Kodowanie i bezpieczeństwo informacji

Laboratorium - lista nr 1 na 12-24 lutego 2012

Zadanie 1 (1 pkt) Jaka jest główna różnica pomiędzy klasami *java.util.Random* i *java.security.SecureRandom*?

Zadanie 2 (5 pkt) Zdefiniuj klasę abstrakcyjną *Cipher* posiadającą metody *Gen, Enc, Dec*. Następnie stwórz klasę *AffineCipher* (implementującą *Cipher*) będącą realizacją schematu szyfrowania afinicznego. Stwórz poprawne testy jednostkowe (za 2 pkt).

Zadanie można realizować w grupach 2-3 osobowych, ale wtedy musicie użyć co najmniej 2 języków programowania (np. jedna osoba implementuje w Javie, druga w C/C++: każdy tworzy klasę abstrakcyjną, a następnie jedna osoba implementuje generowanie klucza i jego eksport do pliku; druga implementuje szyfrowanie/deszyfrowanie i wczytywanie klucza). Trzecia osoba tworzy testy jednostkowe.

Zadanie 3 (1 pkt) Zapisuj kryptogram do pliku xml. Uzgodnijcie jego format (np. ustalając dtd), aby co najmniej jedna inna grupa mogła zaszyfrować/deszyfrować wasze wiadomości. Alternatywnie możecie skorzystać z notacji ASN.1 (preferowane, wykorzystajcie gotowe biblioteki).

Zadanie 4 (1 pkt) Zaimplementuj klasę *Caesar* realizującą szyfr Cezara. Wykorzystaj jako bibliotekę kod powstały w zadaniu 2.

Pamiętaj, aby cytować źródła na które się powołujesz.