Wstęp do Kryptologii
Zadanie Laboratoryjne

mgr inż. Łukasz DZIEŁ

1 Treść zadania laboratoryjnego

Zadanie laboratoryjne polega na:

1. zapoznaniu się z budową algorytmu AES zgodnie z FIPS PUB 197;
2. przeanalizowaniu operacji arytmetycznych i logicznych użytych do konstrukcji algorytmu AES;
3. zaimplementowaniu programu, który umożliwia szyfrowanie i deszyfrowanie jednego bloku danych algorytmem AES;
4. przetestowaniu zaimplementowanego programu;
5. oddaniu wykonanego zadania do oceny.

2 Szczegółowe wymagania

1. program powinien być napisany w języku C lub C++;
2. program powinien kompilować się w środowisku Dev-Cpp nie wymagając instalowania dodatkowych bibliotek;
3. program ma być uruchamiany z okna konsoli tekstowej, bez interfejsu graficznego;
4. po uruchomieniu, program ma się wykonać i zakończyć swoje działanie bez potrzeby dodatkowych działań ze strony użytkownika;
5. w programie poza funkcją main() mają być zaimplementowane oddzielne funkcje z przekazywanymi do nich odpowiednimi parametrami dla poszczególnych operacji;
6. program ma być wywoływany w następujący sposób:
   aes.exe E|D L128|L192|L256 key block
7. opcje programu mają następujące znaczenie:
   a) **E** – tryb pracy programu: szyfrowanie (wymagany);
   b) **D** – tryb pracy programu: deszyfrowanie (wymagany);
   c) **L128**, **L192**, **L256** – długość klucza algorytmu (wymagany);

   d) **key** – blok klucza do algorytmu zapisany w formacie szesnastkowym za pomocą cyfr i liter alfabetu od A do F (wymagany);
   e) **block** – blok tekstu jawnego lub szyfrogramu zapisany w formacie szesnastkowym za pomocą cyfr i liter alfabetu od A do F (wymagany);

8. w obu trybach pracy, program powinien wypisać na standardowe wyjście blok szyfrogramu lub tekstu jawnego w formacie szesnastkowym za pomocą cyfr i liter alfabetu od A do F.

3 Inne ustalenia

1. Zasady oceniania i rozliczania zadania laboratoryjnego zawiera syllabus przedmiotu.
2. Jako temat wszystkich przesyłanych wiadomości należy podawać:
   WDK-NumerGrupySzkoleniowej-NAZWISKO-Imię