1.

Step 0：

选择p=101，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

2.

Step 0：

选择p=103，g=5进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

3.

Step 0：

选择p=107，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

4.

Step 0：

选择p=109，g=6进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

5.

Step 0：

选择p=113，g=3进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

6.

Step 0：

选择p=127，g=3进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

7.

Step 0：

选择p=131，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

8.

Step 0：

选择p=137，g=3进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

9.

Step 0：

选择p=139，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

10.

Step 0：

选择p=149，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

11.

Step 0：

选择p=151，g=6进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

12.

Step 0：

选择p=157，g=5进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

13.

Step 0：

选择p=163，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

14.

Step 0：

选择p=167，g=5进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

15.

Step 0：

选择p=173，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

16.

Step 0：

选择p=179，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

17.

Step 0：

选择p=181，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

18.

Step 0：

选择p=191，g=19进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

19.

Step 0：

选择p=193，g=5进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

20.

Step 0：

选择p=197，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

21.

Step 0：

选择p=199，g=3进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

22.

Step 0：

选择p=211，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

23.

Step 0：

选择p=223，g=3进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

24.

Step 0：

选择p=227，g=2进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

25.

Step 0：

选择p=229，g=6进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

26.

Step 0：

选择p=233，g=3进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

27.

Step 0：

选择p=239，g=7进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

28.

Step 0：

选择p=241，g=7进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

29.

Step 0：

选择p=251，g=6进行D-H密钥交换。

Step 1：

选择A=8，B=9。

Step 2：

计算公开的数：

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：