密码学实验二、 高级加密标准(AES)实验报告

班级 572221 学号 LK123425 姓名 黄睿扬

实验目的	1. 掌握 AES 结构，包括字节代换、行移位、列混合、密钥加、加解密； 2. 利用 C、C++、Java 实现 AES 算法
实验要求	1. 提交实验报告； 2. 提交实验代码
实验内容	1. 实现 AES 密钥扩展； 2. 实现 AES 加密； 3. 实现 AES 解密； 4. 展示实验结果
实验环境	系统：Windows 11 （64 位） 处理器：AMD Ryzen9 7945HX（16 核） IDE：Visual Studio 2022 语言：C++、C 语言 环境：MinGW
实验步骤	**一、代码部分** 1. AES 算法概述 AES 算法是一个基于块的加密算法，主要包括四个阶段：密钥扩展（Key Expansion）、初始轮（Initial Round）、重复轮（Rounds）和最终轮（Final Round）。每一轮的操作又包括若干子步骤，如 SubBytes（字节替换）、ShiftRows（行移位）、MixColumns（列混淆）和 AddRoundKey（轮密钥加）。通过这些操作，AES 能够将明文转化为无法识别的密文，确保信息的安全性。 2. 密钥扩展 密钥扩展是 AES 算法的一个关键部分，这个过程将初始密钥扩展成若干轮次所需的密钥。这一过程我在实验的 C++代码中通过 ScheduleKey 函数实现。ScheduleKey 函数采用原始密钥和目标扩展密钥数组作为输入，通过循环和条件判断逐步填充扩展密钥数组。在这个过程中，包含字循环、S 盒替换和轮常量加等操作，以此来确保密钥的多样性和安全性。 3. 加密过程 加密过程开始于一系列的准备工作，包括密钥扩展。随后，算法进入若干加密轮次，每一轮都包括 SubBytes、ShiftRows、MixColumns 和 AddRoundKey 四个步骤，除了最后一轮不执行

MixColumns 操作。在我的实验 C++代码中，这些步骤被分解为独立的函数，以 AesEncryplaintext 函数调用，从而完成整个加密流程。这种模块化的设计使得每个步骤的功能清晰、易于理解和维护。

4. 解密过程

解密过程是加密过程的逆过程，需要按照相反的顺序执行相反的操作。在我的实验 C++代码中，Contrary_AesEncryplaintext 函数承担这一任务。解密过程首先应用加密过程的最终轮密钥，然后逆向执行 ShiftRows、SubBytes 等操作，最终恢复出原始明文。其中，MixColumns 的逆操作（Contrary_MixColumns）和 S 盒的逆操作（逆 S 盒）是比较关键的步骤。

5. 用户交互

为了增强实验的互动性和用户体验，我在程序的 main 函数里加入了简单的命令行交互界面，允许用户选择加密、解密或退出程序。通过屏幕提示，用户可以方便地输入明文/密文和密钥，程序则根据用户的选择调用相应的加密或解密函数，并显示操作结果。这不仅使得 AES 算法的实现更加实用，也为用户提供了一个直观的方式来观察和理解 AES 加密和解密的过程。

二、实验部分

基于代码的可交互性，为了验证加密对任意字符的通用性，而保障解密时不会出现兼容性问题和乱码，我对程序进行了一些测试：

1. 纯数字明文测试

纯数字明文测试共两步：

（1） 选择加密（Encryption），并选择斐波那契数列作为输入明文数字串“1123581321345589”；选择数字串作为密钥“1234567890123456”。

（2） 选择解密（Decryption），并将上一步生成的密文输入，再输入密钥“1234567890123456”，得到解密后的明文，并与原明文比较，验证是否一致。

2. 纯文字明文测试

纯文字明文测试共四步：

（1） 选择加密（Encryption），并选择无大写的英文字符串作为输入明文字符串“woaidongnandaxue”；选择数字串作为密钥“1234567890123456”。

	（2） 选择解密（Decryption），并将上一步生成的密文输入，再输入密钥“1234567890123456”，得到解密后的明文，并与原明文比较，逐个验证字符是否一致。 （3） 选择加密（Encryption），并选择大小写交错的英文字符串作为输入明文字符串“WoAiDongNanDaXue”；选择数字串作为密钥“1234567890123456”。 （4） 选择解密（Decryption），并将上一步生成的密文输入，再输入密钥“1234567890123456”，得到解密后的明文，并与原明文比较，验证大小写是否保持一致。 3. 数字、文字、符号明文测试 由于前面已经对数字和大小写英文字符进行过测试，因此数字、文字、符号明文测试共只有两步： （1） 选择加密（Encryption），并选择数字、英文、符号交错的字符串作为输入明文字符串“IloveSEUsoMuch!!”；选择数字串作为密钥“1234567890123456”。 （2） 选择解密（Decryption），并将上一步生成的密文输入，再输入密钥“1234567890123456”，得到解密后的明文，并与原明文比较，逐个验证对应字符是否一致。 4. 纯数字密钥测试 纯数字密钥测试共两步： （1） 选择加密（Encryption），并选择数字、英文、符号交错的字符串作为输入明文字符串“CyberSecurity57!”；选择数字串作为密钥“1234567890123456”。 （2） 选择解密（Decryption），并将上一步生成的密文输入，再输入密钥“1234567890123456”，得到解密后的明文，并与原明文比较，验证是否一致。 5. 纯文字密钥测试 纯文字密钥测试共四步： （1） 选择加密（Encryption），并选择数字、英文、符号交错的字符串作为输入明文字符串“CyberSecurity57!”；选择英文字符串作为密钥“woaidongnandaxue”。 （2） 选择解密（Decryption），并将上一步生成的密文输入，再输入密钥“woaidongnandaxue”，得到解密后的明文，并与原明文比较，逐个验证字符是否一致。 （3） 选择加密（Encryption），并选择数字、英文、符号交错的字符串作为输入明文字符串“CyberSecurity57!”；选择数字串作为密钥“WoAiDongNanDaXue”。 （4） 选择解密（Decryption），并将上一步生成的密文输入，

	再输入密钥“WoAiDongNanDaXue”，得到解密后的明文，并与原明文比较，验证大小写是否保持一致。 6. 数字、文字、符号密钥测试 由于前面已经对数字和大小写英文字符进行过测试，因此数字、文字、符号密钥测试共只有两步： （1） 选择加密（Encryption），并选择数字、英文、符号交错的字符串作为输入明文字符串“CyberSecurity57!”；选择数字串作为密钥“IloveSEUsoMuch!!”。 （2） 选择解密（Decryption），并将上一步生成的密文输入，再输入密钥“1234567890123456”，得到解密后的明文，并与原明文比较，逐个验证对应字符是否一致。 **三、实验分析** 通过本实验，我深入探究了 AES 算法的内部工作原理，并通过 C++语言成功实现了算法的核心功能。实验过程中，我对算法的每个细节都有了更加深刻的理解，特别是密钥扩展、各种操作的实现逻辑以及它们如何共同作用来保证加密强度。此外，实验的过程也锻炼了我的编程技能，特别是在处理复杂算法和实现安全相关代码方面。最终，通过构建一个具有用户交互界面的程序，我能够直观地展示 AES 加密和解密的过程，使理论与实践结合，达到了实验的学习目的。 **四、实验结论** AES 算法作为一种先进的加密标准，在保护数据安全方面发挥着重要作用。通过这次实验，不仅加深了对 AES 算法原理的理解，也获得了实际编码和算法实现的经验。这次实验对于加密技术的学习和未来在安全领域的研究具有重要意义。

实验结果	1. 纯数字明文测试
	`You are welcome to use the AES machine of SEUer_LK123425!`
	
	`Please enter the corresponding number for operation:`
	`1.Encryption  2.Decryption  3.Quit`
	`Choice: 1`
	`Please enter the plaintext (length = 16):`
	`1123581321345589`
	`Please enter the secret key (length = 16):`
	`1234567890123456`
	`Cipher text is: 9bf6f2b3323879c57b20f5af76036d68`
	
	`Please enter the corresponding number for operation:`
	`1.Encryption  2.Decryption  3.Quit`
	`Choice: 2`
	`Please enter the ciphertext (length = 32, hex):`
	`9bf6f2b3323879c57b20f5af76036d68`
	`Please enter the secret key (length = 16):`
	`1234567890123456`
	`Plain text is: 1123581321345589`

2. 纯文字明文测试

```
Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 1
Please enter the plaintext (length = 16):
woaidongnandaxue
Please enter the secret key (length = 16):
1234567890123456
Cipher text is: 3f0fdb918c7dc906c959c5865564a10f

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 2
Please enter the ciphertext (length = 32, hex):
3f0fdb918c7dc906c959c5865564a10f
Please enter the secret key (length = 16):
1234567890123456
Plain text is: woaidongnandaxue
```

```
Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 1
Please enter the plaintext (length = 16):
WoAiDongNanDaXue
Please enter the secret key (length = 16):
1234567890123456
Cipher text is: 0049652dd4ceace4785f16ffe905407a

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 2
Please enter the ciphertext (length = 32, hex):
0049652dd4ceace4785f16ffe905407a
Please enter the secret key (length = 16):
1234567890123456
Plain text is: WoAiDongNanDaXue
```

3. 数字、文字、符号明文测试

```
You are welcome to use the AES machine of SEUer_LK123425!

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 1
Please enter the plaintext (length = 16):
IloveSEUsoMuch!!
Please enter the secret key (length = 16):
1234567890123456
Cipher text is: 2d3c29873b584081f5ffe2d92b32d463

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 2
Please enter the ciphertext (length = 32, hex):
2d3c29873b584081f5ffe2d92b32d463
Please enter the secret key (length = 16):
1234567890123456
Plain text is: IloveSEUsoMuch!!
```

4. 纯数字密钥测试

```
You are welcome to use the AES machine of SEUer_LK123425!

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 1
Please enter the plaintext (length = 16):
CyberSecurity57!
Please enter the secret key (length = 16):
1234567890123456
Cipher text is: f837f8f1db97eb571d40d43d83c29760

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 2
Please enter the ciphertext (length = 32, hex):
f837f8f1db97eb571d40d43d83c29760
Please enter the secret key (length = 16):
1234567890123456
Plain text is: CyberSecurity57!
```

5. 纯文字密钥测试

```
You are welcome to use the AES machine of SEUer_LK123425!

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 1
Please enter the plaintext (length = 16):
CyberSecurity57!
Please enter the secret key (length = 16):
woaidongnandaxue
Cipher text is: 99d977768284b697807b4daa41ef213d

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 2
Please enter the ciphertext (length = 32, hex):
99d977768284b697807b4daa41ef213d
Please enter the secret key (length = 16):
woaidongnandaxue
Plain text is: CyberSecurity57!
```

```
You are welcome to use the AES machine of SEUer_LK123425!

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 1
Please enter the plaintext (length = 16):
CyberSecurity57!
Please enter the secret key (length = 16):
WoAiDongNanDaXue
Cipher text is: 8c9ece823bb6e50cf0f5a4f5cf3fab51

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 2
Please enter the ciphertext (length = 32, hex):
8c9ece823bb6e50cf0f5a4f5cf3fab51
Please enter the secret key (length = 16):
WoAiDongNanDaXue
Plain text is: CyberSecurity57!
```

6. 数字、文字、符号密钥测试

```
You are welcome to use the AES machine of SEUer_LK123425!

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 1
Please enter the plaintext (length = 16):
CyberSecurity57!
Please enter the secret key (length = 16):
IloveSEUsoMuch!!
Cipher text is: cc43938a2511ec27d21bfa2efb1822a0

Please enter the corresponding number for operation:
1.Encryption    2.Decryption    3.Quit
Choice: 2
Please enter the ciphertext (length = 32, hex):
cc43938a2511ec27d21bfa2efb1822a0
Please enter the secret key (length = 16):
IloveSEUsoMuch!!
Plain text is: CyberSecurity57!
```

综上，实验验证符合要求，能完成预期结果，密时不会出现兼容性问题和乱码，界面交互性强。