

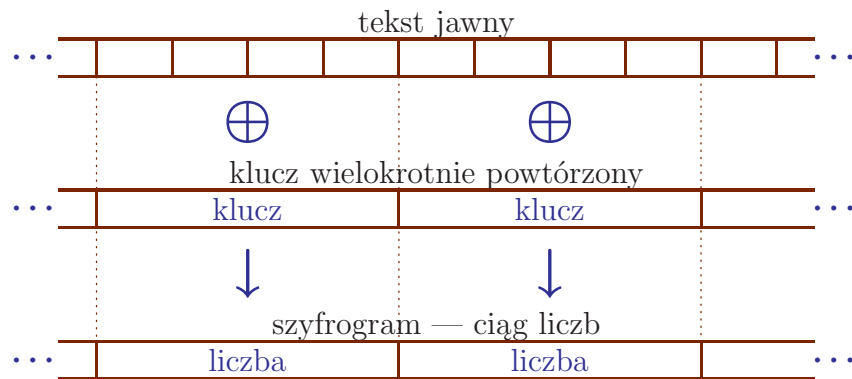
Kryptografia

Laboratorium nr 2

Stefan Sokołowski

Zadanie 1:

Umawiamy się na taki sposób szyfrowania wiadomości:



- kluczem jest dowolny ciąg czterech **char**-ów (liter/cyfr/znaków);
- przykładamy ten klucz wielokrotnie do czwórek **char**-ów z tekstu (jak na rysunku) i na kolejnych **char**-ach tekstu i klucza wykonujemy operację **XOR**¹; ew. można tekst dopełnić na końcu spacjami do pełnej czwórki;
- wynikami każdego takiego **XOR**-owania są cztery **char**-y, zajmujące $4 \times 8 = 32$ bity, czyli składające się na liczbę całkowitą;
- ciąg tych liczb całkowitych stanowi gotowy szyfrogram.

Proszę napisać i uruchomić:

- program wczytujący klucz i tekst, a następnie wyświetlający szyfrogram złożony z liczb;
- program wczytujący klucz i szyfrogram złożony z liczb, a następnie wyświetlający odszyfrowany tekst.

Można zakładać, że tekst cały mieści się w jednym wierszu.

¹Por. wykład 2, iis.ans-elblag.pl/~stefan/Dydaktyka/Krypto/Slajdy/02a.pdf, str. 3–6.

Zadanie 2 (sieć Feistela):

Dany jest następujący ciąg bitów reprezentujący jawną wiadomość:

110100010111

Wykonujemy 2 rundy szyfrowania Feistela² z kluczem 2-bitowym. Stosujemy następujące funkcje szyfrujące:

- **runda 0:** $f_0(c_0c_1) = (c_0c_0)$ — dwukrotne powtórzenie początkowego bitu z pary;
- **runda 1:** $f_1(c_0c_1) = (11)$ — funkcja stała.

Proszę przeprowadzić ręczne szyfrowanie podanej wyżej wiadomości, a następnie odszyfrować wynikowy szyfrogram i wynik porównać z ciągiem wejściowym.

²Por. wykład 2, iis.ans-elblag.pl/~stefan/Dydaktyka/Krypto/Slajdy/02a.pdf, str. 7–8.