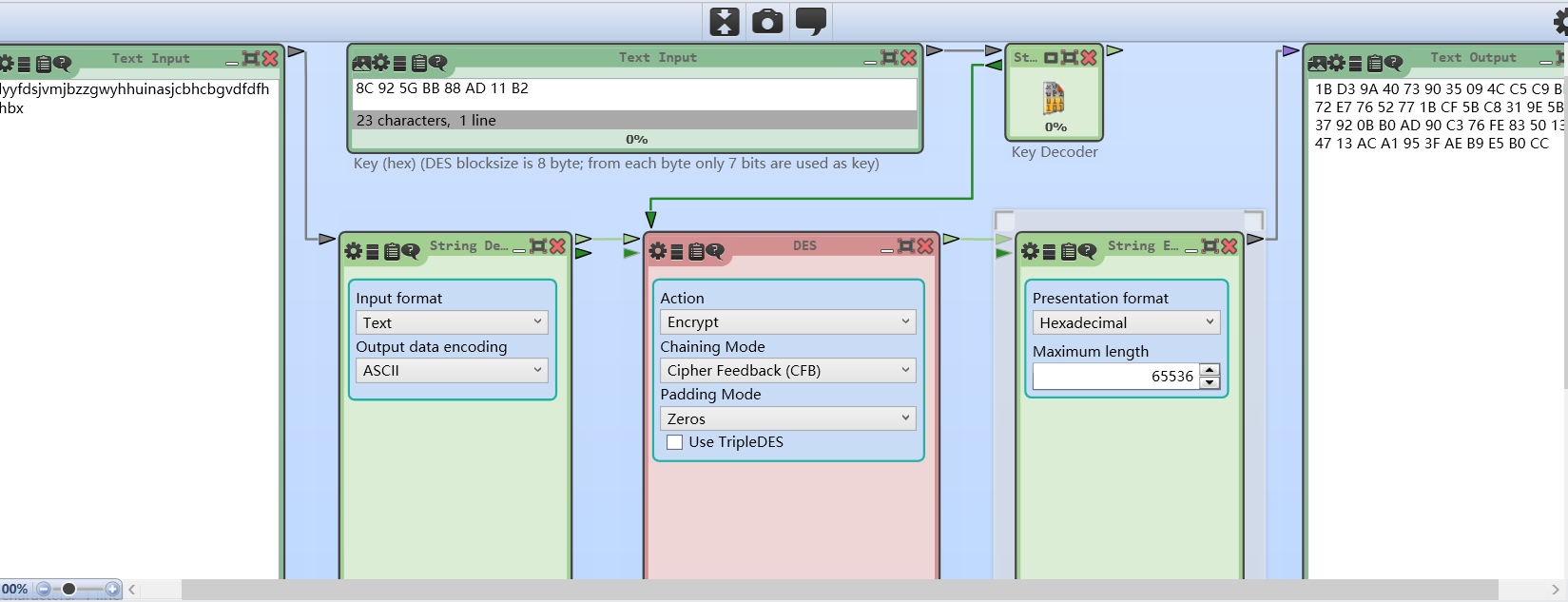
**现代密码加解密与分析实验报告**

1. **DES**

(1)加密

|  |  |  |  |
| --- | --- | --- | --- |
| 明文 | 模式 | 密钥 | 密文 |
| agbfdgrt | ECB | 11 B2 8C 92 5G BB 88 AD | CC C9 48 0E E2 F0 59 4F |
| qedfrgcbskhydrgh | CBC | 11 B2 8C 92 5G BB 88 AD | D6 65 C9 F7 AF B0 1D BD D2 20 23 D3 FD 21 CC FD |
| Iudyyfdsjvmjbzzgwyhhuinasjcbhcbgvdfdfhdbhbx | CFB | 8C 92 5G BB 88 AD 11 B2 | 1B D3 9A 40 73 90 35 09 4C C5 C9 BD 72 E7 76 52 77 1B CF 5B C8 31 9E 5B 4B 37 92 0B B0 AD 90 C3 76 FE 83 50 13 47 13 AC A1 95 3F AE B9 E5 B0 CC |

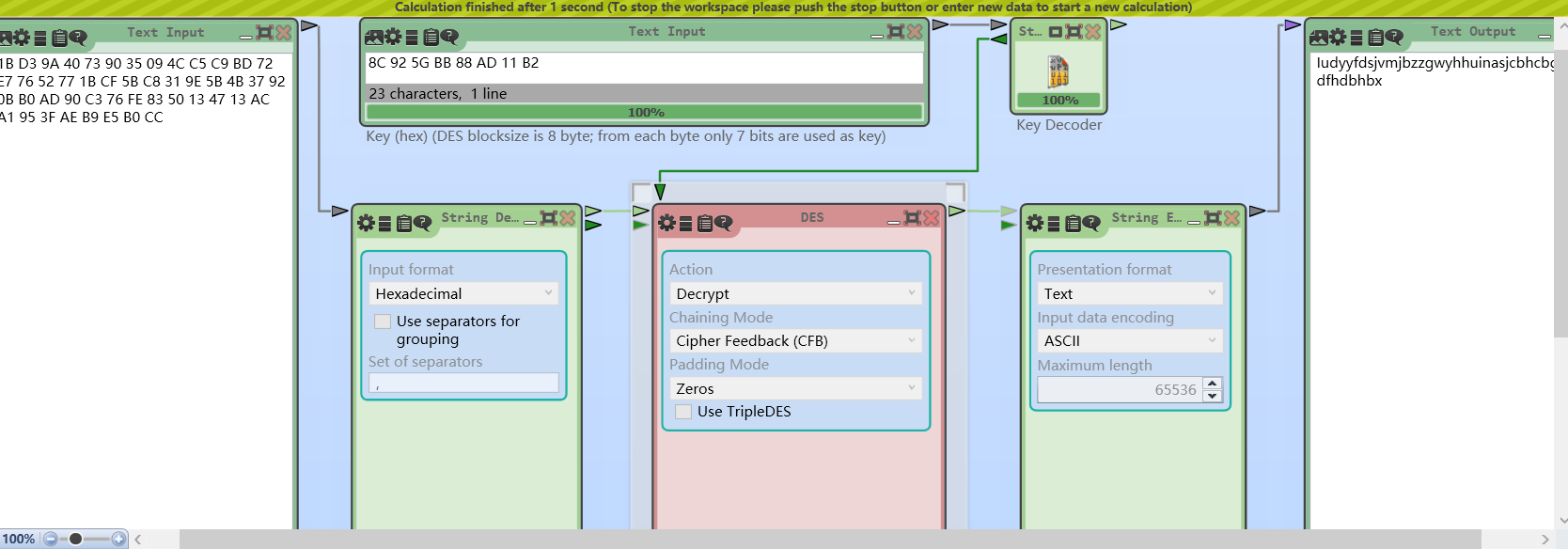
截图：



（2）解密

|  |  |  |  |
| --- | --- | --- | --- |
| 密文 | 模式 | 密钥 | 明文 |
| CC C9 48 0E E2 F0 59 4F | ECB | 11 B2 8C 92 5G BB 88 AD | agbfdgrt |
| D6 65 C9 F7 AF B0 1D BD D2 20 23 D3 FD 21 CC FD | CBC | 11 B2 8C 92 5G BB 88 AD | qedfrgcbskhydrgh |
| 1B D3 9A 40 73 90 35 09 4C C5 C9 BD 72 E7 76 52 77 1B CF 5B C8 31 9E 5B 4B 37 92 0B B0 AD 90 C3 76 FE 83 50 13 47 13 AC A1 95 3F AE B9 E5 B0 CC | CFB | 8C 92 5G BB 88 AD 11 B2 | Iudyyfdsjvmjbzzgwyhhuinasjcbhcbgvdfdfhdbhbx |

截图：



1. 汇总表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 明文 | 明文长度 | 模式 | 密钥 | 密钥长度 | 密文 | 密文长度 |
| qbdfrgcbskhydrgh | 16 | CBC | 8C 92 5G BB 88 AD 11 B2 | 64bit | C6 01 61 C6 7F 72 3D 96 78 99 59 65 4C 66 E7 D6 | 128bit |
| qedfrgcbskhydrgh | A1 A8 AE 3D E6 F2 BE 51 97 77 8E 95 06 5F 94 74 | 128bit |
| qadfrgcbskhydrgh | 90 22 7D 78 F9 89 67 7A CF 62 90 7C 34 86 62 89 | 128bit |
| cbskhydrgh | 10 | ECB | 8C 92 5G BB 88 AD 11 B2 | 64bit | 26 C3 7F A3 01 E4 A3 D0 51 2A DD DB 94 85 18 92 | 128bit |
| qedfrgqedfrgcbskhydrgh | 22 | 37 27 69 9C D5 5A FB 2E E0 D4 BE 00 01 6F 52 B8 09 4C 27 D4 60 FB A2 4B | 192bit |
| qedfrgcbskhydrgh | 16 | A1 A8 AE 3D E6 F2 BE 51 3F 1E E3 82 DD D9 83 0A | 128bit |
| qedfrgcbskhydrgh | 16 | ECB | 8C 92 5G BB 88 AD 11 B2 | 64bit | A1 A8 AE 3D E6 F2 BE 51 3F 1E E3 82 DD D9 83 0A | 128bit |
| CFB | 23 68 E6 10 29 07 15 C0 1A 8E 19 45 6F E0 B8 24 | 128bit |
| OFB | 23 28 80 67 C8 F6 40 79 60 99 00 30 BF 52 D1 73 | 128bit |

**结论：**

**•比较不同明文（微小区别）产生的密文有多少比特或字节不同**

字节都不同。

**•比较不同明文长度时，密文长度的区别，以及与密文长度与明文长度是否一致**

明文变长，密文长度可能会随之变长，也可能不变；明文长度和密文长度不一致。

**•比较相同明文在不同模式下产生的密文的区别**

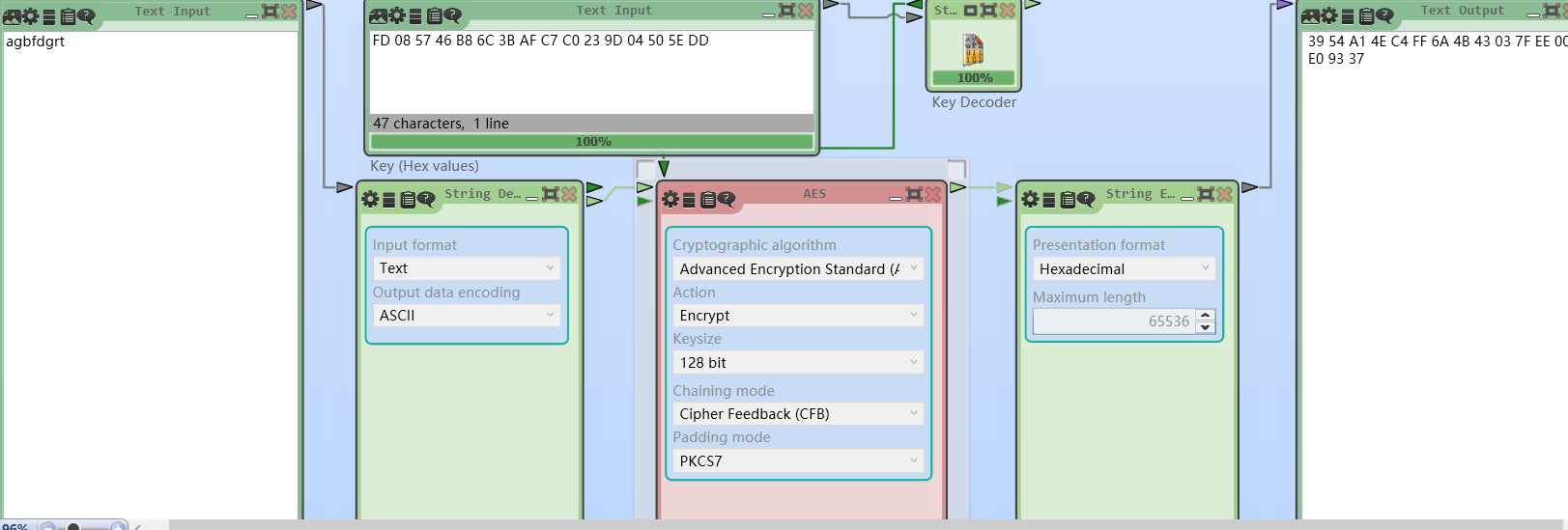
密文长度相同，内容不同。

1. **AES**

(1)加密

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 明文 | 模式 | 密钥长度 | 密钥 | 密文 |
| agbfdgrt | ECB | 128bit | FD 08 57 46 B8 6C 3B AF C7 C0 23 9D 04 50 5E DD | 5F B8 9A 7D 38 E8 A0 1F 5E 68 D9 E5 E2 0B D6 DF |
| qedfrgcbskhydrgh | CBC | 192bit | 4D 95 57 4A 88 6C 3B 9F C7 C0 23 9A 04 50 ED 05 74 A2 B2 89 25 D4 AC 00 | 3B BD 7F BE F0 9C 93 C2 75 35 0A BD 69 8B AD 6B DA 91 F0 D1 CC E9 39 72 43 2B 01 59 0D 05 DF B4 |
| Iudyyfdsjvmjbzzgwyhhuinasjcbhcbgvdfdfhdbhbx | CFB | 256bit | 45 D5 57 4A 88 DC 3B 9F C7 C0 23 9A 00 58 FD 05 74 A2 G2 B9 25 D4 0C 00 20 C8 E9 5B CC 23 46 A1 | F5 20 C1 A2 DE A8 C8 14 B6 34 0B A5 B0 29 E7 22 FD C1 50 AD 1C 08 C6 74 DF A8 55 14 BF 56 32 C0 23 48 54 84 D8 CC 1B FD 6C A7 19 DE 2D 56 8D 87 |

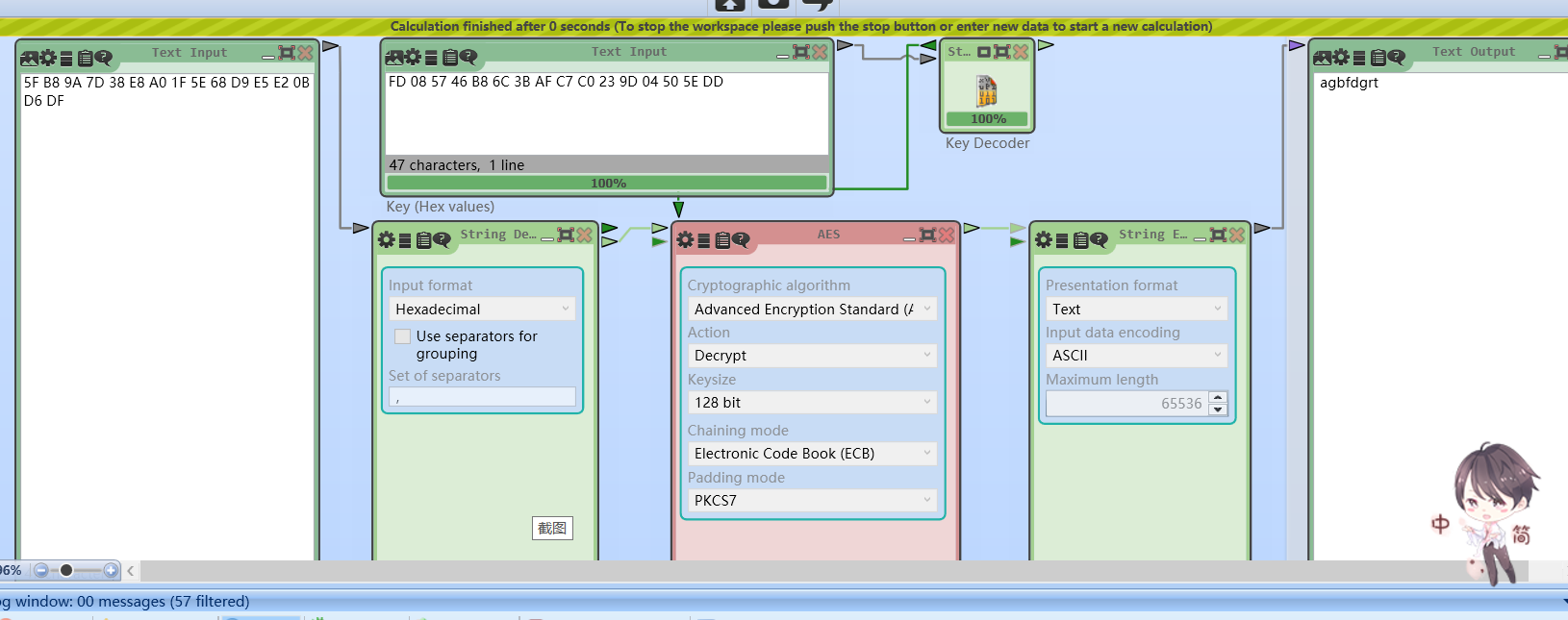
截图：



（2）解密

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 密文 | 模式 | 密钥长度 | 密钥 | 明文 |
| 5F B8 9A 7D 38 E8 A0 1F 5E 68 D9 E5 E2 0B D6 DF | ECB | 128bit | FD 08 57 46 B8 6C 3B AF C7 C0 23 9D 04 50 5E DD | agbfdgrt |
| 3B BD 7F BE F0 9C 93 C2 75 35 0A BD 69 8B AD 6B DA 91 F0 D1 CC E9 39 72 43 2B 01 59 0D 05 DF B4 | CBC | 192bit | 4D 95 57 4A 88 6C 3B 9F C7 C0 23 9A 04 50 ED 05 74 A2 B2 89 25 D4 AC 00 | qedfrgcbskhydrgh |
| F5 20 C1 A2 DE A8 C8 14 B6 34 0B A5 B0 29 E7 22 FD C1 50 AD 1C 08 C6 74 DF A8 55 14 BF 56 32 C0 23 48 54 84 D8 CC 1B FD 6C A7 19 DE 2D 56 8D 87 | CFB | 256bit | 45 D5 57 4A 88 DC 3B 9F C7 C0 23 9A 00 58 FD 05 74 A2 G2 B9 25 D4 0C 00 20 C8 E9 5B CC 23 46 A1 | Iudyyfdsjvmjbzzgwyhhuinasjcbhcbgvdfdfhdbhbx |

截图：



（3）汇总表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 明文 | 明文长度 | 模式 | 密钥 | 密钥长度 | 密文 | 密文长度 |
| qbdfrgcbskhydrgh | 16 | CBC | FD 08 57 46 B8 6C 3B AF C7 C0 23 9D 04 50 5E DD | 128bit | BA F8 DF 76 9D C2 E8 E9 A0 B1 3E 25 AB AF 14 D9 DA 2C 89 8B F7 99 9A 94 C3 DE E9 C9 E0 53 2A 2F | 256bit |
| qedfrgcbskhydrgh | 30 CB E1 67 81 53 0E 3D C8 72 F8 3F 7A F5 D5 F3 0E 0E DD 0C BB B6 02 8B 2B C3 47 4C B5 78 55 2A | 256bit |
| qadfrgcbskhydrgh | 77 14 DC 69 38 B5 4F 52 99 6C 28 CC A2 1B B6 DF C3 86 C2 4F 11 22 09 05 4A 29 74 24 FB A5 03 C6 | 256bit |
| cbskhydrgh | 10 | ECB | FD 08 57 46 B8 6C 3B AF C7 C0 23 9D 04 50 5E DD | 128bit | 32 4A C8 76 BF B8 66 D5 45 6F D9 00 8A 40 79 36 | 128bit |
| qedfrgcbskhydrgh | 16 | 30 CB E1 67 81 53 0E 3D C8 72 F8 3F 7A F5 D5 F3 FE 1F 3C 6C D6 63 70 10 E7 72 3C BE D2 F8 EC 44 | 256bit |
| qedfrgqedfrgcbskhydrgh | 22 | 3E B2 1D 07 3F F3 47 C1 86 AB 9C 5D C0 3B 6E 53 84 77 8B 39 E1 AB EC B0 22 C9 EF FB 59 53 E5 2A | 256bit |
| qedfrgcbskhydrgh | 16 | ECB | FD 08 57 46 B8 6C 3B AF C7 C0 23 9D 04 50 5E DD | 128bit | 30 CB E1 67 81 53 0E 3D C8 72 F8 3F 7A F5 D5 F3 FE 1F 3C 6C D6 63 70 10 E7 72 3C BE D2 F8 EC 44 | 256bit |
| CFB | 29 EF BD F8 74 65 C1 32 48 F5 CF 97 CE 40 83 8B F0 2F 5E 04 92 F1 46 87 4F 67 A2 43 78 7B 42 19 | 256bit |
| OFB | 29 A3 15 42 35 50 17 BF 0B A4 74 24 39 88 D2 3F CD 78 13 55 01 86 78 80 C3 2C 3D 64 7E F3 F4 AE | 256bit |

**结论：**

**•比较不同明文（微小区别）产生的密文有多少比特或字节不同**

字节都不同。

**•比较不同明文长度时，密文长度的区别，以及与密文长度与明文长度是否一致**

明文变长，密文长度可能会随之变长，也可能不变；明文长度和密文长度不一致。

**•比较相同明文在不同模式下产生的密文的区别**

密文长度相同，内容不同。

1. **比较雪崩效应**
2. AES

固定密钥：FD 08 57 46 B8 6C 3B AF C7 C0 23 9D 04 50 5E DD

明文1：cbskhydrgh

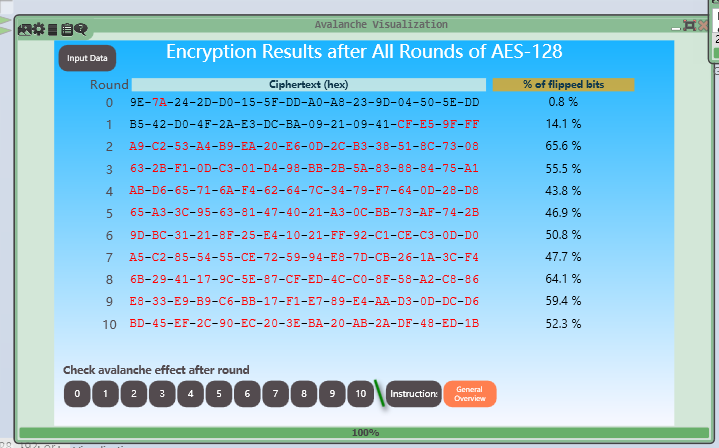
明文2：qedfrgcbskhydrgh

明文3：Iudyyfdsjvmjbzzgwy

第一组：

修改前后的明文比特序列：

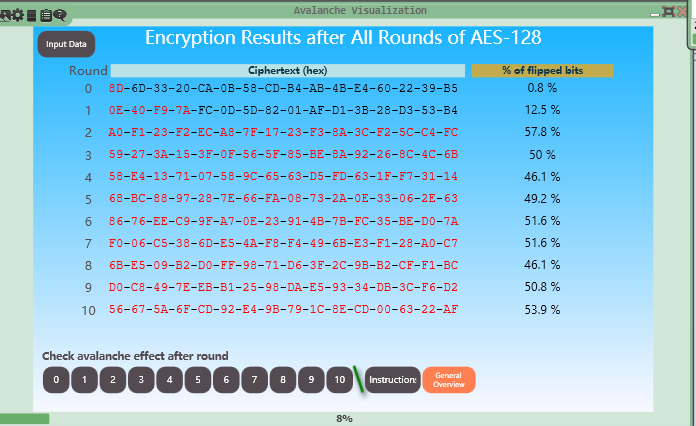




第二组：

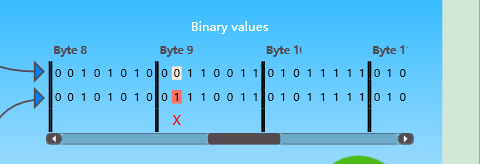
修改前后的明文比特序列：

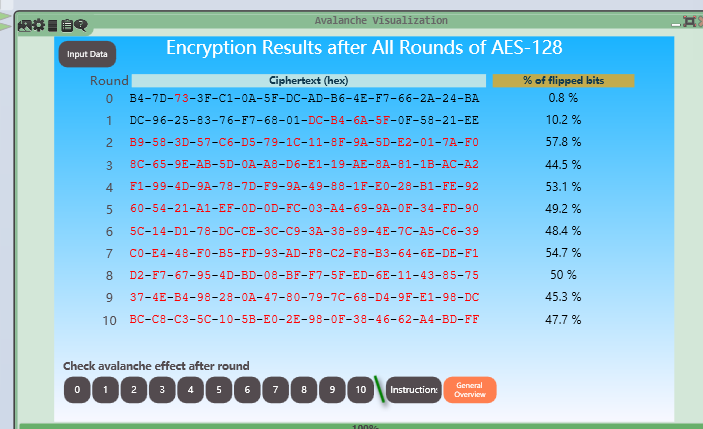




第三组：

修改前后的明文比特序列：





1. Caesar

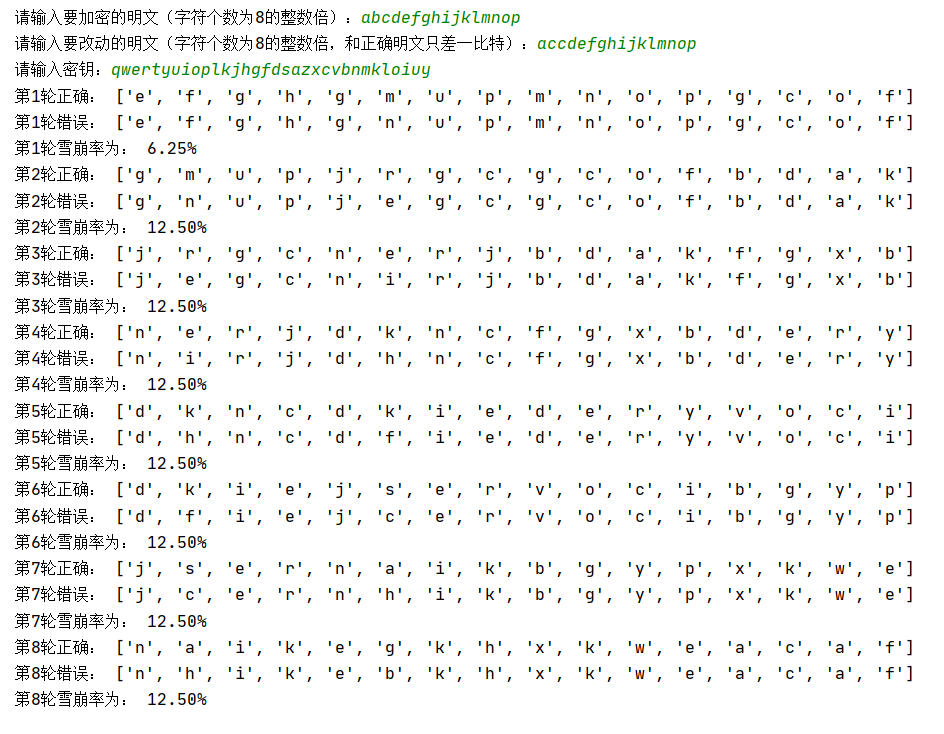
|  |  |  |  |
| --- | --- | --- | --- |
| 明文 | 修改后的明文 | 密文 | 雪崩效应影响的比特位占比 |
| qedfrgcbskhydrgh | wedfrgcbskhydrgh | bpoqcrnmdvsjocrs | 6.3% |
| wedfrgcbskhydrgh | wedfrgcbskhtdrgh | hpoqcrnmdvseocrs | 12.5% |
| wedfrgcbskhtdrgh | wedfrucbskhtdrgh | hpoqcfnmdvseocrs | 18.8% |

区别：

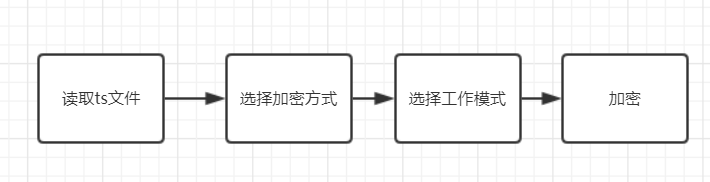
AES中，明文发生小改变，改动会很快扩散到全部密文；

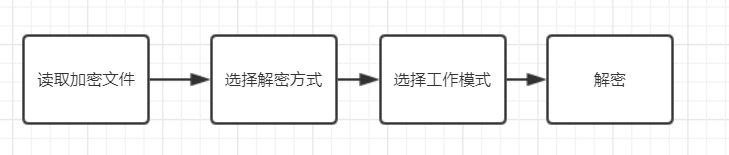
Caesar中，明文发生小改变，密文仅对应位置会发生改变。

1. **基于Feistel结构自行设计分组算法**
2. 步骤：将明文分为八个字节一组（明文长度为8的整数倍），密钥四个字节一组（密钥长度为4的整数倍），密钥长度除以4即为迭代轮次。然后将每一组明文分为左半部分和右半部分（分别为4字节），将左半部分的内容用右半部分替换，将左半部分和右半部分和密钥进行与运算，得到的结果作为新的右半部分，反复迭代计算得出最终结果。
3. 截屏：

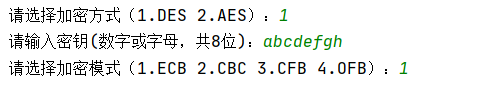


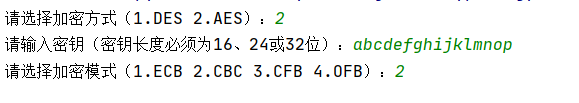
1. **离线内容保护**
2. 流程图





1. 截图







从左到右分别为源文件、加密文件、解密文件，因此加密、解密成功。