Міністерство освіти і науки України

Харківський національний університет ім. В. Н. Каразіна

Факультет комп’ютерних наук

Кафедра безпеки інформаційних систем і технологій

Лабораторна робота №8

*з навчальної дисципліни*

«Прикладна криптологія»

Виконав:

Студент групи КБ-31 Кравченко Є. М.

Перевірив:

Професор

Горбенко І. Д.

Старший викладач

Єсіна М. В.

Харків – 2020

**Лабораторна робота №8**

*на тему:*

**«Методи криптоаналізу асиметричних криптоперетворень в групі точок еліптичних кривих»**

**Мета роботи:** розглянути методи криптоаналізу та дослідити криптостійкість асиметричних криптоперетворень в групі точок еліптичних кривих.

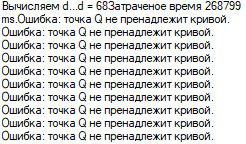
**Хід роботи**

Дані для розрахунків:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| модулі | 15 біт | p = | 26497 | | (4244, 17244) | (4685,10476) |
| n = | 13163 | |
| G = | 17644 | 6553 |
| 20 біт | p = | 959941 | | (880626, 157069) | (356441,849847) |
| n = | 480349 | |
| G = | 676058 | 399379 |
| 25 біт | p = | 29024113 | | (2504318, 22818733) | (5668030, 20322722) |
| n = | 14514667 | |
| G = | 17177079 | 17338199 |
| 27 біт | p = | 106920299 | | (60511798,45341126) | (76692622, 93840895) |
| n = | 106913789 | |
| G = | 12952536 | 38456565 |

Результати розрахунку d та час дискретного логарифмування:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Розмір модуля | перша точка | | друга точка | |
| час | d=… | час | d=… |
| 15 біт |  |  |  |  |
| 20 біт |  |  |  |  |
| 25 біт |  |  |  |  |
| 27 біт |  |  |  |  |

Задана перша точка не належить кривій: 

З наведено нижче графіка видно, що час дискретного логарифмування росте зі збільшенням розміру модуля.

**Висновки**

При виконанні даної лабораторної роботи були розглянуті методи криптоаналізу та досліджено криптостійкість асиметричних криптоперетворень в групі точок еліптичних кривих.