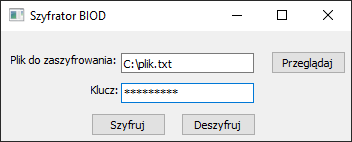
**Algorytm działania oraz prototyp interfejsu aplikacji szyfrującej**

Bezpieczeństwo i ochrona danych

Patryk Konopka  
237980

Prototyp interfejsu:



|  |  |
| --- | --- |
| **Algorytm** | **Przykład** |
| 1. Użytkownik podaję ścieżkę do pliku oraz klucz szyfrujący | * Zawartość pliku: **Patryk Konopka** * Klucz: xyz-2 |
| 1. Dzielimy szyfrowaną wartość na bloki 5 elementowe (ostatni blok może być mniejszy) | |  |  |  |  |  | | --- | --- | --- | --- | --- | | P | a | t | r | y | | k |  | K | o | n | | o | p | k | a | |
| 1. Tworzymy macierz złożoną z sumy wartości kodów ASCII dla każdej pary <znak szyfrowanego tekstu, znak klucza>. Jeżeli suma jest większa niż 255 to od wyniku odejmujemy 255. | |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | |  | P | a | t | r | y | | x | 200 | 217 | 236 | 234 | 241 | | y | 201 | 218 | 237 | 235 | 242 | | z | 202 | 219 | 238 | 236 | 243 | | - | 125 | 142 | 161 | 159 | 166 | | 2 | 130 | 147 | 166 | 164 | 171 |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | |  | k |  | K | o | n | | x | 227 | 152 | 195 | 231 | 230 | | y | 228 | 153 | 196 | 232 | 231 | | z | 229 | 154 | 197 | 233 | 232 | | - | 152 | 77 | 120 | 156 | 155 | | 2 | 157 | 82 | 125 | 161 | 160 |  |  |  |  |  |  | | --- | --- | --- | --- | --- | |  | o | p | k | a | | x | 231 | 232 | 227 | 217 | | y | 232 | 233 | 228 | 218 | | z | 233 | 234 | 229 | 219 | | - | 156 | 157 | 152 | 142 | | 2 | 161 | 162 | 157 | 147 | |
| 1. W następnym kroku pobieramy wartość dla poszczególnych znaków wg. zaznaczenia podanego w poprzednich tabelach. Zamieniamy wynikowy kod ASCII na odpowiadający mu znak. | |  |  |  |  |  | | --- | --- | --- | --- | --- | | P | a | t | r | y | | ‚ | Ž | î | ë | ń |      |  |  |  |  |  | | --- | --- | --- | --- | --- | | k |  | K | o | n | | ť | M | Ĺ | č | ć |      |  |  |  |  | | --- | --- | --- | --- | | o | p | k | a | | ˇ | ť | ĺ | Ú | |
| 1. Następnie w każdym bloku przesuwamy nieparzyste pozycje na następną nieparzystą pozycję (przykładowo:  * **1** 2 **3** 4 **5** -> **5** 2 **1** 4 **3** * **1** 2 **3** 4 -> **3** 2 **1** 4 * **1** 2 -> **1** 2 | |  |  |  |  |  | | --- | --- | --- | --- | --- | | ń | Ž | ‚ | ë | î |      |  |  |  |  |  | | --- | --- | --- | --- | --- | | ć | M | ť | č | Ĺ |      |  |  |  |  | | --- | --- | --- | --- | | ĺ | ť | ˇ | Ú | |
| 1. Łączymy ze sobą wszystkie bloki w odwrotnej kolejności i zapisujemy wartość do pliku. | * Zawartość pliku do zaszyfrowania: **Patryk Konopka** * Zawartość zaszyfrowanego pliku: ÚˇťĺĹčťMćîë‚Žń |