W5 Problem Set && Programming Assignment

Q1

1.
Consider the toy key exchange protocol using an online trusted 3rd party (TTP) discussed in Lecture 9.1. Suppose Alice, Bob, and Carol are three users of this system (among many others) and each have a secret key with the TTP denoted k_a, k_b, k_c respectively. They wish to generate a group session key k_{ABC} that will be known to Alice, Bob, and Carol but unknown to an eavesdropper. How would you modify the protocol in the lecture to accommodate a group key exchange of this type? (note that all these protocols are insecure against active attacks)

- Alice contacts the TTP. TTP generates a random k_{ABC} and sends to Alice

  $E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E_(k_c, E(k_b, k_{ABC})), \quad \text{ticket}_2 \leftarrow E(k_b, E(k_c, k_{ABC}))$

  Alice sends k_{ABC} to Bob and k_{ABC} to Carol.

- Bob contacts the TTP. TTP generates a random k_{AB} and a random k_{BC}. It sends to Bob

  $E(k_a, k_{AB}), \quad \text{ticket}_1 \leftarrow E(k_a, k_{AB}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{BC}).$

  Bob sends ticket_1 to Alice and ticket_2 to Carol.

- Alice contacts the TTP. TTP generates random k_{ABC} and sends to Alice

  $E(k_a, k_{ABC}), \quad \text{ticket}_1 \leftarrow E(k_b, k_{ABC}), \quad \text{ticket}_2 \leftarrow E(k_c, k_{ABC}).$

  Alice sends ticket_1 to Bob and ticket_2 to Carol.

问：考虑一个简易的密钥交换协议，使用TTP，假设Alice、Bob、Carol为该系统中的三个用户（还有其他用户），每个人都有自己的密钥，记为k_a，k_b，k_c，他们三人期望生成一个组内共享的密钥k_{ABC}，仅有他们三人知道，其他人和窃听者不知道，如何修改课程中介绍的协议以适应这种类型的组密钥交换(请注意：所有这些协议对于主动攻击都是不安全的)

答：第三个选项正确，窃听者只能看到k_{ABC}的加密的结果，而Bob和Carol可以正确使用k_{ABC}，前两个都不行

Q2

2. Let G be a finite cyclic group (e.g. $G = \mathbb{Z}_p^*$) with generator g.

Suppose the Diffie-Hellman function $\mathrm{DH}_g(g^x, g^y) = g^{xy}$ is difficult to compute in G. Which of the following functions is also difficult to compute?

As usual, identify the f below for which the contra-positive holds: if $f(\cdot,\cdot)$ is easy to compute then so is $\mathrm{DH}_g(\cdot,\cdot)$. If you can show that then it will follow that if DH_g is hard to compute in G then so must be f.

- [x] $f(g^x, g^y) = g^{xy+x+y+1}$

  ✓ **正确**
  an algorithm for calculating $f(g^x, g^y)$ can
  easily be converted into an algorithm for
  calculating $\mathrm{DH}(\cdot,\cdot)$.
  Therefore, if f were easy to compute then so would DH,
  contrading the assumption.

- [x] $f(g^x, g^y) = (g^2)^{x+y}$

  ✗ **这个选项的答案不正确**
  It is easy to compute f as $f(g^x, g^y) = (g^x \cdot g^y)^2$.

- [ ] $f(g^x, g^y) = \sqrt{g^{xy}}$

- [x] $f(g^x, g^y) = (\sqrt{g})^{x+y}$

  ✗ **这个选项的答案不正确**
  It is easy to compute f as $f(g^x, g^y) = \sqrt{g^x \cdot g^y}$.

问：记G为一有限循环群，生成元为g，假设D-H函数如图所示，其在G上计算困难，则下列哪个函数也是计算困难的?

答：

1. 由于g^{xy}难计算，所以第一个选项的表达式也难计算
2. 第二个选项表达式可以转换成$g^x \cdot g^y$
3. 第三个同理
4. 第四个同理

Q3

3.

Suppose we modify the Diffie-Hellman protocol so that Alice operates as usual, namely chooses a random a in $\{1, ..., p-1\}$ and sends to Bob $A \leftarrow g^a$. Bob, however, chooses a random b in $\{1, ..., p-1\}$ and sends to Alice $B \leftarrow g^{1/b}$. What shared secret can they generate and how would they do it?

- secret $= g^{a/b}$. Alice computes the secret as $B^{1/b}$ and Bob computes A^a.
- secret $= g^{ab}$. Alice computes the secret as $B^{1/a}$ and Bob computes A^b.
- secret $= g^{a/b}$. Alice computes the secret as B^a and Bob computes $A^{1/b}$.

问：假设修改一下D-H协议，Alice和以前一样随机从{1, ..., p−1}中选择a，然后将$A=g^a$发送给Bob，但Bob选择b之后计算$B=g^{1/b}$，则他们之间会生成何种共享信息，应当如何操作?

答：还是和原来一样，Alice把收到的B和自己的A乘起来，Bob同理，最后得到共享信息$g^{a/b}$，然后分别按原来的流程计算各自的参数即可

Q4

4. Consider the toy key exchange protocol using public key encryption described in Lecture 9.4.

Suppose that when sending his reply $c \leftarrow E(pk, x)$ to Alice, Bob appends a MAC $t := S(x, c)$ to the ciphertext so that what is sent to Alice is the pair (c, t). Alice verifies the tag t and rejects the message from Bob if the tag does not verify.

Will this additional step prevent the man in the middle attack described in the lecture?

- ○ yes
- ◉ no
- ○ it depends on what MAC system is used.
- ○ it depends on what public key encryption system is used.

✓ 正确

an active attacker can still decrypt $E(pk', x)$ to recover x

and then replace (c, t) by (c', t')

where $c' \leftarrow E(pk, x)$ and $t \leftarrow S(x, c')$.

问：考虑一个采用公钥加密的密钥交换协议（如9-4中的那种），假设Bob发送c=E(pk,x)给Alice时，在尾部加入一个MAC t:=S(x,c)，Alice此时收到(c,t)，然后Alice验证这个tag t，如果验证不通过则拒绝这条消息，则这个额外的添加MAC的步骤可以防止MITM攻击吗?

答：不行，主动攻击者依然可以用自己的密钥来代替原来的pk，并重新计算密文和MAC

Q5

5. The numbers 7 and 23 are relatively prime and therefore there must exist integers a and b such that $7a + 23b = 1$.

Find such a pair of integers (a, b) with the smallest possible $a > 0$.

Given this pair, can you determine the inverse of 7 in $\mathbb{Z}_{23}$?

Enter below comma separated values for a, b, and for 7^{-1} in $\mathbb{Z}_{23}$.

10,20

✗ 错误

问：对于7a+23b=1这个等式，找到一对整数对(a,b)，使其满足该等式且a为最小正整数，对于这个整数对(a,b)，能否确定7在mod 23下的逆?

答：a=23n+10，b=-7n-3，取n=0即可，即(a,b)=(10,-3)

Q6

6. Solve the equation $3x + 2 = 7$ in $\mathbb{Z}_{19}$.

8

✓ 正确

$x = (7 - 2) \times 3^{-1} \in \mathbb{Z}_{19}$

问：计算3x+2 ≡ 7 (mod 19)

答：8

Q7

7. How many elements are there in $\mathbb{Z}_{35}^*$?

24

✓ 正确

$|\mathbb{Z}_{35}^*| = \varphi(7 \times 5) = (7 - 1) \times (5 - 1).$

问：模35中与35互素的数有几个

答：由欧拉φ函数可知有24个

Q8

8. How much is $2^{10001} \bmod 11$?

Please do not use a calculator for this. Hint: use Fermat's theorem.

2

✓ 正确

By Fermat $2^{10} = 1$ in $\mathbb{Z}_{11}$ and therefore

$1 = 2^{10} = 2^{20} = 2^{30} = 2^{40}$ in $\mathbb{Z}_{11}$.

Then $2^{10001} = 2^{10001 \bmod 10} = 2^1 = 2$ in $\mathbb{Z}_{11}$.

问：2^{10001} mod 11的结果

答：由$2^{10} \equiv 1 \pmod{11}$可知，$2^{10001} \equiv 2 \cdot (2^{10})1000 \equiv 2 \pmod{11}$

Q9

9. While we are at it, how much is $2^{245} \bmod 35$?

Hint: use Euler's theorem (you should not need a calculator)

32

✓ 正确

By Euler $2^{24} = 1$ in $\mathbb{Z}_{35}$ and therefore

$1 = 2^{24} = 2^{48} = 2^{72}$ in $\mathbb{Z}_{35}$.

Then $2^{245} = 2^{245 \bmod 24} = 2^5 = 32$ in $\mathbb{Z}_{35}$.

问：

答：和上一题类似解法

Q10

10. What is the order of 2 in $\mathbb{Z}_{35}^*$?

12

✓ 正确

$2^{12} = 4096 = 1$ in $\mathbb{Z}_{35}$ and 12 is the

smallest such positive integer.

问：模35下2的阶

答：12

Q11

11. Which of the following numbers is a generator of $\mathbb{Z}_{13}^*$?

- [x] 7, $\langle 7 \rangle = \{1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2\}$

✓ 正确
correct, 7 generates the entire group $\mathbb{Z}_{13}^*$

- [x] 3, $\langle 3 \rangle = \{1, 3, 9\}$

✗ 这个选项的答案不正确
No, 3 only generates three elements in $\mathbb{Z}_{13}^*$.

- [ ] 5, $\langle 5 \rangle = \{1, 5, 12, 8\}$
- [ ] 2, $\langle 2 \rangle = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$
- [ ] 10, $\langle 10 \rangle = \{1, 10, 9, 12, 3, 4\}$

问：Z_{13}*的生成元是哪个

答：

Q12

12. Solve the equation $x^2 + 4x + 1 = 0$ in $\mathbb{Z}_{23}$.

Use the method described in Lecture 10.3 using the quadratic formula.

14,5

✓ 正确
The quadratic formula gives the two roots in $\mathbb{Z}_{23}$.

问：mod 23下解二次同余式

答：14和5

Q13

13. What is the 11th root of 2 in $\mathbb{Z}_{19}$?

(i.e. what is $2^{1/11}$ in $\mathbb{Z}_{19}$)

Hint: observe that $11^{-1} = 5$ in $\mathbb{Z}_{18}$.

13

✓ 正确

$2^{1/11} = 2^5 = 32 = 13$ in $\mathbb{Z}_{19}$.

问：模19下2的11次根

答：13

Q14

14. What is the discete log of 5 base 2 in $\mathbb{Z}_{13}$?

(i.e. what is $\mathrm{Dlog}_2(5)$)

Recall that the powers of 2 in $\mathbb{Z}_{13}$ are $\langle 2 \rangle = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$

9

✓ 正确

$2^9 = 5$ in $\mathbb{Z}_{13}$.

问：模13下2为底5的离散对数

答：9

Q15

15. If p is a prime, how many generators are there in $\mathbb{Z}_p^*$?

- ○ $(p+1)/2$
- ○ $\sqrt{p}$
- ○ $p-1$
- ◉ $\varphi(p-1)$

✓ 正确

The answer is $\varphi(p-1)$. Here is why. Let g be some generator of $\mathbb{Z}_p^*$ and let $h = g^x$ for some x.

It is not difficult to see that h is a generator exactly when we can write g as $g = h^y$ for some integer y (h is a generator because if $g = h^y$ then any power of g can also be written as a power of h).

Since $y = x^{-1} \bmod p-1$ this y exists exactly when x is relatively prime to $p-1$. The number of such x is the size of $\mathbb{Z}_{p-1}^*$ which is precisely $\varphi(p-1)$.

问：若p为素数，则Z_p*的生成元有多少个

答：