

Sprawozdanie - Szyfry

Bezpieczeństwo systemów informatycznych



Semestr zimowy 2024/25

Wawrzyniec Ciuła 15560

Spis treści

[Link do repozytorium na Github’ie 2](#_Toc182446497)

[Link do strony z szyframi 2](#_Toc182446498)

[Szyfr Cezara 2](#_Toc182446499)

[Zasada działania 2](#_Toc182446500)

[Fragmenty kodu 2](#_Toc182446501)

[Przykład działania 3](#_Toc182446502)

[Szyfr Playfair’a 4](#_Toc182446503)

[Zasada działania 4](#_Toc182446504)

[Fragmenty kodu 4](#_Toc182446505)

[Przykład działania 5](#_Toc182446506)

[Szyfr Polibeusza 6](#_Toc182446507)

[Zasada działania 6](#_Toc182446508)

[Przykładowa wygenerowana tabela 6](#_Toc182446509)

[Fragmenty kodu 6](#_Toc182446510)

[Przykład działania 7](#_Toc182446511)

[Szyfr Vigenère’a 8](#_Toc182446512)

[Zasada działania 8](#_Toc182446513)

[Fragmenty kodu 8](#_Toc182446514)

[Przykład działania 10](#_Toc182446515)

[Szyfr RSA 11](#_Toc182446516)

[Zasada działania 11](#_Toc182446517)

[Fragmenty kodu 11](#_Toc182446518)

[Przykład działania 14](#_Toc182446519)

## [Link do repozytorium na Github’ie](https://github.com/ciula12/BSI_2024)

## [Link do strony z szyframi](https://ciula12.github.io/BSI_2024/)

# [Szyfr Cezara](https://ciula12.github.io/BSI_2024/Szyfr%20Cezara/index.html)

## Zasada działania

Klasyczny szyfr podstawienny, w którym każda litera w tekście jest przesuwana o określoną liczbę miejsc w alfabecie. Proces ten może być stosowany zarówno do szyfrowania, jak i deszyfrowania, w zależności od kierunku przesunięcia.

## Fragmenty kodu

**Szyfrowanie**Obraz zawierający tekst, zrzut ekranu, oprogramowanie, wyświetlacz

Opis wygenerowany automatycznie

**Deszyfrowanie**Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznie

## Przykład działania

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatyczniePrzykład z przesunięciem litery „A” do litery „E”, czyli o 6 znaków.

# [Szyfr Playfair’a](https://ciula12.github.io/BSI_2024/Szyfr%20Playfaira/index.html)

## Zasada działania

Szyfr blokowy, w którym tekst jest podzielony na pary liter. Zaszyfrowanie każdej pary zależy od tego, czy litery znajdują się w tym samym wierszu, kolumnie, czy tworzą prostokąt.

## Fragmenty kodu

**Tworzenie macierzy Playfair’a**Obraz zawierający tekst, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznieTabela jest generowana na podstawie podanego klucza. Wprowadza klucz na początek tabeli.

**Szyfrowanie**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

**Przykładowa wygenerowana tabela**Obraz zawierający zrzut ekranu, typografia, design

Opis wygenerowany automatycznie

## Przykład działania

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie  
Przykład szyfrowania po wykorzystaniu klucza „skrót”.

# [Szyfr Polibeusza](https://ciula12.github.io/BSI_2024/Szyfr%20Polibeusza/index.html)

## Zasada działania

Metoda szyfrowania, w której każdej literze alfabetu przypisuje się parę współrzędnych na siatce (tzw. kwadracie Polibeusza).

## Przykładowa wygenerowana tabela

Obraz zawierający tekst, zrzut ekranu, numer, linia

Opis wygenerowany automatycznie

## Fragmenty kodu

**Generowanie tabeli szyfru**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznieAlfabet samoczynnie generuje nową tabelę z losowo rozłożonego alfabetu.

**Szyfrowanie tekstu na podstawie koordynatów**Obraz zawierający tekst, zrzut ekranu

Opis wygenerowany automatycznie

## Przykład działania

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznie  
Każda litera ma swoje koordynaty, które są później modyfikowane poprzez różne offsety, co daje każdej literze, nawet powtarzającej się jedna po drugiej, unikalne wartości.

# [Szyfr Vigenère’a](https://ciula12.github.io/BSI_2024/Szyfr%20Vigen%C3%A8re/index.html)

## Zasada działania

Jest to szyfr polialfabetyczny, w którym każdą literę tekstu przesuwa się w alfabecie o wartość odpowiadającą literze z klucza. Klucz jest powtarzany nad tekstem, a każda litera w wiadomości jest przesuwana zgodnie z odpowiadającą jej literą klucza, tworząc zmienną liczbę przesunięć. Dzięki zmiennej liczbie przesunięć unika wzorców typowych dla prostych szyfrów podstawiennych, co zwiększa jego odporność na złamanie.

## Fragmenty kodu

**Tworzenie tabeli Vigenère’a**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

**Szyfrowanie**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie  
Na podstawie litery klucza i litery szyfrowanego tekstu sprawdzane jest, w którym miejscu łączą się one kolumną z wierszem, czego wynikiem jest zaszyfrowana litera.

**Deszyfrowanie**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

## Przykład działania

Obraz zawierający tekst, zrzut ekranu, Czcionka, numer

Opis wygenerowany automatycznieKażda litera jest porównywalna z każdą literą klucza po kolei. Jeżeli zabraknie liter w kluczu, klucz się zapętla.

# [Szyfr RSA](https://ciula12.github.io/BSI_2024/Szyfr%20RSA/index.html)

## Zasada działania

Szyfr RSA działa poprzez generowanie pary kluczy (publicznego i prywatnego) oraz wykorzystanie ich do szyfrowania i deszyfrowania wiadomości. RSA opiera się na trudności rozkładu liczby na czynniki pierwsze. Wiadomość szyfruje się kluczem publicznym, a odszyfrowuje tylko kluczem prywatnym, co zapewnia bezpieczeństwo komunikacji.

## Fragmenty kodu

**Generowanie kluczy**Obraz zawierający tekst, zrzut ekranu, oprogramowanie

Opis wygenerowany automatycznieDwie stałe p i q są generowane losowo spomiędzy liczb pierwszych z zakresu 1000, a 10000.

Liczba e jest wybrana jako 65537, ponieważ jest ona najlepszym wyborem pomiędzy wydajnością, a bezpieczeństwem.

**Generowanie d do klucza prywatnego**Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznieAlgorytm Euklidesa rozszerzonego, aby znaleźć *modularną odwrotność* liczby e względem ϕ.

**Potęgowanie modularne**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie**Szyfrowanie**Obraz zawierający tekst, zrzut ekranu, Czcionka, oprogramowanie

Opis wygenerowany automatycznie

**Deszyfrowanie**Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie

## Przykład działania

Obraz zawierający tekst, zrzut ekranu, Czcionka

Opis wygenerowany automatycznie  
Po wygenerowaniu klucza publicznego i prywatnego tekst jest szyfrowany i przekazywany jest użytkownikowi wraz z kluczem publicznym. Odpowiedź zwrotną system zapamiętuje wygenerowany klucz prywatny i odszyfrowuje wiadomość z jego wykorzystaniem.