信息安全导论作业三

验证 D-H 密钥交换机制

Andrade 小组

1. 作业要求

① 小组两位成员（A 和 B）协作完成；
② 使用 100-255 之间的素数（和原根）构建单向函数；
③ 按照 D-H 协议机制流程进行计算；
④ 创建 Word/PDF 文档记录计算过程；

已知：
① 100-255 之间的素数：

p	g	p	g
101	2	179	2
103	5	181	2
107	2	191	19
109	6	193	5
113	3	197	2
127	3	199	3
131	2	211	2
137	3	223	3
139	2	227	2
149	2	229	6
151	6	233	3
157	5	239	7
163	2	241	7
167	5	251	6
173	2		

② 单向函数：

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

2. 完成情况

① Step 0：协商得到 g=5，p=103：

$$y = 5^x \ mod\ 103$$

Step 1：选择私密整数；

Andrade	Bill
$A = 73$	$B = 92$

Step 2：计算公开的数；

Andrade	Bill
$\alpha = 5^{73}\ mod\ 103 = 65$	$\beta = 5^{92}\ mod\ 103 = 28$

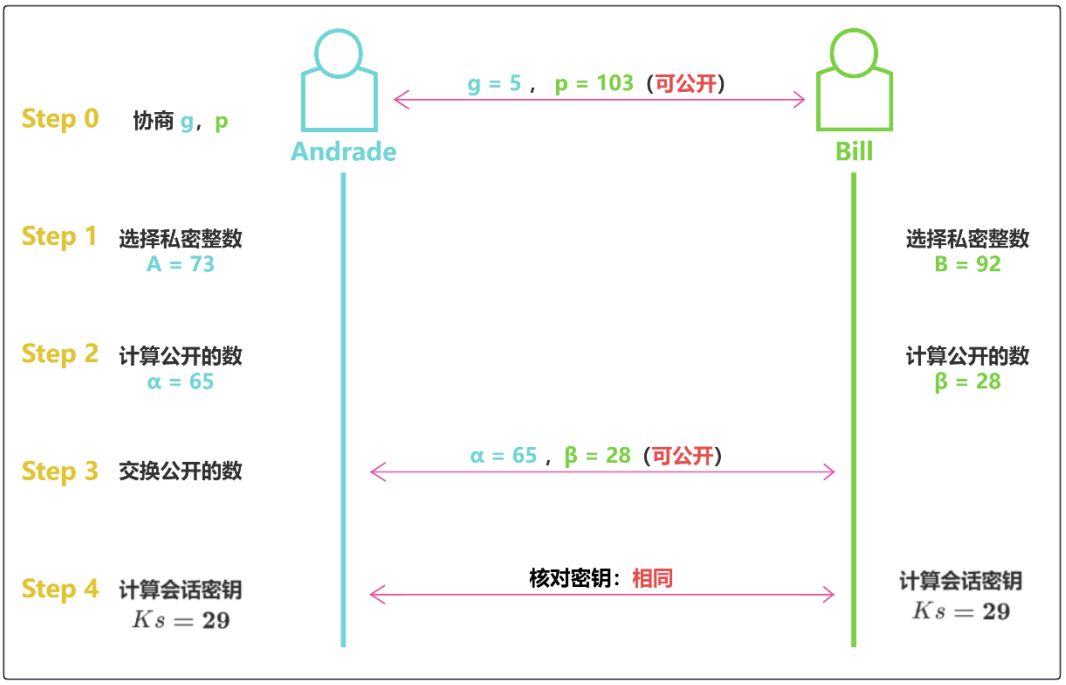
Step 3：相互交换公开的数；

Andrade	Bill
$\alpha = 65$	$\beta = 28$

Step 4：各自计算会话密钥；

Andrade	Bill
$K_s = 28^{73}\ mod\ 103 = 29$	$K_s = 65^{92}\ mod\ 103 = 29$

综上，Andrade 与 Bill 成功交换了密钥$K_s = 29$。



② Step 0：协商得到 g=2，p=107：

$$y = 2^x \ mod \ 107$$

Step 1：选择私密整数；

Andrade	Bill
$A = 50$	$B = 30$

Step 2：计算公开的数；

Andrade	Bill
$\alpha = 2^{50} \ mod \ 107 = 40$	$\beta = 2^{30} \ mod \ 107 = 34$

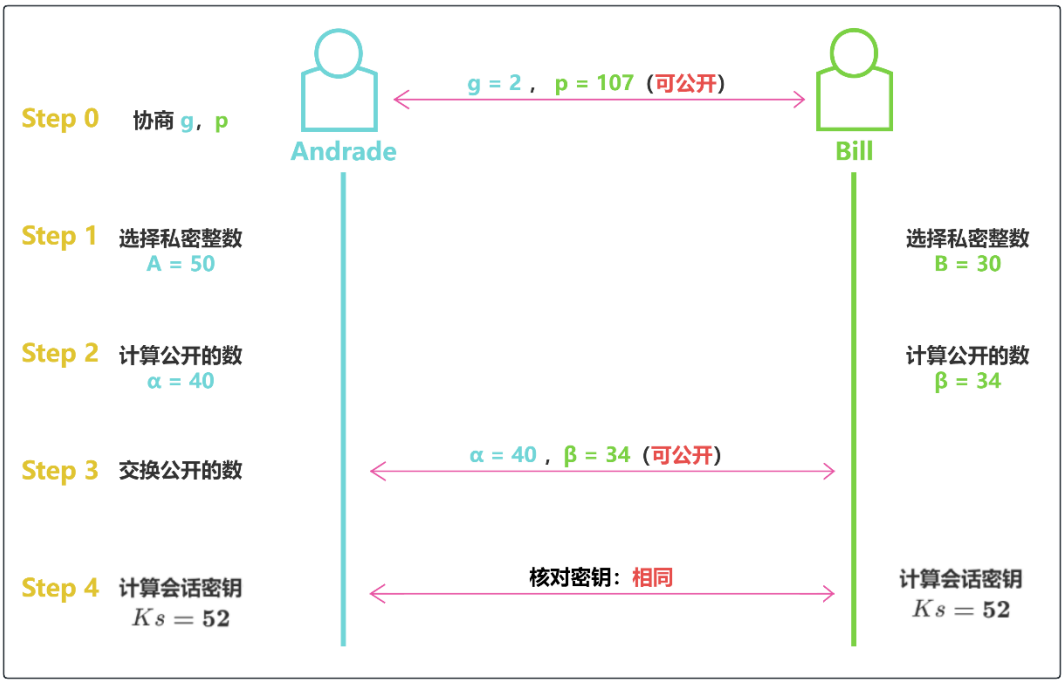
Step 3：相互交换公开的数；

Andrade	Bill
$\alpha = 40$	$\beta = 34$

Step 4：各自计算会话密钥；

Andrade	Bill
$K_s = 34^{50} \ mod \ 107 = 52$	$K_s = 40^{30} \ mod \ 107 = 52$

综上，Andrade 与 Bill 成功交换了密钥$K_s = 52$。



③ Step 0：协商得到 g=3，p=127：

$$y = 3^x \ mod \ 127$$

Step 1：选择私密整数；

Andrade	Bill
$A = 37$	$B = 56$

Step 2：计算公开的数；

Andrade	Bill
$\alpha = 3^{37} \ mod \ 127 = 48$	$\beta = 3^{56} \ mod \ 127 = 68$

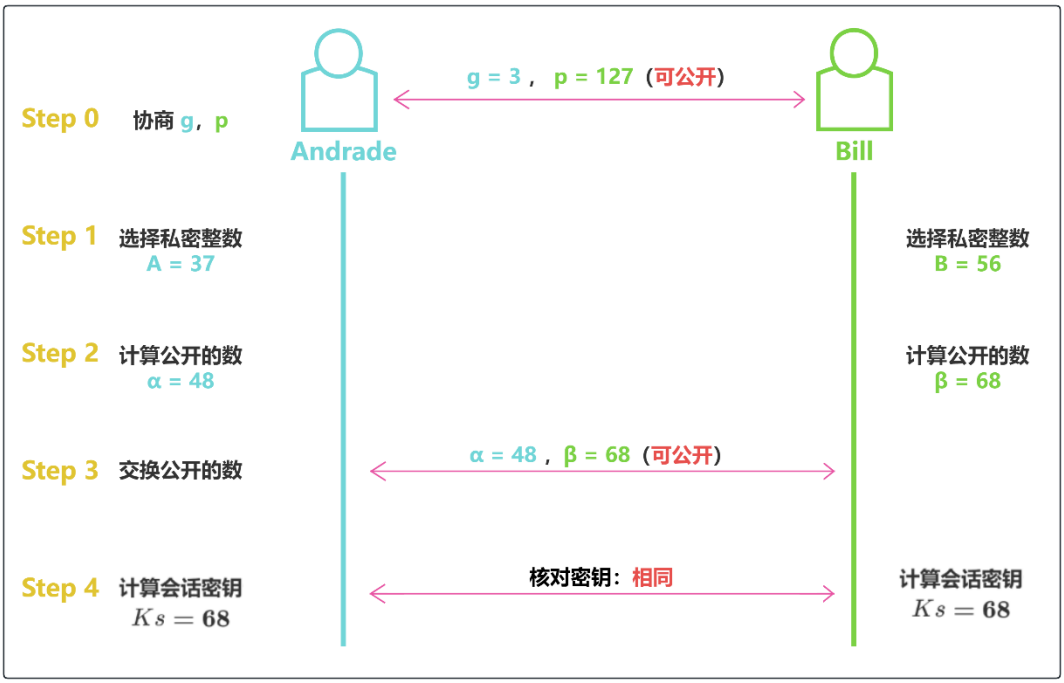
Step 3：相互交换公开的数；

Andrade	Bill
$\alpha = 48$	$\beta = 68$

Step 4：各自计算会话密钥；

Andrade	Bill
$K_s = 68^{37} \ mod \ 127 = 68$	$K_s = 48^{56} \ mod \ 127 = 68$

综上，Andrade 与 Bill 成功交换了密钥$K_s = 68$。



3. 总结

本次信息安全导论课程作业要求小组两位成员（A 和 B）协作完成，使用 100-255 之间的素数（和原根）构建单向函数，并按照 D-H 协议机制流程进行计算，最终将计算过程记录在 Word/PDF 文档中。我们 Andrade 小组通过选取了三组素数和原根的组合进行测试，成功完成了本次的任务，且结果符合预期。

同时我们发现，在有的测试案例（③）中，存在某一方（Bill）公开的整数（β）与最终计算所得会话密钥K_s相同（均为 68）的情况，这可能导致一种安全漏洞，即小子群限制攻击（Small Subgroup Confinement Attack）。这种攻击利用了使用小素数生成的群，导致生成的共享会话密钥的空间非常有限。具体来说，如果 Bill 公开的整数等于生成的会话密钥，由于$K_s = \beta^A \ mod \ p$，攻击者可以通过观察多次密钥交换并比较公开的信息，可能能够推导出 Andrade 的私密整数 A。这是因为在小秘密指数攻击中，攻击者可以观察多个密钥交换，然后根据得到的共享密钥，检查它们是否属于一个小的子群。如果是，攻击者可以利用该信息来推导出私钥，因为在小子群中，可能的私钥值的数量较少，从而降低了安全性。

为了防范这种攻击，选择素数时应确保它足够大，以及避免使用小素数。通常，使用 2048 位或更长的素数是目前推荐的标准，以提供足够的安全性。此外，确保使用良好设计的 D-H 参数也是防范这类攻击的重要措施。

总的而言，在完成本次作业的过程中，我们小组深入理解了 Diffie-Hellman 密钥交换协议的原理，学会了如何使用素数和原根构建安全的单向函数，并了解了该密钥交换协议中可能出现的安全漏洞及防范方法。通过记录计算过程，小组成员更加熟悉了协作过程和文档编写技巧。这次作业对于信息安全课程的学习起到了巩固理论知识和实际操作的作用，使小组成员更加深入地了解了信息安全领域的基础知识，也为今后学习更高级的加密算法和协议打下了坚实的基础。希望在未来的学习中能够更好地应用所学知识，提升信息安全技能。