Congratulations! You passed!

TO PASS 80% or higher

Keep Learning

Retake the assignment in **7h 50m**

GRADE
93.33%

Week 5 - Problem Set

LATEST SUBMISSION GRADE
93.33%

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)

0 / 1 point

- (•) Alice contacts the TTP. TTP generates a random k_{AB} and a random k_{AC}. It sends to Alice

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

  Alice sends ticket_1 to Bob 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.
- ( ) 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 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.

> **Incorrect**
> The protocol does not work because Alice, Bob, and Carol
> end up with different keys: Alice and Bob get k_{AB} while Carol gets k_{AC}.

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

1 / 1 point

Suppose the Diffie-Hellman function $\text{DH}_g(g^x, g^y) = g^{xy}$ 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 $\text{DH}_g(\cdot,\cdot)$. 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] $f(g^x, g^y) = g^{x(y+1)}$

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

- [ ] $f(g^x, g^y) = g^{x+y}$
- [x] $f(g^x, g^y) = (g^{3xy}, g^{2xy})$ (this function outputs a pair of elements in G)

> **Correct**
> an algorithm for calculating $f(\cdot,\cdot)$ can
> easily be converted into an algorithm for
> calculating $\text{DH}(\cdot,\cdot)$.
> Therefore, if f were easy to compute then so would DH,
> contrading the assumption.

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

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

1 / 1 point

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

> **Correct**
> This is correct since it is not difficult to see that
> both will obtain $g^{a/b}$

4. Consider the toy key exchange protocol using public key encryption described in [Lecture 9.4]().

1 / 1 point

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?

- (•) no
- ( ) yes
- ( ) it depends on what MAC system is used.
- ( ) it depends on what public key encryption system is used.

> **Correct**
> 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 $t \leftarrow S(x, c')$.

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

1 / 1 point

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,-3,10

> **Correct**
> $7 \times 10 + 23 \times (-3) = 1$.
> Therefore $7 \times 10 = 1$ in $\mathbb{Z}_{23}$ implying
> that $7^{-1} = 10$ in $\mathbb{Z}_{23}$.

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

1 / 1 point

8

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

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

1 / 1 point

24

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

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

1 / 1 point

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

2

> **Correct**
> 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 $\mathbb{Z}_{11}$.

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

1 / 1 point

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

32

> **Correct**
> 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 $\mathbb{Z}_{35}$.

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

1 / 1 point

12

> **Correct**
> $2^{12} = 4096 = 1$ in $\mathbb{Z}_{35}$ and 12 is the
> smallest such positive integer.

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

1 / 1 point

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

> **Correct**
> correct, 6 generates the entire group $\mathbb{Z}_{13}^*$

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

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

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

1 / 1 point

Use the method described in [Lecture 10.3]() using the quadratic formula.

14,5

> **Correct**
> The quadratic formula gives the two roots in $\mathbb{Z}_{23}$.

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

1 / 1 point

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

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

13

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

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

1 / 1 point

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

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

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

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

1 / 1 point

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

> **Correct**
> 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 $\varphi(p-1)$.