# Dokumentacja wielowarstwowego szyfru prostego

Ksawery Wawrzyniak

27 listopada 2022

# Spis treści

# 1 Ustawienia domyślne

$keycodes = [7, 2, "SZYFR", "SZYFR", "SZYFR", ("SZYFR", 3),$
$("SZYFR", (2, 1)), ("SZYFR", (1, 2)), "SZYFROWANIE", 7, 5, 7, -7, 5, 7, 35]$

## 1.1 Warstwy szyfru

0. warstwa: tekst jawny
1. warstwa: szyfr przestawieniowy
2. warstwa: szyfr przestawieniowy podwójny
3. warstwa: szyfr przestawieniowy grupowany o kluczu keycodes[0]
4. warstwa: szyfr przestawieniowy wyrazowy
5. warstwa: szyfr przestawieniowy zdaniowy
6. warstwa: szyfr z losowo wybranymi fałszywkami
7. warstwa: szyfr z fałszywkami dobranymi pod bramkę bitową "AND"
8. warstwa: szyfr z fałszywkami dobranymi pod bramkę bitową "OR"
9. warstwa: szyfr z fałszywkami dobranymi pod bramkę bitową "XOR"
10. warstwa: przekładaniec o kluczu keycodes[1]
11. warstwa: prosty szyfr wahadłowy
12. warstwa: szyfr wahadłowy zewnątrzsłowny
13. warstwa: szyfr wahadłowy wewnątrzsłowny
14. warstwa: szyfr ze szlakiem o kluczu keycodes[2]
15. warstwa: szyfr ze szlakiem pod prąd o kluczu keycodes[3]
16. warstwa: prosty synchroniczny szyfr dwukierunkowy o kluczu keycodes[4]
17. warstwa: synchroniczny szyfr dwukierunkowy o kluczu keycodes[5]
18. warstwa: asynchoniczny szyfr dwukierunkowy o kluczu keycodes[6]
19. warstwa: asynchroniczny szyfr o kluczu keycodes[7]
20. warstwa: szyfr z alfabetem ze słowem kluczowym keycodes[8]
21. warstwa: szyfr z przesuniętym alfabetem o daną ilość pozycji określoną kluczem keycodes[9]
22. warstwa: szyfr atbasz
23. warstwa: szyfr tablicowy o kluczu keycodes[10]
24. warstwa: szyfr tablicowy o kluczu keycodes[11]
25. warstwa: szyfr z przesuniętym alfabetem o daną ilość pozycji określoną kluczem keycodes[12]
26. warstwa: szyfr z rosnąco przesuniętym alfabetem
27. warstwa: szyfr przestawieniowy rosnący
28. warstwa: konwersja liczby na litery
29. warstwa: szyfr klawiaturowy
30. warstwa: szyfr przestawieniowy grupowany o kluczu keycodes[13]
31. warstwa: szyfr przestawieniowy grupowany o kluczu keycodes[14]
32. warstwa: konwersja z systemu 10 na 9
33. warstwa: konwersja z systemu 10 na 8
34. warstwa: konwersja z systemu 10 na 7
35. warstwa: konwersja z systemu 10 na 6
36. warstwa: konwersja z systemu 10 na 5
37. warstwa: konwersja z systemu 10 na 4
38. warstwa: konwersja z systemu 10 na 3
39. warstwa: konwersja z systemu 10 na 2
40. warstwa: szyfr płotkowy o kluczu keycodes[15]

# 2 Opisy warstw szyfru

## 2.1 Szyfr przestawieniowy

Algorytm szyfrujący i deszyfrujący tej warstwy jest dokładnie taki sam. Szyfrogram z warstwy o niższym numerze zawsze przy danej warstwie bierzemy jako tekst jawny. W tej warstwie szyfrogram to po prostu tekst jawny tej warstwy zapisany od tyłu, czyli gdy mamy tekst jawny, np.: «Nazywam się Ksawery Wawrzyniak.», to szyfrogram dla tego tekstu jawnego w tej warstwie wygląda tak: «.kainyzrwaW yrewasK ęis mawyzaN».

## 2.2 Szyfr przestawieniowy podwójny

Jest to szyfr przestawieniowy grupowany o kluczu równym 2.

## 2.3 Szyfr przestawieniowy grupowany

Algorytm szyfrujący i deszyfrujący tej warstwy jest dokładnie taki sam. Najpierw dzielimy tekst jawny na kawałki o długości równej kluczowi keycodes[0]. Następnie każdy taki kawałek z osobna zapisujemy od tyłu. Na końcu łączymy fragmenty tekstu ze sobą przy użyciu łącznika "". Dla przykładowego tekstu jawnego z przykładowym kluczem keycodes[0] równym 5 «Nazywam się Ksawery Wawrzyniak.» szyfrogram powinien wyglądać «wyzaNis maasK ę yrew zrwaWkainy.».

## 2.4 Szyfr przestawieniowy wyrazowy

Algorytm szyfrujący i deszyfrujący tej warstwy jest dokładnie taki sam. Najpierw dzielimy tekst jawny na słowa. Następnie każde słowe zapisujemy od tyłu. Na końcu łączymy fragmenty takie tekstu ze sobą przy użyciu łącznika " ". Dla przykładowego tekstu jawnego «Nazywam się Ksawery Wawrzyniak.» szyfrogram powinien wyglądać «mazywaN ęis yrewasK .kainyzrwaW».

## 2.5 Szyfr przestawieniowy zdaniowy

Algorytm szyfrujący i deszyfrujący tej warstwy jest dokładnie taki sam. Najpierw dzielimy tekst jawny na zdania. Następnie każde takie zdanie zapisujemy od tyłu. Na końcu łączymy takie fragmenty tekstu ze sobą przy użyciu łączników: ".", "!", "?", [znak nowej linii] dla odpowiednich w pierwotnym ustawieniu dla tekstu jawnego. Dla przykładowego tekstu jawnego «Nazywam się Ksawery Wawrzyniak.» szyfrogram powinien wyglądać «kainyzrwaW yrewasK ęis mawyzaN.».

## 2.6 Szyfr z losowo wybranymi fałszywkami

### 2.6.1 Algorytm szyfrujący

Najpierw dzielimy tekst jawny na dwuznakowe fragmenty. Następnie w każdym takim fragmencie pomiędzy znakami dodajemy losowo wybraną fałszywkę. Na końcu łączymy ze sobą fragmenty tekstu łącznikiem "".

### 2.6.2 Algorytm deszyfrujący

Najpierw dzielimy szyfrogram na trzyznakowe fragmenty. Następnie środkowy znak w każdym takim fragmencie usuwamy. Na końcu łączymy fragmenty tekstu ze sobą łącznikiem "".

## 2.7 Szyfr z fałszywkami dobranymi pod bramkę bitową "AND"

### 2.7.1 Algorytm szyfrujący

Najpierw dzielimy tekst jawny na dwuznakowe fragmenty. Nastepnie w każdym takim fragmencie dodajemy literę, która wg tablicy 1. ma wartość koniunkcji bitowej znaków będących częścią pierwotną fragmentu albo jeśli nie można dokonać takiej koniunkcji, to losowo dodajemy jakąś fałszywkę. Na końcu łączymy ze sobą fragmenty tekstu łącznikiem "".

### 2.7.2 Algorytm deszyfrujący

Najpierw dzielimy szyfrogram na trzyznakowe fragmenty. Następnie środkowy znak w każdym takim fragmencie usuwamy. Na końcu łączymy fragmenty tekstu ze sobą łącznikiem "".

## 2.8 Szyfr z fałszywkami dobranymi pod bramkę bitową "OR"

### 2.8.1 Algorytm szyfrujący

Najpierw dzielimy tekst jawny na dwuznakowe fragmenty. Nastepnie w każdym takim fragmencie dodajemy literę, która wg tablicy 1. ma wartość alternatywy bitowej znaków będących częścią pierwotną fragmentu albo jeśli nie można dokonać takiej alternatywy, to losowo dodajemy jakąś fałszywkę. Na końcu łączymy ze sobą fragmenty tekstu łącznikiem "".

### 2.8.2 Algorytm deszyfrujący

Najpierw dzielimy szyfrogram na trzyznakowe fragmenty. Następnie środkowy znak w każdym takim fragmencie usuwamy. Na końcu łączymy fragmenty tekstu ze sobą łącznikiem "".

## 2.9 szyfr z fałszywkami dobranymi pod bramkę bitową "XOR"

### 2.9.1 Algorytm szyfrujący

Najpierw dzielimy tekst jawny na dwuznakowe fragmenty. Następnie w każdym takim fragmencie dodajemy literę, która wg tablicy 1. ma wartość alternatywy wykluczającej bitowej znaków będących częścią pierwotną fragmentu albo jeśli nie można dokonać takiej alternatywy, to losowo dodajemy jakąś fałszywkę. Na końcu łączymy ze sobą fragmenty tekstu łącznikiem "".

### 2.9.2 Algorytm deszyfrujący

Najpierw dzielimy szyfrogram na trzyznakowe fragmenty. Następnie środkowy znak w każdym takim fragmencie usuwamy. Na końcu łączymy fragmenty tekstu ze sobą łącznikiem "".

## 2.10 Przekładaniec

Jest to szyfr o zasadzie szyfru ze szlakiem, ale nie ma dodatkowych znaków oraz algorytmy szyfrujący i deszyfrujący są odwrotnie i słowo kodowe to zawsze alfabet albo jego kawałek (a w skrajnym przypadku dodatnia wielokrotność).

## 2.11 Prosty szyfr wahadłowy

### 2.11.1 Algorytm szyfrujący

Zapisujemy tekst jawny w taki sposób, że pierwszy znak tekstu jawnego jest na środku szyfrogramu, nieparzyste (liczymy od miejsca zerowego) znaki w tekście zapisujemy na lewo od pierwszego znaku, ale w taki sposób, że im większy indeks znaku, tym bardziej na lewo, a parzyste na prawo, przy czym im większy indeks, tym bardziej na prawo.

### 2.11.2 Algorytm deszyfrujący

Zapisujemy szyfrogram w taki sposób, że środkowy znak zapisujemy na początku, potem zapisujemy pary znaków równoodległych od środka szyfrogramu coraz dalsze od siebie nawzajem.

## 2.12 Szyfr wahadłowy zewnątrzsłowny

### 2.12.1 Algorytm szyfrujący

Na początku dzielimy tekst jawny na słowa. Następnie zamieniamy kolejność słów w taki sposób, że pierwsze słowo będzie na środku tekstu, nieparzyste słowa (liczymy od słowa zerowego) dajemy na lewo od pierwszego słowa, im większa liczba, tym dalej na lewo, a parzyste dajemy na prawo, przy czym im większa liczba, tym dalej na prawo.

### 2.12.2 Algorytm deszyfrujący

Najpierw dzielimy szyfrogram na słowa. Następnie zamieniamy kolejność słów w taki sposób, że środkowe słowo zapisujemy na początku, potem zapisujemy pary słów równoodległych od środka szyfrogramu coraz dalsze od siebie.

## 2.13 Szyfr wahadłowy wewnątrzsłowny

### 2.13.1 Algorytm szyfrujący

Na początku dzielimy tekst jawny na słowa, a następnie z każdym słowem postępujemy tak, jakby to był cały tekst jawny do prostego szyfru wahadłowego.

### 2.13.2 Algorytm deszyfrujący

Najpierw dzielimy szyfrogram na słowa, potem z każdym słowem postępujemy tak, jakby to był cały szyfrogram do prostego szyfru wahadłowego.

## 2.14 Szyfr ze szlakiem

Słowo kodowe powinno posiadać tylko litery oraz żadna litera nie powinna się powtarzać we słowie kodowym.

### 2.14.1 Algorytm szyfrujący

Najpierw tworzymy tablicę szyfrującą o ilości wierszy (albo kolumn, zależy jak wygodniej) takiej, jaka jest długość słowa kodowego. Następnie w pierwszym wierszu (jeśli mamy określoną ilość kolumn; albo w pierwszej kolumnie, jeśli odwrotnie) zapisujemy w każdej kolejnej kolumnie (wierszu) zapisujemy kolejny znak ze słowa kodowego. Potem w każdym kolejnym wierszu (kolumnie) zapisujemy tekst jawny tak samo, jak słowo kodowe. Jeśli po zapisaniu tekstu jawnego tablica szyfrująca posiada niezapełniony wiersz(kolumnę), to dodajemy do niej x (i wpisujemy, ile dopisaliśmy x-ów). Na końcu łączymy znaki z całych kolumn (wierszy) w kolejności alfabetycznej indeksu znaku słowa kodowego pomijając znaki słowa kodowego, np. jeśli mamy słowo kodowe: «SZYFR», to układamy kolumny (wiersze) w kolejności znaków słowa kodowego: «FRSYZ», bo w takiej kolejności są dane litery w alfabecie.

### 2.14.2 Algorytm deszyfrujący

Najpierw tworzymy tablicę deszyfrującą o ilości wierszy (albo kolumn) takiej, jaka jest długość słowa kodowego. W pierwszej kolumnie (wierszu) wpisujemy słowo kodowe (tak samo jak w algorytmie szyfrującym). Następnie dzielimy szyfrogram na tyle równych kawałków, ile jest znaków w słowie kodowym. Potem do kolumny odpowiadającej kolejności alfabetycznej znakom słowa kodowego taki kawałek szyfrogramu, który w takiej kolejności pasuje. Na koniec wypisujemy po

kolei zawartość kolejnych kolumn (wierszy) dochodząc do znaku o indeksie równym długości szyfrogramu minus liczba dodanych podczas szyfrowania znaków x.

## 2.15 Szyfr ze szlakiem pod prąd

Tutaj robimy to samo, co w przypadku szyfru ze szlakiem, jednakże tekst jawny zapisujemy od przeciwnej strony kolumny (wiersza) szyfrującej).

## 2.16 Prosty synchroniczny szyfr dwukierunkowy

Jest to synchroniczny szyfr dwukierunkowy o kluczu liczbowym równym 1.

## 2.17 Synchroniczny szyfr dwukierunkowy

Algorytmy szyfrujący oraz deszyfrujący działają podobnie do algorytmów szyfrującego i deszyfrującego szyfru ze szlakiem, jednakże w przypadku wpisywania tekstu jawnego do tablicy szyfrującej wpisujemy tyle wierszy znaków, ile wynosi klucz keycode[5, 1], zgodnie ze słowem kodowym, a następnie tyle samo wierszy, ale w przeciwną stronę, po czym powtarzamy, aż skończą się znaki w tekście jawnym.

## 2.18 Asynchroniczny szyfr

Algorytmy szyfrujący i deszyfrujący są podobne do algorytmów szyfrującego i deszyfrującego, jednakże przepisywanie znaków tekstu jawnego nie jest symetryczne w znaczeniu takim, że jak się zapisuje się w jednym kierunku znaki tekstu jawnego w innej ilości pod rząd niż w przeciwnym kierunku.

## 2.19 Szyfr z alfabetem ze słowem kluczowym

Tworzymy nowy alfabet, który zaczyna od słowa kluczowego, a reszta to zwykły alfabet bez liter, które są w słowie kluczowym. Porównujemy ze sobą normalny alfabet z alfabetem stworzonym pod ten szyfr i zamieniamy litery z tekstu jawnego ze zwykłego alfabetu na litery z alfabetu szyfrującego (patrzymy na indeksy).

## 2.20 Szyfr z przesuniętym alfabetem

ALgorytmy szyfrujący i deszyfrujący tej warstwy są takie same, z tą różnicą, że algorytm deszyfrujący przesuwa alfabet w lewo, a nie jak w szyfrującym w prawo. Najpierw przesuwamy alfabet o taką ilość pozycji, jaka jest określona w kluczu keycodes[9]. Następnie zastępujemy każdą literę w słowie jawnym literą z przesuniętego alfabetu o odpowiednim indeksie.

## 2.21 Szyfr atbasz

Jest to podobny szyfr do szyfru z przesuniętym alfabetem z tą różnicą, że nie ma przesunięcia alfabetu, a sam alfabet jest zapisany od tyłu.

## 2.22 Szyfr tablicowy

Klucz tego szyfru powinien być liczbą pierwszą, przez którą liczba określająca długość alfabetu była podzielna.

### 2.22.1 Algorytm szyfrujący alfabet do szyfrowania

Najpierw tworzymy tablicę szyfrującą o ilości kolumn równej kluczowi keycodes[10] i o ilości wierszy równej ilorazowi długości alfabetu przez klucz. Potem do każdej komórki tablicy wpisujemy literę alfabetu oraz literę alfabetu przesuniętego o sumie liczb ilości kolumn oraz ilości wierszy pomnożonej przez klucz.

### 2.22.2 Szyfrowanie i deszyfrowanie

Algorytmy szyfrując i deszyfrując tej warstwy to algorytmy szyfrujący i deszyfrujący szyfru z przesuniętym alfabetem, jednakże przesunięcie liter jest określone przez tablicę szyfrującą tej warstwy.

## 2.23 Szyfr z rosnąco przesuniętym alfabetem

Jest to szyfr, w którym co znak słowa jawnego alfabet się przesuwa o wartość przesuwającą się zaczynając od prędkości przesunięcia o jedną pozycję, a następnie przy wartości podzielnej przez długość alfabetu rosnącą o jedną pozycję na znak.

## 2.24 Szyfr przestawieniowy rosnący

Jest to szyfr grupowany, gdzie grupy znaków przestawianych się zwiększa o jeden zaczynając od pary znaków.

## 2.25 Szyfr klawiaturowy

Jest to szyfr wykorzystujący sposób wprowadzania znaków w telefonach komórkowych, które jeszcze wykorzystywały fizyczne klawiatury.

## 2.26 Szyfr płotkowy

Jest to szyfr podobny do szyfru ze szlakiem, ale bez dodatkowych znaków oraz słowo kodowe to zawsze alfabet albo jego kawałek (a w skrajnym przypadku dodatnia wielokrotność).

# 3 Tabele szyfrujące

| litera | b5 | b4 | b3 | b2 | b1 | b0 |
|---|---|---|---|---|---|---|
| A | 0 | 0 | 0 | 0 | 0 | 0 |
| Ą | 0 | 0 | 0 | 0 | 0 | 1 |
| B | 0 | 0 | 0 | 0 | 1 | 0 |
| C | 0 | 0 | 0 | 0 | 1 | 1 |
| Ć | 0 | 0 | 0 | 1 | 0 | 0 |
| D | 0 | 0 | 0 | 1 | 0 | 1 |
| E | 0 | 0 | 0 | 1 | 1 | 0 |
| Ę | 0 | 0 | 0 | 1 | 1 | 1 |
| F | 0 | 0 | 1 | 0 | 0 | 0 |
| G | 0 | 0 | 1 | 0 | 0 | 1 |
| H | 0 | 0 | 1 | 0 | 1 | 0 |
| I | 0 | 0 | 1 | 0 | 1 | 1 |
| J | 0 | 0 | 1 | 1 | 0 | 0 |
| K | 0 | 0 | 1 | 1 | 0 | 1 |
| L | 0 | 0 | 1 | 1 | 1 | 0 |
| Ł | 0 | 0 | 1 | 1 | 1 | 1 |
| M | 0 | 1 | 0 | 0 | 0 | 0 |
| N | 0 | 1 | 0 | 0 | 0 | 1 |
| Ń | 0 | 1 | 0 | 0 | 1 | 0 |
| O | 0 | 1 | 0 | 0 | 1 | 1 |
| Ó | 0 | 1 | 0 | 1 | 0 | 0 |
| P | 0 | 1 | 0 | 1 | 0 | 1 |
| Q | 0 | 1 | 0 | 1 | 1 | 0 |
| R | 0 | 1 | 0 | 1 | 1 | 1 |
| S | 0 | 1 | 1 | 0 | 0 | 0 |
| Ś | 0 | 1 | 1 | 0 | 0 | 1 |
| T | 0 | 1 | 1 | 0 | 1 | 0 |
| U | 0 | 1 | 1 | 0 | 1 | 1 |
| V | 0 | 1 | 1 | 1 | 0 | 0 |
| W | 0 | 1 | 1 | 1 | 0 | 1 |
| X | 0 | 1 | 1 | 1 | 1 | 0 |
| Y | 0 | 1 | 1 | 1 | 1 | 1 |
| Z | 1 | 0 | 0 | 0 | 0 | 0 |
| Ź | 1 | 0 | 0 | 0 | 0 | 1 |
| Ż | 1 | 0 | 0 | 0 | 1 | 0 |

Tabela 1. Wartości bitowe kolejnych liter w polskim alfabecie zawierającym dodatkowo litery Q, V i X

| Znak | Wartość | Znak | Wartość |
|---|---|---|---|
| ( | 01 | Ę | 333 |
| ) | 10 | F | 3333 |
| [ | 101 | G | 4 |
| ] | 010 | H | 44 |
| { | 001 | I | 444 |
| } | 100 | J | 5 |
| < | 1001 | K | 55 |
| > | 0110 | L | 555 |
| ” | 110 | Ł | 5555 |
| ’ | 011 | M | 6 |
| SPACJA | 0 | N | 66 |
| ENTER | 00 | Ń | 666 |
| TAB | 000 | O | 6666 |
| . | 1 | Ó | 66666 |
| , | 11 | P | 7 |
| ! | 111 | Q | 77 |
| ? | 1111 | R | 777 |
| / | 11111 | S | 7777 |
| \ | 111111 | Ś | 77777 |
| : | 1111111 | T | 8 |
| ; | 11111111 | U | 88 |
| A | 2 | V | 888 |
| Ą | 22 | W | 9 |
| B | 222 | X | 99 |
| C | 2222 | Y | 999 |
| Ć | 22222 | Z | 9999 |
| D | 3 | Ź | 99999 |
| E | 33 | Ż | 999999 |

Tabela 2. Jest to tablica szyfrująca do szyfru klawiaturowego przy użyciu polskiego alfabetu wykorzystanego w poprzedniej tablicy.