ЗАДАЧА 1

Розрахувати значення складності криптоаналізу та безпечного часу для алгоритмів, що базуються на перетвореннях у полі, кільці та групі точок ЕК (DSA, RSA, EC) методом решета числового поля.

Вихідні дані:

- довжина ключа *N*=*P*=*n*=21024, 22048, 23072

- потужність Криптосистеми γ=1012 [оп. за сек.]

- кількість секунд в році *K*=3,15107 [сек./рік]

Складність для RSA:



 – параметри методу. Для решета числового поля *δ*=1,92; *ν*=1/3.

-Складність для DSA:



 – параметри методу. Для решета числового поля *δ*=1,90; *ν*=1/3.

Складність для EC:

Результати звести у таблицю вигляду:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| довжина ключа  криптоалгорим | 21024 | | 22048 | | 23072 | |
| *I* | *tб* | *I* | *tб* | *I* | *tб* |
| Перетворення у полі DSA |  |  |  |  |  |  |
| Перетворення у кільці RSA |  |  |  |  |  |  |
| Перетворення в групі точок ЕК |  |  |  |  |  |  |

ЗАДАЧА 2

Нехай точка *G*=(5,19) належить ЕК *y2*=*x*3+*ax*+*b*(mod *p*), *a*=1, *b*=1 і *p*=23, тобто . Відкритий ключ користувача , порядок точки . Необхідно знайти секретний ключ  із порівняння .

ЗАДАЧА 1

Розрахувати значення складності криптоаналізу та безпечного часу для алгоритмів, що базуються на перетвореннях у полі, кільці та групі точок ЕК (DSA, RSA, EC) методом решета числового поля.

Вихідні дані:

- довжина ключа *N*=*P*=*n*=21024, 22048, 23072

- потужність Криптосистеми γ=1012 [оп. за сек.]

- кількість секунд в році *K*=3,15107 [сек./рік]

***Обов’язково навести всі розрахунки!***

Результати звести у таблицю вигляду:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| довжина ключа  криптоалгорим | 21024 | | 22048 | | 23072 | |
| *I* | *tб* | *I* | *tб* | *I* | *tб* |
| Перетворення у полі DSA |  |  |  |  |  |  |
| Перетворення у кільці RSA |  |  |  |  |  |  |
| Перетворення в групі точок ЕК |  |  |  |  |  |  |

ЗАДАЧА 2

Нехай точка *G*=(5,19) належить ЕК *y2*=*x*3+*ax*+*b*(mod *p*), *a*=1, *b*=1 і *p*=23, тобто . Відкритий ключ користувача , порядок точки . Необхідно знайти секретний ключ  із порівняння .