



Міністерство освіти і науки України

КПІ ім. Ігоря Сікорського

Звіт

З дисципліни “Безпека інформаційних систем”

студента III курсу ФІОТ

групи ІК-12

Мельнічука Іллі

Перевірив:

Викладач кафедри

Інформаційних систем та технологій

Шимкович Л. Л.

Київ 2023

Тема: Дослідження криптосистеми Діффі-Хеллман (Diffie-Hellman)

РўРµСѓС, — □ ×

1. Для чего используется алгоритм Diffie-Hellman?

☐ Шифрование сообщений

☒ Обмен секретным ключом

☐ Оба варианта

>>

РўРµСѓС, — □ ×

2. Каким необходимо выбрать число n ?

☐ Комплексное число

☒ Большое простое число

☐ Возможны оба варианта

>>

РўРµСѓС, — □ ×

3. Каким необходимо выбрать число g ?

☒ Любое g , которое является примитивом mod n

☐ Любое число

☐ Только большое простое число

>>

РўРµСғС,

4. Какое число наибольшим образом влияет на безопасность шифра?

☐ x

☐ g

☒ n

>>

РўРµСғС,

5. Какое условие выбора числа n ?

☐ n - большое простое число

☐ $(n-1)/2$ - простое число

☒ Оба варианта

>>

РўРµСғС,

6. Можно ли передавать числа n, g, x, y по несекретному каналу?

☒ Да

☐ Нет

☐ Только n и g

>>

РўРµСғС,

**7. Заданы числа $n=563$, $g=467$, $x=123$, $y=321$.
Посчитайте число X , которое необходимо переслать
стороне В**

X

>>

$$X = g^x \bmod(n) = 467^{123} \bmod(563) = 518$$

РўРµСғС,

**8. Сторона В пересылает число $Y=427$ ($n=563$ $x=123$).
Вычислите ключ k**

k

>>

$$k = Y^x \bmod(n) = 427^{123} \bmod(563) = 381$$

РўРµСғС,

**9. Заданы числа $n=107$, $g=59$, $x=123$, $y=321$, $z=345$.
Посчитайте ключ k для 3-х участников**

k

>>

Обчисляемо X , Y , Z

$$X = g^x \bmod(n) = 59^{123} \bmod(107) = 74$$

$$Y = g^y \bmod(n) = 59^{321} \bmod(107) = 46$$

$$Z = g^z \bmod(n) = 59^{345} \bmod(107) = 72$$

$$Z^x = Z^x \bmod(n) = 72^{123} \bmod(107) = 51$$

$$X^y = X^y \bmod(n) = 74^{321} \bmod(107) = 15$$

$$Y^z = Y^z \bmod(n) = 46^{345} \bmod(107) = 32$$

$$k = Y^x \bmod(n) = 32^{123} \bmod(107) = 78$$

$$k = Z^y \bmod(n) = 51^{321} \bmod(107) = 78$$

$$k = X^z \bmod(n) = 15^{345} \bmod(107) = 78$$

Результат:

