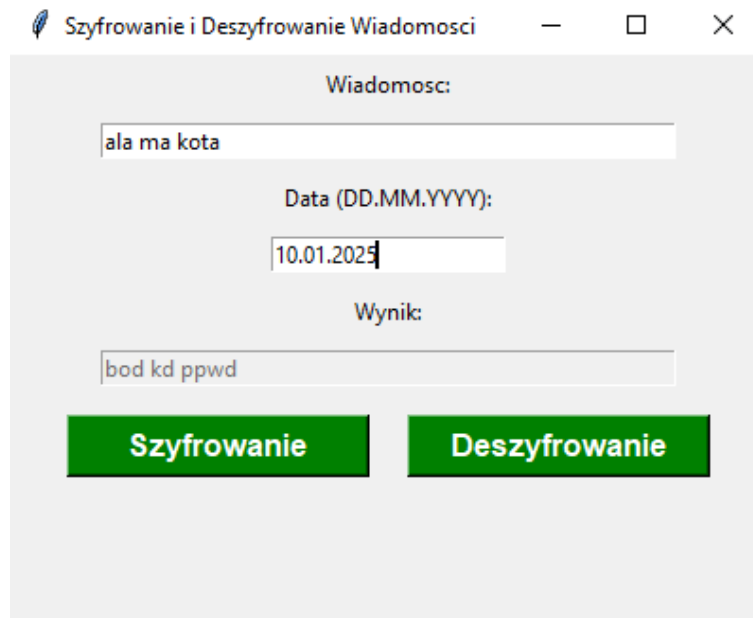


Kacper Sieczko – 273154 – Projekt na Kryptografia 2

Szyfr z kluczem generowanym na podstawie daty.

W celu napisania kodu do realizacji tego projektu posłużyłem się językiem python. Program został wysłany w pliku .exe wraz z tym dokumentem, który zawiera krótki opis jego działania.



Rysunek 1 - Interfejs programu, z przykładowym szyfrowaniem

1. Metoda Generowania klucza

Wpisana przez użytkownika data jest konwertowana na prosty ciąg liczb w powyższym przykładzie: 10.01.2025 -> 10012025

Jednak by uniknąć liter, które pozostały bez zmian cyfra 0 ma specjalną właściwość, która sprawia że każde jej potencjalne wystąpienie w kluczu jest zastępowane przez sumę zer w dacie.

W przykładzie: 10.01.2025 -> 0 -> 3, więc cały klucz będzie równy: 10012025 -> 13312325

2. Metoda Szyfrowania z klucza

Szyfrowanie na podstawie wygenerowanego wcześniej klucza, działa na zasadzie przesunięcia po alfabecie o wartość odczytaną z klucza z delikatnym utrudnieniem.

- Dla wartości nieparzystych – przesunięcie odbywa się zgodnie z alfabetem np. w przykładzie pierwsza literka „a” zgodnie z kluczem jest przesuwana o 1, więc a -> b,
- Dla wartości parzystych – przesunięcie odbywa się przeciwnie z alfabetem np. literce „m” w słowie „ma” w przykładzie odpowiada przesunięcie o 2, więc m->k.

Deszyfrowanie działa na zasadzie metody odwrotnej, więc pozwala na 100 % odczytanie zaszyfrowanej wiadomości w przypadku znajomości daty z jaką wiadomość została zakodowana.