Wyższa Szkoła Bankowa w Poznaniu

Wydział Finansów i Bankowości

Kierunek: Informatyka

Studia niestacjonarne I stopnia

Przedmiot: **Elementy kryptografii**

Grupa:zIinz\_3\_5s\_21/22\_INF\_Sp4\_EK\_gr.x zIinz\_3\_6s\_21/22\_INF\_Sp4\_EK\_gr.x

Prowadzący: dr inż. Izabela Janicka-Lipska

**Zadanie domowe nr 3**

Temat: **Implementacja prostego szyfru blokowego**

Student: **Adam Xiński**

Ćwiczenie z dnia: 26.03.2023

**Prosty szyfr blokowy**

Szyfr jest 8-rundowy, przekształca bloki w postaci bajtów z kluczem użytkownika *k\** 8-bitowym. Schemat blokowy szyfru:



Blok S tworzą 4 nieliniowe funkcje boolowskie:

*f*1(*x*1,*x*2,*x*3,*x*4) = *x*1 ⊕ *x*1*x*3 ⊕ *x*2*x*4 ⊕*x*2*x*3*x*4 ⊕ *x*1*x*2*x*3*x*4

*f*2(*x*1,*x*2,*x*3,*x*4) = *x*2 ⊕ *x*1*x*3 ⊕ *x*1*x*2*x*4 ⊕ *x*1*x*3*x*4 ⊕ *x*1*x*2*x*3*x*4

*f*3(*x*1,*x*2,*x*3,*x*4) = 1 ⊕ *x*3 ⊕ *x*1*x*4 ⊕ *x*1*x*2*x*4 ⊕ *x*1*x*2*x*3*x*4

*f*4 (*x*1,*x*2,*x*3,*x*4) = 1 ⊕ *x*1*x*2 ⊕ *x*3*x*4 ⊕ *x*1*x*2*x*4 ⊕ *x*1*x*3*x*4 ⊕ *x*1*x*2*x*3*x*4

Permutacja Feistela:



4-bitowy klucz rundowy *k* = *k*1*k*2*k*3*k*4 dodajemy do funkcji tworzących blok S:

*f*1(*x*1,*x*2,*x*3,*x*4) = *x*1 ⊕ *x*1*x*3 ⊕ *x*2*x*4 ⊕*x*2*x*3*x*4 ⊕ *x*1*x*2*x*3*x*4 ⊕ *k*1

*f*2(*x*1,*x*2,*x*3,*x*4) = *x*2 ⊕ *x*1*x*3 ⊕ *x*1*x*2*x*4 ⊕ *x*1*x*3*x*4 ⊕ *x*1*x*2*x*3*x*4 ⊕ *k*2

*f*3(*x*1,*x*2,*x*3,*x*4) = 1 ⊕ *x*3 ⊕ *x*1*x*4 ⊕ *x*1*x*2*x*4 ⊕ *x*1*x*2*x*3*x*4 ⊕ *k*3

*f*4 (*x*1,*x*2,*x*3,*x*4) = 1 ⊕ *x*1*x*2 ⊕ *x*3*x*4 ⊕ *x*1*x*2*x*4 ⊕ *x*1*x*3*x*4 ⊕ *x*1*x*2*x*3*x*4 ⊕ *k*4

Układ generowania kluczy rundowych:



*RL*1 jest rotacją cykliczną bitów w lewo o jeden bit.

Funkcja wyboru W działa następująco:

jeśli na wejściu mamy słowo 8-bitowe *a*1*a*2*a*3*a*4*a*5*a*6*a*7*a*8, to *k*1*k*2*k*3*k*4  = *a*1*a*3*a*5*a*7.

Uwaga: przy deszyfrowaniu klucze rundowe K1, K2,…,K8 muszą być podawane w odwrotnej kolejności, tj. używany do szyfrowania w ósmej rundzie, przy deszyfrowaniu musi być użyty w rundzie pierwszej, itd.

**Zadanie**

Zaimplementować w dowolnym środowisku programistycznym przedstawiony powyżej szyfr blokowy zapewniający szyfrowanie i deszyfrowanie bloków 8-bitowych.

Na wejście podajemy z klawiatury blok 8 bitów widoczny na ekranie, np. 01101110. Na wyjściu wypisujemy na ekranie blok 8 bitów, np. 01010011.

Implementację wraz z wersją wykonywalną należy dołączyć do sprawozdania w skompresowanym archiwum na platformie Moodle. Zadanie należy przedstawić na kolejnych zajęciach.

**Rozwiązanie**

1. Opis implementacji
2. Kod programu
3. Rezultaty testowania funkcjonalnego

Szyfrowanie:

|  |  |  |  |
| --- | --- | --- | --- |
| *m*= | 00 | 78 | FA |
| *k*\*= | E0 | B1 | AC |
| *c*= |  |  |  |

Deszyfrowanie (w wierszu c należy wpisać rezultaty szyfrowania uzyskane powyżej, dla odpowiednich kluczy):

|  |  |  |  |
| --- | --- | --- | --- |
| *c*= |  |  |  |
| *k*\*= | E0 | B1 | AC |
| *m*= |  |  |  |

Komentarz dla studenta

1. Plik z dokumentacją (czyli ten plik) proszę zapisać w formacie PDF nadając mu nazwę:

3-Lp-Nazwisko-Imię.pdf

gdzie Lp jest liczbą porządkową studenta na liście studentów.

Implementację wraz z wersją wykonywalną należy dołączyć do sprawozdania w skompresowanym archiwum o nazwie (np. w przypadku archiwum z rozszerzeniem zip)

3-Lp-Nazwisko-Imię.zip

1. Tekst zapisany czerwoną czcionką (te stronę) należy usunąć przed skonwertowaniem tego sprawozdania do formatu PDF i umieszczeniem na platformie Moodle.
2. Tekst zapisany niebieską czcionką (na stronie tytułowej) należy zamienić na aktualne dane.