VISIT MATH

Dofinansowane przez Unię Europejską

Kodowanie

Temat	Algorytmy
Cele kształcenia	Znajomość różnych sposobów kodowania i nauka dekodowania.
Grupa wiekowa	12-16 lat (do dostosowania w każdym kraju)
Przewidywany czas	45 min
Zadania	Szyfrowanie i odszyfrowywanie
Powiązane wycieczki	Paryż

Wymagana wcześniejsza wiedza

Nie są wymagane żadne szczególne umiejętności, ani wiedza.

Krok po kroku: zajęcia w klasie

Krok 1: Przedstawienie tematu

Krótka prezentacja poszczególnych elementów dorobku w tej sekcji

Kryptografia jest nauką znajdującą się gdzieś pomiędzy matematyką a informatyką, ale z bardzo praktycznymi zastosowaniami. Jej celem jest ochrona informacji, zwykle poprzez sprawienie, że wydają się one niezrozumiałe poprzez mieszanie i przekształcanie ich zgodnie z określoną metodą.

Istnieje również technika kryptograficzna zwana „steganografią", która służy do ukrywania wiadomości w pozornie nieszkodliwym tekście lub obrazie. Wiadomości te mogą być wysyłane w domenie publicznej bez obawy, że zostaną przechwycone lub odkryte, nawet przypadkowo.

Odrobina historii

- Od 800 r. p.n.e. do 200 r. p.n.e.: Spartanie używali kości.
- Około 600 r. p.n.e.: Nabuchodonozor używał ogolonych czaszek.
- Około 480 r. p.n.e.: Dematarus (Grek), odizolowany w Persji, używa tabliczek woskowych, aby ostrzec swój kraj przed planami Kserksesa (Persja).
- 100 P.N.E. / 44 P.N.E.: Szyfr Cezara (przesunięcie alfabetyczne)
- I wiek: Pojawienie się niewidzialnego atramentu (płyny organiczne bogate w węgiel)
- 1580: Cyfra przez podstawienie symboli (nomenklatura kodowa) - Mary Stuart
- 1586: Traktat o szyfrach: Szyfr Vigenère'a
- 1930: Szyfrator Enigma
- Koniec XX wieku: Pojawienie się szyfrowania z kluczem jawnym - RSA

Definicja kodowania:

Kryptologia: Nauka o kryptografii i kryptoanalizie.

Kryptografia: Nauka o tworzeniu kryptogramów.

Kryptoanaliza: Nauka o analizie kryptogramów w celu ich odszyfrowania.

Kryptogram: Zaszyfrowana wiadomość.

Kod / Szyfr / Krypta: Przekształcenie tekstu lub informacji poprzez zastąpienie liter (lub słów do zaszyfrowania) skryptem składającym się z wcześniej zdefiniowanych znaków.

Deszyfrowanie / Dekodowanie: przekształcenie zaszyfrowanej wiadomości w czystą wiadomość zgodną z oryginałem.

Deszyfrowanie: znalezienie szyfru użytego w kryptogramie.

Tekst jawny: oryginalna wiadomość przed zaszyfrowaniem.

Szyfrogram: tekst uzyskany po zaszyfrowaniu.

Klucz: Element (słowo lub liczba), który zmienia zastosowanie metody szyfrowania i/lub deszyfrowania.

Klasyfikacja kodów

Szyfr podstawieniowy: System kryptograficzny, w którym każda litera wiadomości jest zastępowana innym znakiem, ale zachowuje swoje miejsce w wiadomości.

Szyfr transpozycyjny: System kryptograficzny, w którym każda litera wiadomości pozostaje niezmieniona, ale jest przenoszona w inne miejsce w wiadomości.

Zastępowanie monoalfabetyczne: Szyfr substytucyjny, w którym zaszyfrowany alfabet pozostaje taki sam przez cały czas szyfrowania. Zastępowanie literami, symbolami, cyframi lub liczbami itp.

Podstawianie polialfabetyczne: Szyfr podstawieniowy, w którym szyfrowany alfabet zmienia się podczas szyfrowania. Zmiana ta jest przeprowadzana zgodnie z kluczem.

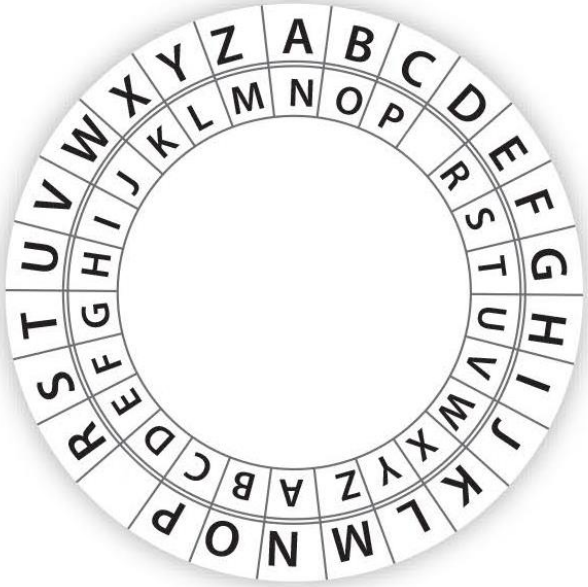
Szyfr nomenklaturowy: Ten typ szyfru łączy prostą substytucję (każda litera jest zastępowana symbolem) i **szyfr repertuarowy** (niektóre słowa są również zastępowane symbolem, a także symbolami zakłócającymi).

Krok 2: Ćwiczenia do wykonania na lekcji

Przykład najbardziej znanych systemów kodowania

1. Szyfr Cezara lub kod Cezara

Cezar szyfrował swoje wiadomości na potrzeby ważnej komunikacji z armią. To, co jest znane jako szyfr Cezara (podstawienie monoalfabetyczne), to przesunięcie liter 4. stopnia: aby zaszyfrować wiadomość, **A staje się D, B staje się E, C staje się F** itd. Aby uwzględnić wszystkie litery alfabetu, rozsądniej jest przedstawić alfabet na kole.



Źródła: Fermat Science

Aby odszyfrować wiadomość:

DOHD MDFWD HVW

więc wszystko, co musisz zrobić, to przesunąć litery w innym kierunku: **D jest dekodowane jako A, E jako B** itd.

Odszyfrowana wiadomość wygląda następująco:

ALEA IACTA EST

Odszyfruj 3 poniższe wiadomości:

WKH URPDQV

YLFWRUB

HPSHURU

2. Szyfr Vigenère'a

Szyfr Vigenère'a to polialfabetyczny algorytm subsytucji.

Zamiast kołowego dopasowywania liter, każda litera jest teraz powiązana z inną literą (bez ustalonej kolejności lub zgodnie z ogólną zasadą).

Na przykład:

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

Aby zaszyfrować wiadomość:

BYĆ ALBO NIE BYĆ - OTO JEST PYTANIE

spójrz na powiązania i zamień literę **B na literę Q, następnie literę Y na literę J, następnie literę C na literę B**...

Zaszyfrowana wiadomość wygląda następująco:

QJB FWQD SPX QJB DGD AXVG OJGFSPX

Aby to odszyfrować, znając podstawienia, wykonujemy operację odwrotną.

Odszyfruj następujące 3 wiadomości:

HFGE PV IFSGF VGPB

OWFJ NPGE SRHQX KV

FSDGEXK PMXF IKDH HFGEV

3. System szyfrowania Porta

Porta był włoskim fizykiem i wynalazcą pierwszego dosłownego systemu podwójnego klucza, tj. pierwszego szyfru, w którym alfabet zmienia się z każdą literą.
Ten polialfabetyczny system był niezwykle solidny jak na swoje czasy, do tego stopnia, że wielu uważa Portę za „ojca współczesnej kryptografii". Giovanni Della Porta wynalazł swój system szyfrowania w 1563 roku i był z powodzeniem używany przez trzy stulecia.

Oto przykład tabeli szyfrowania Porta:

AB	a b c d e f g h i j k l m	n o p q r s t u v w x y z
CD	a b c d e f g h i j k l m	z n o p q r s t u v w x y
EF	a b c d e f g h i j k l m	y z n o p q r s t u v w x
GH	a b c d e f g h i j k l m	x y z n o p q r s t u v w
IJ	a b c d e f g h i j k l m	w x y z n o p q r s t u v
KL	a b c d e f g h i j k l m	v w x y z n o p q r s t u
MN	a b c d e f g h i j k l m	u v w x y z n o p q r s t
OP	a b c d e f g h i j k l m	t u v w x y z n o p q r s
QR	a b c d e f g h i j k l m	s t u v w x y z n o p q r
ST	a b c d e f g h i j k l m	r s t u v w x y z n o p q
UV	a b c d e f g h i j k l m	q r s t u v w x y z n o p
WX	a b c d e f g h i j k l m	p q r s t u v w x y z n o
YZ	a b c d e f g h i j k l m	o p q r s t u v w x y z n

Źródło: apprendre-en-ligne.net

Aby szyfrować przy użyciu jednego z tych alfabetów, wybiera się literę znajdującą się naprzeciwko niego w tabeli, aby zastąpić literę w tekście jawnym. Na przykład, jeśli szyfrujesz przy użyciu alfabetu AB, **zastąpisz a literą n, b literą o, q literą d** itd.

Na przykład, jeśli słowem kluczowym jest STEEL, do zaszyfrowania wiadomości używane są kolejno alfabety S, T, E, E, L, S, T, E, E, L itd. Jeśli zaszyfrujemy frazę "Porta cipher" za pomocą klucza STEEL, otrzymamy:

System	p	o	r	t	a	c	i	p	h	e	r
Klucz	**S**	**T**	**E**	**E**	**L**	**S**	**T**	**E**	**E**	**L**	**S**
Zakodowanie	L	K	G	I	V	T	Z	E	S	Z	A

Szyfr porta został użyty przez królową Marię Antoninę do zmodyfikowania i ulepszenia szyfru PORTA do użytku w jej korespondencji. W szczególności dodała funkcję kodowania tylko co drugiej litery.

Krok 3: Praca domowa i wskazówki do dalszej pracy

A może wyzwanie? Przekaż zakodowane wiadomości kolegom z klasy, aby mogli je odszyfrować.
Na przykład wybierz metodę kodowania i zaszyfruj wiadomość, a następnie przekaż ją dalej, nie zdradzając użytej metody.
Dodaj trochę napięcia, wyznaczając limit czasu lub nagrodę.

Możesz także stworzyć własne koło deszyfrujące, które można łatwo znaleźć w Internecie: https://www.youtube.com/watch?v=0Xuv58Uwu9o

Materiał potrzebny do realizacji wycieczki:

Uczniowie biorący udział w wycieczce będą musieli mieć ołówek, gumkę i papier, aby znaleźć właściwy szyfr.

VISIT MATH

Dofinansowane przez Unię Europejską

Sfinansowane ze środków UE. Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Europejskiej Agencji Wykonawczej ds. Edukacji i Kultury (EACEA). Unia Europejska ani EACEA nie ponoszą za nie odpowiedzialności.

Kod projektu: 1-FR01-KA220-SCH-00027771

Aby dowiedzieć się więcej o projekcie VisitMath, odwiedź:

https://visitmath.eu

FERMAT SCIENCE
Une autre idée des maths

5th High School
Agrinio · Greece

Istituto Statale "E. Montale" Pontedera

LogoPsyCom

ZS 31

YuzuPulse