Kodowanie i bezpieczeństwo informacji

Laboratorium - lista nr 3, 6 XI

Zadanie 1 (8 pkt) Napisz program który szyfruje/deszyfruje wskazany plik na dysku. Parametrami programu są:

- schemat szyfrowania (co najmniej: AES),
- tryb szyfrowania (co najmniej: CBC/CTR/GCM/...),
- ścieżka do keystore'a przechowującego klucz,
- identyfikator klucza.

Hasło do klucza z keytore'a należy wczytać interaktywnie (wczytywane znaki nie mogą pojawiać się na terminalu).

Nie musisz implementować swojej wersji AES, zamiast tego wykorzystaj np. *openssl* (patrz: *include/openssl/aes.h*).

Zadanie 2 (7 pkt) Wykorzystaj program z poprzedniego zadania. Napisz odtwarzacz plików muzycznych, który będzie odtwarzał wskazane przez Ciebie utwory, przechowywane w zaszyfrowanych (kluczem k_1) plikach (wykorzystaj w tym celu program/bibliotekę stworzoną na potrzeby zadania 1). Nie musisz implementować swojego dekodera mp3 – możesz wykorzystać istniejące biblioteki.

Integralną częścią odtwarzacza jest plik konfiguracyjny, który powstaje podczas "instalacji" programu, zawiera: ścieżkę do keystore'a, identyfikator klucza i hasło. Plik konfiguracyjny jest zaszyfrowany kluczem k_2, który jest zaszyty w programie.

Przy kolejnych uruchomieniach programu należy wprowadzić PIN ustalony przy instalacji.

Wybierz odpowiedni tryb szyfrowania dla plików muzycznych, który umożliwi np. sprawne odtwarzanie utworu od wybranego momentu. Pomyśl nad buforowaniem – jak będzie zachowywać się Twoja aplikacja gdy plik będzie miał 500MB?

Bonus: Odtwarzane (zdeszyfrowane) pliki nie mogą być przechowywane na dysku, a jedynie w pamięci operacyjnej.