

<p>Bezpieczeństwo systemów teleinformatycznych</p> <p>mgr inż. Paweł Kubczak</p>
<p>Implementacja algorytmu DES</p> <p>09.09.2021</p>
<p>Jakub Lewandowski 139968</p> <p>Teleinformatyka</p> <p>rok 3 sem 6</p>

1. Celem zadania jest utworzenie programu szyfrującego, który dla wprowadzonego tekstu pobierze z generatora (offline lub online) klucz odpowiedniej długości, dokona szyfrowania DES, a następnie zwróci szyfrogram.
2. Działanie programu:

Zaimplementowane zostały dwa systemy wprowadzania danych i klucza do programu:

1. Jest to decymalny który zostanie skonwertowany na binarny
 - klucz oraz dane wejściowe powinny się składać z 8 znaków.
2. Jest to hexadecymalny który zostanie skonwertowany na decymalny
 - klucz powinien się składać z 12 znaków a wprowadzane dane z 16 znaków.

Przykład:

1. System DEC

Dane wejściowe:

```
string klucz="vgyhbjun";
string dane="asdfghkg";
```

Dane wyjściowe:

```
uytrewqh
wpisz dane wejsciowe:
przyklad:vgyhbjun
asdfgh
Zaszyfrowane dane wyjsciowe 1011111011111011111011111011111010111111101011101111111011101011
```

2. System Hex

Dane wejściowe:

```
string klucz= "FFFFFFFFFFFF";  
string dane="AAAAAAAAAAAAAAAA";
```

Dane wyjściowe:

```
Wybrano system hex, prosze wpisac klucz i dane skladajace sie z 16 znakow  
przyklad klucz: FFFFFFFFFFFFFF  
wpisz dane wejscowe:  
przyklad:AAAAAAAAAAAAAAAA  
Zaszyfrowane dane wyjscowe 11101011111010111111101010111011101010101111101110101111110
```

Wynik w każdym przypadku jest pokazywany w systemie binarnym.

Link do kodu na Githubie:

<https://github.com/Ploydb/BST>