

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

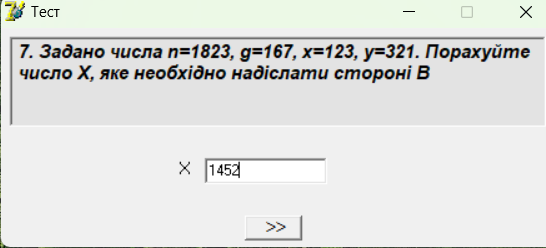
з дисципліни «Безпека інформаційних систем»

|  |  |
| --- | --- |
| Виконав: | Перевірив: |
| студент групи ІА-23:  Лядський Д.С. | Шимкович Л.Л. |
|  |  |

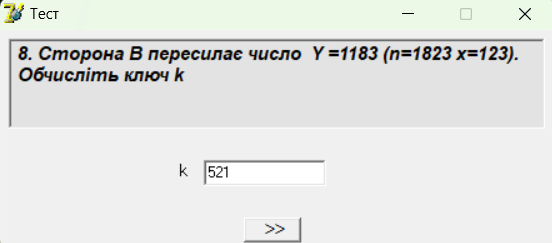
Київ 2024

|  |
| --- |
| Дослідження криптосистеми Діффі-Хеллман ( Diffie-Hellman). |

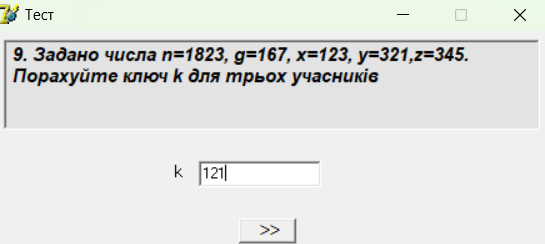
**Хід роботи:**



X = g^x mod n = 167^123 mod 1823 = 1452



k = Y ^x mod n = 521



X = g^x mod n = 167^123 mod 1823 = 1452

Y = g^y mod n = 167^123 mod 1823 = 1183

Z = g^z mod n = 167^123 mod 1823 = 1778

Z’ = Z^x mod n = 1778^123 mod 1823 = 952

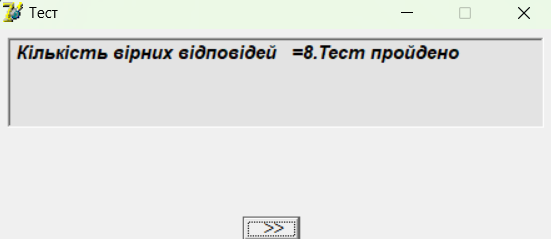
X’ = X^y mod n = 1452^321 mod 1823 = 521

Y’ = Y^z mod n = 1183^345 mod 1823 = 511

k = Y’^x mod n = 511^123 mod 1823 = 121

k = X’^z mod n = 521^345 mod 1823 = 121

k = Z’^y mod n = 952^321 mod 1823 = 121



**Висновок:** Отже, на цій лабораторній роботі ми дослідили криптосистеми Діффі-Хеллман.