Міністерство освіти і науки України

КПІ ім. Ігоря Сікорського

Звіт

З дисципліни “Безпека інформаційних систем”

студента III курсу ФІОТ

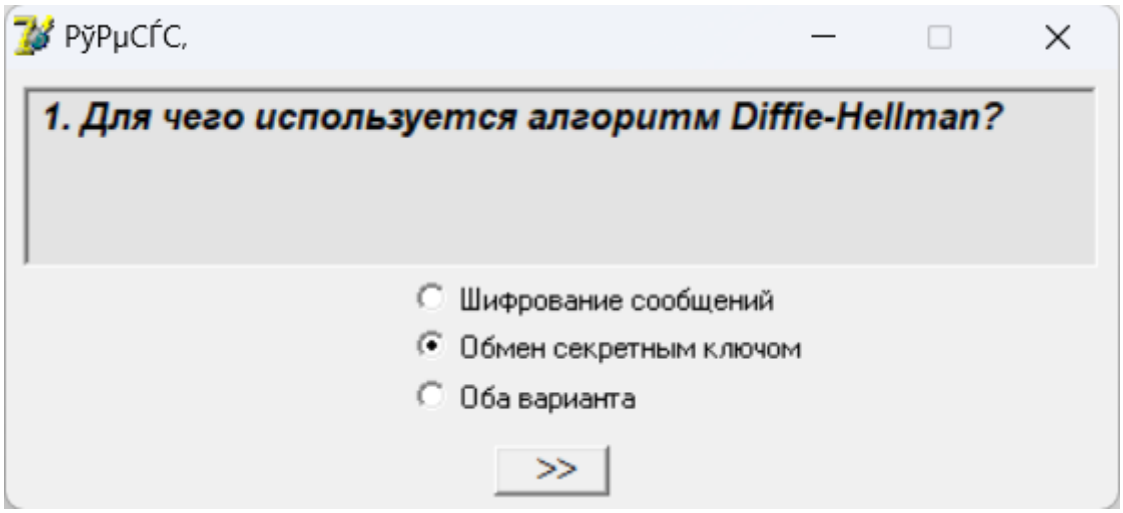
групи ІК-12

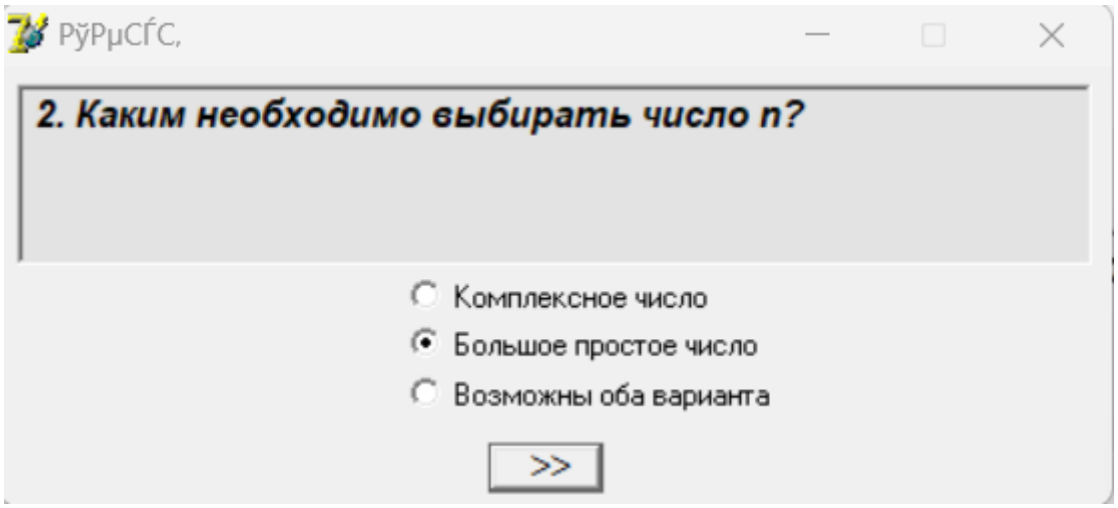
Мельнічука Іллі

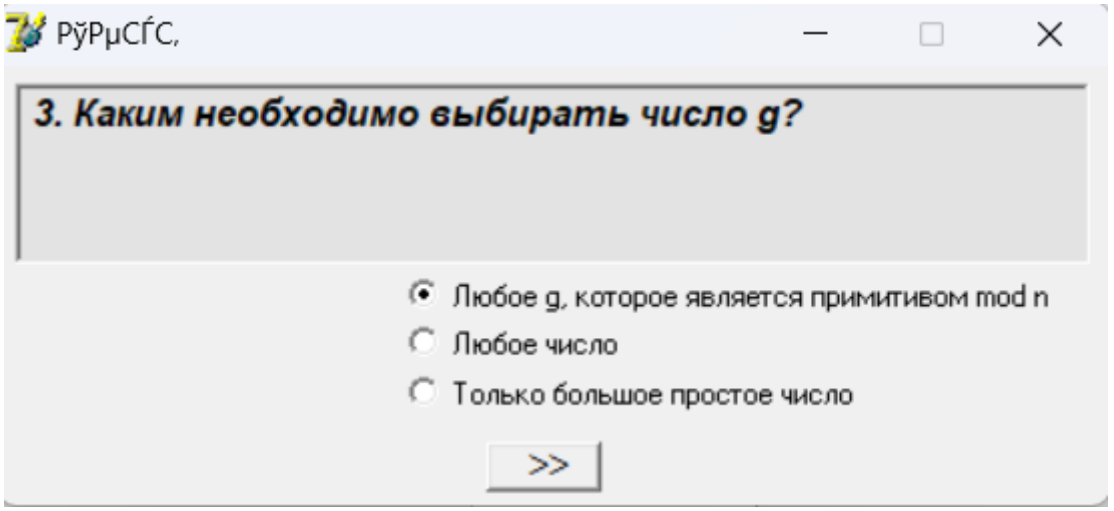
Перевірив:
Викладач кафедри
Інформаційних систем та технологій
Шимкович Л. Л.

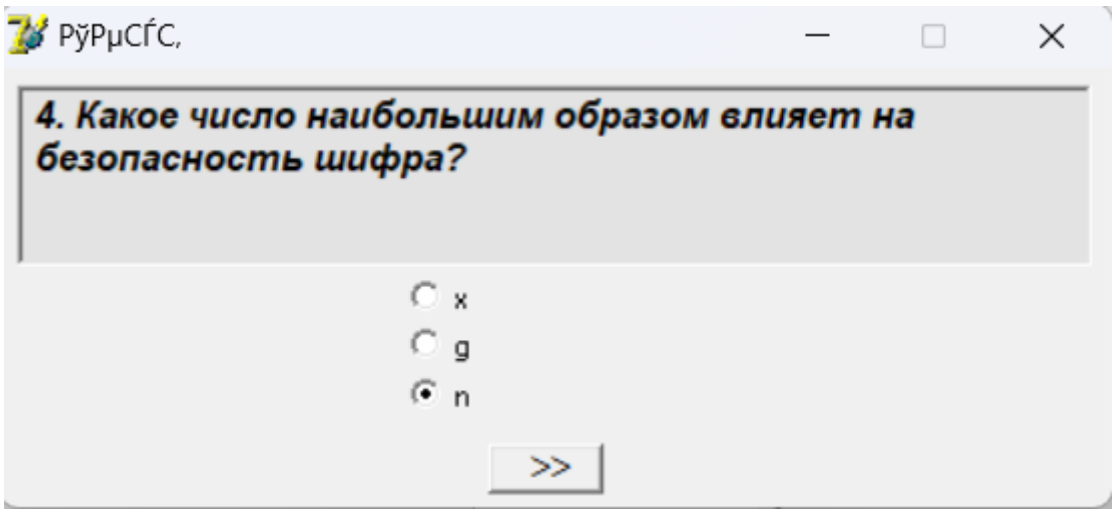
Київ 2023

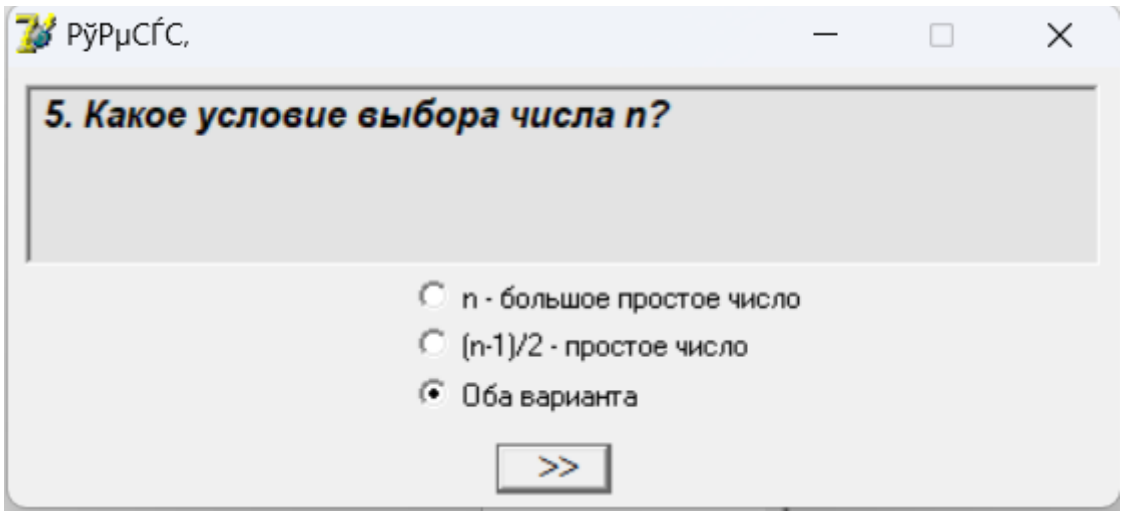
Тема: Дослідження криптосистеми Діффі-Хеллман (Diffie-Hellman)

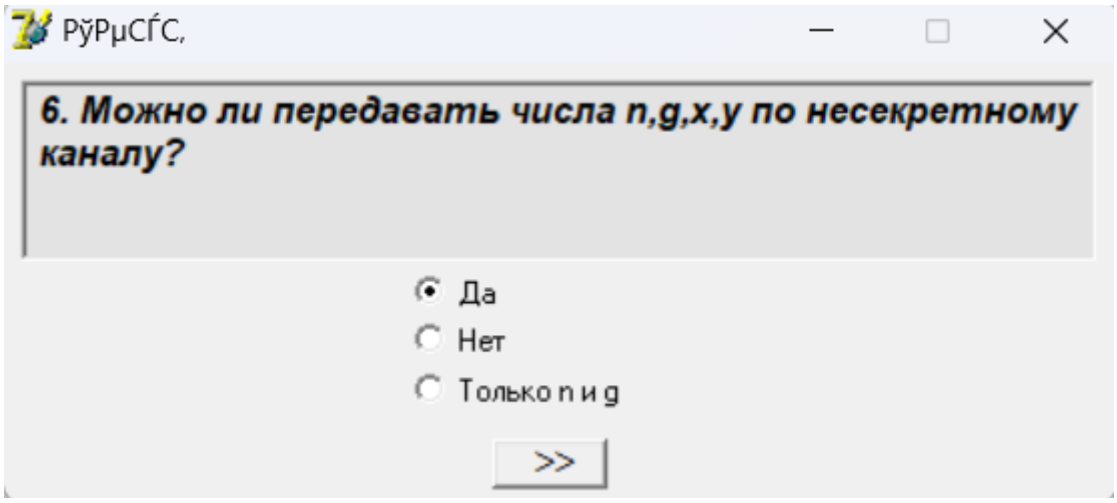


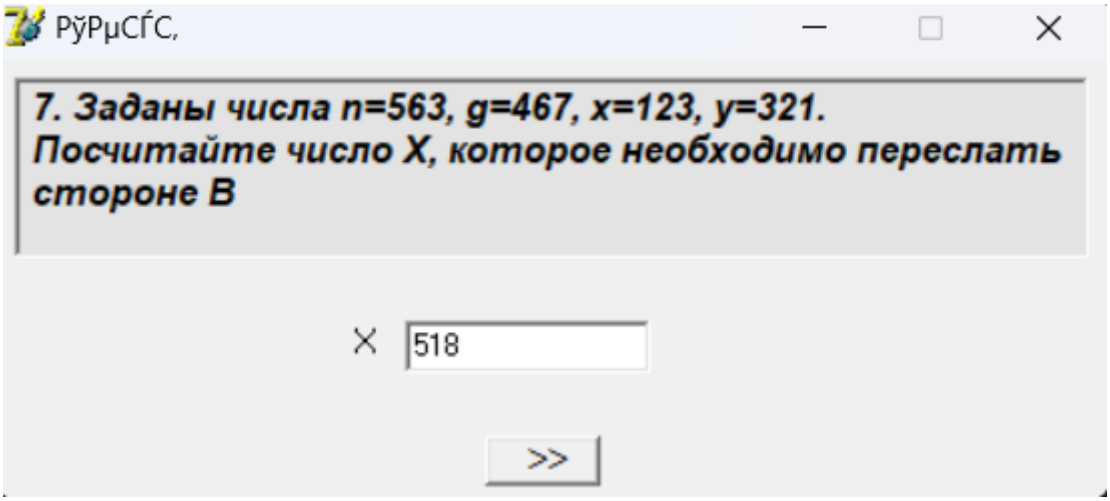




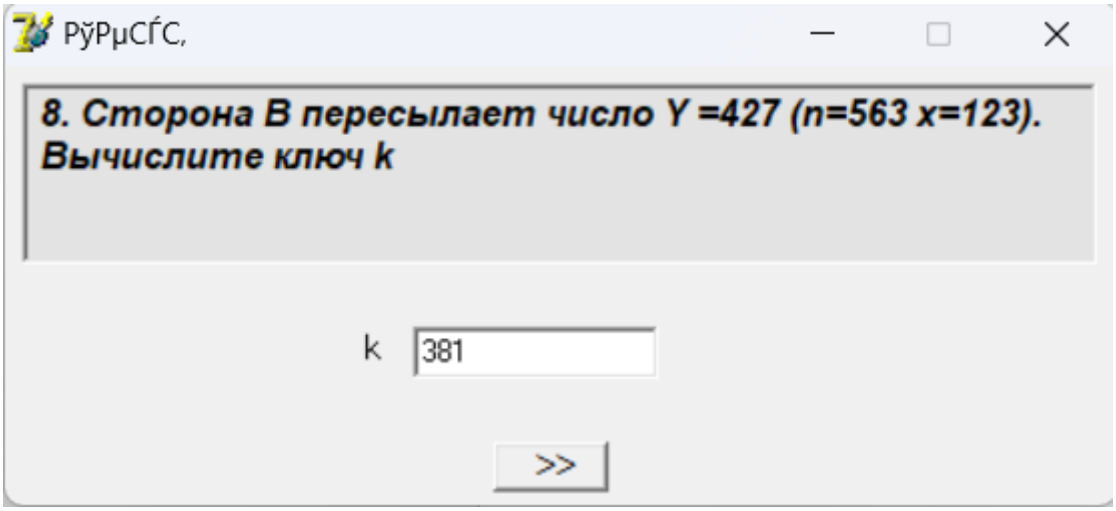

РўРµСЃС‚
4. Какое число наибольшим образом влияет на безопасность шифра?
x
g
n
>>


РўРµСЃС‚
5. Какое условие выбора числа n?
n - большое простое число
(n-1)/2 - простое число
Оба варианта
>>

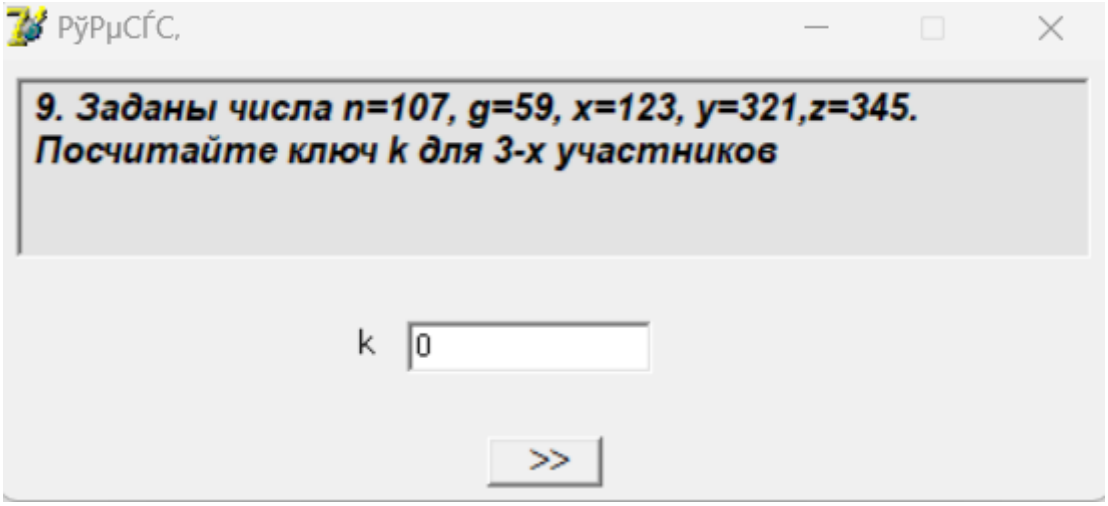

РўРµСЃС‚
6. Можно ли передавать числа n,g,x,y по несекретному каналу?
Да
Нет
Только n и g
>>



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



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



Обчислюємо X, Y, Z

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

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

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

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

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

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

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

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

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

Результат: