

**Akademia Techniczno-Humanistyczna**

**w Bielsku-Białej**

Wydział Budowy Maszyn i Informatyki

**Bezpieczeństwo technologii informatycznych**

**(ćwiczenia laboratoryjne)**

**Ćwiczenie numer:**

**4**

**Czas realizacji zajęć:** 135 min.

**Temat ćwiczenia:**

**Szyfr Playfair**

**1. Wstęp teoretyczny.**

**Szyfr Playfair** (czasem nazywany też **szyfrem Playfaira**) został wymyślony przez sir [Charlesa Wheatstone'a](https://pl.wikipedia.org/wiki/Charles_Wheatstone) w [1854](https://pl.wikipedia.org/wiki/1854), a spopularyzowany przez barona[Lyona Playfaira](https://pl.wikipedia.org/wiki/Lyon_Playfair).

Aby szyfrować tym sposobem będziemy potrzebowali do tego celu specjalnie przygotowanej tabelki i słowa klucza, które pomoże nam w przygotowaniu tej tabelki. A samo szyfrowanie opiera się na podzieleniu wiadomości w pary liter a następnie zastąpieniu tych par innymi, według tabelki i trzech zasad.

Więc zaczynamy...

Najpierw wymyślamy sobie słowo klucz, które oczywiście musi być znane osobie odszyfrowującej naszą wiadomość. Jeśli w naszym kluczu powtarzałyby się jakieś litery to należałoby pominąć ich powtórzenia np. użycie słowa ANANAS dałoby nam klucz ANS gdyż wszystkie powtórzenia liter należy pominąć. Ja jako klucza użyje słowa DRES.

Następnie tworzymy tabelkę 5x5 liter. W pierwszym wierszu naszej tabelki umieszczamy nasz klucz a następnie pozostałe miejsca uzupełniamy kolejnymi literami alfabetu łacińskiego (26 znaków). Literę „ I ” oraz „ J ” traktujemy jako jedną.

D R E S A

B C F G H

I/J K L M N

O P Q T U

V W X Y Z

Teraz dzielimy naszą wiadomość na pary liter. Każda para musi się składać z dwóch różnych liter, jeśli tak nie jest to litery musimy rozdzielić przez wstawienie pomiędzy nie dowolnej, innej od nich, litery np. manna zmienimy na ma - nx - na. Również, gdy nasz tekst ma nieparzystą liczbę liter to dodajemy jakąś na końcu tak, aby było parzyście.

Nasza wiadomość: **Wesołe szyfrowanie**

Po podziale: **We - so - łe - sz - yf - ro - wa - ni - ex**

Teraz przechodzimy do szyfrowania naszych par.

Szyfrowanie zachodzi według trzech zasad:

Jeśli obie litery z pary leżą w tej samej kolumnie tabelki to zastępujemy każdą z nich literą leżącą pod nią np. **LE** zamienimy w **QF**. Jeśli litera znajduje się na końcu kolumny to zastępujemy ją pierwszą literą tej kolumny np. **Y** w **S**.

Jeśli obie litery z pary leżą w tym samym wierszu to zastępujemy każdą z nich literą leżącą z prawej strony np. **NI** zamienimy w **IK**. Jeśli litera znajduje się na końcu wiersza to zastępujemy ją pierwszą literą tego wiersza np. **Z** w **V**.

Jeśli obie litery leżą w różnych wierszach i kolumnach to dla każdej z liter szukamy w wzdłuż wiersza kolumny z drugą literą i zastępujemy literą znajdującą się w miejscu ich przecięcia np. **SO** zamienimy w **DT**. Dla **S** szukamy kolumny z **O** a dla **O** szukamy kolumny z **S**.

Tak, że nasz szyfrogram będzie wyglądał tak: **Xr - dt - qf - ay - xg - dp - zr - ik - fe**

Przykład:

Klucz: **Dres**

Tekst jawny: Fajnie

Pary: **Fa - jn - ie**

Szyfrogram: **He - ki - ld**

Aby odszyfrować wiadomość należy odwrócić procedurę i używać tego samego klucza i tabelki.

Podpowiem że dla 1 zasady odczytujemy litery leżące nad, dla 2 zasady odczytujemy litery z lewej strony a dla 3 zasady można postąpić tak samo jak przy szyfrowaniu.

**2. Plan wykonania ćwiczenia.**

1. Napisz program, który szyfruje tekst zgodnie z algorytmem szyfru Playfair.
2. Napisz program, który odszyfrowuje tekst zgodnie z algorytmem szyfru Playfair.
3. Napisz sprawozdanie.