✓ 答案! 恭喜了!

提交时间: 10/1 (周四)

提交内容

得分 100%

Week 5 - Problem Set

提交时间: 10/1 (周四)

100%

1. Consider the ring ring perhaps protect using an online research Kapsity. 10分

FTP Microsoft Kapsity Kapsity online Web, Web, and are is or find

cases of this system protect ring ring Kapsity protect Kapsity are or find

with the FTP Microsoft $\mathbb{Z}_2$, $\mathbb{Z}_3$, respectively. Ring systems

generate a group second ring. Even. Web and the server is Web,

Web, and room from and room is or a second group. How

would you modify the protocol in the lecture to accommodate a group ring

exchange of this type? Note that all these protocols are insecure against

active attacks.

- Web and room is the FTP. FTP generates a random k or, and is an Web Even. It sends to Web

$$E(k, K_{pub}), \text{ where } c_1 = E(k, K_{pub}) \quad \text{Web key} = E(k, K_{pub})$$

Web and room is Web, k is Web and Web, k is room

- Web and room is the FTP. FTP generates a random k_{pub}, and is an Web k_{pub}. It sends to Web

$$E(k, K_{pub}), \text{ where } c_1 = E(k, K_{pub}) \quad \text{Web key} = E(k, K_{pub})$$

Web and room is Web k is Web and Web k is room

- Web and room is the FTP. FTP generates a random k_{pub}, and sends to Web

$$E(k_1, \text{Even}), \text{ where } c_1 = E(k_1, \text{Even}) \quad \text{Web key} = E(k_1, E(k_2, \text{Even}))$$

Web and room is Web and k_{pub} is room

- Web and room is the FTP. FTP generates a random k_{pub}, and sends to Web

$$E(k_1, \text{Even}), \text{ where } c_1 = E(k_1, \text{Even}) \quad \text{Web key} = E(k_1, E(k_2, \text{Even}))$$

Web and room is Web and Web k_{pub} is room

- Web and room is the FTP. FTP generates a random k_{pub}, and sends to Web

$$E(k, K_{pub}), \text{ where } c_1 = E(k, K_{pub}) \quad \text{Web key} = E(k_1, E(k_2, K_{pub}))$$

Web and room is Web, k is Web and Web, k is room

✓ 答案

The protocol works because both Web, Web, and room

either know or have a common key, and are ignorant

of k_{pub}, and thus they know that

$$E(k_{pub}, \text{Web key}) = \text{Web key}$$

2. Let Z Nov. 分解 prime group $(p, G) = (\mathbb{Z}_{11}, \text{gen generator})$. 10分

Suppose the Web Web Web Even Even $\mathrm{DH}_{\mathbb{Z}_{11}}(\mathbb{Z}^{\text{Web}}, \mathbb{Z}^{\text{Even}}) = \mathbb{Z}^{\text{Web}}$ is difficult to compute in G. Which of the following functions is also difficult to compute?

As usual, identify the $\mathbb{Z}$ Web for which the online protocols Web $\in \mathbb{Z}_{11}^*$. Use key to compute the exp in $\mathbb{Z}_{\mathbb{Z}_{11}^*} \cong \mathbb{Z}$ if you

are unsure that Even Web Even Web Even is a hard to compute. Hint: Use Even Web $\mathbb{Z}$

- $\mathrm{DH}_{\mathbb{Z}_{11}^*}(\mathbb{Z}^{\text{Even}}, \mathbb{Z}^{\text{Web}})$
- $\mathrm{DH}_{\mathbb{Z}_{11}^*}(\mathbb{Z}^{\text{Even}}, \mathbb{Z}^{\text{Even}})$

✓ 答案

an algorithm for calculating $\mathrm{DH}_{\mathbb{Z}_{11}^*}(\mathbb{Z}^{\text{Even}}, \mathbb{Z}^{\text{Even}})$ can

easily be converted into an algorithm for

calculating $\mathrm{DH}(\ldots)$.

Therefore, if $\mathbb{Z}$ were easy to compute then so would DH,

contradicting the assumption.

- $\mathrm{DH}_{\mathbb{Z}_{11}^*}(\mathbb{Z}^{\text{Even}}, \mathbb{Z}^{\text{Even}})$
- $\mathrm{DH}_{\mathbb{Z}_{11}^*}(\mathbb{Z}^{\text{Even}}, \mathbb{Z}^{\text{Even}})$
- $\mathrm{DH}_{\mathbb{Z}_{11}^*}(\mathbb{Z}^{\text{Even}}, \mathbb{Z}^{\text{Even}})$

✓ 答案

an algorithm for calculating $\mathrm{DH}_{\mathbb{Z}_{11}^*}(\mathbb{Z}^{\text{Even}}, \mathbb{Z}^{\text{Even}})$ can

easily be converted into an algorithm for

calculating $\mathrm{DH}(\ldots)$.

Therefore, if $\mathbb{Z}$ were easy to compute then so would DH,

contradicting the assumption.

3. Suppose we modify the Web Web protocol protocol so that Web squares

at random. Identify Web Even Even Even Even $(c_1, \ldots, c_n) = (c_1^2, \ldots, c_n^2)$ and

sends to Web $d_1, \ldots, d_n$. Web receives, chooses a random b,

$$b \in \{0, \ldots, p-1\}, \text{ and sends to Web Even } \mathbb{Z} = \mathbb{Z}^{b \bmod p}$$

Web Even and Web Even Even Even and Web Even Web Even Web

- answer: $c_1 = \mathbb{Z}^{b}$ Even computes the secret as $\mathbb{Z}^{b}$

and Web computes $\mathbb{Z}^{b}$

- answer: $c_1 = \mathbb{Z}^{b}$ Even computes the secret as $\mathbb{Z}^{b/2}$

and Web computes $\mathbb{Z}^{b}$

- answer: $c_1 = \mathbb{Z}^{b}$ Even computes the secret as $\mathbb{Z}^{b}$

and Web computes $\mathbb{Z}^{b}$

- answer: $c_1 = \mathbb{Z}^{b}$ Even computes the secret as $\mathbb{Z}^{b/2}$

and Web computes $\mathbb{Z}^{b}$

✓ 答案

This is correct since it is not difficult to see that

both sides compute $\mathbb{Z}^{b/2}$.

4. Consider the ring ring perhaps protect using public key and given described Web. 10分

Suppose the online sending the key $c_1 = E(pk, k)$ is insecure, Web upgrade a new $c_1 = E(c_1, c)$ to be a ciphertext on the

value c sent to Even. Web c_1 $E(pk)$ remains, chosen a random k.

$$c_1 = E(c_1, c) \quad c_1 = E(c_1, c) \text{ is intended to Web } c = \mathbb{Z}^{k \bmod p}$$

Web Even and Web Even Even Even and Web Even Web Even Web

- answer: $c_1 = \mathbb{Z}^{k}$ Even computes the secret as $\mathbb{Z}^{k}$

and Web computes $\mathbb{Z}^{k}$

- answer: $c_1 = \mathbb{Z}^{k}$ Even computes the secret as $\mathbb{Z}^{k/2}$

and Web computes $\mathbb{Z}^{k}$

- answer: $c_1 = \mathbb{Z}^{k}$ Even computes the secret as $\mathbb{Z}^{k}$

and Web computes $\mathbb{Z}^{k}$

- answer: $c_1 = \mathbb{Z}^{k}$ Even computes the secret as $\mathbb{Z}^{k/2}$

and Web computes $\mathbb{Z}^{k}$

✓ 答案

This is correct since it is not difficult to see that

both sides compute $\mathbb{Z}^{k/2}$.

5. Prove Lemma 1 and show rapidly prime and find the cheap mod-exp integer a and $\mathbb{Z}$ with the Web Web. 10分

Find such a pair of integers $(a, \mathbb{Z})$ satisfy the whether predicate $a = 10$.

Search the pair, can you determine the mod-exp of $\mathbb{Z}$ in Even

Web Web. Write separated values for a, $\mathbb{Z}$, a series $\mathbb{Z} = a_0 \mathbb{Z}_{\mathbb{Z}}$

a_0, a_1, a_2

✓ 答案

$\{1, 10, 100, 1, 10, -1\}$.

Therefore $\mathbb{Z} = 10 \in \mathbb{Z}_{\mathbb{Z}}$ mapping

$\mathrm{exp}\,\mathbb{Z}^{-1} = 10 \in \mathbb{Z}_{\mathbb{Z}}$.

6. Solve the equation for x: $3 = 7 \bmod \mathbb{Z}_{\mathbb{Z}}$. 10分

x

✓ 答案

$x = \mathbb{Z}^{-1}(3) = \mathbb{Z}^{-1} \in \mathbb{Z}_{\mathbb{Z}}$.

7. How many elements are there in $\mathbb{Z}_{\mathbb{Z}}^{\mathbb{Z}}$? 10分

$\mathbb{Z}$

✓ 答案

$|\mathbb{Z}_{\mathbb{Z}}^{\mathbb{Z}}| = \varphi(\mathbb{Z}^{\mathbb{Z}}) = (\mathbb{Z}^{\mathbb{Z}} - \mathbb{Z}) \in \{\mathbb{Z}, \ldots, \mathbb{Z}\}$.

8. How much is $\mathbb{Z}^{\text{Web}}$ Web Even? 10分

Please do not use a calculator for this. Web, you know it's Even.

$\mathbb{Z}$

✓ 答案

By Even $\mathbb{Z}^{\mathbb{Z}} = 1 \in \mathbb{Z}_{\mathbb{Z}}$ and therefore

$$\mathbb{Z} = \mathbb{Z}^{\mathbb{Z}} = \mathbb{Z}^{\mathbb{Z}} = \mathbb{Z}^{\mathbb{Z}} \in \mathbb{Z}_{\mathbb{Z}}.$$

$$\text{Hence } \mathbb{Z}^{\text{Web}} = \mathbb{Z}^{\text{Web} \bmod \mathbb{Z}} = \mathbb{Z}^{\mathbb{Z}} = \mathbb{Z} \in \mathbb{Z}_{\mathbb{Z}}.$$

9. Write one x or y $\in$ Even such $\mathbb{Z}^{\text{Web}}$ and $\mathbb{Z}^{\mathbb{Z}}$. 10分

Hint: note that $\mathbb{Z}$ Web Even Even Even Web Web is a solution.

$\mathbb{Z}$

✓ 答案

By Even $\mathbb{Z}^{\mathbb{Z}} = 1 \in \mathbb{Z}_{\mathbb{Z}}$ and therefore

$$x = \mathbb{Z}^{\text{Web}}, \; y^{\mathbb{Z}} = \mathbb{Z}^{\text{Web}} \in \mathbb{Z}_{\mathbb{Z}}$$

$$\text{Hence } \mathbb{Z}^{\text{Web}} = \mathbb{Z}^{\text{Web} \bmod \mathbb{Z}} = \mathbb{Z}^{\mathbb{Z}} = \mathbb{Z} \in \mathbb{Z}_{\mathbb{Z}}.$$

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

$\mathbb{Z}$

✓ 答案

$\mathbb{Z}^{\mathbb{Z}} = \mathbb{Z}\mathbb{Z} = 1 \in \mathbb{Z}_{\mathbb{Z}}$ and so we the

smallest such positive integer.

11. Which of the following numbers is a

generator of $\mathbb{Z}_{\mathbb{Z}}^{\mathbb{Z}}$? 10分

- A. $\{\mathbb{Z}\} = \{\mathbb{Z}, \mathbb{Z}\}$
- B. $\mathbb{Z}\mathbb{Z}$. $\{\mathbb{Z}\} = \{\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\}$
- C. $\{\mathbb{Z}\} = \{\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\}$

✓ 答案

Indeed, $\mathbb{Z}$ generates the entire group $\mathbb{Z}_{\mathbb{Z}}^{\mathbb{Z}}$.

- A. $\{\mathbb{Z}\} = \{\mathbb{Z}, \mathbb{Z}\mathbb{Z}\}$
- B. $\{\mathbb{Z}\} = \{\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}\mathbb{Z}, \mathbb{Z}