

Scenariusz nr 3 lekcji, do przeprowadzenia w klasie I liceum z matematyki

1. TEMAT: **Szyfrowanie i deszyfrowanie informacji – szyfry klasyczne.**
2. Autor: Małgorzata Ludwikowska
3. Klasa: I (liczba uczniów 20 -30).
4. Czas trwania: 45 minut
5. Metody przeprowadzenia lekcji: dyskusja, ćwiczenie laboratoryjne.
6. Formy pracy: swobodna rozmowa, praca w zespołach dwuosobowych
7. Cele:
8. Spodziewane efekty (umiejętności, jakie powinien zdobyć uczeń)
 - znajomość podstawowych zasad szyfrowania wiadomości
 - postawa ostrożności w stosowaniu modelu matematycznego
 - świadomość historycznych i obecnych uwarunkowań szyfrowania
 - postawa współpracy w wykonywaniu zadaniaWymagania szczegółowe:
Uczeń:
 - przedstawia liczby rzeczywiste w różnych postaciach – kategoria taksonomiczna C;
9. Metody sprawdzania osiągniętych celów
 - słuchanie wypowiedzi uczniów
 - przeglądanie notatek i rysunków
 - obserwacja pracy grup
10. Sposoby motywowania uczniów
 - odniesienie tematu do doświadczeń i zainteresowań uczniów
 - „odczarowanie” modelowania matematycznego przez jego konkretyzację
 - powiązanie tematu z problemami otaczającego świata
11. Przygotowanie do lekcji (warunki, jakie powinny być spełnione, aby prawidłowo przeprowadzić lekcję):
 - nie za wielka liczebność klasy
 - dość miejsca na pracę dwuosobowych grup
12. Środki dydaktyczne:
 - kalkulatory
 - wydrukowane materiały - załączniki

Projekt „Żyj twórczo. Zostań M@T.e-MANIAKIEM” jest współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego



KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚĆ



**WYŻSZA SZKOŁA
EUROPEJSKA**
IM. KS. JÓZEFA TISCHNERA

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY



Lp.	Czynności nauczyciela	Czynności uczniów	czas	Umiejętności kształcone w czasie lekcji
1.	Przypomina temat poprzedniej lekcji, kontroluje wykonanie zadania domowego poprzez podanie krótkiego tekstu do rozszyfrowania. Uczniowie, którzy przygotowali klucz deszyfrujący zrobią to bardzo szybko.	Uczniowie deszyfrują samodzielnie podany tekst.	5 minut	Wzmocnienie przekonania o sensowności odrabiania zadań domowych.
2.	Pokazuje i objaśnia zasady szyfrowania metodą Vigenère'a (Załącznik 4.). Uczniowie otrzymują klucz za pomocą którego szyfrują wybrany tekst a następnie wymieniają się zaszyfrowanym tekstem między grupami i próbują go rozszyfrować.	Uczniowie szyfrują i deszyfrują otrzymane teksty.	15 minut	Umiejętność pracy zespołowej, poznanie najprostszych zasad kryptografii. Ćwiczenie w stosowaniu poznanego algorytmu
3.	Przekazuje uczniom wydrukowany załącznik 5. Prosi o samodzielne przestudiowanie tekstu i rozwiązanie zadania w nim zaproponowanego	Uczniowie czytają przygotowany załącznik 5. i samodzielnie rozwiązują zadanie.	20 minut	Umiejętność samodzielnego zrozumienia przedstawionego algorytmu.
4.	Ocenia zaangażowanie i wyniki pracy poszczególnych uczniów.		5 minut	
5.				

Załącznik 4.

„Przyjrzymy się jeszcze jednemu systemowi kryptograficznemu. Od poprzedniego systemu będzie się on różnił tym, że ta sama litera może być zaszyfrowana w różny sposób, w zależności od tego, w którym miejscu tekstu występuje. Weźmy ciąg kilku liczb mniejszych od 26, na przykład (3, 7, 1, 11, 2). Sposób szyfrowania polega teraz na tym, że zamiast pierwszej litery tekstu piszemy literę znajdującą się w alfabecie 3 miejsca dalej, zamiast drugiej litery tekstu piszemy literę znajdującą się w alfabecie 7 miejsc dalej, zamiast trzeciej litery znajdującą się 1 miejsce dalej, potem literę znajdującą się 11 miejsc dalej, potem 2 miejsca i zaczynamy od początku: 3 miejsca, 7 miejsc, 1 miejsce itd. A więc zdanie ALEA IACTA EST po zaszyfrowaniu będzie brzmiało DSFL KDJUL GVA. Zauważmy, że litery A w pierwszym słowie zostały zaszyfrowane inaczej. Natomiast pierwsza litera A i druga w drugim słowie zostały zaszyfrowane tak samo - dlatego, że druga z nich występuje w tekście pięć miejsc dalej i klucz ma pięć liczb. Ten system kryptograficzny, nazywany szyfrem Vigenère'a, jest więc jakby kombinacją wielu systemów Cezara, a kluczem szyfrowania jest odpowiedni ciąg liczb. Klucze, oczywiście, mogą być dowolnej długości. Często zapamiętujemy klucz w postaci słowa. Na przykład słowo CEZAR odpowiada ciągowi (3, 5, 26, 1, 18): litera C jest trzecią literą alfabetu, litera E piątą itd. Liczba kluczy w tym systemie jest naprawdę olbrzymia. Kluczy długości 26, a więc takiej długości jak permutacje w poprzednim systemie, jest 26^{26} ; ta liczba jest znacznie większa niż $26!$ ”

Załącznik 5.

Niżej jest zaszyfrowana wiadomość i klucz do jej odczytania.

A oto klucz: 142857142857142857...

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

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

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

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

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

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

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

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

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

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

Wiadomość: **TALES Z MILETU** po zaszyfrowaniu ma postać: **ŚYJŻŃ Ś ŁĘJŻÓO**

Sposób szyfrowania:

Piszemy wiadomość, którą chcemy zaszyfrować, a pod nią cyfry z klucza:

TALES Z MILETU

14285 7 142857

1. W wierszu poziomym 1 znajdujemy literę T, a następnie stojącą nad nią w wierszu 0 literę **Ś**.
2. W wierszu poziomym 4 znajdujemy literę A, a następnie stojącą nad nią w wierszu 0 literę **Y**.
3. W wierszu poziomym 2 znajdujemy literę L, a następnie stojącą nad nią w wierszu 0 literę **J**.
4. W wierszu poziomym 8 znajdujemy literę E, a następnie stojącą nad nią w wierszu 0 literę **Ż** itd.

Przy odszyfrowywaniu postępujemy odwrotnie, tzn. piszemy wiadomość, którą chcemy odszyfrować, a pod nią cyfry z klucza:

ŚYJŻŃ Ś ŁĘJŻÓO

14285 7 142857

1. W wierszu poziomym 0 znajdujemy literę **Ś**, a następnie stojącą pod nią w wierszu 1 literę **T**.
2. W wierszu poziomym 0 znajdujemy literę **Y**, a następnie stojącą pod nią w wierszu 4 literę **A**.
3. W wierszu poziomym 0 znajdujemy literę **J**, a następnie stojącą pod nią w wierszu 2 literę **L**.
4. W wierszu poziomym 0 znajdujemy literę **Ż**, a następnie stojącą pod nią w wierszu 8 literę **E** itd.

Odszyfruj wiadomość: **ŁYSŻIVŚIUÓJ PBJUFM**