<table>
<tr><td colspan="3">Politechnika Świętokrzyska w Kielcach
Wydział Elektrotechniki, Automatyki i Informatyki</td></tr>
<tr><td colspan="3">ALGORYTMY I STRUKTURY DANYCH – PROJEKT
Informatyka - I rok, Rok akademicki - 2021/2022</td></tr>
<tr><td>Kamień milowy: 1</td><td colspan="2">Temat projektu: Szyfr Cezara i szyfr Vigenère'a</td></tr>
<tr><td>Grupa: 1ID14B</td><td rowspan="2">Wykonujący:
Marek Supierz,
Andrzej Mysior,
Adrian Nowak</td><td rowspan="2">Ocena:</td></tr>
<tr><td>Data oddania sprawozdania:
02.04.2022</td></tr>
</table>

Prace przewidziane na pierwszy kamień milowy:

1. Przygotowanie harmonogramu i podział prac w zespole,
2. Zapoznanie się z działaniem szyfrów Cezara, oraz Vigenère'a przez członków zespołu,
3. Przeniesienie harmonogramu z wersji pisemnej do wersji online – do narzędzia Trello,
4. Omówienie pomysłów na projekt,
5. Wybór metody rozwiązania zadanego tematu,
6. Przygotowanie środowiska programistycznego „Visual Studio 2022”
7. Przygotowanie repozytorium w serwisie „GitHub”,
8. Implementacja algorytmu realizującego szyfr Cezara,
9. Testowanie i poprawa znalezionych błędów,
10. Implementacja algorytmu realizującego szyfr Vigenère'a,
11. Testowanie i poprawa znalezionych błędów,
12. Przygotowanie do połączenia kodów w jedną, spójną całość,
13. Przygotowanie sprawozdania z postępów prac nad projektem.

Przygotowanie harmonogramu i podział prac w zespole

Harmonogram został przygotowany a następnie przedstawiony na zajęciach. Wprowadzono jedną poprawkę - dopisanie Adriana Nowaka. Prace zostały rozdzielone w następujący sposób:
Marek Supierz: Programowanie, przygotowanie repozytorium, testowanie, poprawa błędów
Andrzej Mysior: Testowanie, przeniesienie harmonogramu do Trello, sporządzenie sprawozdania
Adrian Nowak: Testowanie, wyszukiwanie potrzebnych zasobów, sporządzenie sprawozdania

Zapoznanie z szyframi

Szyfr to rodzaj kodu, system umownych znaków stosowany celu zatajenia wiadomości, żeby była ona niemożliwa (lub bardzo trudna) do odczytania przez każdego, kto nie posiada odpowiedniego klucza. Szyfrowanie natomiast jest procedurą przekształcania wiadomości nie zaszyfrowanej w zaszyfrowaną. Wiadomość przed zaszyfrowaniem nazywa się tekstem jawnym, a wiadomość zaszyfrowaną – szyfrogramem. Szyfry historyczne musiały umożliwiać szyfrowanie i deszyfrowanie przez człowieka, a więc opierać się na bardzo prostych operacjach. Współczesne komputery potrafią złamać praktycznie każdy tego typu szyfr.

Szyfr przesuwający (ang. shift cipher) to szyfr, w którym każdemu znakowi tekstu jawnego odpowiada dokładnie jeden znak w szyfrogramie, przesunięty o określoną, stałą liczbę znaków w alfabecie. Litery z końca alfabetu stają się literami z jego początku.

Szyfr Cezara szyfr stosowany przez Gajusza Juliusza Cezara, rzymskiego wodza i polityka, będący klasycznym przykładem szyfru przesuwającego.

Przykład: **Ala ma kota** → **Dod pd nrwd**. W tym przypadku przesunięcie wynosi 3.

Opis metody: Każdą literę tekstu jawnego zamieniamy na literę przesuniętą o 3 miejsca w prawo. I tak literę A szyfrujemy jako literę D, literę B jako E itd. W przypadku litery Z wybieramy literę C. W celu odszyfrowania tekst powtarzamy operację tym razem przesuwając litery o 3 pozycje w lewo.

Szyfr polialfabetyczny – uogólnienie szyfru monoalfabetycznego na większą liczbę przekształceń. Szyfr taki składa się z n przekształceń, takich że pierwszą literę szyfrujemy pierwszym przekształceniem, drugą drugim itd., po czym powtarzamy przekształcenia od początku począwszy od litery n+1.

Szyfr Vigenère'a

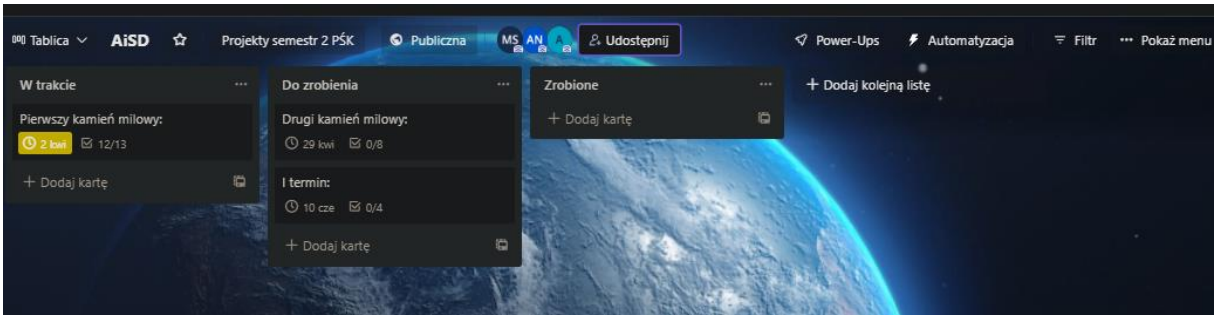
Słabość szyfrów monoalfabetycznych sprawiła, że próbowano wymyślać bardziej rozbudowane szyfry. Dało to początek polialfabetycznym szyfrom podstawieniowym. Idea takiego szyfru pojawiła się już w XV wieku (Leon Battista Alberti). Kolejne pomysły związane są z takimi nazwiskami jak Johannes Trithemius oraz Giovanni della Porta. Najbardziej znanym szyfrem polialfabetycznym jest szyfr stworzony przez Blaise de Vigenere`a, oficjalnie opublikowany w jego pracy "Traicte des Chiffres" w 1586 roku. Podczas tworzenia swojego szyfru Vigenere opierał się na przemyśleniach wcześniej wymienionych osób.

Opis metody: Tekst szyfrujemy na podstawie hasła. Szyfrowanie odbywa się w sposób następujący. Każdą literę tekstu jawnego szyfrujemy korzystając z alfabetu zaczynającego się od odpowiadającej litery w haśle. W przypadku, gdy hasło jest krótsze od szyfrowanego tekstu powtarzamy je wielokrotnie. Szyfrowanie i deszyfrowanie odbywa się na podstawie tablicy Vigenere`a.

Tablica Vigenere`a

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Przeniesieni harmonogramu do Trello



Link: https://trello.com/b/BZRM1xfR/aisd

Omówienie pomysłów na projekt

Została podjęta decyzja o stworzeniu programów konsolowych, które będą realizowały szyfr Cezara i szyfr Vigenère'a. Pracują one na danych podanych przez użytkownika. W pierwszym kamieniu szyfrowanie i deszyfrowanie obydwu szyfrów są osobnymi programami, w drugim kamieniu milowym zostaną połączone.

Przygotowanie środowiska programistycznego „Visual Studio 2022”

Podczas instalacji programu wystąpił błąd instalacji pakietu Win10SDK. Problem ten nie ma wpływu na poprawne kompilowanie kodu C.

Przygotowanie repozytorium w serwisie GitHub

W serwisie GitHub została założona organizacja „PSK-projekty” a w niej repozytorium „AiSD”. Zostały tam umieszczone pliki powstałe w wyniku prac nad projektem.

Link: https://github.com/PSK-projekty/AiSD

Implementacja algorytmu realizującego Szyfr Cezara

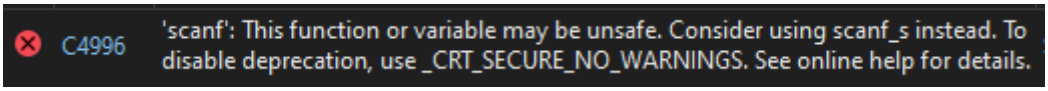
```
void szyfrowanie(char tekst[], int przesuniecie) {

    for (int i=0; tekst[i]!=0; ++i) {

      if (tekst[i] >= 'A' && tekst[i] <= 'Z') {

                  tekst[i] -= 'A';
                  tekst[i] += przesuniecie;
                  tekst[i] = tekst[i] % 26;
                  tekst[i] += 'A';

              }

              if (tekst[i] >= 'a' && tekst[i] <= 'z') {

                  tekst[i] -= 'a';
                  tekst[i] += przesuniecie;
                  tekst[i] = tekst[i] % 26;
                  tekst[i] += 'a';

              }

   }
    printf("%s", tekst);
}
```

Funkcja przyjmuje dwa parametry, podany przez użytkownika tekst oraz przesunięcie. Algorytm realizuje klasyczny szyfr Cezara tj. szyfrowanie wielkich i małych liter. Bez większych problemów udało się stworzyć także algorytm szyfrowania wszystkich znaków nie białych z tablicy ASCII.

```
void szyfrowanie(char tekst[], int przesuniecie) {

    for (int i=0; tekst[i]!=0; ++i) {

       if (tekst[i] >= 'A' && tekst[i] <= 'Z') {

                    tekst[i] -= '!';
                    tekst[i] += przesuniecie;
                    tekst[i] = tekst[i] % 94;
                    tekst[i] += '!';

                }
   }
    printf("%s", tekst);
}
```

Testowanie i poprawa błędów

Podczas prac nad programem ujawnił się następujący błąd



Nie wynika on z błędów programisty lecz z nadgorliwości środowiska programistycznego. Dodanie `#define _CRT_SECURE_NO_WARNINGS` przed `#include<stdio.h>` wyeliminowała pojawianie się problemu. Nie odnotowano innych poważnych błędów, mniejsze były spowodowane nieuwagą programisty, najczęściej występowały literówki.

Wyniki działania programu zostały porównane z poniższą stroną internetową

https://www.dcode.fr/caesar-cipher

Implementacja algorytmu realizującego Szyfr Vigenère'a

```
void szyfrVigenera(char *tekst, char *klucz) {

	char odszyfrowany_tekst;
	int szyfr;
	int dlugosc_klucza = strlen(klucz);

	//Pętla interująca aż do końca tekstu
	for (int i = 0; i < strlen(tekst); i++) {

		//Małe litery znajdują się od numeru 97 do 122 w ASCII
		if (tekst[i] >= 'a' && tekst[i] <= 'z'){
			szyfr = ((tekst[i] - 'a') - (klucz[i % dlugosc_klucza] - 'a')
+ 26) % 26 + 'a';
			odszyfrowany_tekst = szyfr;
		}

		//Wielkie litery znajdują się od numeru 65 do 90 w ASCII
		if (tekst[i] >= 'A' && tekst[i] <= 'Z') {
			szyfr = ((tekst[i] - 'A') - (klucz[i % dlugosc_klucza] - 'A')
+ 26) % 26 + 'A';
			odszyfrowany_tekst = szyfr;
		}

		//Wyświetl jeśli jest znakiem np literą
		if (isalpha(tekst[i])){
			printf("%c", odszyfrowany_tekst);
		}

		//Jeśli znak nie jest literą
		else
			printf("%c", tekst[i]);
	}
}
```

Testowanie i poprawa błędów

Tak w szyfrze Cezara pojawił się błąd C4996, został wyeliminowany w taki sam sposób. Wyniki działania były porównywane z wynikami na stronie https://calcoolator.pl/szyfr-vigenerea.html

Przygotowanie do połączenia kodów w całość

Podczas pisania harmonogramu naszym pomysłem i celem stworzenia tego punktu była, na ile to możliwe, podobna implementacja algorytmów. W trakcie prac okazało się jednak, że algorytmy znacząco się od siebie różnią. Aktualnie punkt ten można odnieść do łączenia algorytmu szyfrowania i deszyfrowania. Programy szyfrujące i deszyfrujące niewiele się różnią więc można uznać, że 12 punkt harmonogramu został spełniony.

Podsumowanie:

Spełniono wszystkie założenia pierwszego kamienia milowego. Prace przebiegały bez większych przeszkód.