# Protokół Diffiego-Hellmana

Z1. Dokonać próby ataku na protokół Diffiego-Hellmana. Przechwycone zostały: p=1117 (liczba pierwsza), g=6 (generator w  $\mathbb{Z}_p^*$ ), klucz  $h=527=g^a$ .

#### WYMAGANIA PODSTAWOWE

1. znalezienie liczby a dowolną metodą i opisanie podjętych kroków w sprawozdaniu.

### WYMAGANIA DODATKOWE

- 2. użycie dwóch metod,
- 3. porównanie metod, ich szybkości oraz dokładności,
- 4. napisanie i przetestowanie działania funkcji potega(a, b, p) wyliczającą  $a^b \pmod{p}$  szybszą metodą, wskazaną na laboratorium,
- 5. napisanie i przetestowanie działania funkcji generator(g,p) sprawdzająca, czy g jest generatorem w pierścieniu  $\mathbb{Z}_p^*$ ,
- 6. napisanie i przetestowanie działania funkcji generatory(g, p) wypisująca generatory g w pierścieniu  $\mathbb{Z}_p^*$  (zapis do pliku),
- 7. napisanie i przetestowanie działania funkcji euklid(a, p) wyliczający  $a^{-1}$  w  $\mathbb{Z}_p^*$ .
- Z2. Zaprogramować protokół Diffiego-Hellmana:

### WYMAGANIA PODSTAWOWE

- 1. dla 2 osób,
- 2. dane publiczne są wpisywane z konsoli,
- 3. dane tajne od każdej osoby są pobierane z osobnym plików,
- 4. wspólny klucz jest zapisywany do nowego pliku oraz wyświetlany na ekranie (porównać wyniki z obu obliczeń),

## WYMAGANIA DODATKOWE

- 5. dla od 2 do 5 osób,
- 6. napisanie i przetestowanie działania funkcji potega(a, b, p) wyliczającą  $a^b \pmod{p}$  szybszą metodą, wskazaną na laboratorium,
- 7. napisanie i przetestowanie działania funkcji generator(g, p) sprawdzająca, czy g jest generatorem w pierścieniu  $\mathbb{Z}_p^*$ ,
- 8. napisanie i przetestowanie działania funkcji generatory(g, p) wypisująca generatory g w pierścieniu  $\mathbb{Z}_p^*$  (zapis do pliku),
- 9. napisanie i przetestowanie działania funkcji euklid(a,p) wyliczający  $a^{-1}$  w  $\mathbb{Z}_p^*$ .