Kryptografia z elementami algebry

Ćwiczenia 2, notacja wielkie-O, funkcje jednokierunkowe

Wykonaj oszacowania wykorzystując notację wielkie-O .

1. Niech $n \in \mathbb{N}$ będzie liczbą złożoną. Oszacuj ile operacji elementarnych na bitach potrzeba do znalezienia liczby pierwszej $p \mid n$.

2. Wyznacz rzędy wszystkich elementów w nastepujących grupach:

   (a) $\mathbb{Z}_9^+$,

   (b) $\Phi(13)$,

   (c) $\Phi(12)$.

   Które grupy są cykliczne?

3. Zaproponuj efektywną metodę generowania grupy $\Phi(p)$ oraz jej generatora, gdzie p jest liczbą pierwszą.

4. Niech p będzie liczbą pierwszą, g generatorem grupy $\Phi(p)$. Niech $y \in \Phi(p)$. Oszacuj ile operacji elementarnych na bitach potrzeba do znalezienia $x = \log_g(y)$.

5. Zapoznaj się z algorytmem szyfrowania z kluczem publicznym ElGamala. Na jakich trudnych problemach obliczeniowych oparte jest bezpieczeństwo tego kryptosystemu?

6. Zapoznaj się z algorytmem *baby step, giant step*. Oszacuj jego złożoność obliczeniową.