



Міністерство освіти і науки України

Національний технічний університет України

“Київський політехнічний інститут імені Ігоря Сікорського”

Факультет інформатики та обчислювальної техніки

Кафедра інформаційних систем та технологій

Лабораторна робота №4

Безпека інформаційних систем

«Дослідження криптосистеми Діффі-Хеллман (Diffie-Hellman).»

Виконала:

студентка групи IA-34

Мартинюк Т.В.

Перевірила:

Шимкович Л. Л.

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

Хід роботи:

Тест

1. Для чого застосовується алгоритм Diffie-Hellman?

Шифрування повідомень
 Обмін секретним ключем
 Два варіанти

>>

Тест

2. Яким потрібно вибирати число n ?

Комплексне число
 Велике просте число
 Можливі два варіанти

>>

Тест

3. Яким необхідно вибирати число g ?

Будь-яке g , яке є первісним mod n
 Любой число
 Тільки велике просте число

>>

Тест

4. Яке число найбільше впливає на безпеку шифру ?

x
 g
 n

>>

Тест

5. Яка умова вибору числа n ?

n - велике просте число
 $(n-1)/2$ - просте число
 Оба варіанти

>>

Тест

6. Чи можна передавати числа n, g, X, Y несекретним каналом?

Да
 Ні
 Тільки n

>>

Num	A	Відкритий канал	B
1	x – випадкове велике ціле число	n, g	y – випадкове велике ціле число
2	$X \equiv g^x \pmod{n}$	<Обмін>	$Y \equiv g^y \pmod{n}$
3	$k \equiv Y^x \pmod{n}$		$k' \equiv X^y \pmod{n}$

Тест

7. Задано числа $n=479$, $g=107$, $x=123$, $y=321$. Порахуйте число X , яке необхідно надіслати стороні B

X

>>

$$X = (g^x) \pmod{n} = (107^{123}) \pmod{479} = 323$$

$$Y = (g^y) \pmod{n} = (107^{321}) \pmod{479} = 448$$

$$k = (Y^x) \pmod{n} = (448^{123}) \pmod{479} = 11$$

Тест

**8. Сторона В пересилає число $Y = 448$ ($n=479$ $x=123$).
Обчисліть ключ k**

k

$$k = (X^y) \bmod n = (323^321) \bmod 479 = 11$$

Nu m	A	Відкритий канал	B	Відкритий канал	C	Відкритий канал
1	x – випадкове велике ціле число	n, g	y – випадкове велике ціле число		z – випадкове велике ціле число	
2	$X \equiv g^x \pmod{n}$	Обмін>	$Y \equiv g^y \pmod{n}$	Обмін>	$Z \equiv g^z \pmod{n}$	Обмін>
3	$Z' \equiv Z^x \pmod{n}$	Обмін>	$X' \equiv X^y \pmod{n}$	Обмін>	$Y' \equiv Y^z \pmod{n}$	Обмін>
4	$k = Y'^x \pmod{n}$		$k1 = Z'^y \pmod{n}$		$k2 = X'^z \pmod{n}$	

$$X = (g^x) \bmod n = (107^123) \bmod 479 = 323$$

$$Y = (g^y) \bmod n = (107^321) \bmod 479 = 448$$

$$Z = (g^z) \bmod n = (107^345) \bmod 479 = 361$$

$$Z' = (Z^x) \bmod n = (361^123) \bmod 479 = 220$$

$$X' = (X^y) \bmod n = (321^321) \bmod 479 = 11$$

$$Y' = (Y^z) \bmod n = (448^345) \bmod 479 = 112$$

$$k = (Y'^x) \bmod n = (112^123) \bmod 479 = 161$$

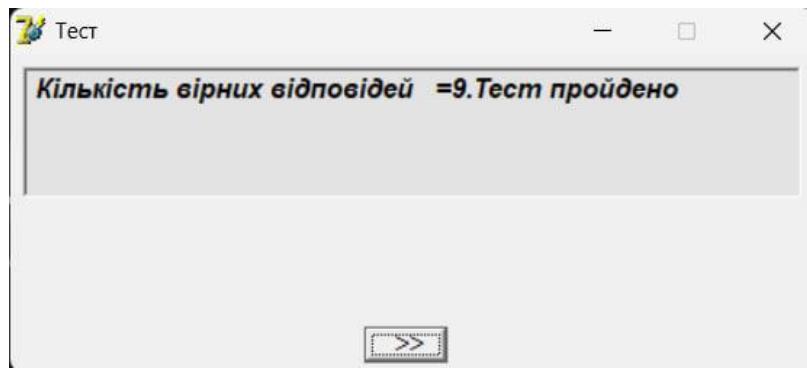
$$k1 = (Z'^y) \bmod n = (220^321) \bmod 479 = 161$$

$$k2 = (X'^z) \bmod n = (11^345) \bmod 479 = 161$$

Тест

**9. Задано числа $n=479$, $g=107$, $x=123$, $y=321$, $z=345$.
Порахуйте ключ k для трьох учасників**

k



Висновок: Під час виконання даної лабораторної роботи ми дослідили крипtosистему Діффі-Хеллмана.