

Szyfry i kody – polski radiowywiad



Scenariusz zajęć połączonych z pokazem filmu VR „Wiktoria 1920”

Grupa: szkoła podstawowa



Ministerstwo
Kultury
i Dziedzictwa
Narodowego

niepodległa

Opracowanie:

KONCEPT
Kultura



Materiał edukacyjny uzupełnia pokazy filmu VR „Wiktoria 1920”.

CEL ZAJĘĆ

- Przekazanie wiedzy o roli radiowywiadu w wojnie polsko-bolszewickiej 1920 roku.
- Pokazanie historii szyfrów na przykładach z epoki.
- Powtórzenie podstawowych informacji o początkach niepodległej Polski.
- Aktywna zabawa odnosząca się do materiału historycznego.

WSTĘP

Prowadzący zajęcia informuje o atrakcji zajęć, którą jest film VR Cinematic 360 „Wiktorja 1920”.

- Rozdaje cardboardy lub headsety VR i wyjaśnia zasadę ich działania (załącznik: Instrukcja korzystania z cardboardów).
- Uczestnicy oglądają film – 28 minut.

Prowadzący przedstawia podstawowe zasady dotyczące szyfrów, działania wywiadu ze szczególnym uwzględnieniem radiowywiadu podczas I wojny światowej. Animuje krótką rozmowę na temat filmu i pokazanych tam działań wywiadowczych. Upewnia się, że wszyscy uczestnicy zrozumieli na czym polegało zagłuszanie i czemu służyło, a także jak działały stacje radiotelegraficzne. Prowadzący może posłużyć się zdjęciami z I wojny światowej i wojny polsko-bolszewickiej 1920 roku, żeby pokazać wyzwania, trudności, ale też rozwiązania techniczne związane z użyciem radiotelegrafii na wojnie. Na czym polegała największa trudność z przekazami radiowymi i dlaczego tak ważne było szyfrowanie wiadomości? Czy odszyfrowane informacje ze sztabu wojska przeciwnika mogły wpłynąć na losy wojny i poszczególnych bitew? Dlaczego pozbawianie wroga informacji i kontaktu radiotelegraficznego było tak znaczące dla losów wojny?

Prowadzący może pokrótce omówić różne zadania, które stały przed wywiadem i radiotelegrafią podczas konfliktu:

a) ochrona własnej korespondencji:

zachowanie dyscypliny w ruchu,
posługiwanie się jak najczęściej zmienianymi kodami i szyframi,
częsta zmiana elementów ruchu – sygnałów wywoławczych, kryptonimów i zakresów fal,
używanie radia wyłącznie w sytuacji niemożności zastosowania innych środków łączności,
redukcja mocy nadawania w celu ograniczenia zasięgu w dopuszczalnych ramach,
ograniczenie pracy radiostacji – skracanie dokumentów i dzielenie ich na części przesyłane np. na różnych falach i w innym czasie,
szybkość emisji, unikanie stałego formularza dokumentów,
prace pozorne, sztuczne wzbudzanie ruchu, tworzenie sieci i radiostacji pozornych.

WIKTORIA 1920

b) dywersja radiowa:

- nadawanie fałszywych lub pozornych radiodepesz,
- zagłuszanie,
- agitacja i propaganda,

c) radiowywiad:

- lokalizacja stacji radiofonicznych,
- ustalenie struktury sieci stacji radiotelegraficznych,
- przejmowanie korespondencji,
- maskowanie, dezinformacja, zagłuszanie,
- ustalanie kluczy szyfrowych i kodów,
- odczytywanie korespondencji szyfrowej,
- ewidencja, dystrybucja do celów operacyjnych,
- przesyłanie informacji między ogniwami.

ROZGRZEWKA

Prowadzący dzieli na grupy uczestników i na początek przedstawia im jeden z najstarszych polskich szyfrów.

SZYFR LITEROWY STOSOWANY W POLSCE W XVII WIEKU

A aaaaa	B abaaa	C aabaa	D aaaba	E aaaab	F abbbb	G aabbb	H ababb
I abbab	K abbba	L bbbbb	M babbb	N bbabb	O bbbab	P bbbba	R bbaaa
S babaa	T baaba	V baaab	W aaabb	X abaab	Y aabab	Z abbab	

Następnie każda z grup dostaje jeden pasek do odszyfrowania. Paski różnią się od siebie sposobem rozdzielenia liter. Prowadzący, jeśli grupa nie będzie mogła sobie z tym poradzić, może podpowiedzieć, że zastosowano tu dzielenie liter (na grupy) w celu jeszcze większego utajnienia wiadomości, ale nie ma ono znaczenia dla odczytania całości (dwucyfrowy, trzycyfrowy, czterocyfrowy).

- 1. Ab bb ab bb ab aa ab ba aa aa bb bb ba aa ab aa ab bb ab aa ab bb aa bb ab
- 2. Abb bab bba baa abb aaa aab bbb baa aab aaa bbb aba aab bba abb ab
- 3. Abbb abbb abaa abba aaaa bbbb baaa abaa abbb abaa abbb aabb ab

Prowadzący może zadać dodatkowe zadanie każdej grupie. Poniżej zaszyfrowane jest to samo słowo co na paskach, tylko zapisano je w jeszcze inny sposób. Uczestnicy mają za zadanie zgadnąć, jak powstał taki układ liter, wiedząc, że odpowiedzią jest nazwisko KOWALEWSKI.

abaabaabaa
bbaabaaabb
bbaabaabbb
bababababa
abbabbbaab

Rozwiązanie: litery zostały zapisane w kolumnach jedna pod drugą.

K	O	W	A	L	E	W	S	K	I
a	b	a	a	b	a	a	b	a	a
b	b	a	a	b	a	a	a	b	b
b	b	a	a	b	a	a	b	b	b
b	a	b	a	b	a	b	a	b	a
a	b	b	a	b	b	b	a	a	b

Po odczytaniu nazwiska prowadzący może przedstawić postać Jana Kowalewskiego i jego udział w odszyfrowywaniu przechwyconych meldunków rosyjskich (Załącznik_Jan Kowalewski – biografia).

Prowadzący może też zaangażować krótką dyskusję na temat użytego szyfru. Dlaczego nie zaszyfrowaliśmy imienia? Czemu nie ma niektórych liter w szyfrze (prawdopodobnie pisano wiadomości po łacinie)? Na czym polega trudność związana z tym szyfrem? Czy bez klucza dałoby się ten szyfr złamać? Może uczestnicy mieliby jakieś pomysły jak go ulepszyć albo utrudnić?

ZADANIE GŁÓWNE

SZYFR KRATKOWY

Bardziej skomplikowany szyfr kratkowy stosowany był już w dawnych czasach, ale popularny był jeszcze w XX wieku i właśnie na nim oparte były szyfry rosyjskie, które rozwiązał Jan Kowalewski: „Rewolucja”, „Delegat” i inne. Prowadzący, na przykładzie imienia Jan, może pokazać na czym polega szyfr i z jakimi trudnościami musieli się mierzyć dekryptolodzy przy odszyfrowywaniu go. Słowo Jan można było zapisać na różne sposoby. Łatwo było, kiedy w ręce wpadł klucz do szyfru, trudniej, kiedy trzeba było go samemu rozpoznać.

JAN/ 131 193/ 7696 31/ 25329 3

	1	2	3	4	5	6	7	8	9
1	a		j						
2					j				
3	n	a							
4									
5									
6									
7		n				j			
8									
9			n			a			

Warto tu wprowadzić temat rozwiązania właśnie szyfru „Rewolucja” krok po kroku (źródło: <https://niepodlegla.gov.pl/o-niepodleglej/kryptologia-w-ii-rp-od-rewolucji-do-enigmy/>).

„Rosjanie używali szyfrów kratkowych, o układzie podobnym do tabliczki mnożenia, np. jeśli w pole mnożenia – 2 x 2 – wpiszemy rosyjską literę „p” – czyli (r), wówczas w szyfrogramie będzie ona oznaczona jako „22”; jeśli w pole 1 x 0 (choć to matematycznie niepoprawne) wpiszemy rosyjską literę „и” – czyli (i) wówczas będzie ona oznaczona w szyfrogramie jako „10”. Słowo „dywizja”, ma w języku rosyjskim, charakterystyczny układ sylab i liter. Każda druga litera w sylabie – na którą składają się dwie litery – to litera и (i): („ди-ви-зия”).

Jan Kowalewski posłużył się więc grzebieniem, z którego wyłamał zęby w regularny sposób, tak aby w miejsce po ich wyłamaniu wchodziły dwie cyfry oznaczające literki „и” i przesuwając nim po tekście szukał takiej sekwencji znaków (cyfr, które zastępowały w szyfrogramie literę „и”), gdzie co druga grupa (dwóch cyfr) będzie się powtarzała. Gdy ją znalazł, odczytał słowo dywizja. Dzięki temu dysponował już pięcioma literami, co stanowiło około 1/5 alfabetu rosyjskiego.

Kolejne litery odkrył dzięki ewidentnemu, wręcz szkolnemu błędowi szyfrujących, którzy podali nazwisko dowódcy i szefa sztabu dwukrotnie, raz tekstem otwartym (jawnym) – jak być powinno, a innym razem tekstem zaszyfrowanym. Z zasady nie wolno było szyfrować podpisów i nagłówków, bowiem były one niezienne, a zmieniały się jedynie klucze szyfrowe. W ten sposób znając te nagłówki i nazwiska, można było metodą podkładania tekstu jawnego pod tajny, złamać klucz i odczytać szyfrogram.

Znając ze słowa „ди–ви–зия” („di-wi-zija”) litery: „и” („i”) oraz „я” („ja”), mógł sprawdzić, że był to Iona Jakir („иона якир”) i poznać dzięki temu kilka kolejnych nowych liter: „о” („o”), „н” („n”), „а” („a”), „к” („k”), „р” („r”). Ponadto podwójna litera „сс” – („ss”) – w słowie Odessa, umieszczonym w nagłówku i powtórzonym w treści szyfrogramu, przy znajomości: „д” (d), „а” („a”), dopomogła, w odszyfrowaniu kilku kolejnych liter: „е” („e”) i „с” („s”). Dzięki temu poznał już 12 liter, a więc niemal połowę alfabetu. Podstawiając w szyfrogramie znane litery pod grupy cyfr, poszukiwał brakujących liter i w ten sposób odczytywał kolejne słowa, a następnie całą treść szyfrogramu. W ten sposób w sierpniu 1919 roku Jan Kowalewski złamał – metodą „ataku” lingwistycznego – pierwszy rosyjski szyfr o nazwie „Delegat”.

Grupa ma za zadanie stworzyć własny szyfr kratkowy i zaszyfrować 3 słowa, które kojarzą się z treścią filmu i wojną z 1920 roku. A następnie dać innej drużynie słowa zaszyfrowane razem ze słowami nieszyfrowanymi.

Po wymianie na podstawie znajomości słów niezaszyfrowanych, grupy próbują odtworzyć przynajmniej część szyfrów, podobnie jak Kowalski, korzystając ze słowa „dywizja”. Następnie grupy porównują swoje klucze.

	1	2	3	4	5	6	7	8	9
1									
2									
3									
4									
5									
6									
7									
8									
9									

Szyfrowanie i kodowanie

Ostatni szyfr łączy dwa rodzaje szyfrowania:

- szyfr typu „kratkowego”,
- tabela kodowa (całe pojęcia i nazwy są zapisywane w formie liczbowej).

Ten szyfr jest jeszcze trudniejszy do dekryptażu, czyli rozszyfrowania, ale za to same klucze są bardzo charakterystyczne i mogą nam wiele powiedzieć o korespondencji i czasach, kiedy służyły.

Grupa dostaje jeden z kluczy i ma za zadanie określić z jakiej epoki pochodzi klucz i czego mniej więcej mógł dotyczyć (klucz pochodzi z drugiej połowy XVII w. prawdopodobnie szyfrem posługiwała się frakcja magnacka stronników króla Jana Kazimierza, przeciwnych wyborowi „Piasta” na króla - Załącznik_Klucz).

STWÓRZ KLUCZ!

1. Grupa ma za zadanie stworzyć własny francuski szyfr połączony z tabelą kodową. Szyfr musi dotyczyć wojny polsko-bolszewickiej w 1920 roku. 20 pojęć, nazwisk, nazw geograficznych związanych z tym okresem, tematyką filmu, radiowywiadem, Janem Kowalewskim.
2. Następnie grupy wymieniają się kodami i próbują zakodować jakieś dłuższe zdanie używając co najmniej 4 pojęć z klucza i kodowania.
3. Na końcu grupy jeszcze raz zamieniają się zaszyfrowanymi wiadomościami i kluczami i próbują odkodować wiadomości.

WIKTORIA 1920

PODSUMOWANIE

Prowadzący podsumowuje z uczestnikami doświadczenia z warsztatów i zadania z szyframi. Które zdaniem uczestników szyfry były najlepsze, a które najtrudniejsze do rozwiązania?

Warto, żeby prowadzący poświęcił chwilę na przedstawienie przede wszystkim roli alfabetu Morsa w radiotelegrafii i szyfrowaniu. Prowadzący może zapytać o współczesne szyfry i czy uczestnicy wiedzą jak i co się szyfruje w dzisiejszych czasach? Czy zmieniły się metody odszyfrowywania?

Jakie umiejętności były potrzebne kiedyś, a jakie są dziś, by pracować w wywiadzie i czy radiotelegrafia miałaby jakiś sens w dzisiejszych czasach, a jeśli tak, to gdzie i przy jakiej okazji.

Bibliografia:

1. Grzegorz Nowik, *Zanim złamano „Enigmę”... Polski radiowywiad podczas wojny z bolszewicką Rosją 1918-1920*. Część 1, Oficyna Wydawnicza RYTM, 2021
2. Grzegorz Nowik, *Zanim Złamano „Enigmę”... Rozszyfrowano Rewolucję. Polski radiowywiad podczas wojny z bolszewicką Rosją 1918-1920*. Część 2, Oficyna Wydawnicza RYTM, 2021
3. Andrzej Chwalba, *Przegrane zwycięstwo. Wojna polsko-bolszewicka 1918–1920*, Wydawnictwo Czarne, 2020
4. Agnieszka Knyt, *Wojna o wolność 1920. Bitwa warszawska*. Tom 1 i 2, Wydawnictwo Karta, 2020
5. Agnieszka Knyt, *Bitwa warszawska 1920. Jak Polska zatrzymała bolszewików*, Wydawnictwo Karta, 2020
6. <https://niepodlegla.gov.pl/o-niepodleglej/kryptologia-w-ii-rp-od-rewolucji-do-enigmy/>



Ministerstwo
Kultury
i Dziedzictwa
Narodowego

niepodległa

Opracowanie:

KONCEPT
Kultura

Monika Rejtner
Anna Osiadacz
Anna Piątkowska
Zygmunt Fit

Producentem filmu „Wiktoria 1920” jest Biuro
Programu „Niepodległa”.
Narodowe Centrum Kultury jest koproducentem filmu.
Partnerem filmu jest Narodowy Bank Polski.

Film został dofinansowany ze środków Ministra Kultury
i Dziedzictwa Narodowego.