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 ІА-34

Мартинюк Т.В.

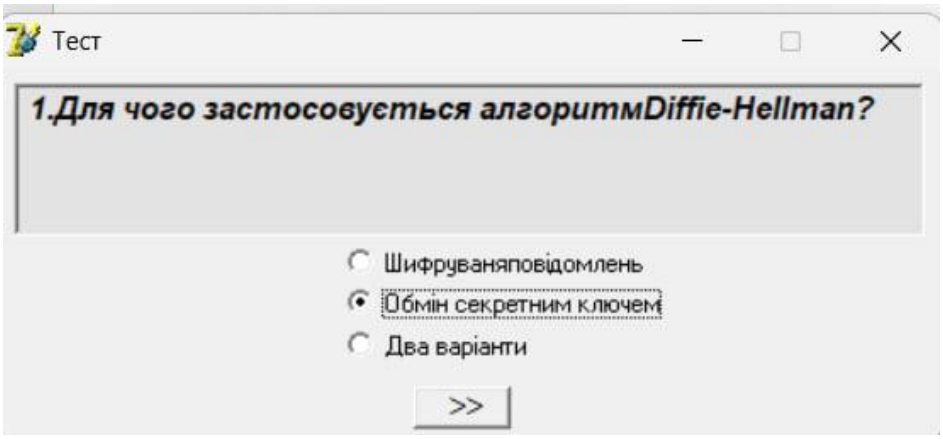
Перевірила:

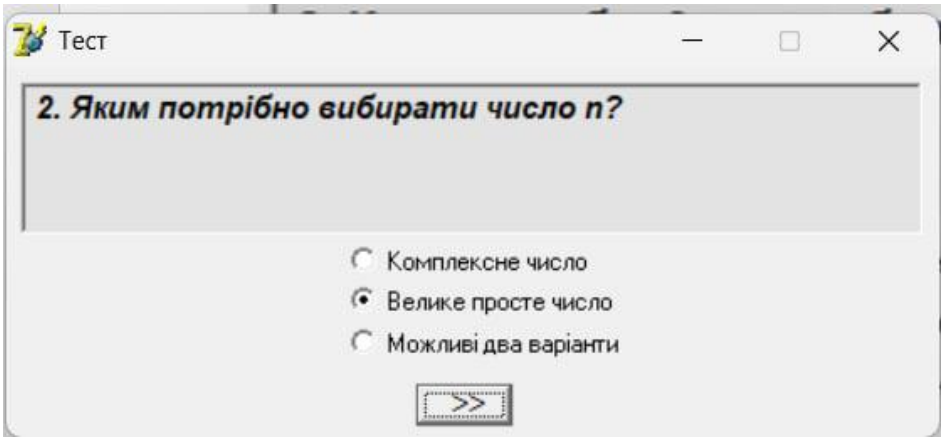
Шимкович Л. Л.

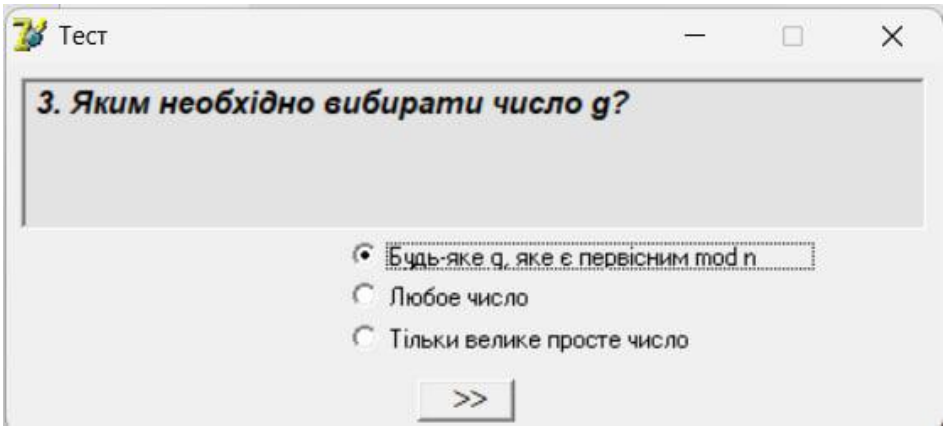
Київ – 2025

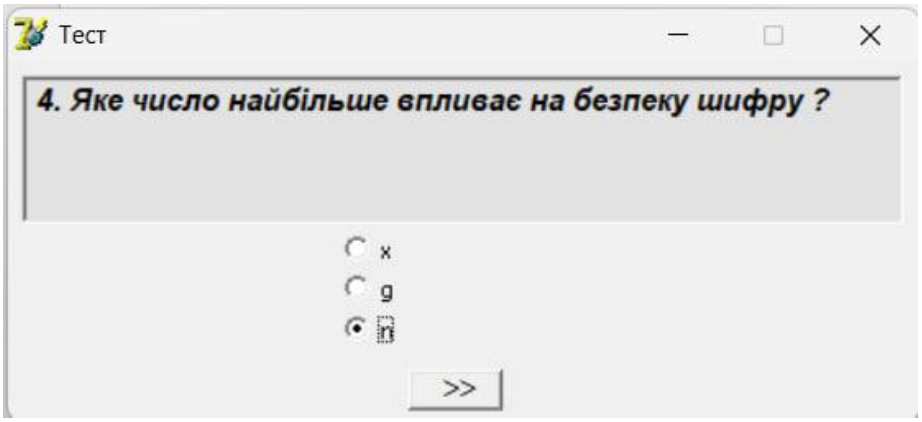
Тема: Дослідження криптосистеми Діффі-Хеллман (Diffie-Hellman).

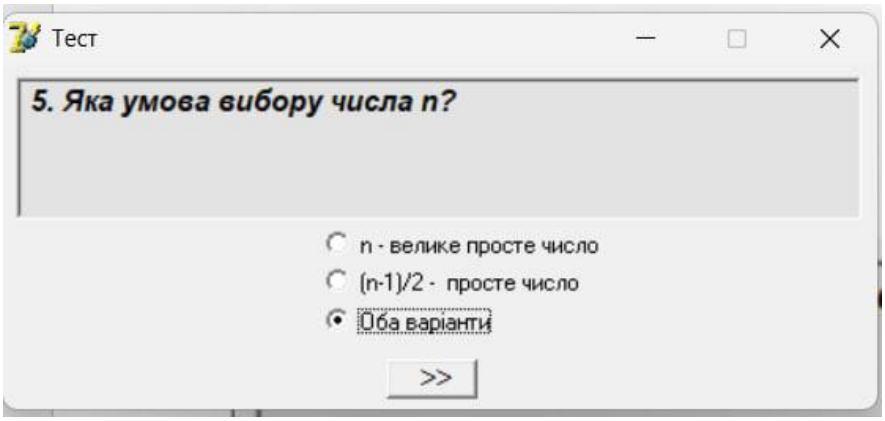
Хід роботи:

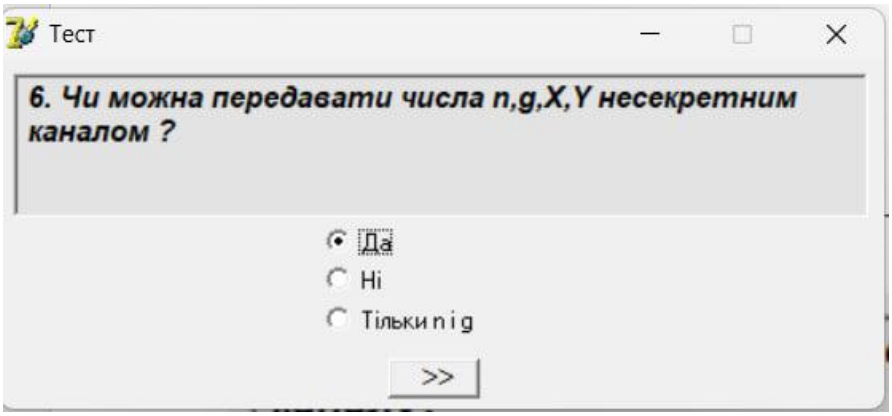




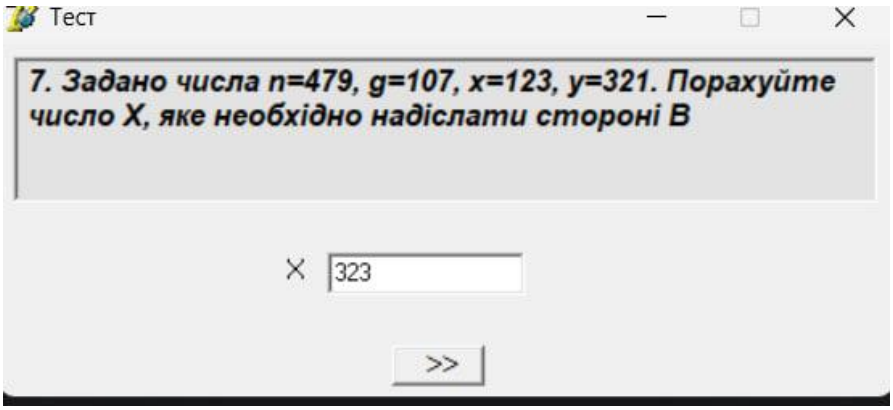








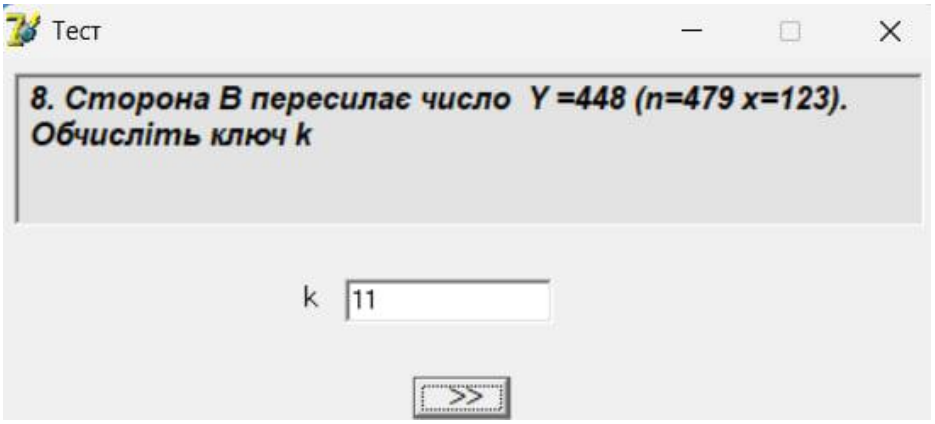
Num	A	Відкритий канал	B
1	x – випадкове велике ціле число	n, g	y – випадкове велике ціле число
2	X≡g^x mod n	<Обмін>	Y≡g^y mod n
3	k≡Y^x mod n		k`≡X^y mod n



X = (g^x)mod n = (107^123)mod 479 = 323

Y = (g^y)mod n = (107^321)mod 479 = 448

k = (Y^x)mod n = (448^123) mod 479 = 11



k = (X^y)mod n = (323^321)mod 479 = 11

Num	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≡g^x mod n	Обмін>	Y≡g^y mod n	Обмін>	Z≡g^z mod n	Обмін>
3	Z`≡Z^x mod n	Обмін>	X`≡X^y mod n	Обмін>	Y`≡Y^z mod n	Обмін>
4	k=Y`^x mod n		k1=Z`^y mod n		k2=X`^z mod n	

X = (g^x)mod n = (107^123)mod 479 = 323

Y = (g^y)mod n = (107^321)mod 479 = 448

Z = (g^z)mod n = (107^345) mod 479 = 361

Z`=(Z^x)mod n = (361^123) mod 479 = 220

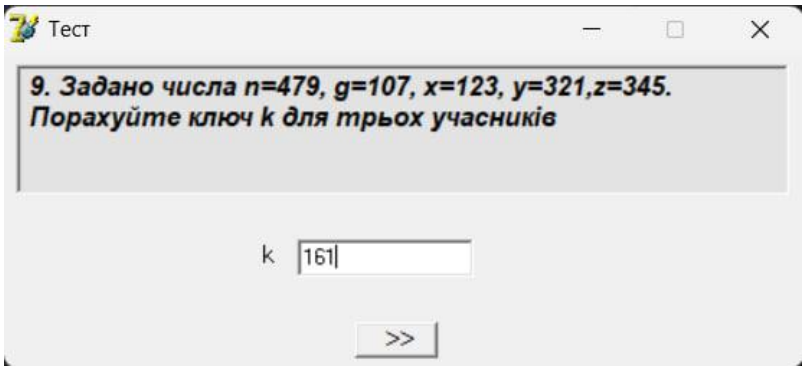
X`=(X^y)mod n = (321^321) mod 479 = 11

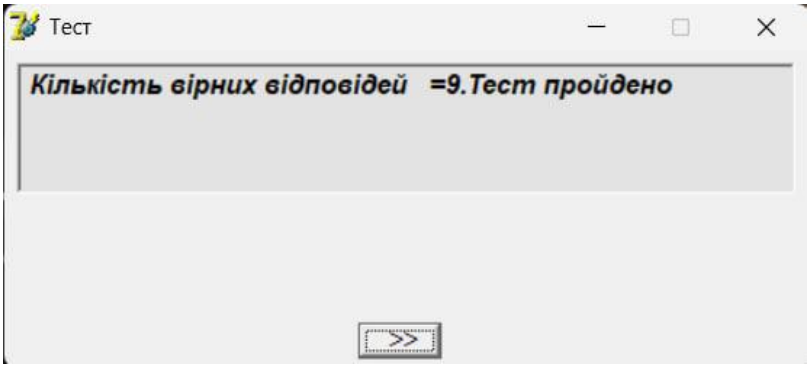
Y`=(Y^z)mod n = (448^345) mod 479 = 112

k = (Y`^x)mod n = (112^123)mod 479 = 161

k1 = (Z`^y)mod n = (220^321)mod 479 = 161

k2 = (X`^z)mod n = (11^345)mod 479 = 161





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