Kodowanie i bezpieczeństwo informacji

Laboratorium - lista nr 4, 19 IV

Zadanie 1 (5 pkt) Napisz program, który otrzymuje na wejściu wiadomość m (bądź ścieżkę do pliku zawierającego m) i zwraca jej kryptogram. Jako schematu szyfrowania użyj np. RC4, klucz k odczytaj z keystore'a (skorzystaj z Bouncy Castle).

Wykorzystaj ten program do wygenerowania danych potrzebnych do zadania 2. Jako teksty wiadomości wiadomości weź teksty wiadomości z serwisów informacyjnych.

Zadanie 2 (10 pkt) Napisz program, który na wejściu wczytuje kryptogramy wygenerowane za pomocą szyfru strumieniowego. Przy założeniu, że każdy z kryptogramów został wygenerowany za pomocą tego samego klucza: $c_i = m_i \oplus G(k)$ (jako G możesz przyjąć RC4), program ma zwrócić odpowiadające teksty jawne m_i.

Zobacz ile potrzebujesz średnio wiadomości, aby program poprawnie zgadywał teksty jawne? Jak długie muszą być wiadomości? Jaki wpływ na efektywność Twojego programu ma użyte kodowanie (ASCII/UTF-8/ISO-8859-2)?

UWAGA: program ma nie znać wartości k użytej do tworzenia kryptogramów.