Szymon Dąbrowski

Kurs kryptologii - scenariusz zajęć dodatkowych

**Przedział wiekowy uczestników:** 14-18 lat

**Zakładany czas:** 45 minut

**Temat:** Śladami pogromców Enigmy

1. Główne zagadnienia zajęć:
    - Historia złamania szyfru Enigma, jej wpływ na dzieje II wojny światowej i czasy współczesne,
    - Historia utajniania informacji,
    - Podstawowe zagadnienia kryptologiczne.
2. Cele zajęć

    Cel ogólny
    - Zwiększenie wśród uczestników poziomu wiedzy na temat historii złamania kodu Enigmy ze szczególną rolą kursu szyfrów oraz popularyzacja kryptologii.

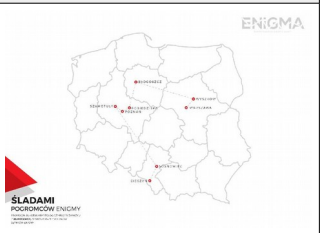
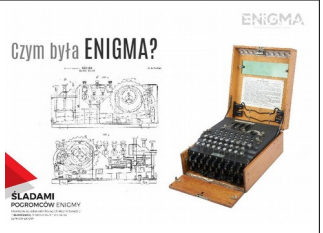
    Cele szczegółowe:
    - zapoznanie uczestników z różnymi metodami utajniania informacji,
    - praktyczne zapoznanie uczestników z wybranymi metodami szyfrowania i łamania szyfrów,
    - zwiększenie świadomości wśród uczestników gry na temat roli kryptologii na przestrzeni wieków,
    - ukazanie przełomowej roli polskich kryptologów dla kryptoanalizy
    - podkreślenie znaczenia dorobku poznańskich matematyków dla trwania II wojny światowej;
    - wprowadzenie do współczesnej kryptologii uwzględniające czas od złamania Enigmy do chwili obecnej – ukazanie roli kryptologii w świecie współczesnym.

3. Metody:
    - rozmowa nauczająca;
    - praca w grupach;
    - konkurs;
    - linia czasu;
    - prezentacja.

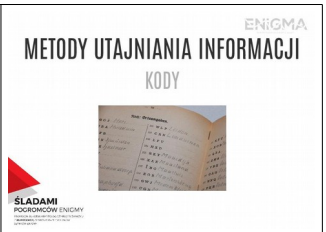
4. Środki dydaktyczne:

- tablica interaktywna lub rzutnik multimedialny, zestaw komputerowy,
- prezentacja,
- karty do zadań szyfr Cezara (szyfrowanie, odszyfrowywanie i łamanie szyfru) oraz „Po co kryptologowi nożyczki”, nożyczki, materiały piśmienne

5. Przebieg lekcji:

| LP | Przebieg lekcji | Slajd prezentacji |
|---|---|---|
| 1. | Śladami pogromców Enigmy |  |
| 2. | Co oznacza słowo Enigma? - rozmowa nauczająca:<br>• uczestnicy zajęć dzielą się swoimi skojarzeniami dotyczącymi słowa Enigma. Pojawiają się hasła: maszyna szyfrująca, tajemnica po grecku, słowo enigmatyczny, film o Enigmie, zespół muzyczny, inne,<br>• uściślenie tematu – kilka słów o maszynie szyfrującej, ustalenie wspólnej wiedzy o roli Polaków w złamaniu Enigmy,<br>• zwrócenie uwagi na fakt, że maszyny szyfrujące stały się potrzebne gdy wojsko zaczęło na wielką skalę używać radia, a wojna straciła pozycyjny charakter. |  |
| 3. | Konstrukcja maszyny – rozmowa nauczająca / film:<br>• porównanie wyglądu Enigmy do komputera (np. laptopa) – z jego charakterystycznymi elementami (klawiatura, ekran i panel lamp w Enigmie oraz procesor i rotory w Enigmie).<br>• zapoznanie z krótkim filmem o konstrukcji maszyny (https://youtu.be/uXnyf0ses7c). |  |
| 4. | Obsługa maszyny – wykład / film:<br>• omówienie zdjęcia z kampanii wrześniowej na którym generał Guderian dyktuje szyfrantowi depeszę a ten przekazuje szyfrogram radiotelegrafiście,<br>• podkreślenie, że odczytywanie depeszy było operacją odwrotną,<br>• zapoznanie się z krótkim filmem przedstawiającym obsługę maszyny (https://youtu.be/wHKqedSt6XE),<br>• omówienie ilustracji z przykładową depeszą Enigmy, podkreślenie tego, że o mocy szyfru decydowały ustawienia rotorów określone w nagłówku depeszy i w książce szyfru na dany dzień. |  |
| 5. | Oni dokonali niemożliwego – wykład:<br>• dotychczasowe metody łamania szyfrów zawiodły i europejskie służby wywiadowcze zrezygnowały z prób łamania Enigmy,<br>• wówczas Maksymilian Ciężki ze współpracownikami |  |

| | | |
|---|---|---|
| | opracował dalekosiężny plan, który w efekcie spowodował przewrót kopernikański w kryptologii,<br>• Ciężki zaproponował przeprowadzenie kursu szyfrów dla studentów matematyki w Poznaniu.<br>• Burza mózgów – dlaczego w Poznaniu? Bo jeszcze 10 lat wcześniej ci sami studenci uczyli się tu w niemieckiej szkole i mieli wielu niemieckich kolegów – znali więc dobrze język niemiecki. | |
| 6. | Skoro Enigmę złamano dzięki kursowi szyfrów, zapraszamy do... kursu szyfrów:<br>• szyfr i kod to nie to samo, a to nie wszystkie metody utajniania. Jakie więc znamy metody ukrywania informacji?<br>• co to jest STEGANOGRAFIA. Od greckich słów stegano (ukryć) i grafein (pisać, rysować) – ukrywać zapis. Nie szyfrujemy, ale ukrywamy fakt przesyłania informacji.<br>• Herodot opisał historię Histiajosa, Greka, który przekazał wiadomość na wytatuowanej głowie niewolnika (któremu uprzednio odrosły włosy).<br>• Rozmowa: kto słyszał o atramencie sympatycznym? Jak on działa? To także Steganografia. |  |
| 7 | Steganografia – ćwiczenia.<br>Do steganografii nie potrzebujemy koniecznie ani tatuaży anie specjalnych atramentów. Wystarczy trochę wyobraźni:<br>1. Na pierwszym zadaniu widoczny jest list, w którego tekście ukryte są litery tajnego przekazu. Spróbujmy przeczytać tylko pierwsze litery. Wynik TAJNOPIS – to polskie określenie steganografii.<br>2. Zadanie nr 2. Ułożyć listę zakupów tak by skrywała ona słowo alarm (rozwiązania są 2 dla układu 3 liter wszystkich wyrazów).<br>3. Zadanie nr 3. to wcale nie depesza Enigmy. Kto znajdzie tu przekaz steganograficzny (chodzi o ostatnie litery każdego z bloków).<br>4. Zadanie 4 to żart bo nikt nie odgadnie co jest ukryte na fotografii, ale jest to dobry pretekst by wspomnieć, że dziś metodami steganografii można użyć do ukrycia obrazu w obrazie lub innym pliku. |  |
| 8. | Szyfry – omówienie tematu:<br>• szyfry inaczej niż steganografia nie ukrywają przekazu, a sprawiają, że ten staje się nieczytelny. Możemy np. zamieniać jedne litery na inne (szyfry podstawieniowe) lub przestawiać litery względem siebie (szyfry przestawieniowe inaczej transpozycyjne),<br>• na rysunku skytale – jeden z najstarszych szyfrów, używany w starożytnej Sparcie – litery były przestawiane przez rozwinięcie paska skóry na którym były zapisane |  |
| 9. | Szyfry – ćwiczenie:<br>• jeden ze starożytnych szyfrów – szyfr biblijny był bardzo prosty (ale na swoje czasy skuteczny) – pierwsza litera alfabetu zamieniała się na ostatnią, druga na przedostatnią itd. (stąd nazwa AtBasz),<br>• w księdze Jeremiasza Babilon (Babel) nazwany jest Szeszak,<br>• jak zaszyfrujemy Babel szyfrem AtBasz opartym o alfabet angielski? (rozwiązanie na kolejnym slajdzie). |  |

| | | |
|---|---|---|
| 10. | Kody omówienie tematu:<br>• pytanie do uczniów: czym różni się kod od szyfru?<br>• odpowiedź: kody inaczej niż szyfry nie operują na literach, ale na wyrażeniach, które są zebrane w księdze kodów. |  |
| 11. | Szyfry – ćwiczenia:<br>1. Odkoduj. Odpowiedź: Pluton wycofać się. Dowództwo<br>2. Zakoduj. Zadanie i odpowiedź na slajdach.<br>3. | |
| 12 | Metody utajniania informacji – podsumowanie:<br>• pytanie uczniów czym różnią się poszczególne metody utajniania. |  |
| 13. | Rodzaje szyfrów – wprowadzenie:<br>• wspomnieliśmy o tym, że są szyfry podstawieniowe i przestawieniowe,<br>• jednym z najbardziej znanych szyfrów podstawieniowych jest szyfr Cezara,<br>• było stosowany przez swojego wynalazcę jako szyfr dla celów wojskowych – Cezar stosował zawsze przesunięcie o 3 litery. |  |
| 14. | Szyfr cezara – ćwiczenia<br>• szyfrowanie – zadanie i odpowiedź na slajdzie – wspólne wyjaśnienie słów sentencji VENI VIDI VICI,<br>• odszyfrowanie – zadanie i odpowiedź na slajdzie – wspólne wyjaśnienie słów sentencji ALEA IACTA EST,<br>• łamanie szyfrów – Cezar przestawiał zawsze o 3 pola, ale gdyby nie było pewności co do wielkości przesunięcie złamanie szyfru i tak byłoby czynnością trywialną – zadanie i odpowiedź na slajdzie,<br>• podsumowanie – było tu trochę łaciny - czy w pracy szyfranta potrzebna jest znajomość języka? NIE, a w pracy szyfranta? JAK NAJBARDZIEJ. I dlatego kurs szyfrów zorganizowano w Poznaniu. |  |
| 15. | Szyfry transpozycyjne – omówienie:<br>• szyfry transpozycyjne to szyfry, w których przestawiamy litery względem siebie, przykładem jest przestawienie kolumunowe widoczne na obrazku. |  |
| 16. | Po co kryptologowi nożyczki? Ćwiczenie<br>• aby złamać szyfr transpozycyjny należy rozpisać wszystkie liczby depeszy w tabeli, a następnie pociąć kolumny i manipulować w układzie kolumn tak by uzyskać czytelny tekst.<br>• spróbuj złamać depeszę (wynik: Jesteś łamaczem Szyfrów ) | |

| | | |
|---|---|---|
| 19 | Co było dalej? - prezentacja<br>• sukcesy polskich matematyków do wojny (złamanie Enigmy, maszyny wspomagające dekryptaż),<br>• „Sztafeta Enigmy” - przekazanie sekretu aliantom i wpływ tego faktu na losy wojny,<br>• od Bomby do Komputera - wprowadzenie do współczesnej kryptologii uwzględniające czas od złamania Enigmy do chwili obecnej – ukazanie roli kryptologii w informatyce. |  |

6. Ewaluacja

1. Zadanie domowe – każdy uczeń otrzymuje depeszę do złamania
   - DEPESZA (szyfr transpozycyjny)
     RAKCEWOENIYNWEYCAHLWKDYEPIECTYSIAOEYSNOBDULIYMESIOMCOLIXPZONUPRZMLTE
     TIONFAPCEJOHGOEXKIUAIOWINZRWAIGARWTEMEDKONSXOLZEDLSWAYLYZX
   - ODPOWIEDŹ (cytat ze wspomnień Mariana Rejewskiego): Kryptologia, czyli nauka o szyfrach, nie ma wielu adeptów. W Polsce, w okresie międzywojennym, samodzielnych kryptologów nie było nawet dziesięciu.
2. Po przeprowadzonych zajęciach uczeń powinien:

- opisać podstawowe metody utajniania informacji,
- opisać różnice pomiędzy szyframi transpozycyjnym i podstawieniowym oraz monoalfabetycznym i polialfabetycznym,
- opowiedzieć skrótowo dzieje kryptologii podając ciekawe przykłady z historii,
- zastosować w praktyce metody szyfrowania i dekryptażu prezentowane na zajęciach,
- powiedzieć dlaczego złamanie Enigmy było trudne i jakie były następstwa tego Enigmę udało się złamać.