**实验三 RSA、AES数据传输加解密实验**

1. **实验目的**

（1）理解RSA与AES的加密流程；

（2）理解RSA与AES之间的区别；

（3）掌握使用Openssl进行数据加密、解密的基本方法；

（4）掌握结合socket进行加密数据传输的基本方法。

**2 实验要求**

（1）利用openssl提供的相应功能实现简单的数据传输加、解密；

（2）实现基于RSA的密钥种子传输；

（3）实现基于AES的文件加密传输；

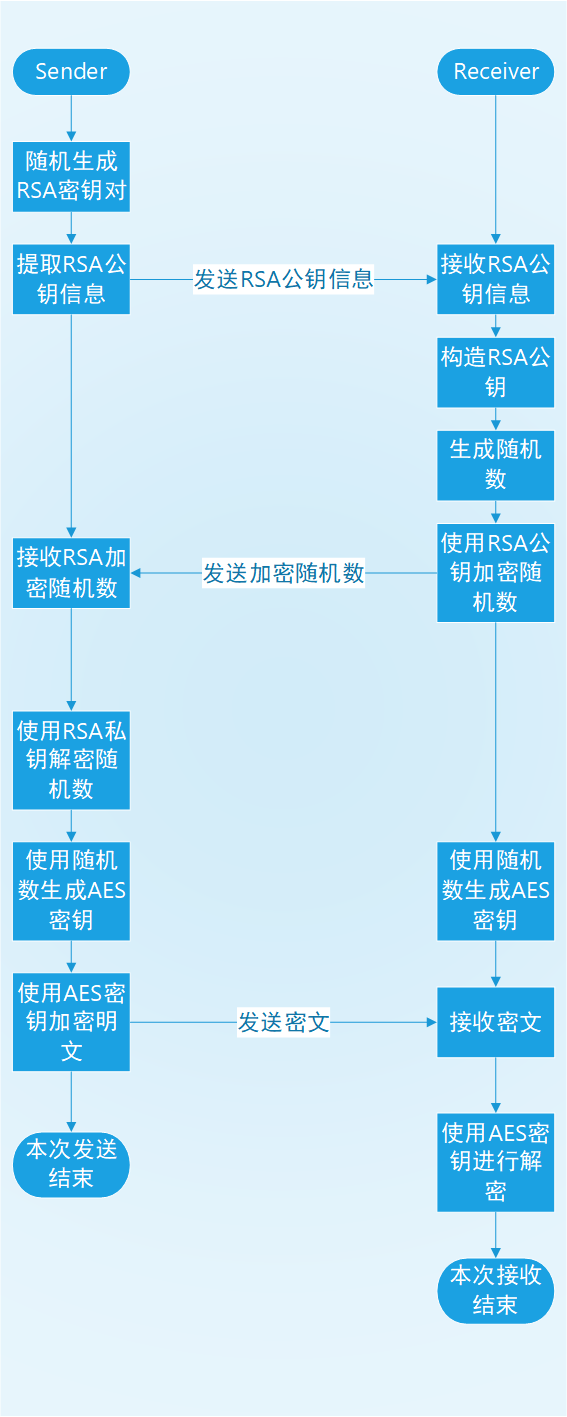
**3 实验内容**

根据所学知识，在Linux平台上利用Openssl，结合RSA与AES两种加密方法实现两台计算机间的加密数据传输。

编写发送端和接收端程序，实现密钥协商和文件的加密解密。可以尝试摆脱Openssl，自行编写RSA和AES加解密函数，也可以对程序的当前功能进行完善，例如添加SHA256文件校验等。

1. **实验原理**

实验程序分为两个部分，分别是用于发送加密数据的sender和接收加密数据receiver，分别运行于两台计算机上。sender实现RSA密钥生成，公钥传输，AES数据加密发送，receiver实现AES密钥种子生成以及数据接收解密，程序的大体流程如下图：



在此过程中，会用到如下函数：

RSA \*RSA\_generate\_key(int num, unsigned long e, void (\*callback)(int, int, void \*),

void \*cb\_arg); //生成RSA密钥对

int i2d\_RSAPublicKey(RSA \*a, unsigned char \*\*pp); //从RSA中提取公钥信息

RSA \*d2i\_RSAPublicKey(RSA \*\*val\_out, const unsigned char \*\*der\_in, long length);

//根据信息构造RSA公钥

int RSA\_public\_encrypt(int flen, unsigned char \*from, unsigned char \*to,

RSA \*rsa, int padding); //使用RSA密钥加密数据

int RSA\_private\_decrypt(int flen, unsigned char \*from, unsigned char \*to,

RSA \*rsa, int padding); //使用RSA密钥解密数据

int  [AES\_set\_encrypt\_key](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#af2a2a79bf29fae1cc93b4aa43c2b833c) (const unsigned char \*userKey, const int [bits](https://docs.huihoo.com/doxygen/openssl/1.0.1c/include_2openssl_2x509v3_8h.html#ab3c186980893d6836a68407d221ae9c9), [AES\_KEY](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#a8f7795796ab08087e20c6d603bf25a8c) \*[key](https://docs.huihoo.com/doxygen/openssl/1.0.1c/des_8c.html#a6a4ff80275090619f35902b61a8c6bf6));

//生成AES加密密钥（程序中256位的密钥只能加解密16字节数据）

int  [AES\_set\_decrypt\_key](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#a2091bfbf02d00a2f4ce67085d1a0d0ac) (const unsigned char \*userKey, const int [bits](https://docs.huihoo.com/doxygen/openssl/1.0.1c/include_2openssl_2x509v3_8h.html#ab3c186980893d6836a68407d221ae9c9), [AES\_KEY](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#a8f7795796ab08087e20c6d603bf25a8c) \*[key](https://docs.huihoo.com/doxygen/openssl/1.0.1c/des_8c.html#a6a4ff80275090619f35902b61a8c6bf6));

//生成AES解密密钥

[void](https://docs.huihoo.com/doxygen/openssl/1.0.1c/hw__4758__cca_8h.html#afad4d591c7931ff6dc5bf69c76c96aa0) [AES\_encrypt](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#a5e9cae0f27ffa404595a3c9f7ea7eb56) (const unsigned char \*[in](https://docs.huihoo.com/doxygen/openssl/1.0.1c/test_2ideatest_8c.html#a006e60e2361d5936856cf2b1883c6d61), unsigned char \*[out](https://docs.huihoo.com/doxygen/openssl/1.0.1c/test_2ideatest_8c.html#afdf65de9e264331943a9e5a248271311), const [AES\_KEY](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#a8f7795796ab08087e20c6d603bf25a8c) \*[key](https://docs.huihoo.com/doxygen/openssl/1.0.1c/des_8c.html#a6a4ff80275090619f35902b61a8c6bf6));

//AES加密

[void](https://docs.huihoo.com/doxygen/openssl/1.0.1c/hw__4758__cca_8h.html#afad4d591c7931ff6dc5bf69c76c96aa0) [AES\_encrypt](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#a5e9cae0f27ffa404595a3c9f7ea7eb56) (const unsigned char \*[in](https://docs.huihoo.com/doxygen/openssl/1.0.1c/test_2ideatest_8c.html#a006e60e2361d5936856cf2b1883c6d61), unsigned char \*[out](https://docs.huihoo.com/doxygen/openssl/1.0.1c/test_2ideatest_8c.html#afdf65de9e264331943a9e5a248271311), const [AES\_KEY](https://docs.huihoo.com/doxygen/openssl/1.0.1c/crypto_2aes_2aes_8h.html#a8f7795796ab08087e20c6d603bf25a8c) \*[key](https://docs.huihoo.com/doxygen/openssl/1.0.1c/des_8c.html#a6a4ff80275090619f35902b61a8c6bf6));

//AES解密

程序中的数据通过socket进行传输，关于加解密相关函数的使用细节，可以参考Openssl帮助文档。

1. **实验环境**

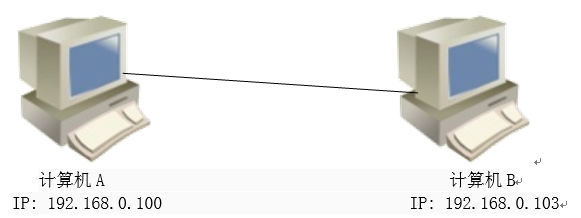
（1）Linux系统：Ubuntu 14.04 LTS

（2）Openssl版本：OpenSSL 1.0.1f

（3）g++ : 4.8.4

1. **实验组网**

本实验组网如下图所示：



1. **实验步骤**

**步骤1** 配置OpenSSL库，执行sudo apt-get install libssl-dev安装。

**步骤2** 修改代码。在计算机A和B分别创建文件夹sender和receiver，文件夹下包含对应相应源代码文件（main.cpp sender/receiver.cpp sender/receiver.h）和makefile，并对代码进行修改，例如IP地址和端口号等。在sender文件夹下存入想要发送的文件。

**步骤3**  编译源代码。在Linux终端下，进入到包含有源代码的文件夹，执行make命令，生成可执行文件。文件路径不要包含空格。

**步骤4** 首先在发送端执行程序./send，之后在接收端执行程序./rec，双方建立TCP连接，并协商密钥信息。协商完成后，在发送端终端输入想要发送的文件名称，敲击回车后，文件会发送至接收端，并保存在receiver文件夹下。

**步骤5** 结束程序。分别在发送端和接收端终端上敲击ctrl+c，可以关闭当前程序。程序运行过程中的部分错误会以错误代号的形式打印在终端上，可以依据信息进行排查。

1. **预期实验结果**

**8.1发送端终端输出示例如下：**

Sender socket ready.

Waiting for connection...

Connection built.

Private-Key: (1024 bit)

modulus:

00:b4:32:0d:70:a2:f2:e7:7b:82:7b:d6:69:a0:cc:

ad:5a:17:62:6e:01:a1:1e:87:53:7f:5f:7d:8a:38:

92:41:51:bc:2e:34:64:8f:48:e8:15:0f:80:f5:e0:

b4:39:22:68:6c:16:ba:ed:bd:12:ff:66:23:ec:12:

0c:0c:0d:28:85:60:e1:31:ac:0f:94:bd:85:5c:a5:

c8:a8:48:00:76:b2:1f:a6:47:48:0f:01:fa:17:06:

ce:8a:07:7b:35:89:f5:8d:4a:d4:90:06:dd:2e:15:

e4:db:ba:ea:cd:d7:28:6b:95:93:4d:44:b3:83:cb:

20:ff:8d:eb:8c:a1:5d:2f:2f

publicExponent: 65537 (0x10001)

privateExponent:

00:80:bf:16:5d:38:ff:c6:a6:b7:87:15:9e:28:d6:

b4:b1:1e:ee:23:dd:24:2a:34:d4:52:b8:7e:71:08:

94:6e:f9:20:33:ff:19:2e:4b:10:0f:24:21:a7:0b:

e2:98:c3:dd:ca:04:bf:90:67:3c:30:a0:e0:df:a5:

d1:57:b6:fb:10:84:ef:0e:ee:cf:9b:ac:50:bf:93:

e9:95:3a:d1:45:b0:42:e7:1c:45:60:3f:3a:51:bc:

56:e8:0b:38:8a:76:79:9b:b3:bc:28:c1:3c:5f:6f:

f5:f6:71:a2:16:ce:cc:15:dd:31:95:b9:ac:75:e9:

cb:37:db:50:33:43:0d:32:91

prime1:

00:eb:f0:b1:f5:64:7c:c3:16:d2:82:19:d7:69:4c:

a0:da:a9:00:2d:a0:8d:00:94:a7:54:86:97:31:72:

cf:1f:f2:20:0f:22:07:0c:1b:6e:7f:56:99:23:a3:

fc:93:43:ff:c5:6d:ce:dc:df:01:20:be:9a:63:f6:

37:50:56:88:59

prime2:

00:c3:84:0e:f2:d2:12:68:5a:30:ff:c6:0e:58:94:

49:79:88:ca:d5:48:e6:b3:ad:69:67:d3:60:26:bd:

ca:98:27:e7:13:f9:47:0b:18:f4:f9:20:62:61:15:

4b:1f:9b:76:b3:bf:5f:7f:8f:e3:89:70:41:9f:da:

1a:88:3c:82:c7

exponent1:

00:bf:57:93:2a:fc:94:85:ae:93:87:b9:27:4e:19:

3b:f6:38:ca:91:36:3c:43:b5:4a:c2:ac:e8:1e:cd:

0a:16:d1:48:98:9d:32:f3:e9:a7:42:13:db:db:e0:

98:ec:61:60:23:1f:bb:7c:ba:49:f2:e1:40:da:42:

8a:77:57:c5:f9

exponent2:

00:a7:2a:68:25:91:1b:90:01:5d:57:b3:1d:5c:fb:

1c:7f:3f:48:3d:68:21:68:8a:e2:4e:95:59:e6:85:

eb:8c:80:c1:80:40:68:4f:c2:bc:e1:ac:a0:b0:e5:

25:e0:16:6a:3d:71:68:d3:86:51:43:97:a9:64:65:

74:bd:fb:0e:cd

coefficient:

59:aa:80:4b:70:e4:fa:a7:eb:81:38:bf:4b:78:a4:

8e:0d:69:3b:99:26:59:35:43:23:ed:1d:8d:f2:17:

89:d4:65:89:47:1b:74:34:9f:cb:7c:e8:32:6a:c5:

34:e6:48:11:92:5b:87:25:04:23:53:17:dc:1e:2d:

14:59:e1:37

PublicKeyBuff, Len=140

0x30, 0x81, 0x89, 0x02, 0x81, 0x81, 0x00, 0xb4, 0x32, 0x0d, 0x70, 0xa2, 0xf2, 0xe7, 0x7b, 0x82, 0x7b, 0xd6, 0x69, 0xa0, 0xcc, 0xad, 0x5a, 0x17, 0x62, 0x6e, 0x01, 0xa1, 0x1e, 0x87, 0x53, 0x7f, 0x5f, 0x7d, 0x8a, 0x38, 0x92, 0x41, 0x51, 0xbc, 0x2e, 0x34, 0x64, 0x8f, 0x48, 0xe8, 0x15, 0x0f, 0x80, 0xf5, 0xe0, 0xb4, 0x39, 0x22, 0x68, 0x6c, 0x16, 0xba, 0xed, 0xbd, 0x12, 0xff, 0x66, 0x23, 0xec, 0x12, 0x0c, 0x0c, 0x0d, 0x28, 0x85, 0x60, 0xe1, 0x31, 0xac, 0x0f, 0x94, 0xbd, 0x85, 0x5c, 0xa5, 0xc8, 0xa8, 0x48, 0x00, 0x76, 0xb2, 0x1f, 0xa6, 0x47, 0x48, 0x0f, 0x01, 0xfa, 0x17, 0x06, 0xce, 0x8a, 0x07, 0x7b, 0x35, 0x89, 0xf5, 0x8d, 0x4a, 0xd4, 0x90, 0x06, 0xdd, 0x2e, 0x15, 0xe4, 0xdb, 0xba, 0xea, 0xcd, 0xd7, 0x28, 0x6b, 0x95, 0x93, 0x4d, 0x44, 0xb3, 0x83, 0xcb, 0x20, 0xff, 0x8d, 0xeb, 0x8c, 0xa1, 0x5d, 0x2f, 0x2f, 0x02, 0x03, 0x01, 0x00, 0x01,

You can compare this with the public key on the receiver.

Public-Key: (1024 bit)

Modulus:

00:b4:32:0d:70:a2:f2:e7:7b:82:7b:d6:69:a0:cc:

ad:5a:17:62:6e:01:a1:1e:87:53:7f:5f:7d:8a:38:

92:41:51:bc:2e:34:64:8f:48:e8:15:0f:80:f5:e0:

b4:39:22:68:6c:16:ba:ed:bd:12:ff:66:23:ec:12:

0c:0c:0d:28:85:60:e1:31:ac:0f:94:bd:85:5c:a5:

c8:a8:48:00:76:b2:1f:a6:47:48:0f:01:fa:17:06:

ce:8a:07:7b:35:89:f5:8d:4a:d4:90:06:dd:2e:15:

e4:db:ba:ea:cd:d7:28:6b:95:93:4d:44:b3:83:cb:

20:ff:8d:eb:8c:a1:5d:2f:2f

Exponent: 65537 (0x10001)

The encrypted seed is <�a��g�ۈ�ktZvk�+2�i�Օl����H8�L�4δ�@�g�ʋ�nd�M\*`gn��i4��c������|ok[B��j�l�j����ylam���(�sǝ,}

�\*��j���:��Za�

The origin seed is 6ONY9h69u4OZ21Az8sPW06xnN99bx4OL9hXoMNGFru43uIgbxn9n7ObFF2cyShZQWtIs04G8hcr04mCh65L661m4ifN7ED3j5KcyzpyGjiauYs6t65vVK17t5Tan7cg

Negotiation completes.

Please input path of the file you wanna send:

test

File opening...

File size:18 bytes

File name:test

Sending File...

Completes!

Please input path of the file you wanna send:

**8.2接收端终端输出示例如下：**

connection built!

0x30, 0x81, 0x89, 0x02, 0x81, 0x81, 0x00, 0xbf, 0xdd, 0x0f, 0x47, 0xab, 0x6c, 0x86, 0x06, 0xf8, 0xf9, 0xff, 0x2a, 0xc7, 0x1d, 0x50, 0x50, 0x33, 0x5e, 0xfd, 0x5d, 0x37, 0x74, 0x0f, 0x98, 0x0d, 0x60, 0xcf, 0xf6, 0x8b, 0x95, 0x76, 0xeb, 0xc0, 0x4d, 0x56, 0xb5, 0xc3, 0xdf, 0x13, 0xd9, 0x56, 0x81, 0x49, 0xed, 0x25, 0x03, 0x76, 0x75, 0x5c, 0x84, 0x92, 0x81, 0x74, 0xf4, 0x2e, 0xd3, 0xb4, 0x95, 0x93, 0xda, 0x1c, 0x25, 0x18, 0x09, 0xf7, 0x9e, 0xd7, 0x33, 0xf6, 0x31, 0x89, 0x85, 0x71, 0x35, 0xe0, 0x73, 0x92, 0xd3, 0x6f, 0xac, 0x73, 0x73, 0x73, 0x01, 0xbf, 0x75, 0xf8, 0x01, 0xbc, 0xdd, 0x0c, 0xcf, 0x1e, 0x5b, 0xe1, 0x35, 0xe6, 0x13, 0x0e, 0x56, 0x6f, 0xb6, 0x7a, 0xc0, 0xeb, 0x5e, 0xfd, 0xc0, 0x91, 0xeb, 0xd9, 0xb8, 0xa2, 0x1b, 0x56, 0x12, 0x2d, 0x7a, 0x98, 0xa4, 0x70, 0xf4, 0xfb, 0xb2, 0x9e, 0xcb, 0x9f, 0xd9, 0x02, 0x03, 0x01, 0x00, 0x01,

pklen from server:140

Public-Key: (1024 bit)

Modulus:

00:bf:dd:0f:47:ab:6c:86:06:f8:f9:ff:2a:c7:1d:

50:50:33:5e:fd:5d:37:74:0f:98:0d:60:cf:f6:8b:

95:76:eb:c0:4d:56:b5:c3:df:13:d9:56:81:49:ed:

25:03:76:75:5c:84:92:81:74:f4:2e:d3:b4:95:93:

da:1c:25:18:09:f7:9e:d7:33:f6:31:89:85:71:35:

e0:73:92:d3:6f:ac:73:73:73:01:bf:75:f8:01:bc:

dd:0c:cf:1e:5b:e1:35:e6:13:0e:56:6f:b6:7a:c0:

eb:5e:fd:c0:91:eb:d9:b8:a2:1b:56:12:2d:7a:98:

a4:70:f4:fb:b2:9e:cb:9f:d9

Exponent: 65537 (0x10001)

The seed is mqOaN6DL53kThMis8p129IPv2t2eBNs6r7LzaQE0zv00r5AyJhDUpx2CwWWuzaVSyaIIgVUE382mqIorDp71JA83Ke5dGarh882pjoyEC02PWCjIMpruXW9g0du07GM

Wainting For File...

File size:18

File name:test

Writing file...

Completes!

Wainting For File...

^C

root@ubuntu:/home/sun/Desktop/ff\_encrypt# ./rec

connection built!

0x30, 0x81, 0x89, 0x02, 0x81, 0x81, 0x00, 0xb4, 0x32, 0x0d, 0x70, 0xa2, 0xf2, 0xe7, 0x7b, 0x82, 0x7b, 0xd6, 0x69, 0xa0, 0xcc, 0xad, 0x5a, 0x17, 0x62, 0x6e, 0x01, 0xa1, 0x1e, 0x87, 0x53, 0x7f, 0x5f, 0x7d, 0x8a, 0x38, 0x92, 0x41, 0x51, 0xbc, 0x2e, 0x34, 0x64, 0x8f, 0x48, 0xe8, 0x15, 0x0f, 0x80, 0xf5, 0xe0, 0xb4, 0x39, 0x22, 0x68, 0x6c, 0x16, 0xba, 0xed, 0xbd, 0x12, 0xff, 0x66, 0x23, 0xec, 0x12, 0x0c, 0x0c, 0x0d, 0x28, 0x85, 0x60, 0xe1, 0x31, 0xac, 0x0f, 0x94, 0xbd, 0x85, 0x5c, 0xa5, 0xc8, 0xa8, 0x48, 0x00, 0x76, 0xb2, 0x1f, 0xa6, 0x47, 0x48, 0x0f, 0x01, 0xfa, 0x17, 0x06, 0xce, 0x8a, 0x07, 0x7b, 0x35, 0x89, 0xf5, 0x8d, 0x4a, 0xd4, 0x90, 0x06, 0xdd, 0x2e, 0x15, 0xe4, 0xdb, 0xba, 0xea, 0xcd, 0xd7, 0x28, 0x6b, 0x95, 0x93, 0x4d, 0x44, 0xb3, 0x83, 0xcb, 0x20, 0xff, 0x8d, 0xeb, 0x8c, 0xa1, 0x5d, 0x2f, 0x2f, 0x02, 0x03, 0x01, 0x00, 0x01,

pklen from server:140

Public-Key: (1024 bit)

Modulus:

00:b4:32:0d:70:a2:f2:e7:7b:82:7b:d6:69:a0:cc:

ad:5a:17:62:6e:01:a1:1e:87:53:7f:5f:7d:8a:38:

92:41:51:bc:2e:34:64:8f:48:e8:15:0f:80:f5:e0:

b4:39:22:68:6c:16:ba:ed:bd:12:ff:66:23:ec:12:

0c:0c:0d:28:85:60:e1:31:ac:0f:94:bd:85:5c:a5:

c8:a8:48:00:76:b2:1f:a6:47:48:0f:01:fa:17:06:

ce:8a:07:7b:35:89:f5:8d:4a:d4:90:06:dd:2e:15:

e4:db:ba:ea:cd:d7:28:6b:95:93:4d:44:b3:83:cb:

20:ff:8d:eb:8c:a1:5d:2f:2f

Exponent: 65537 (0x10001)

The seed is 6ONY9h69u4OZ21Az8sPW06xnN99bx4OL9hXoMNGFru43uIgbxn9n7ObFF2cyShZQWtIs04G8hcr04mCh65L661m4ifN7ED3j5KcyzpyGjiauYs6t65vVK17t5Tan7cg

Wainting For File...

File size:18

File name:test

Writing file...

Completes!

Wainting For File...