Programowanie systemów kryptograficznych z wykorzystaniem Java Security

Kryptografia asymetryczna: szyfrowanie algorytmem RSA

Maciej Kocot, Laura Uchwat

Data wykonania	
Skład grupy	
Ocena	

Podczas wykonywania ćwiczenia odznaczaj wykonane podpunkty!
Celem ćwiczenia jest stworzenie programu umożliwiającego szyfrowanie i deszyfrowanie danych o dowolnej wielkości z wykorzystaniem algorytmu RSA i porównanie wydajności tych operacji z wybranym szyfrem symetrycznym. Pomocny może okazać się przewodnik po bibliotece: https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

1. Tworzenie oprogramowania

Zespół ma zadanie napisać program lub programy realizujące poniższą funkcjonalność:

- ❏ Generowanie pary kluczy: prywatnego i publicznego. Użytkownik ma możliwość podania rozmiaru klucza. Klucze mają być przechowywane w plikach. W celach kontrolnych program wypisuje na ekranie składniki klucza.
- ❏ Szyfrowanie kluczem publicznym pliku binarnego o dowolnej długości.
- ❏ Deszyfrowanie kluczem prywatnym wiadomości zapisanej w pliku.

Nazwy plików, na których działają programy mają być podawane jako argumenty wywołania programów.
Uwaga: Plik może mieć dowolny rozmiar, dlatego należy go szyfrować blokami.

2. Porównanie wydajności algorytmów kryptografii symetrycznej i asymetrycznej

Do realizacji tego punktu potrzebne będą programy szyfrujące metodami kryptografii symetrycznej napisane podczas wcześniejszych zajęć.

- ❏ Przygotuj zbiory danych o dowolnej (najlepiej losowej) zawartości i rozmiarach: 512b, 512kB, 4MB, 32MB, 64MB i 128MB.
- ❏ Zmierz czas szyfrowania i deszyfrowania tych zbiorów z wykorzystaniem kryptografii symetrycznej, wyniki zapisz w tabelce.
- ❏ Zmierz czas szyfrowania i deszyfrowania tych zbiorów z wykorzystaniem kryptografii symetrycznej dla różnych rozmiarów klucza: 1024, 2048, 4096. Wyniki zapisz w tabelce.

Po wykonaniu zadania wezwij prowadzącego celem sprawdzenia poprawności wykonania zadania.

	Symmetric cipher		RSA 1024		RSA 2048		RSA 4096	
	Enc	Dec	Enc	Dec	Enc	Dec	Enc	Dec
512b								
512kB								
4MB								
32MB								
64MB								
128MB								