bf round5-1subBytes: 8edbd8748453ef294b7422cc8c2e9d08
round5-2shiftRows: 8e53220884749d744b2ed8298cdbefcd
round5-3mikColumns: d84681e866a44d96154db57956c7dd38
round5-4addRoundKey: a768aa609ee0739f9897c9c2a58c4fa8
round5-5output: a768aa609ee0739f9897c9c2a58c4fa8
round6-0input: a768aa609ee0739f9897c9c2a58c4fa8
round6-1subBvtes: 5c45acd00be18fdb4688dd25066484c2
round6-2shiftRows: 5ce1ddc20b8884d04664acdb06458f25
round6-3mixColumns: 9f3b4147c147fbaa57ba17af6923298a
round6-4addRoundKey: 735a0ac2d5628e26ce451e980397b22d
round6-5output: 735a0ac2d5628e26ce451e980397b22d
round7-0input: 735a0ac2d5628e26ce451e980397b22d
round7-1subBvtes: 8fbe672503aa19f78b6e72467b8837d8
round7-2shiftRows: 8faa72d8036e37258b8867f77bbe1946
round7-3mixColumns: 4a8eb2f9a6a36c161edecf9c70713da6
round7-4addRoundKey: 6bfba57e93f30e1db271a4a0b66acd3d
round7-5output: 6bfba57e93f30e1db271a4a0b66acd3d
round8-0input: 6bfba57e93f30e1db271a4a0b66acd3d
round8-1subBytes: 7f0f06f3dc0daba437a349e04e02bd27 round8-2shiftRows: 7f0d4927dca3bdf3370206a44e0fabe0
round8-3mixColumns: 8799898b13ae109cca9dce0ec65637ad
round8-4addRoundKey: 89608ab8280771a45d9bc40a974bcd32
round8-5output: 89608ab8280771a45d9bc40a974bcd32
round9-0input: 89608ab8280771a45d9bc40a974bcd32
round9-1subBytes: a7d07e6c34c5a3494c141c6788b3bd23
round9-2shiftRows: a7c51c233414bd6c4cb37e4988d0a367
round9-3mixColumns: 3e313f6d85acf52d61fad88ba4aaac3e
round9-4addRoundKey: 8fe5e78f0fd14cf77c816b55e8cce57f
round9-5output: 8fe5e78f0fd14cf77c816b55e8cce57f
round10-0input: 8fe5e78f0fd14cf77c816b55e8cce57f
round10-1subBytes: 73d99473763e2968100c7ffc9b4bd9d2
round10-2shiftRows: 733e7fd2760cd973104b94689bd929fc
round10-3addRoundKey: c7d12419489e3b6233a2c5a7f4563172
round10-4output: c7d12419489e3b6233a2c5a7f4563172
Generated Ciphertext: c7d12419489e3b6233a2c5a7f4563172
```

Figure 3.7: Encryption Result Screenshot 2

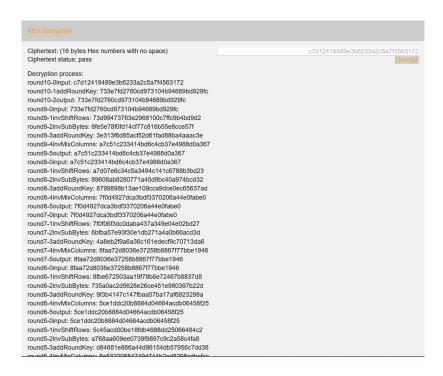


Figure 3.8: Decryption Result Screenshot 1

```
round5-0input: 5ce1ddc20b8884d04664acdb06458f25
round5-1invShiftRows: 5c45acd00be18fdb4688dd25066484c2
round5-2invSubBytes: a768aa609ee0739f9897c9c2a58c4fa8
round5-3addRoundKey: d84681e866a44d96154db57956c7dd38
round5-4invMixColumns: 8e53220884749d744b2ed8298cdbefcc
round5-5output: 8e53220884749d744b2ed8298cdbefcc
round4-0input: 8e53220884749d744b2ed8298cdbefcc
round4-1invShiftRows: 8edbd8748453ef294b7422cc8c2e9d08
round4-2invSubBytes: e69f2dca4f50614cccca9427f0c375bf round4-3addRoundKey: 0899f7b1c83a74cdb954d6958e529b94
round4-4invMixColumns: d5d09f4dd472fe1376cb5e4d68ffc084
round4-5output: d5d09f4dd472fe1376cb5e4d68ffc084
round3-0input: d5d09f4dd472fe1376cb5e4d68ffc084
round3-1invShiftRows: d5ff5e13d4d0c04d76729f8468cbfe4d
round3-2invSubBytes: b57d9d8219601f650f1e6e4ff7590c65
round3-3addRoundKey: 25eaa9d2700cd09ffdea397cfc56a0fc
round3-4inVMixColumns: c5ef3aa48e6548901acd7affdf387465
round3-5output: c5ef3aa48e6548901acd7affdf387465
round2-0input: c5ef3aa48e6548901acd7affdf387465
round2-1invShiftRows: c5387a908eef74ff1a653a65dfcd48a4
round2-2invSubBytes: 0776bd96e661ca7d43bca2bcef80d41d
round2-3addRoundKey: 9cee255f1f9a31d7d8243a75167b2fb7
round2-4invMixColumns: e2d94b78e0ae0825c21b5d3734d2fcef
round2-5output: e2d94b78e0ae0825c21b5d3734d2fcef
round1-0input; e2d94b78e0ae0825c21b5d3734d2fcef
round1-1invShiftRows: e2d25d25e0d9fc37c2ae4bef341b0878
round1-2invSubBytes: 3b7f8dc2a0e555b2a8becc612844bfc1
round1-3addRoundKey: 591ceea1c28636d1caddaf024a27dca2
round1-4invMixColumns: 637bc0d27b76d27c76757cc57563c5c0
round1-5output: 637bc0d27b76d27c76757cc57563c5c0
round0-0input: 637bc0d27b76d27c76757cc57563c5c0
round0-1invShiftRows: 63637c7c7b7bc5c57676c0c07575d2d2
round0-2invSubBvtes: 00000101030307070f0f1f1f3f3f7f7f
round0-3addRoundKey: 00000101030307070f0f1f1f3f3f7f7f
round0-4output: 00000101030307070f0f1f1f3f3f7f7f
Generated plaintext: 00000101030307070f0f1f1f3f3f7f7f
```

Figure 3.9: Decryption Result Screenshot 2