

Informatyka klasa VI 15.06.2020

Temat: Tajna wiadomość – szyfrowanie.

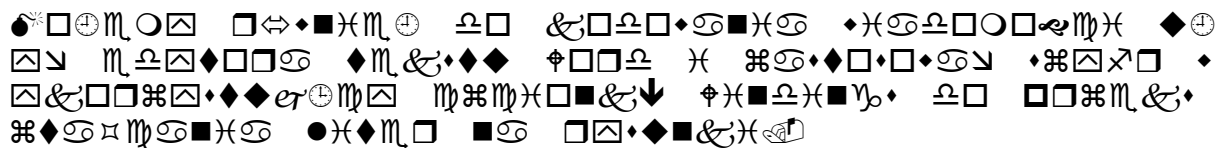
Aby przekazać tajną informację tak, aby nikt obcy nie mógł jej odczytać można ją zakodować. Co to jest kodowanie? To zapisywanie informacji w innym języku. Może to być język angielski, włoski, koreański czy czeski. Może być to również język zrozumiały dla komputera lub wybranej grupy osób, które znają jego zasady.

Jednym z najbardziej znanych sposobów kodowania wiadomości jest szyfr Cezara. Jest to sposób pochodzący od Juliusza Cezara, który szyfrował swoją korespondencję z Cyceronem w I w. przed naszą erą. Szyfrowanie polegało na zamianie danej litery na literę występującą w alfabecie o 3 miejsca dalej, np. zamiast litery B Juliusz Cezar pisał literę E.

Obecnie nie musimy stosować szyfru z przestawieniem o 3 litery. Możemy przesuwać litery również o dowolną liczbę miejsc w prawo, ale również w lewo. Konieczne natomiast jest poinformowanie osoby, do której nadajemy wiadomość, jakie przesunięcie zastosowaliśmy.

Możemy również do kodowania wiadomości użyć edytora tekstu Word i zastosować szyfr wykorzystujący czcionkę Windings do przekształcania liter na rysunki.

Poprzednie zdanie zapisane za pomocą tej czcionki wygląda następująco:



Aby odszyfrować tą informację wystarczy zmienić krój czcionki.

Jedną z najsłynniejszych na świecie maszyn szyfrujących była Enigma. Była to niemiecka maszyna stosowana głównie podczas II wojny światowej do szyfrowania ważnych meldunków wojennych. Enigma była w tamtym czasie uznawana za niemożliwą do złamania z uwagi na ogromną liczbę kombinacji, które trzeba było przeanalizować, aby odkryć klucz, według którego były szyfrowane wiadomości.

Po raz pierwszy udało się ją rozszyfrować polskim kryptologom: Marianowi Rejewskiemu, Jerzemu Różyckiemu oraz Henrykowi Zygalskiemu. Dzięki nim dalsze prace nad dekodowaniem ciągle ulepszanej Enigmy prowadził Alan Turing, uznawany za jednego z ojców współczesnej informatyki.

Karta pracy

Ćwiczenie 1. Wykonaj poniższe zadania przy użyciu szyfru Cezara:

Zaszyfruj wiadomość, która składa się przynajmniej z 5 słów. Zastosuj podane przestawienie.

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

Wiadomość:

Zaszyfrowana wiadomość:

Ćwiczenie 2. Wykonaj poniższe zadania z wykorzystaniem symulatora Enigmy dostępnego na stronie: http://enigmaco.de/enigma/enigma_pl.html.

Zaszyfruj wiadomość, która składa się z przynajmniej 5 słów za pomocą symulatora Enigmy i podaj klucz szyfrowania.

Wiadomość:

Klucz szyfrowania:

Zaszyfrowana wiadomość:

Dzisiaj jest ostatni dzień przesyłania zaległości, we wtorek wpisuję oceny końcoworoczne do dziennika.