**Szyfr ADFGVX** – prosty szyfr **podstawieniowy.**

Załóżmy, że chcemy zaszyfrować wiadomość „Tajna wiadomosc”.

Na początku wypełniamy szachownice Polibiusza o wymiarach 5x5 alfabetem o zmienionej kolejności liter (która jest znana tylko nadawcy i odbiorcy wiadomości).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **A** | **D** | **F** | **G** | **V** | **X** |
| **A** | A | B | C | D | E | F |
| **D** | G | H | I | J | K | L |
| **F** | M | N | O | P | Q | R |
| **G** | S | T | U | V | W | X |
| **V** | Y | Z | 0 | 1 | 2 | 3 |
| **X** | 4 | 5 | 6 | 7 | 8 | 9 |

Używając tej tabeli zamieniamy tekst jawny na odpowiadający mu szyfrogram:

**T a j n a w i a d o m o s c**

GD AA DG FD AA GV DF AA AG FF FA FF GA AF

Następnie wybieramy tajne słowo, które będzie służyło do dalszego szyfrowania (w naszym przypadku ARCDEF) i wypisujemy pod nim, w wierszach, otrzymany wcześniej szyfrogram. Hasło musimy wybrać takie, żeby ono nie mało dwóch jednakowych liter.

**A R C D E F**

G D A A D G

F D A A G V

D F A A A G

F F F A F F

G A A F X X

Dalej sortujemy alfabetycznie kolumny (po piwerszym wierszu):

**A C D E F R**

G A A D G D

F A A G V D

D A A A G F

F F A F F F

G A F X X A

Żeby dostać zaszyfrowany kod musimy czytać z gory na dół każdą kolumnę. Czyli GFDFG… .

Czytając kolumnami otrzymujemy szyfrogram: **GFDFGAAAFAAAADFDGAFVVGGDFGGA.**

**Dla tekstu “Tylko kryptografia”:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **A** | **D** | **F** | **G** | **V** | **X** |
| **A** | A | B | C | D | E | F |
| **D** | G | H | I | J | K | L |
| **F** | M | N | O | P | Q | R |
| **G** | S | T | U | V | W | X |
| **V** | Y | Z | 0 | 1 | 2 | 3 |
| **X** | 4 | 5 | 6 | 7 | 8 | 9 |

Używając tej tabeli zamieniamy tekst jawny na odpowiadający mu szyfrogram:

**T y l k o k r y p t o g r a f I a**

GD VA DX DV FF DV FX VA FG GD FF DA FX AA AX DF AA

Robimy macierz, wpisując po kolei:

**A R C D E F**

G D V A D X

D V F F D V

F X V A F G

G D F F D A

F X A A A X

D F A A X X

Dalej sortujemy alfabetycznie kolumny (po piwerszym wierszu):

**A C D E F R**

G V A D X D

D F F D V V

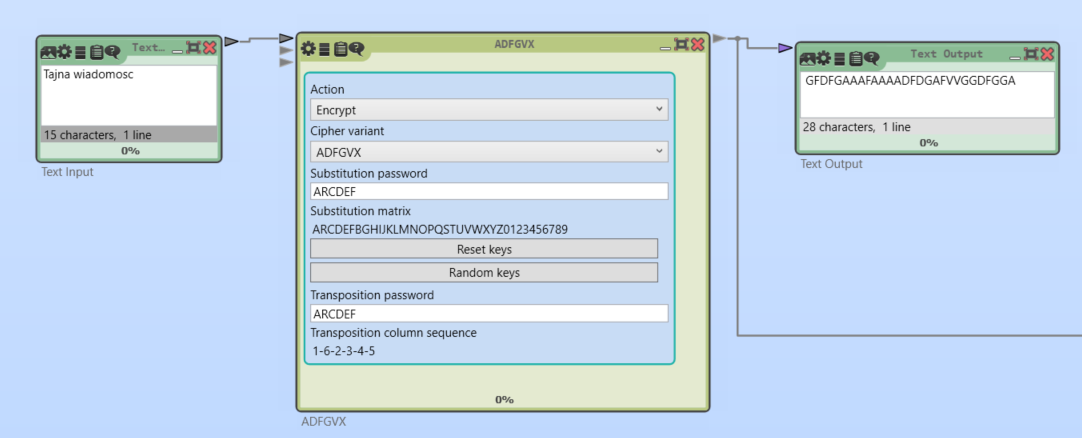
F V A F G X

G F F D A D

F A A A X X

D A A X X F

Otrzymujemy: **GDFGFDVFVFAAAFAFAADDFDAXXVGAXXDVXDXF**

**Przykład działania w Cryptools.**

Mamy tekst “Tajna wiadomosc” i **ADFGVX** blok z hasłem ARCDEF. Po zakończeniu szyfrowania otrzymujemy podobny wynik do tego, jaki otrzymaliśmy w poprzednim obliczeniu.