Języki i paradygmaty programowania
Lista nr 3 na laboratorium 7 i 8

Zadanie 1

Stwórz w języku $C++$ (zgodnie ze standardem co najmniej C++14) szablony klas implementujące obliczenia w protokole wymiany kluczy Diffie–Hellman używając później ciała stworzonego na poprzedniej liście do jego inicjalizacji.

W tym celu stwórz szablon klasy `DHSetup`, której konstruktor losowo wybiera i ustawia generator ciała[1], posiadający dwie metody publiczne

- `T getGenerator()` - zwracającą stworzony generator ciała,
- `T power(T a, unsigned long b)` - podnoszącą `a` do potęgi `b` (implementacja powinna to robić używając tylko $O(\log b)$ mnożeń).

Następnie stwórz szablon klasy `User`, której konstruktor przyjmuje referencję do klasy `DHSetup` i ustawia losowy sekret, posiadający następujące metody publiczne

- T getPublicKey() - zwracającą generator ciała podniesiony do potęgi będącej sekretem,
- void setKey(T a) - tworzącą klucz szyfrujący (przechowywany w klasie w polu prywatnym) przez podniesienie `a` do potęgi będącej sekretem,
- T encrypt(T m) - szyfrującą `m` przez pomnożenie jej przez klucz szyfrujący,
- T decrypt(T c) - deszyfrującą `c` przez podzielenie jej przez klucz szyfrujący.

Zadbaj, aby sygnalizowane było niewłaściwe użycie metod, np. szyfrowanie/deszyfrowanie bez ustawienia klucza.

Na koniec napisz program testujący protokół Diffie-Hellmana na stworzonych szablonach w ciele o charakterystyce 1234567891.

Zadanie 2

Stwórz w języku Java analogiczny program jak w zadaniu 1.

Zadanie 3

Powtórz zadanie 1 dla innego języka programowania spełniającego paradygmat programowania obiektowego.

[1] Generator ciała o charakterystyce p to taki element $a \in \{1, \ldots, p-1\}$, który dla wszystkich liczb pierwszych q dzielących $p-1$ spełnia nierówność $a^{\frac{p-1}{q}} \neq 1$. Generatorów w ciele o charakterystyce p jest $\phi(p-1)$, więc na tyle dużo, aby można go było dość szybko znaleźć przez losowanie.