

## Kryptografia z elementami algebry

Laboratorium 1, arytmetyka w strukturach algebraicznych

### miniprojekt nr 1

- (2pkt) Zaimplementuj algorytm (funkcję) obliczania odwrotności w grupie  $\Phi(n)$ . Wykorzystaj Rozszerzony Algorytm Euklidesa.  
**Dane:**  $n \in \mathbb{N}$ ,  $b \in \Phi(n)$   
**Wynik:**  $b^{-1} \in \Phi(n)$
- (3pkt) 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:**  $b^k \in \mathbb{Z}_n^*$
- (3pkt) Zaimplementuj test (funkcję), który sprawdza czy liczba naturalna  $n$  jest liczbą pierwszą. Wykorzystaj test Fermata.  
**Dane:**  $n \in \mathbb{N}$   
**Wynik:** `True` jeśli  $n$  jest liczbą pierwszą, `False` w przeciwnym wypadku.
- (1pkt) 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.
- (1pkt) Niech  $p \equiv 3 \pmod{4}$  będzie liczbą pierwszą. Zaimplementuj funkcję, która oblicza pierwiastek kwadratowy w  $\Phi(p)$ . Wykorzystaj twierdzenie Eulera.  
**Dane:**  $p \equiv 3 \pmod{4}$ ,  $b \in \Phi(p)$ ,  $b$  jest resztą kwadratową  $\pmod{p}$   
**Wynik:**  $a \in \Phi(p)$  taki, że  $a^2 \equiv b \pmod{p}$ .