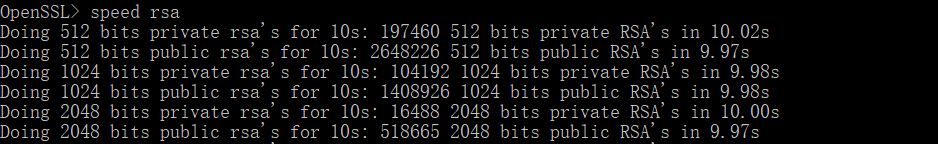
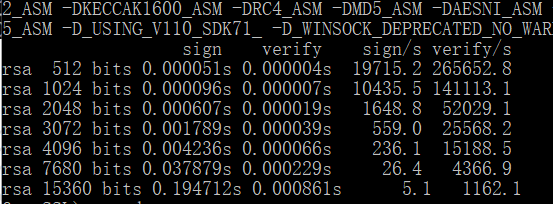
**SSL传输安全实验报告**

1. **RSA和AES比较**
2. RSA

|  |  |  |  |
| --- | --- | --- | --- |
| 密钥长度/bit | 密钥类型 | 数据量/bit | 时长/s |
| 512 | 私钥 | 101099520 | 10.02 |
| 公钥 | 1355891712 | 9.97 |
| 1024 | 私钥 | 106692608 | 9.98 |
| 公钥 | 1442740224 | 9.98 |
| 2048 | 私钥 | 33767424 | 10.00 |
| 公钥 | 1062225920 | 9.97 |

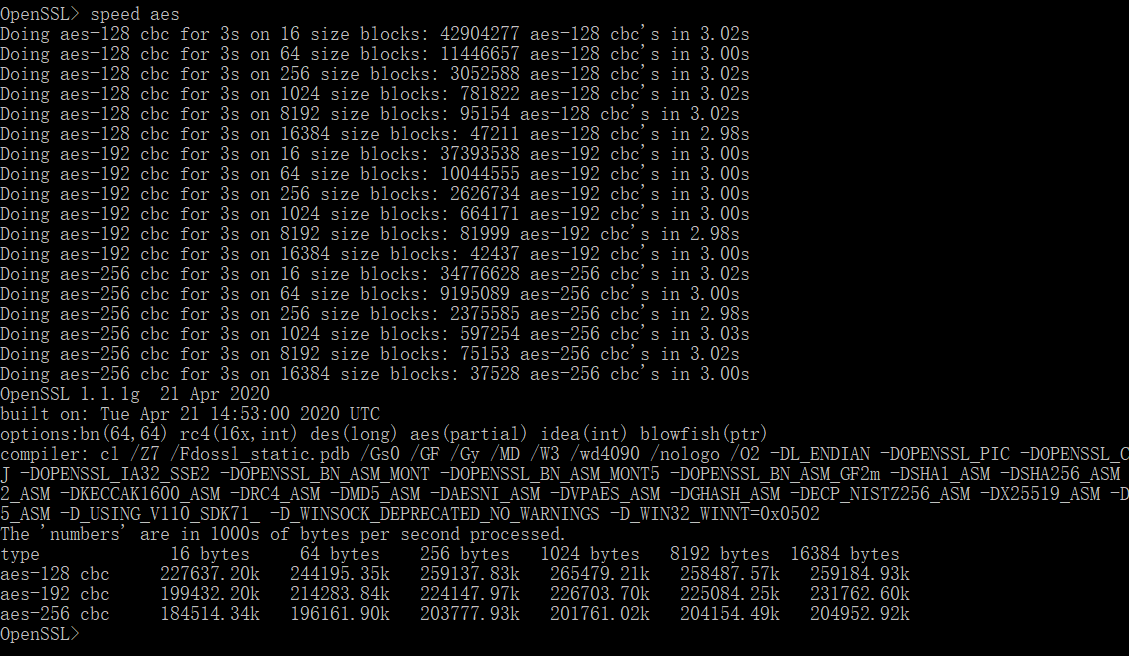


|  |  |  |  |
| --- | --- | --- | --- |
| 密钥长度/bit | 类型 | 每秒处理的数据量/bit | 时长/s |
| 512 | 签名 | 19715.2 | 0.000051 |
| 验签 | 265652.8 | 0.000004 |
| 1024 | 签名 | 10435.5 | 0.000096 |
| 验签 | 141113.1 | 0.000007 |
| 2048 | 签名 | 1648.8 | 0.000607 |
| 验签 | 52029.1 | 0.000019 |



1. AES

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 密钥长度/bit | 工作模式 | 每秒处理的数据量/kb | | | | | |
| 16bytes | 64bytes | 256bytes | 1024bytes | 8192bytes | 16384bytes |
| 128 | cbc | 227637.20k | 244195.35k | 259137.83k | 265479.21k | 258487.57k | 25918.93k |
| 192 | cbc | 199432.20k | 214283.84k | 224147.97k | 226703.70k | 225084.25k | 231762.60k |
| 256 | cbc | 184514.34k | 196161.90k | 203777.93k | 201761.02k | 204154.49k | 204952.92k |

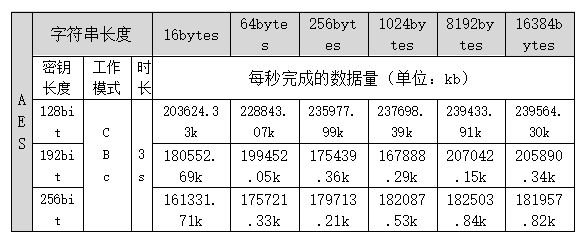


1. RSA和AES的比较

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | RSA | AES |
| 加密 | 处理的数据量/bit | 1355891712 |  |
| 时长/s | 9.97 |  |
| 每秒处理数据量/bit | 135997.16k | 227637.20k |
| 解密 | 处理的数据量/bit | 101099520 |  |
| 时长/s | 10.02 |  |
| 平均每秒处理数据量/bit\*s-1 | 10089.772k | 227637.20k |

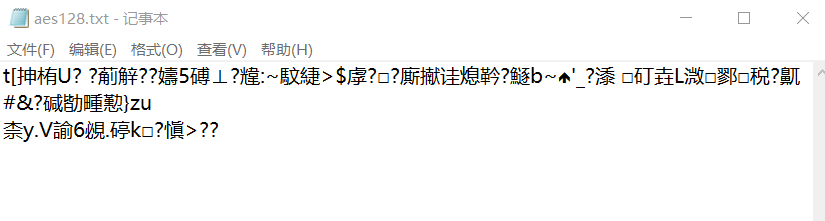
所以AES速度更快。

1. 比较

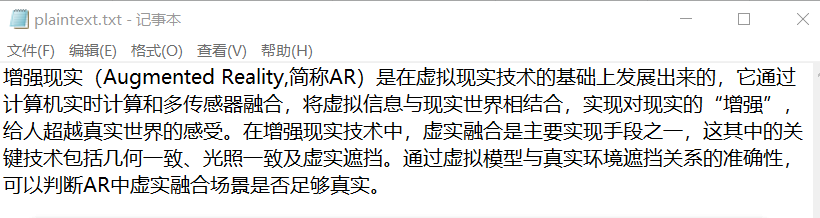


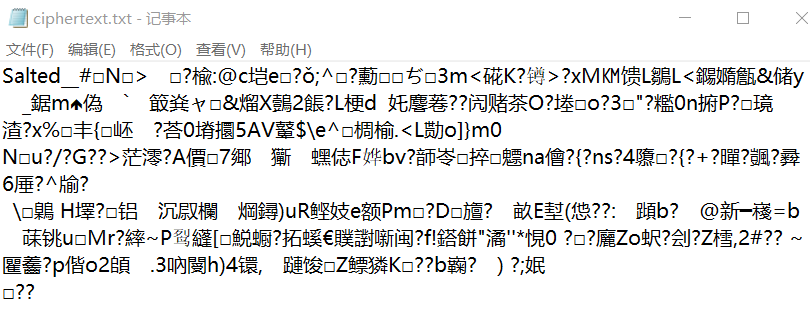
所以我的电脑主机运算速度更快。

1. **命令行加密、签名操作**
2. 文件的加密、解密
3. 生成随机数作为对称算法的密钥

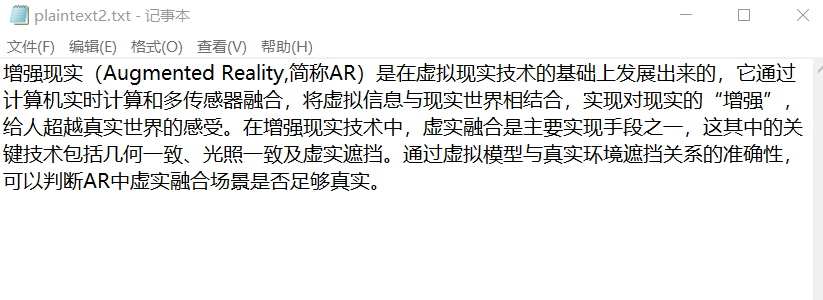


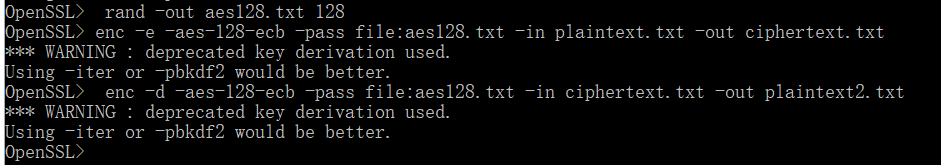
1. 加密





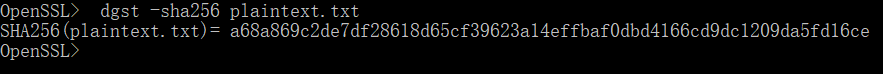
1. 解密



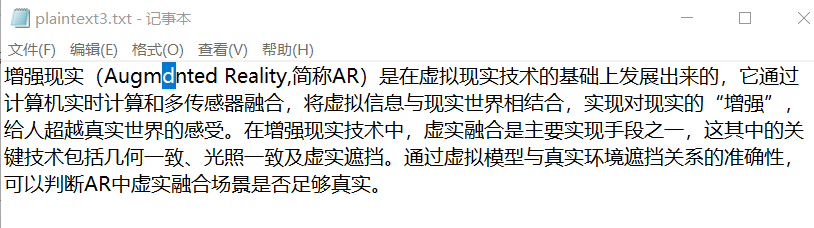


加密、解密成功。

1. 计算文件摘要
2. 计算文件的SHA256值



1. 修改1bit或1字节，重新计算SHA256值



SHA256_2

1. 对比

原SHA256值：a68a869c2de7df28618d65cf39623a14effbaf0dbd4166cd9dc1209da5fd16ce

现SHA256值：825b943e63ae4e23c8c2e38a0783ea5925caf32619d59851e08b60402008a806

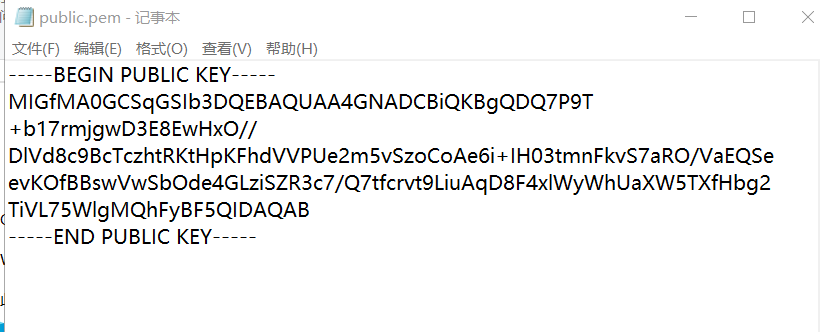
变化位数：61

比例：61/64=95.3%

1. RSA密钥生成与管理
2. 生成RSA密钥对

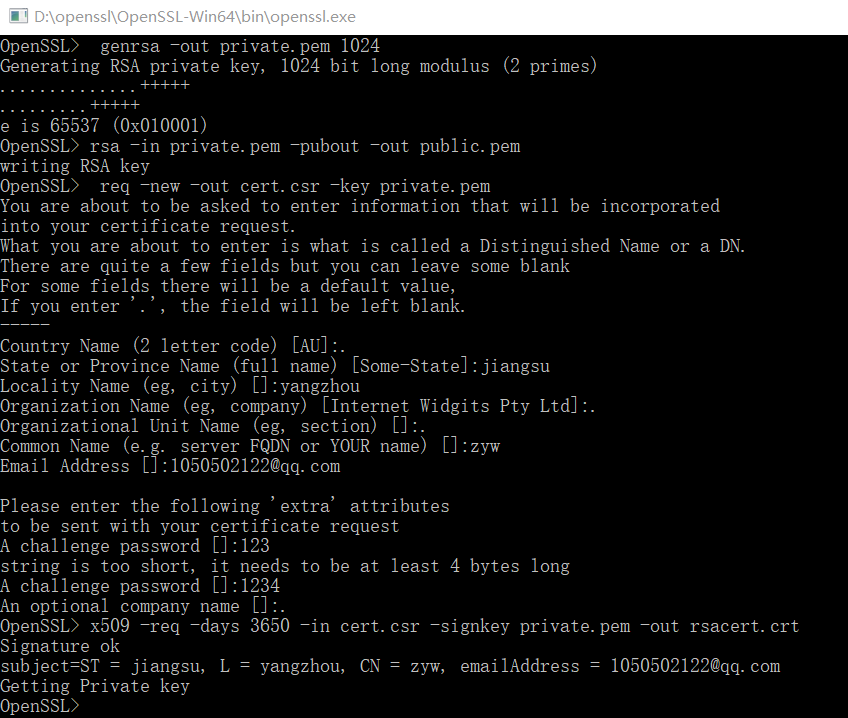


1. 取出RSA公钥



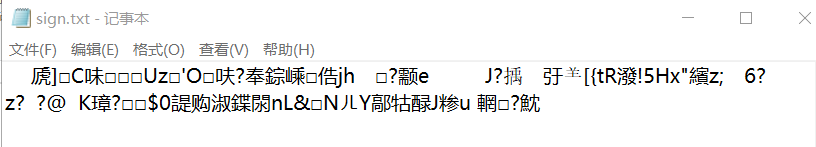
1. 生成公钥证书





1. 文件的签名与验证
2. 签名

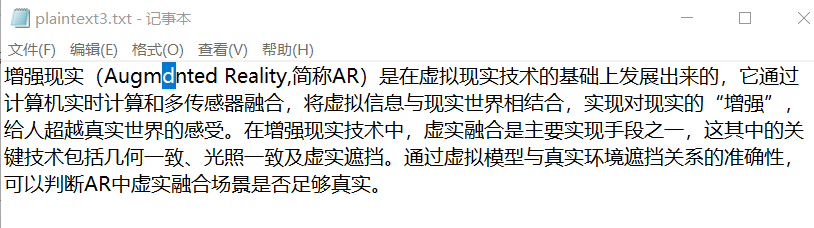
签名指令

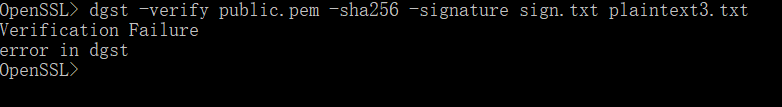


1. 验证

验证

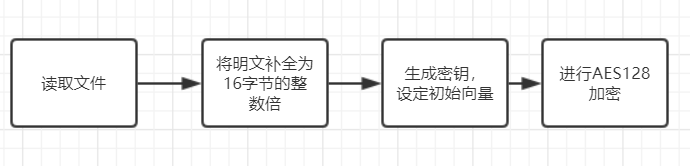
1. 修改文件，再验证

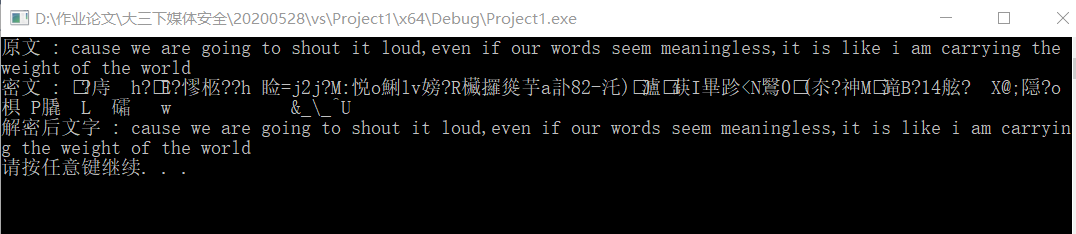




1. **SSL基础编程**
2. 基本文件加解密

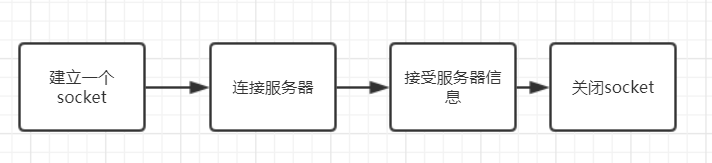
aes加密流程：



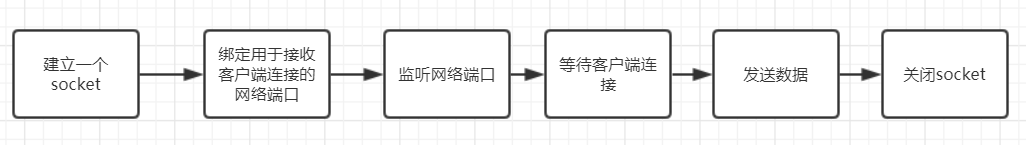


1. 基本的面向socket通信

客户端：



服务器：



运行结果：

