Programowanie systemów kryptograficznych z wykorzystaniem Java Security

Kryptografia symetryczna

Maciej Kocot, Laura Uchwat

Data wykonania	
Skład grupy	
Ocena	

Podczas wykonywania ćwiczenia odznaczaj wykonane podpunkty!
Przed przystąpieniem do ćwiczenia sprawdź stan sprzętu. Wszelkie nieprawidłowości należy natychmiast zgłosić prowadzącemu.

1. Czynności początkowe

- ❏ Na początku zajęć prowadzący wybiera dla każdego zespołu algorytm szyfrujący: **Blowfish / DES** oraz metodą dopełniania szyfrogramu: **PKCS7 / Ciphertext Stealing / ANSI X.923 / ISO10126-2**
- ❏ Pomocny może okazać się przewodnik po bibliotece: https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

2. Cel ćwiczenia

Celem ćwiczenia jest napisanie prostego programu(-ów) w języku Java, który potrafi szyfrować i deszyfrować dowolne pliki tekstowe i binarne. W trakcie ćwiczenia należy porównać rezultat szyfrowania w trybie CBC i ECB.

Uwaga: Plik może mieć dowolny rozmiar, dlatego należy go szyfrować blokami.

3. Zadanie: Implementacja

- ❏ Napisz program(-y) szyfrujący i deszyfrujący dowolny plik przy pomocy wskazanej metody szyfrowania i dopełnienia. Program ma umożliwiać wybór jednego z dwóch trybów szyfrowania (CBC i ECB).
- ❏ Zweryfikuj poprawność działania programu(-ów) szyfrując i deszyfrując plik tekstowy (np. kopię pliku z kodem źródłowym programu), używając dowolnego polecenia obliczającego skrót wiadomości (np. md5sum) sprawdź czy pliki są identyczne.
- ❏ Wybróbuj działanie swojego programu (w trybach CBC i ECB) na pliku image.raw4
- ❏ Poproś prowadzącego o sprawdzenie poprawności wykonania zadania.