

Szyfrowanie wiadomości

I etap edukacyjny / II etap edukacyjny

Już w starożytności ludzie używali szyfrów do przesyłania tajnych wiadomości. Początkowo były one proste, jednak z biegiem czasu wprowadzano coraz bardziej skomplikowane metody szyfrowania. Wraz z rozwojem techniki rozwinęły się takie dziedziny jak [kryptologia](#) i [kryptografia](#). Dzisiaj większość szyfrów jest niemożliwa do odszyfrowania bez użycia komputerów i specjalistycznych maszyn.

Czy potrafisz napisać wiadomość szyfrem? Zabawy, które przedstawię, nie wymagają stosowania skomplikowanych urządzeń. Będą to proste metody szyfrowania wiadomości używane m.in. przez harcerzy.

Cel zabawy:

- ćwiczenie wyobraźni i logicznego myślenia,
- kształcenie spostrzegawczości i kojarzenia,
- analizowanie i interpretowanie,
- współpraca w zespole.

Materiały:

- kartki papieru,
- przybory do pisania.

Czy znasz sposoby na przekazywanie tajnych informacji, tak by inni nie mogli ich odczytać. Wspólnie z kolegami zapisz swoje pomysły np. na tablicy.

Co jest potrzebne, aby zakodować wiadomość? a co, aby wiadomość odkodować?

Zadanie 1 - Szyfr Polibiusza

Grecki historyk Polibiusz wymyślił prosty szyfr nazwany od jego imienia. Kluczem do szyfru jest tabela z umieszczonym w niej alfabetem. (bez polskich liter).

Zaszyfrowana informacja będzie przedstawiona za pomocą ciągu cyfr oznaczających położenie danej litery w tabeli: pierwsza cyfra jest numerem wiersza, druga - kolumny.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Zaszyfrowane słowo **PROGRAMOWANIE** na postać:

35 42 34 22 42 11 32 34 52 11 33 24 15

Nauczyciel może modyfikować tabelę szyfru na potrzeby zajęć. Np. z tabeli można usunąć litery nie występujące w polskim alfabecie (Q i X) a wprowadzić literę np. Ł i Ó.

Na przykładzie szyfru Polibiusza uczniowie sami mogą zbudować swój własny kod szyfrów.

Wspólnie z kolegą ułóżcie tabelę szyfrów. Wykorzystajcie do tego pustą tabelę, którą dostaniecie od prowadzącego zajęcia.

	A	B	C	D	E	F	G	H
1								
2								
3								
4								

W tabeli na szarych polach kolumny zostały określone literami alfabetu od A do H, a wiersze cyframi od 1 do 4. W puste pola wpiszcie wszystkie litery polskiego alfabetu w dowolny sposób. Dla przypomnienia wykaz liter polskiego alfabetu: a, ą, b, c, ć, d, e, ę, f, g, h, i, j, k, l, ł, m, n, ó, o, ó, p, r, s, ś, t, u, w, y, z, ż, ź.

Przykładowy sposób uzupełnienia tabeli.

	A	B	C	D	E	F	G	H
1	g	r	f	p	w	c	ó	j
2	m	a	z	ą	k	u	i	y
3	ż	s	ł	d	t	ć	b	o
4	ś	e	h	ź	ę	n	l	ń

Właśnie zbudowaliście swoją tablicę szyfrów.

Pora na zaszyfowaną wiadomość. Aby zaszyfować słowo np. robot zamiast odpowiednich liter wpisz współrzędne litery określone cyfrą i literą z szarego pola.

Szyfr słowa "robot" według tej tabeli to:

B1 - H3 - G3 - H3 - E3

Zaszyfruj krótką informację dla swojego kolegi lub koleżanki, a następnie przekaz ją do odszyfrowania. Nie zapomnij dołączyć swojej tabeli szyfrów, bo tylko przy jej pomocy można rozszyfrować twoją wiadomość. Dobrej zabawy 

Czy są prostsze metody szyfrowania wiadomości?

Zadanie 2

Zastosowanie słowa, które będzie kluczem do szyfru to prosta metoda szyfrowania. Polega ona na zamianie liter w sylabach zgodnie z przyjętym kluczem, który jest łatwy do zapamiętania. Tabela już nie będzie potrzebna. Wystarczy zapamiętać słowo - klucz.

Jakie mogą być słowa klucze?

Znane i popularne to słowo - klucz: **GA-DE-RY-PO-LU-KI**

Jak zastosować taki szyfr?

Szyfr stosujemy w ten sposób, że jeśli w szyfrowanym tekście występuje litera G to zastępujemy ją literą A, jeśli występuje A to zastępujemy ją literą G. Litery, które nie znajdują się w kluczu pozostają niezmienione.

Zaszyfrujmy wiadomość: **Uczymy się programowania.**

Wiadomość zaszyfrowania zgodnie z kluczem GA-DE-RY-Po-Lu-KI to: **LCZRM R SKĘ OYPAYGMPWGNKG.**

Prawda że proste. Zaletą takiego szyfrowania jest łatwe zapamiętanie słowa klucza przez osoby, które porozumiewają się tym szyfrem. Jeśli w grupie chcecie porozumiewać się swoim szyfrem możecie wymyśleć swój własny klucz.

Inne, słowa klucze, często stosowane to:

RE-GU-LA-MI-NO-WY

NO-WE-BU-TY-LI-SA

BI-TW-AO-CH-MU-RY

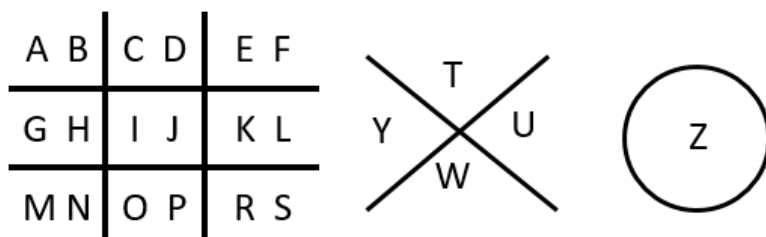
MA-LI-NO-WE-BU-TY

Przećwiczcie szyfrowanie tajnej wiadomości za pomocą słowa - klucza.

Zadanie 3 - Szyfr Czekoladka

Harcerze najczęściej używają bardzo prostego i łatwego do zapamiętania szyfru o nazwie **Czekoladka**. Jak używać tego szyfru?

Musimy zapamiętać następujący układ liter w odpowiednich polach.



Jak szyfrujemy? Wystarczy narysować kontury pola szyfrowanej litery, a następnie wybraną literę oznaczyć kropką. Ważne jest, by kropkę oznaczyć na właściwej pozycji.

Spróbujmy zaszyfrować słowo ROBOT.

Zaszyfrowane słowo wygląda następująco:



Odszyfrowanie wiadomości odbywa się w podobny sposób. Odpowiedni znak przypisujemy do właściwego pola szyfru i odczytujemy literę z miejsca wskazanego przez kropkę. Proste?

Zadanie 4 - Szyfr komórkowy

Szyfr ten powinien przypaść do gustu osobom nierozstającym się ze swoimi telefonami. Szyfrując wiadomości można posłużyć się znakami umieszczonymi na klawiaturze telefonu komórkowego.

Sprawdź, jak wygląda taka klawiatura. W starszych wersjach telefonów komórkowych, w słuchawkach bezprzewodowych czy nawet w smartfonach na przyciskach klawiatury, poza numerami, znajdują się również litery alfabetu. Sprawdź, czy klawiatura w twoim telefonie wygląda podobnie. Jeśli tak, spróbujmy wykorzystać ten układ do szyfrowania wiadomości.



Jak zastosować szyfr z klawiatury telefonu?

Każdy klawisz numeryczny, poza jedynką, obok numerów ma przypisane trzy litery alfabetu.

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

W starych telefonach komórkowych z klawiaturą, aby napisać SMS należy, w zależności od pozycji litery, wielokrotnie naciskać dany klawisz. Np. aby napisać literę "O" - naciskamy trzykrotnie klawisz z cyfrą 6. Do szyfrowania wiadomości szyfrem komórkowym stosuje się te same zasady, jak w pisaniu SMS telefonem z klawiaturą - wpisujemy cyfrę z klawisza, na którym jest litera. Ilość cyfr zależy od pozycji, na której stoi litera.

Zaszyfrujmy słowo **PROGRAMOWANIE**:

7 77 666 4 77 2 6 666 9 2 66 444 33

Zadanie 5 - Szyfr matematyczny

Bardzo prosty do zastosowania jest szyfr matematyczny. Kolejnym literom alfabetu przyporządkowane są kolejne liczby od 1 do 24. Klucz do szyfru matematycznego wygląda następująco:

A	1	I	9	P	17
B	2	J	10	R	18
C	3	K	11	S	19
D	4	L	12	T	20
E	5	ł	13	U	21
F	6	M	14	W	22
G	7	N	15	Y	23
H	8	O	16	Z	24

Zaszyfrowane litery przedstawiamy w postaci liczb. Dodatkowym atutem szyfru jest to, że liczby przedstawiamy w postaci dowolnego działania matematycznego. Uwaga - działanie matematyczne nie musi być równe.  W ten sposób ta sama wiadomość może być różnie przedstawiona. Sposób doboru działań matematycznych jest dowolny.

Zaszyfruj słowo **ZASZYFRUJ**

$$24+1/19*(24+23)=6*18+21-10$$

Ten sam wyraz można zaszyfrować również tak:

$$24+1+19+24+23+6+18+21=10$$

Czy znasz inne szyfry? Sposobów szyfrowania jest bardzo dużo i dlatego do tematu na pewno wrócimy. CDN 

Kryptologia (z [gr.](#) κρυπτός – *kryptos* – „ukryty” i λόγος – *logos* – „rozum”, „słowo”) . To dziedzina wiedzy (m.in. z zakresu matematyki, informatyki teorii informacji i bezpieczeństwa komputerowego) o przekazywaniu informacji zabezpieczonej przed niepowołanym dostępem. Kryptologia ma szerokie zastosowanie w utajnianiu wiadomości wojskowych i dyplomatycznych. Do tych celów stosuje się specjalne urządzenia kryptograficzne. Powołane są specjalne instytucje odpowiedzialne za bezpieczeństwo teleinformatyczne w danym państwie. W Polsce jest to Agencja Bezpieczeństwa Wewnętrznego. Społeczeństwa rozwinięte technicznie wykorzystują kryptologię m.in. do zapewnienia bezpieczeństwa w płatnościach elektronicznych, e-handlu, zabezpieczeniach komputerowych. /Źródło: Wikipedia/

Kryptografia to zamiana jawnej formy wiadomości w ukrytą formę, w celu uniemożliwienia odczytania wiadomości przez osoby niepowołane. W Kryptografii zwykle używane są książki kodów zawierające spis powszechnie używanych

zwrotów i odpowiadające im słowa - kody. /Źródło: Wikipedia/
