

Kryptografia z elementami algebry

Laboratorium 1, arytmetyka w strukturach algebraicznych

(Moduł 1)

1. Zaimplementuj algorytm (funkcję), która generuje losowy element zbioru \mathbb{Z}_n .
Dane: $k \in \mathbb{N}$
Wynik: k -bitowa liczba $b \in \mathbb{Z}_n$
2. Zaimplementuj algorytm (funkcję) obliczania odwrotności w grupie $\Phi(n)$. Wykorzystaj Rozszerzony Algorytm Euklidesa.
Dane: $n \in \mathbb{N}$, $b \in \Phi(n)$
Wynik: $b^{-1} \in \Phi(n)$
3. Zaimplementuj algorytm (funkcję) efektywnego potęgowania w zbiorze \mathbb{Z}_n . Wykorzystaj algorytm iterowanego podnoszenia do kwadratu.
Dane: $n, k \in \mathbb{N}$, $b \in \mathbb{Z}_n$
Wynik: $b^k \in \mathbb{Z}_n$
4. Niech p będzie liczbą pierwszą. Zaimplementuj test (funkcję), który sprawdza czy element zbioru \mathbb{Z}_p jest resztą kwadratową w \mathbb{Z}_p . Wykorzystaj twierdzenie Eulera.
Dane: $b \in \mathbb{Z}_p$
Wynik: `True` jeśli b jest resztą kwadratową, `False` w przeciwnym wypadku.
5. Zaimplementuj algorytm (funkcję), który oblicza pierwiastek kwadratowy w ciele \mathbb{Z}_p , gdzie $p \equiv 3 \pmod{4}$ jest liczbą pierwszą. Wykorzystaj twierdzenie Eulera.
Dane: $b \in \mathbb{Z}_p$, b jest resztą kwadratową \mathbb{Z}_p
Wynik: $a \in \mathbb{Z}_p$ taki, że $a^2 \equiv b \pmod{p}$.
6. Wykorzystaj test pierwszości zaimplementowany w języku programowania, w którym zaimplementowałeś powyższe **Dane:** $n \in \mathbb{N}$
Wynik: `True` jeśli n jest liczbą pierwszą, `False` w przeciwnym wypadku.