

**Akademia Techniczno-Humanistyczna**

**w Bielsku-Białej**

Wydział Budowy Maszyn i Informatyki

**Sprawozdanie z przedmiotu:**

**Bezpieczeństwo technologii informatycznych**

**(ćwiczenia laboratoryjne)**

**Ćwiczenie numer:**

**2**

**Temat ćwiczenia: Szyfr Vigenere’a**

**Wykonał: Piotr Olearczyk (nr alb. 49691)**

1. **Wykonanie programu**

**Program został napisany w języku C#**

* 1. **Metoda szyfrowania**

Na początku utworzyłem klasę statyczną **VignereCipher**, która miała za zadanie dostęp do szyfrowania oraz deszyfrowania informacji szyfrem Vigenera. Zawiera ona dwie metody – szyfrującą **Encrypt** oraz deszyfrującą **Decrypt.** Obie z nic przyjmują 2 parametry typu string: **textToEncrypt/textToDecrypt** oraz **password,** które są wymagane do zastosowania szyfrowania. Z racji podobnej struktury szyfrowania jak i odszyfrowywania (zmiana wyłącznie znaku przy zmiennej lokalnej **k,** po wstępnym napisaniu programu zdecydowałem się na refaktoryzację, która pozwoliła na użycie szyfrowania oraz deszyfrowania w jednej metodzie za pomocą podanego parametru **encrypt**. Metoda ta jest metodą prywatną i dostęp do niej mają uprzednio wymienione metody **Encrypt** oraz **Decrypt.**

public static class VignereCipher

{

public static string Encrypt(string textToEncrypt, string password)

{

return VignereCipher.Cipher(textToEncrypt, password, true);

}

public static string Decrypt(string textToDecrypt, string password)

{

return VignereCipher.Cipher(textToDecrypt, password, false);

}

private static string Cipher(string input, string password, bool encrypt)

{

if (password.Any(t => !char.IsLetter(t)))

{

throw new ArgumentException("Jeden lub więcej znaków nie jest literą lub spacją.");

}

var output = string.Empty;

int nonAlphaCharCount = default;

for (var i = 0; i < input.Length; ++i)

{

if (!char.IsLetter(input[i]))

{

output += input[i];

++nonAlphaCharCount;

}

else

{

var cIsUpper = char.IsUpper(input[i]);

var offset = cIsUpper ? 'A' : 'a';

var keyIndex = (i - nonAlphaCharCount) % password.Length;

var k = (cIsUpper ? char.ToUpper(password[keyIndex]) : char.ToLower(password[keyIndex])) - offset;

k = encrypt ? k : -k;

var ch = (char)(Modulo(((input[i] + k) - offset), 26) + offset);

output += ch;

}

}

return output;

}

private static int Modulo(int a, int b)

{

return (a % b + b) % b;

}

}

* 1. **Struktura główna programu – wywołanie szyfrowania/deszyfrowania**
     1. Program został zaprojektowany w taki sposób, aby pytać użytkownika o wybór szyfrowania/deszyfrowania
     2. Po wyborze program prosi o podanie tekstu do szyfrowania/deszyfrowania po wpisaniu tekstu, należy wcisnąć przycisk ENTER
     3. Następnie użytkownik musi podać hasło szyfrujące.
     4. Po wciśnięciu przycisku ENTER program zwraca zaszyfrowany lub odszyfrowany tekst.

internal class Program

{

private static void Main(string[] args)

{

Console.WriteLine("Szyfrowanie Vigenere'a, wybierz opcję:");

Console.WriteLine("1. Szyfrowanie");

Console.WriteLine("2. Deszyfrowanie");

var key = Console.ReadKey();

if (key.Key == ConsoleKey.D1)

{

Console.WriteLine("\nWybrano szyfrowanie");

Console.WriteLine("Podaj tekst do zaszyfrowania:");

var textToEncrypt = Console.ReadLine();

Console.WriteLine("Podaj hasło:");

var password = Console.ReadLine();

var encryptedText = VignereCipher.Encrypt(textToEncrypt, password);

Console.WriteLine($"Zaszyfrowany tekst: \"{encryptedText}\"");

}

else if (key.Key == ConsoleKey.D2)

{

Console.WriteLine("\nWybrano deszyfrowanie");

Console.WriteLine("Podaj tekst do deszyfrowania:");

var textToDecrypt = Console.ReadLine();

Console.WriteLine("Podaj hasło:");

var password = Console.ReadLine();

var decryptedText = VignereCipher.Decrypt(textToDecrypt, password);

Console.WriteLine($"Odszyfrowany tekst: \"{decryptedText}\"");

}

else

{

Console.WriteLine("Wybrany klawisz musi być 1 lub 2");

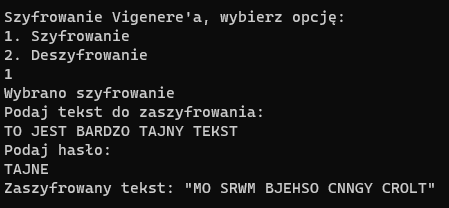
}

}

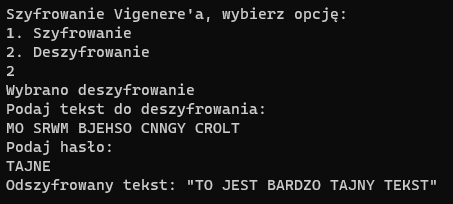
}

1. **Testy**

Testy programu w konsoli PowerShell

****

* 1. Jak można zobaczyć na powyższym zdjęciu ekranu celem szyfrowania był tekst „TO JEST BARDZO TAJNY TEKST”
  2. Hasło jakie użyłem do szyfrowania to „TAJNE”
  3. Otrzymałem zaszyfrowany tekst „MO SRWM BJEHSO CNNGY CROLT”
  4. Następnie uruchomiłem ponownie program wybierając opcję deszyfrowania.



* 1. Wpisałem uprzednio otrzymany zaszyfrowany tekst
  2. Podałem hasło „TAJNE”
  3. Otrzymałem odszyfrowany tekst „TO JEST BARDZO TAJNY TEKST”

1. **Wnioski**
   1. Szyfrowanie szyfrem Vigenere’a jest prosty do zrozumienia i implementacji – dopiero 3 wieki po opracowaniu szyfru powstały algorytmy odszyfrujące.
   2. W porównaniu do szyfrowania sposobem Caesara jest on silniejszy.
   3. Jak widzimy te 2 metody szyfrujące dzieli tylko i wyłącznie znak przy ustawianiu indeksu litery – świadczy to o symetrycznym sposobie szyfrowania.