

Imię i nazwisko	Kierunek	Rok i grupa studiów
Anna Jasielec	Informatyka Techniczna	rok 1, grupa 4
Data zajęć:	Numer i temat sprawozdania:	
14.12.2022	9. Kryptografia	

1. Przebieg zajęć: Zajęcia 9. dotyczyły kryptografii.

- Poznanie definicji kryptografii oraz kryptoanalizy.
- Poznanie rodzajów szyfrów (monoalfabetyczne i polialfabetyczne).
- Szyfr Cezara – do wartości każdego znaku dodaje się 3 według tabeli ASCII.
- Szyfr ROT - 13 - do wartości każdego znaku dodaje się 13 według tabeli ASCII.
- Szyfr z dowolnym przesunięciem - do wartości każdego znaku dodaje się dowolną, ustaloną wcześniej liczbę.
- Szyfr AtBash – wartość znaku odejmuje się od 127 (czyli ostatniego znaku w tabeli ASCII).
- Szyfr Vigenere’a – jest oparty na tablicy, słowo kluczowe mówi, z którego wiersza (lub kolumny) należy w danym momencie skorzystać.
- Szyfr metodą przestawiania – wiadomość wpisuje się do tablicy, a następnie odczytuje w innej kolejności.

2. Zadania:

Stwórz program z 2 wybranymi funkcjami szyfrującymi / deszyfrującymi (*tylko jeden z przesunięciem):

- Menu: rodzaj szyfrowania / deszyfrowania:

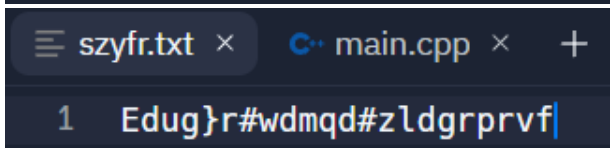
```
MENU
[1] - Szyfrowanie Cezara
[2] - Szyfrowanie metodą przestawiania
```

1.) Szyfrowanie Cezara:

- Dodaj wiadomość -> zaszyfruj -> zapisz do pliku:

```
Podaj wiadomość którą chcesz zaszyfrować:
Bardzo tajna wiadomosc

Którą metodą chcesz zaszyfrować swoją wiadomość?
1
Twoja wiadomość została zaszyfrowana i zapisana w pliku.
```



```
1 Edug}r#wdmqd#zldgrprvf|
```

- Odczytaj wiadomość z pliku -> odszyfruj:

```
Którą metodą chcesz odszyfrować wiadomość z pliku? 1
Odszyfrowana wiadomosc:
Bardzo tajna wiadomosc>
```

2.) Szyfrowanie metodą przestawiania:

- Dodaj wiadomość -> zaszyfruj -> zapisz do pliku:

```
Podaj wiadomość którą chcesz zaszyfrować:
tajneslowa42

Którą metodą chcesz zaszyfrować swoją wiadomość?
2
Twoja wiadomość została zaszyfrowana i zapisana w pliku.
```

```
szyfr.txt x ma
1  tewasajl4no2
```

- Odczytaj wiadomość z pliku -> odszyfruj:

```
Którą metodą chcesz odszyfrować wiadomość z pliku? 2
Odszyfrowana wiadomosc:
tajneslowa42>
```

3. Wnioski:

- Znam pojęcie kryptografii oraz kryptoanalizy.
- Kryptografia zajmuje się utajnianiem danych, natomiast kryptoanaliza łamaniem szyfrów.
- Wiem jak działają metody szyfrowania, takie jak: szyfrowanie Cezara, szyfrowanie ROT – 13, szyfrowanie z dowolnym przesunięciem, szyfrowanie AtBash, szyfrowanie Vigenere'a i szyfrowanie metodą przestawiania.
- Umiem zaszyfrować i odszyfrować dowolną wiadomość tymi metodami.
- Ta wiedza pozwoliła mi stworzyć program, który szyfruje i deszyfruje wiadomość.