$$y = g^x \ mod \ p$$

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：

$$y_1 = 2^8 \ mod \ 101 = 256 \ mod \ 101 = 54$$
$$y_2 = 2^9 \ mod \ 101 = 512 \ mod \ 101 = 7$$

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

$$K_s = 7^8 \ mod \ 101 = 5764801 \ mod \ 101 = 24$$
$$K_s = 54^9 \ mod \ 101 = 3904305912313344 \ mod \ 101 = 24$$

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：

$$y_1 = 5^8 \ mod \ 103 = 390625 \ mod \ 103 = 49$$
$$y_2 = 5^9 \ mod \ 103 = 1953125 \ mod \ 103 = 39$$

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

$$K_s = 39^8 \ mod \ 103 = 5352009260481 \ mod \ 103 = 13$$
$$K_s = 49^9 \ mod \ 103 = 1628413597910449 \ mod \ 103 = 13$$

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：

$$y_1 = 2^8 \ mod \ 107 = 256 \ mod \ 107 = 42$$
$$y_2 = 2^9 \ mod \ 107 = 512 \ mod \ 107 = 84$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 84^8 \ mod \ 107 = 2478758911082496 \ mod \ 107 = 12$$
$$K_s = 42^9 \ mod \ 107 = 406671383849472 \ mod \ 107 = 12$$

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：

$$y_1 = 6^8 \ mod \ 109 = 1679616 \ mod \ 109 = 35$$
$$y_2 = 6^9 \ mod \ 109 = 10077696 \ mod \ 109 = 101$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 101^8 \ mod \ 109 = 10828567056280801 \ mod \ 109 = 45$$
$$K_s = 35^9 \ mod \ 109 = 78815638671875 \ mod \ 109 = 45$$

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：

$$y_1 = 3^8 \ mod \ 113 = 6561 \ mod \ 113 = 7$$
$$y_2 = 3^9 \ mod \ 113 = 19683 \ mod \ 113 = 21$$

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

$$K_s = 21^8 \ mod \ 113 = 37822859361 \ mod \ 113 = 64$$
$$K_s = 7^9 \ mod \ 113 = 40353607 \ mod \ 113 = 64$$

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：

$$y_1 = 3^8 \ mod \ 127 = 6561 \ mod \ 127 = 84$$
$$y_2 = 3^9 \ mod \ 127 = 19683 \ mod \ 127 = 125$$

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

$$K_s = 125^8 \ mod \ 127 = 5960464477539062 5 \ mod \ 127 = 2$$
$$K_s = 84^9 \ mod \ 127 = 208215748530929664 \ mod \ 127 = 2$$

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：

$$y_1 = 2^8 \ mod\ 131 = 256 \ mod\ 131 = 125$$
$$y_2 = 2^9 \ mod\ 131 = 512 \ \ mod\ 131 = 119$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 119^8 \ mod\ 131 = 40213853471634241 \ mod\ 131 = 3$$
$$K_s = 125^9 \ mod\ 131 = 7450580596923828125 \ mod\ 131 = 3$$

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：

$$y_1 = 3^8 \ mod\ 137 = 6561 \ mod\ 137 = 122$$
$$y_2 = 3^9 \ mod\ 137 = 19683 \ mod\ 137 = 92$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 92^8 \ mod\ 137 = 5132188731375616 \ mod\ 137 = 56$$
$$K_s = 122^9 \ mod\ 137 = 5987402799531080192 \ mod\ 137 = 56$$

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：

$$y_1 = 2^8 \ mod \ 139 = 256 \ mod \ 139 = 117$$
$$y_2 = 2^9 \ mod \ 139 = 512 \ mod \ 139 = 95$$

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

$$K_s = 95^8 \ mod \ 139 = 6634204312890625 \ mod \ 139 = 131$$
$$K_s = 117^9 \ mod \ 139 = 41084003326878533397 \ mod \ 139 = 131$$

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：

$$y_1 = 2^8 \ mod \ 149 = 256 \ mod \ 149 = 107$$
$$y_2 = 2^9 \ mod \ 149 = 512 \ mod \ 149 = 65$$

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

$$K_s = 65^8 \ mod \ 149 = 318644812890625 \ mod \ 149 = 37$$
$$K_s = 107^9 \ mod \ 149 = 18384592124201545 07 \ mod \ 149 = 37$$

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：

$$y_1 = 6^8 \ mod \ 151 = 1679616 \ mod \ 151 = 43$$
$$y_2 = 6^9 \ mod \ 151 = 10077696 \ mod \ 151 = 107$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 107^8 \ mod \ 151 = 17181861798319201 \ mod \ 151 = 72$$
$$K_s = 43^9 \ mod \ 151 = 502592611936843 \ mod \ 151 = 72$$

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：

$$y_1 = 5^8 \ mod \ 157 = 390625 \ mod \ 157 = 9$$
$$y_2 = 5^9 \ mod \ 157 = 1953125 \ mod \ 157 = 45$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 45^8 \ mod \ 157 = 16815125390625 \ mod \ 157 = 67$$
$$K_s = 9^9 \ mod \ 157 = 387420489 \ mod \ 157 = 67$$

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：

$$y_1 = 2^8 \ mod \ 163 = 256 \ mod \ 163 = 93$$
$$y_2 = 2^9 \ mod \ 163 = 512 \ \ mod \ 163 = 23$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 23^8 \ mod \ 163 = 78310985281 \ mod \ 163 = 85$$
$$K_s = 93^9 \ mod \ 163 = 520411082988487293 \ mod \ 163 = 85$$

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：

$$y_1 = 5^8 \ mod \ 167 = 390625 \ mod \ 167 = 12$$
$$y_2 = 5^9 \ mod \ 167 = 1953125 \ mod \ 167 = 60$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 60^8 \ mod \ 167 = 167961600000000 \ mod \ 167 = 56$$
$$K_s = 12^9 \ mod \ 167 = 5159780352 \ mod \ 167 = 56$$

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：

$$y_1 = 2^8 \ mod \ 173 = 256 \ mod \ 173 = 83$$
$$y_2 = 2^9 \ mod \ 173 = 512 \ mod \ 173 = 166$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 166^8 \ mod \ 173 = 576586811427594496 \ mod \ 173 = 95$$
$$K_s = 83^9 \ mod \ 173 = 186940255267540403 \ mod \ 173 = 95$$

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：

$$y_1 = 2^8 \ mod \ 179 = 256 \ mod \ 179 = 77$$
$$y_2 = 2^9 \ mod \ 179 = 512 \ mod \ 179 = 154$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 154^8 \ mod \ 179 = 316348490636206336 \ mod \ 179 = 61$$
$$K_s = 77^9 \ mod \ 179 = 95151694449171437 \ mod \ 179 = 61$$

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：

$$y_1 = 2^8 \ mod \ 181 = 256 \ mod \ 181 = 75$$
$$y_2 = 2^9 \ mod \ 181 = 512 \ mod \ 181 = 150$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 150^8 \ mod \ 181 = 256289062500000000 \ mod \ 181 = 42$$
$$K_s = 75^9 \ mod \ 181 = 75084686279296875 \ mod \ 181 = 42$$

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：

$$y_1 = 19^8 \ mod \ 191 = 16983563041 \ mod \ 191 = 43$$
$$y_2 = 19^9 \ mod \ 191 = 322687697779 \ mod \ 191 = 53$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 53^8 \ mod \ 191 = 62259690411361 \ mod \ 191 = 97$$
$$K_s = 43^9 \ mod \ 191 = 502592611936843 \ mod \ 191 = 97$$

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：

$$y_1 = 5^8 \ mod\ 193 = 390625 \ mod\ 193 = 186$$
$$y_2 = 5^9 \ mod\ 193 = 1953125 \ mod\ 193 = 158$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 158^8 \ mod\ 193 = 388379855336079616 \ mod\ 193 = 184$$
$$K_s = 186^9 \ mod\ 193 = 266450474490105494016 \ mod\ 193 = 184$$

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：

$$y_1 = 2^8 \ mod\ 197 = 256 \ mod\ 197 = 59$$
$$y_2 = 2^9 \ mod\ 197 = 512 \ mod\ 197 = 118$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 118^8 \ mod\ 197 = 37588592026706176 \ mod\ 197 = 53$$
$$K_s = 59^9 \ mod\ 197 = 8662995818654939 \ mod\ 197 = 53$$

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：

$$y_1 = 3^8 \ mod\ 199 = 6561 \ mod\ 197 = 193$$
$$y_2 = 3^9 \ mod\ 199 = 19683 \ mod\ 197 = 181$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 181^8 \ mod\ 199 = 1151936657823500641 \ mod\ 199 = 62$$
$$K_s = 193^9 \ mod\ 199 = 371548729913362368193 \ mod\ 199 = 62$$

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：

$$y_1 = 2^8 \ mod\ 211 = 256 \ mod\ 211 = 45$$
$$y_2 = 2^9 \ mod\ 211 = 512 \ mod\ 211 = 90$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 90^8 \ mod\ 211 = 4304672100000000 \ mod\ 211 = 151$$
$$K_s = 45^9 \ mod\ 211 = 756680642578125 \ mod\ 211 = 151$$

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：

$$y_1 = 3^8 \ mod\ 223 = 6561 \ mod\ 223 = 94$$
$$y_2 = 3^9 \ mod\ 223 = 19683 \ mod\ 223 = 59$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 59^8 \ mod\ 223 = 146830437604321 \ mod\ 223 = 169$$
$$K_s = 94^9 \ mod\ 223 = 572994802228616704 \ mod\ 223 = 169$$

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：

$$y_1 = 2^8 \ mod\ 227 = 256 \ mod\ 227 = 29$$
$$y_2 = 2^9 \ mod\ 227 = 512 \ mod\ 227 = 58$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 58^8 \ mod\ 227 = 128063081718016 \ mod\ 227 = 65$$
$$K_s = 29^9 \ mod\ 227 = 14507145975869 \ mod\ 227 = 65$$

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：

$$y_1 = 6^8 \ mod \ 229 = 1679616 \ mod \ 229 = 130$$
$$y_2 = 6^9 \ mod \ 229 = 10077696 \ mod \ 229 = 93$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 93^8 \ mod \ 229 = 5595818096650401 \ mod \ 229 = 57$$
$$K_s = 130^9 \ mod \ 229 = 10604499373000000000 \ mod \ 229 = 57$$

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：

$$y_1 = 3^8 \ mod \ 233 = 6561 \ mod \ 233 = 37$$
$$y_2 = 3^9 \ mod \ 233 = 19683 \ mod \ 233 = 111$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 111^8 \ mod \ 233 = 23045377697175681 \ mod \ 233 = 2$$
$$K_s = 37^9 \ mod \ 233 = 129961739795077 \ mod \ 233 = 2$$

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：

$$y_1 = 7^8 \ mod\ 239 = 5764801 \ mod\ 239 = 121$$
$$y_2 = 7^9 \ mod\ 239 = 40353607 \ mod\ 239 = 130$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 130^8 \ mod\ 239 = 81573072100000000 \ mod\ 239 = 122$$
$$K_s = 121^9 \ mod\ 239 = 5559917313492231481 \ mod\ 239 = 122$$

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：

$$y_1 = 7^8 \ mod\ 241 = 5764801 \ mod\ 241 = 81$$
$$y_2 = 7^9 \ mod\ 241 = 40353607 \ mod\ 241 = 85$$

Step 3：
交换公开的数。

Step 4：
各自计算会话密钥：

$$K_s = 85^8 \ mod\ 241 = 2724905250390625 \ mod\ 241 = 143$$
$$K_s = 81^9 \ mod\ 241 = 150094635296999121 \ mod\ 241 = 143$$

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：

$$y_1 = 6^8 \ mod \ 251 = 1679616 \ mod \ 251 = 175$$
$$y_2 = 6^9 \ mod \ 251 = 10077696 \ mod \ 251 = 46$$

Step 3：

交换公开的数。

Step 4：

各自计算会话密钥：

$$K_s = 46^8 \ mod \ 251 = 20047612231936 \ mod \ 251 = 119$$
$$K_s = 175^9 \ mod \ 251 = 153936794281005859375 \ mod \ 251 = 119$$