m@t.e-maniak

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 zadania

   Wymagania 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

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.	Inicjuje rozmowę o szyfrowaniu, jego historycznych (szyfr Cezara) i współczesnych uwarunkowaniach.	Dzielą się posiadanymi informacjami o: szyfrowaniu, zastosowaniu szyfrowania, przykładach konieczności stosowania szyfrów	10 minut	Świadomość konieczności posiadania metody ochrony informacji.
2.	Pokazuje i objaśnia zasady najprostszego szyfrowania Szyfr Cezara i jego wersje (pomoc dla nauczyciela Załącznik 1.) Proponuje uczniom – podzielonym na dwuosobowe grupy zaszyfrowanie tekstu szyfrem Cezara a następnie wymianę zaszyfrowanego tekstu między grupami i jego rozszyfrowanie.	Uczniowie szyfrują i deszyfrują swoje teksty.	15 minut	Umiejętność pracy zespołowej, poznanie najprostszych zasad kryptografii.
3.	Inicjuje rozmowę o sposobie odnalezienia klucza szyfrowania (Załącznik 2.). Jedną z metod ułatwiających znalezienie klucza jest badanie częstości występowania liter w tekście zapisanym w danym języku.	Uczniowie proponuję metody np. prób i błędów (warto skierować rozmowę na problem możliwości wyboru klucza)	5 minut	Poszukiwanie rozwiązania nietypowego problemu
4.	Przedstawia bardziej zaawansowaną metodę szyfrowania – szyfr Cardano (załącznik 3.). Podaje tylko klucz szyfrowania.	Uczniowie otrzymują kartki z kluczem szyfrowania Cardano i szyfrują swój tekst a następnie wymieniają zaszyfrowany tekst między grupami i następuje jego rozszyfrowanie.	15 minut	Współpraca w wykonywaniu zadania. Ćwiczenie w stosowaniu poznanego algorytmu
5.	Proponuje usprawnienie dekryptażu przez zapisanie jako pracy domowej gotowego klucza deszyfrującego (Załacznik 3.).			

Załącznik 1.

„Jeden z najstarszych sposobów szyfrowania pochodzi od Juliusza Cezara, który szyfrował swoją korespondencję z Cyceronem. Sposób ten polegał na tym, że zamiast każdej litery pisało się literę występującą w alfabecie trzy miejsca dalej. Tak więc, jeśli użyjemy dzisiejszego alfabetu łacińskiego

ABCDEFGHIJKLMNOPQRSTUVWXYZABCD…

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

to zamiast A będziemy pisać D, zamiast K piszemy N, zamiast Y piszemy B. Widzimy więc, że alfabet traktujemy "cyklicznie", tzn. po ostatniej literze Z następuje znów pierwsza A itd.

Słynne słowa Cezara ALEA IACTA EST (kości zostały rzucone) zaszyfrowalibyśmy więc jako DOHD LDFWD HVW. Na tym przykładzie objaśnimy dwa ważne pojęcia kryptografii (czyli nauki o szyfrowaniu): systemu kryptograficznego i klucza. System kryptograficzny to, mówiąc nieprecyzyjnie, ogólny sposób szyfrowania. W naszym przykładzie polega on na tym, że zamiast danej litery alfabetu piszemy literę występującą w tym samym alfabecie ileś miejsc dalej. Cezar zdecydował się akurat na trzy miejsca dalej, ale równie dobrze mógłby pisać literę występującą siedem miejsc dalej. Sposób szyfrowania (tzn. system kryptograficzny) byłby w zasadzie ten sam, różniłby się tylko wyborem *klucza*, czyli liczby wskazującej, o ile miejsc dalej w alfabecie stoi litera, którą mam napisać. Można powiedzieć, że system kryptograficzny polega tu na pisaniu litery stojącej *k* miejsc dalej, a liczba *k* jest kluczem. Podsumujmy: szyfrowanie polega na wyborze ogólnego sposobu, algorytmu szyfrowania, zwanego systemem kryptograficznym i pewnych parametrów, od których ten algorytm jest zależny, nazywanych kluczem szyfrowania.

Każdą zaszyfrowaną wiadomość trzeba kiedyś rozszyfrować. W szyfrze Cezara znajdujemy literę stojącą w alfabecie trzy miejsca bliżej, czyli w istocie stosujemy ten sam algorytm szyfrowania z innym kluczem. Do szyfrowania używamy klucza +3, a do rozszyfrowywania klucza -3. Gdy znamy klucz szyfrowania, to znamy też klucz rozszyfrowywania. Tak naprawdę jest to ten sam klucz, jeśli pominiemy jego znak."

Załącznik 2.

„Jeśli ktoś zadaje sobie tyle trudu, by szyfrować wiadomości wysyłane do kogoś innego, to pewnie dlatego, że nie chce, by inne, niepowołane do tego osoby, mogły te wiadomości odczytać. I pewnie znajdą się te inne osoby, które chcą koniecznie przeczytać to, co zostało zaszyfrowane. Jeśli nie znają one sposobu szyfrowania, to muszą ten szyfr "złamać". W jaki sposób można tego dokonać?

Po pierwsze, będziemy zakładać, że osoba łamiąca szyfr zna system kryptograficzny i nie zna tylko klucza. Dlaczego przyjmujemy takie założenie? Wśród wielu powodów można wymienić ten, że system kryptograficzny na ogół trudniej zmienić niż klucz. Używa się więc tego samego systemu na tyle długo, że osoby niepowołane mogą wykraść informacje o samym systemie. Bezpieczeństwo szyfrowania będzie zapewnione dzięki częstym zmianom kluczy. Innym powodem jest ten, że często tego samego systemu używa bardzo wiele osób i sam system jest dobrze wszystkim znany.

A jak w takim razie zdobyć klucz, jeśli dysponuje się tylko tekstem zaszyfrowanym? Czasami nie jest to trudne. Np. szyfr Cezara można złamać bardzo łatwo. Przecież ma on tylko 26 kluczy. Wystarczy spróbować wszystkich, by przekonać się, że tylko jedna wiadomość brzmi sensownie, a pozostałe stanowią niezrozumiały bełkot. Klucz użyty w tym rozszyfrowywaniu jest właściwym kluczem. Widzimy więc, że system kryptograficzny dopuszczający niewiele kluczy nie jest bezpieczny i łatwo taki szyfr złamać."

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

Załącznik 3.

„Girolamo Cardano, wybitny uczony XVI wieku, pisał, że niemożliwy do złamania jest nieco inny szyfr, polegający na tym, że zamiast każdej litery alfabetu piszemy ustaloną inną literę. Wyjaśni to najlepiej przykład. Przyjmijmy, że zamiast litery A piszemy Q, zamiast B piszemy W itd. według następującego schematu:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

QWERTYUIOPASDFGHJKLZXCVBNM

(zamiast litery stojącej w górnym wierszu piszemy literę znajdująca się pod nią w dolnym wierszu). Zdanie ALEA IACTA EST zostanie teraz zaszyfrowane jako QSTQ OQEZQ TLZ. System kryptograficzny polega tu na zastępowaniu każdej litery inną, a kluczem jest stojąca w dolnym wierszu permutacja liter alfabetu. Kluczem rozszyfrowywania jest oczywiście permutacja odwrotna, którą nietrudno wypisać:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

KXVMCNOPHQRSZYIJADLEGWBUFT

Liczba kluczy jest ogromna. Jest ich 26! - czyli 403291461126605635584000000. Oczywiście, przeszukanie wszystkich możliwych kluczy nie jest wykonalne, trwałoby zbyt długo. Jak więc można złamać ten szyfr? Sięgamy do metod statystycznych. Okazuje się, że w tekstach napisanych w danym języku poszczególne litery nie występują z tą samą częstotliwością. I tak, na przykład, w języku angielskim najczęściej występuje litera E (około 13% wszystkich liter odpowiednio długiego tekstu). Drugą z kolei jest litera T (około 9%), następnymi są A, O, N, I, R. W języku polskim nie ma litery bardzo wyróżniającej się od innych i dlatego łamanie zaszyfrowanego tekstu napisanego po polsku będzie nieco trudniejsze. Najczęściej występują litery A oraz I (po około 9%), a po nich E i O (po około 7,5%).
Taki sposób łamania szyfru opisał w opowiadaniu "Tańczące sylwetki" Artur Conan Doyle.”
Przypuśćmy teraz, że mamy dany tekst zaszyfrowany za pomocą opisanego wyżej systemu. Musimy, oczywiście, wiedzieć, w jakim języku napisano zaszyfrowaną wiadomość i znać rozkład częstości występowania liter alfabetu w tekstach napisanych w tym języku. Jeśli nasz tekst jest wystarczająco długi (wystarczy już kilkaset liter), to rozkład częstości jego liter powinien być podobny. Najczęściej występujące litery w tekście zaszyfrowanym powinny odpowiadać najczęstszym literom danego języka (choć niekoniecznie w tej samej kolejności). Próbujemy przypisać te litery sobie; po kilku próbach okaże się, że dość łatwo możemy domyślić się znaczenia następnych liter, potem jeszcze następnych, aż wreszcie domyślamy się znaczenia wszystkich liter klucza i odczytujemy cały tekst. Duża liczba kluczy nie jest więc warunkiem wystarczającym bezpieczeństwa szyfru.”

Przygotowując załączniki korzystano z artykułu Wojciecha Guzickiego

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