Łamanie szyfrów

Kryptografia w szkole podstawowej

Jerzy Kołodziejczyk, **dyrektor Szkoły Podstawowej nr 4 w Gryficach**

Uczniowie klas IV–VI Szkoły Podstawowej nr 4 w Gryficach wykazujący zainteresowanie matematyką mają możliwość rozwijania swoich pasji na zajęciach pozalekcyjnych zorganizowanych w związku z realizacją dwuletniego projektu „Możliwości na miarę umiejętności. Program edukacyjny dla Szkoły Podstawowej i Gimnazjum gminy Gryfice", finansowanego w ramach programu operacyjnego Kapitał Ludzki. W naszej szkole stworzyliśmy dwie grupy: jedna liczy dziewięcioro, a druga szesnaścioro uczniów. Tygodniowo uczestnicy każdej z nich pracują od dwóch do trzech godzin.

Interdyscyplinarność kryptografii

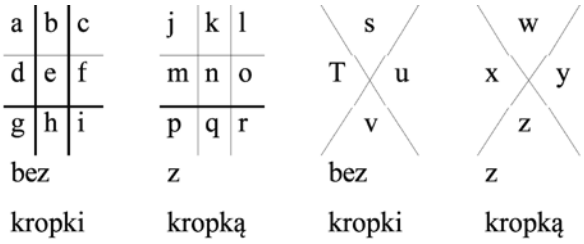
W pierwszym semestrze zaplanowano dla tych grup zajęcia z kryptografii. Problematyka ta pozwoliła połączyć treści wielu różnych dyscyplin wiedzy: matematyki, historii, języka polskiego i angielskiego, informatyki. Specyficzna tematyka zajęć sprzyja pracy w grupach, zdobywaniu wiedzy i umiejętności drogą eksperymentów, z wykorzystywaniem arkusza kalkulacyjnego itp. Kolejną korzyścią jest stwarzanie sytuacji, w których niezbędne jest myślenie i postępowanie według zadanych algorytmów oraz odkrywanie algorytmów odwrotnych.

Zajęcia rozpoczęto od przedstawienia historii złamania szyfrów niemieckiej maszyny szyfrującej ENIGMA i roli polskich matematyków: Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego w tym ważnym odkryciu. Przez kilka kolejnych tygodni omawiano elementarne metody szyfrowania, zdefiniowano podstawowe pojęcia (tekst jawny, tekst zaszyfrowany – szyfrogram, klucz, sposób pisania szyfrogramów – słowa po pięć znaków, alfabet – bez polskich znaków diakrytycznych). Poznawanie każdej metody szyfrowania poprzedzano prezentacją oraz kilkoma wspólnie wykonanymi ćwiczeniami. Po upewnieniu się, że wszyscy zrozumieli daną metodę, uczniowie wcielali się w rolę szyfrantów. Każdy szyfrował własny tekst. Następnie wymieniali się przygotowanymi szyfrogramami i próbowali odczytać zaszyfrowaną wiadomość kolegi lub koleżanki. Kilka spotkań poświęcono na pogłębienie wiedzy i kształcenie umiejętności matematycznych uczniów z zakresu podstaw arytmetyki modularnej oraz przedstawienie przykładów jej zastosowania w kryptografii. Oprócz „ręcznego" szyfrowania, uczniowie wykorzystywali koło szyfrowe oraz arkusz kalkulacyjny Excel. Szczególnie emocjonujące było „zbudowanie" przez każdego ucznia własnej maszyny szyfrującej i deszyfrującej, a następnie poddanie jej weryfikacji, tj. sprawdzenie jej skuteczności w deszyfrowaniu wiadomości otrzymanych od pozostałych członków grupy. Przy okazji formułowano i rozwiązywano zadania matematyczne, które w naturalny sposób wiązały się z omawianymi metodami szyfrowania. Większość zajęć była poświęcona szyfrom podstawieniowym, tj. takim, w których jedna litera była zastępowana przez inną, oraz szyfrom przestawieniowym, czyli takim, w których litery tekstu jawnego występują w szyfrogramie w zmienionej kolejności.

W szyfrach przestawieniowych litery tekstu jawnego występują w zaszyfrowanym tekście, ale w innej kolejności. W tej grupie szyfrów poznaliśmy szyfr płotkowy oraz szyfr przestawieniowy kolumnowy.

Szyfr masonów

Szyfr masonów pozwala litery alfabetu zastąpić znakami graficznymi. Wszystkie 26 liter alfabetu rozmieszczono w komórkach czterech kwadratów (patrz rysunek poniżej). Każdą z liter utożsamiamy łamaną zbudowaną z odcinków tworzących daną komórkę. Jeżeli litera jest z drugiego lub czwartego kwadratu, to oprócz łamanej dopisujemy kropkę.



Dla przykładu słowo *koza* przyjmie postać:

Szyfr płotkowy

Szyfr płotkowy wykorzystuje specyficzną formę zapisu „zygzakiem" (po skosie w dół i w górę). Jeśli zapiszemy frazę *nasza szkoła jest wesoła* w trzech wierszach,

n a o e e a
a z s k l j s w s l
s z a t o

to czytając znaki poziomo otrzymamy szyfrogram tej informacji: *naoeeaazskljswslszato*, co pisane po pięć znaków (przyjmujemy umowę – tekst jawny zapisujemy małymi literami, szyfrogramy wielkimi, po pięć liter w jednym słowie): NAOEE AAZSK LJSWS LSZAT A. Kluczem w tej metodzie szyfrowania jest liczba wierszy. Jako ćwiczenie proponujemy zaszyfrowanie tej samej informacji przy pomocy czterech wierszy. Odczytanie informacji tak zaszyfrowanej pozostawiamy Czytelnikowi.

Szyfr przestawieniowy

Zapiszmy w kwadracie frazę *kwadrat jest rombem*, a puste pola wypełnijmy dowolnymi literami. Czytając litery kolumnami, otrzymamy szyfrogram: kated wtrme ajoaf dembg rsbch.

k	w	a	d	r
a	t	j	e	s
t	r	o	m	b
e	m	a	b	c
d	e	f	g	h

Odszyfrowanie tak powstałego tekstu jest bardzo proste: wystarczy szyfrogram zapisać w kolumnach, a utworzone wiersze będą zawierały tekst jawny. Jeżeli tekst, który chcemy zaszyfrować jest długi, to można użyć kilku kwadratów.

Szyfr książkowy

Szyfr książkowy to metoda szyfrowania liter, a nawet słów, za pomocą określonej książki. Każdą kolejną literę tekstu jawnego szyfrujemy za pomocą trzech liczb, pierwsza podaje numer strony, druga wiersza, a trzecia litery (lub słowa) w tym wierszu. Szyfrogram jest ciągiem trójek liczbowych, określających kolejne litery (słowa) ukrywanej informacji.

Szyfr Cezara

Ten szyfr wykorzystuje prostą zasadę zamiany liter: każda litera alfabetu zostaje zastąpiona literą, która jest w alfabecie o 3 pozycje dalej. Oczywiście alfabet należy traktować cyklicznie, tj. po literze *z* następną jest *a*, później *b* itd. Poniżej pokazano dwa alfabety (pisane małymi i wielkimi literami). Drugi powstał z przesunięcia pierwszego o 3 miejsca w prawo.

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

Zdanie *Liczba parzysta może być pierwsza* po zaszyfrowaniu metodą Cezara będzie miało postać: OLFCE DSDUC BVWDP RCHEB FSLHU ZVCD. Jeśli informację zaszyfrowano za pomocą klucza 3, to do jej odszyfrowania potrzeba klucza – lub klucza dodatniego 23. Przyjmując klucz 13 – otrzymamy szyfr ROT13, który jest ciekawy z tego względu, że powtórne zaszyfrowanie szyfrogramu prowadzi do odszyfrowania wiadomości. Podczas omawiania szyfrów podobnych do szyfru Cezara uczniowie zauważyli, że wygodnie jest ponumerować litery alfabetu, a następnie, znając klucz, obliczyć numery liter, których użyją w szyfrogramach. Ten moment wykorzystano do zapoznania uczniów z podstawami arytmetyki modularnej. Omówiono dodawanie i mnożenie modulo 12 i modulo 26. Wybór modułu 12 wynikał z doświadczeń uczniów w posługiwaniu się zegarem. Uczniowie rozumieli, dlaczego 9+5 modulo 12 jest równe 2, a $3 \cdot 5$ modulo 12 jest równe 3. Ułatwiło to definiowanie tabelek dodawania i mnożenia przy innych modułach. Wybór modułu 26 był związany z liczbą liter w alfabecie (bez polskich znaków diakrytycznych). Matematyczne rozważania umożliwiły uczniom zauważenie i rozwiązanie następującego problemu: jeśli znamy klucz, którym

zaszyfrowano daną informację, to jaki jest klucz do jej deszyfracji. Szczególnym przypadkiem był szyfr ROT 13.

Szyfry indywidualne

Przy omawianiu szyfru Cezara i jego modyfikacji uczniowie zwrócili uwagę na inny problem matematyczny – że istnieją szyfry podstawieniowe, w których zamiana liter nie musi opierać się na stałym przesunięciu alfabetu, ale na dowolnych (nawet przypadkowych) podstawieniach. Ile takich szyfrów można stworzyć? Pierwszą literę alfabetu można zamienić dowolną z 26 liter, drugą – dowolną z 25 pozostałych liter, trzecią dowolną z pozostałych 24, itd. Stąd ogólna liczba szyfrów podstawieniowych jest równa $26 \cdot 25 \cdot ... 2 \cdot 1 = 26!$ Wynik ten nie dziwi, gdyż każdy szyfr tego typu jest permutacją zbioru 26 liter.

Jeden z uczniów zaproponował dwukrotne szyfrowanie: najpierw z kluczem 3, później z kluczem 5. Później ten sam uczeń zauważył, że takie dwukrotne szyfrowanie można zastąpić jednym, i wskazał klucz tego nowego szyfru.

Inny zaproponował nowy sposób szyfrowania: pierwszą literę alfabetu zastąpimy ostatnią, drugą przedostatnią, itd.

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

Po wykonaniu powyższej tablicy zauważono, że może ona posłużyć zarówno do szyfrowania, jak i deszyfrowania, choć nie ma tu klucza takiego jak w szyfrze Cezara.

Zauważmy, że ostatnia tablica podstawień może być zapisana w krótszej postaci, a zamiana liter obowiązuje w obie strony, tj. z góry na dół i odwrotnie.

a	b	c	d	e	f	g	h	i	j	k	l	m
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

Maszyny na bazie Excela

Bardzo pouczające okazały się próby stworzenia mechanicznej maszyny (koła szyfrowego) do szyfrowania informacji metodą Cezara, ale z dowolnym kluczem. Koło szyfrowe umożliwiało szybkie ustalenie zamiany liter i zaszyfrowanie ustalonej wiadomości oraz odszyfrowanie wiadomości otrzymanej od kolegi. Po takich próbach zdecydowano się na zaprojektowanie w arkuszu kalkulacyjnym Excel nowej maszyny szyfrującej i deszyfrującej opartej na metodzie Cezara. Jednak w tym przypadku uczniowie musieli poznać kilka informacji o stronie kodowej ASCII oraz kilka poleceń programu Excel.

Strona kodowa ASCII literom *a, b, c, d,…, z* przypisuje kody o wartościach odpowiednio równych 97, 98, 99, …, 122. Litery wielkie A, B, C, …, Z mają kody 65, 66, 67, …, 90. Arkusz kalkulacyjny Excel dostarcza dwóch funkcji, które pozwolą zamieniać litery na liczby i odwrotnie. Za pomocą polecenia *kod* otrzymamy kody liter, a za pomocą polecenia *znak* zamienimy kody na litery. Dzięki temu w dość prosty sposób wykorzystamy arkusz Excel do szyfrowania i deszyfrowania informacji na przykład za pomocą szyfru Cezara (patrz schemat poniżej).

Litery tekstu jawnego wpisywano w komórki B2, B3, …, a ich kody w komórkach C2, C3, … otrzymywano za pomocą poleceń =KOD(B2), =KOD(B3), …. Obliczenie kodu szyfrogramu wkomórkach D2, D3, itp. było wykonane za pomocą poleceń w postaci: = MOD(B3+$C$1;26)+65, =MOD(B4+$C$1;26)+65, itd. Ostatni wiersz zawiera litery szyfrogramu, które otrzymano za pomocą poleceń =ZNAK(D2), =ZNAK(D3), itd. Po wpisaniu do maszyny tekstu jawnego i ustaleniu wartości klucza jednym kliknięciem otrzymywano szyfrogram. Deszyfrowanie przebiegało podobnie. Najpierw wprowadzano kolejne litery szyfrogramu, później ustalano wartość klucza, przyjmując kolejno 1, 2, itd. Po wprowadzeniu wartości klucza arkusz kalkulacyjny wyświetlał nową postać szyfrogramu. Jeśli była ona nieczytelna i niezrozumiana, to zmieniano wartość klucza na następną liczbę, itd. Po kilku próbach szyfrogram przestawał skrywać tajemnicę. W tej części zajęć uczniowie bardzo aktywnie szyfrowali oraz deszyfrowali informacje otrzymane od innych.

Słowo – klucz

Wśród szyfrów podstawieniowych omówiono również takie, w których kluczem było słowo. Jeśli odbiorca wiadomości znał słowo kluczowe, mógł sam zbudować tabelę podstawień i odczytać zaszy-

Klucz	k=	3																			
Tekst jawny	m	o	j	a	m	a	s	z	y	n	a	s	z	y	f	r	u	j	a	c	a
Kod tekstu	109	111	106	97	109	97	115	122	121	110	97	115	122	121	102	114	117	106	97	99	97
Kod szyfrogramu	73	75	70	87	73	87	79	86	85	74	87	79	86	85	66	78	81	70	87	89	87
Szyfrogram	I	K	F	W	I	W	O	V	U	J	W	O	V	U	B	N	Q	F	W	Y	W

frowaną informację. Załóżmy, że słowem kluczowym jest *Szymon*. Każda litera występująca w kluczu jest użyta tylko raz. W pierwszym wierszu jest cały alfabet, a wiersz drugi rozpoczynamy od słowa kluczowego, po którym dopisujemy kolejne niewykorzystane w kluczu litery alfabetu.

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

Alfabet zamknięty w kwadracie

Szyfrowanie za pomocą kwadratu 5 x 5 (bez litery j, którą w razie potrzeby zastąpi litera i).

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

	1	2	3	4	5
1	a	f	l	q	v
2	b	g	m	r	w
3	c	h	n	s	x
4	d	i	o	t	y
5	e	k	p	u	z

Powyżej przedstawiono dwa kwadraty, które mogą być wykorzystane do szyfrowania wiadomości. W obrębie każdego z nich znajduje się 25 liter alfabetu (litery i oraz j będziemy używali zamiennie, stosownie do potrzeb). Oba kwadraty różnią się sposobem rozmieszczenia liter. Każda litera jest określona za pomocą pary liczb, pierwsza określa numer wiersza, druga kolumny, np. litera h w pierwszym kwadracie będzie zapisana jako para (2,3) lub krócej 23. Ta sama litera w drugim kwadracie określona jest za pomocą pary (3,2) lub 32. Przy okazji poznajemy lub ćwiczymy kartezjański układ współrzędnych na płaszczyźnie. Tytuł *Kwiaty Polskie* zaszyfrowany za pomocą pierwszego z tych kwadratów będzie następującym ciągiem liczb: 25522411445435343143252415. Deszyfrowanie polega na podstawieniu w miejsca kolejnych par liczb liter danego kwadratu.

Opisana wyżej konstrukcja kwadratu jest łatwa do odtworzenia, a tym samym odczytanie szyfrogramów będzie równie proste. By skomplikować sytuację i lepiej zabezpieczyć ukrytą informację, zmodyfikujemy proces tworzenia kwadratu do szyfrowania. Wykorzystamy w tym celu klucz, którym będzie ustalone słowo lub fraza. Niech to będzie np. *autobus*. Litery, z których utworzony jest nasz klucz, wpisujemy do kwadratu poziomo. Po wpisaniu liter klucza wypełniamy wolne miejsca kolejnymi literami alfabetu, których nie było w tym kluczu. Ponieważ kwadrat ma zawierać 25 liter całego alfabetu pamiętajmy, by powtarzające się litery w kluczu wpisać tylko raz (np. w przyjętym kluczu litera u wystąpiła dwukrotnie, ale została zapisana tylko raz). Tak powstały kwadrat będzie utrudniał złamanie szyfrogramów.

	1	2	3	4	5
1	a	u	t	o	b
2	s	c	d	e	f
3	g	h	i	k	l
4	m	n	p	q	r
5	v	w	x	y	z

W ramach ćwiczenia pozostawiamy Czytelnikowi ponowne zaszyfrowanie *Kwiatów Polskich*.

Szyfr Playfaira również wykorzystuje tak utworzony kwadrat, ale sam sposób szyfrowania jest nieco bardziej złożony. Opiszemy to na przykładzie szyfrowania frazy *pechowy piątek* z kluczem *sobota*. Kwadrat szyfrujący tworzymy od wpisania klucza, pamiętając o niepowtarzaniu liter.

	1	2	3	4	5
1	s	o	b	t	a
2	c	d	e	f	g
3	h	i	k	l	m
4	n	p	q	r	u
5	v	w	x	y	z

Szyfrowanie rozpoczynamy od podziału tekstu jawnego na dwuliterowe cząstki. Jeśli tekst jawny ma nieparzystą liczbę znaków, to na końcu dopiszemy dodatkową literę x. Każda para liter będzie generowała parę liter szyfrogramu. Sposób generowania nowych liter zależy od rozmieszczenia danej pary w kwadracie szyfrowym. Litery danej pary mogą leżeć w tym samym wierszu, w tej samej kolumnie lub swoim położeniem wyznaczyć prostokąt, stanowiąc jego przeciwległe narożniki. W pierwszym przypadku każdą z liter zastępujemy literą po

jej prawej stronie (ostatnią literę wiersza – pierwszą). W sytuacji, gdy litery leżą w jednej kolumnie, zastępujemy je literami poniżej, a gdyby któraś z nich była ostatnią, zastąpimy ją pierwszą z tej kolumny. W przypadku, gdy litery położone są w narożnikach prostokąta, zastąpimy je literami położonymi w pozostałych narożnikach tego samego prostokąta. A zatem *pechowy piątek* rozbity na pary ma postać:

Tekst jawny	*pe*	*ch*	*ow*	*yp*	*ia*	*te*	*kx*
Szyfrogram	QD						

Para *pe* zostanie zastąpiona przez parę QD, gdyż litery pe wyznaczają prostokąt, w którego pozostałych dwóch narożnikach leżą litery *q* oraz *d*. Każdą z liter pary *pe* zastępujemy odpowiednią literą położoną w tym samym wierszu, a więc *p* zastępujemy literą *q*, zaś *e* literą *d*.

	1	2	3	4	5
1	s	o	b	t	a
2	c	d	**e**	f	g
3	h	i	k	l	m
4	n	**p**	q	r	u
5	v	w	x	y	z

Kolejna para *ch* leży w jednej kolumnie, dlatego każdą z tych liter zastąpimy literą położoną niżej, tj. *c* zastąpimy przez *h*, zaś *h* przez *n*.

	1	2	3	4	5
1	s	o	b	t	a
2	c	d	e	f	g
3	h	i	k	l	m
4	n	p	q	r	u
5	v	w	x	y	z

Analogicznie *ow* wyznaczy *do*, itd. Ostatecznie otrzymamy zaszyfrowany tekst.

Tekst jawny	*pe*	*ch*	*ow*	*yp*	*ia*	*te*	*kx*
Szyfrogram	QD	HN	DO	WR	MO	BF	QB

W ramach ćwiczenia proponujemy zaszyfrowanie tej samej frazy, ale z innym kluczem, np. *marzec*.

Szyfr Nihilistów wykorzystuje kwadrat szyfrujący zbudowany w taki sam sposób, jak opisany powyżej. Słowo klucz użyte do budowy tego kwadratu jest jednym z dwóch kluczy. Drugim kluczem jest nowe słowo, które szyfruje się tak samo jak tekst jawny i dodaje do wyniku. Szyfrogram nie zawiera liter, lecz liczby. Dla przykładu zaszyfrujmy słowo *konkurs*, przyjmując jako pierwszy klucz słowo *uczeń*, a klucz drugi *laureat*. Nasz kwadrat szyfrujący ma postać:

	1	2	3	4	5
1	u	c	z	e	n
2	a	b	d	f	g
3	h	i	k	l	m
4	o	p	q	r	s
5	t	v	w	x	y

Drugi klucz szyfrujemy w ten sposób, że kolejne litery słowa *laureat* znajdujemy wewnątrz kwadratu, a ich współrzędne (numer wiersza i kolumny, w których są położone) tworzą szyfr. Litera *l* leży w trzecim wierszu i czwartej kolumnie, a więc zaszyfrujemy ją jako 34. Analogicznie zaszyfrujemy kolejne litery.

Tekst jawny	l	a	u	r	e	a	t
Szyfr klucza	34	21	11	44	14	21	51

Teraz zaszyfrujemy tekst jawny w taki sam sposób, a następnie do otrzymanych liczb dodamy odpowiadające im liczby zaszyfrowanego klucza. Otrzymane w ten sposób liczby utworzą szyfrogram.

Tekst jawny	k	o	n	k	u	r	s
Szyfr tekstu	33	41	15	33	11	44	45
Szyfr klucza	34	21	11	44	14	21	51
Szyfrogram	67	62	26	77	25	65	96

Należy zwrócić uwagę, że jeżeli tekst ma więcej liter niż klucze, to należy je powtórzyć kilka raz, aż liczby te będą równe. W ramach ćwiczenia proponujemy zaszyfrować frazę *twierdzenie Pitagorasa*, używając kluczy: *trójkąt i kwadrat*. Dla dociekliwych: odczytać informację, znając szyfrogram 45 26 56 80 108 57 38 66 88 67 57 oraz klucze użyte podczas szyfrowania tej informacji: *zima* oraz *narty*.

Szyfr Vigenere'a oparty jest na wielokrotnym wykorzystaniu alfabetu. Kwadrat szy-

frujący zbudowany jest z 26 wierszy (alfabetów) – pierwszy zaczyna się literą A, drugi literą B, itd. Zaszyfrujemy frazę *krytpografia jest OK*, używając klucza *szyfrant*.

Pod tekstem jawnym zapisujemy klucz (lub kilka jego kopii), tak by każdej literze tekstu odpowiadała jedna litera klucza. Tak utworzone pary liter wskazują odpowiednie kolumny i wiersze, na przecięciu których znajdują się litery szyfrogramu. A więc pierwsza para *ks* wyznacza kolumnę rozpoczynającą się literą *K* oraz wiersz rozpoczynający się literą *S*, na ich przecięciu znajdziemy literę *C*. Druga para *rz* wyznacza literę *Q*, trzecia literę *W*, itd.

Tekst jawny	k	r	y	p	t	o	g	r	a	f	i	a	j	e	s	t	o	k
Klucz	s	z	y	f	r	a	n	t	s	z	y	f	r	a	n	t	s	z
Szyfrogram	C	Q	W															

Dokończenie szyfrowania pozostawiamy Czytelnikowi. Zauważmy, że do deszyfrowania tak otrzymanych szyfrogramów wykorzystujemy ten sam kwadrat oraz klucz. Na przykład szyfrogram WMKBVA oraz klucz *szyfrant* pozwalają odczytać kolejne litery tekstu jawnego. Wiersz rozpoczynający się

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

pierwszą literą klucza, tj. literą S, zawiera literę W w kolumnie, która rozpoczyna się literą E. W wierszu rozpoczynającym się literą Z, znajdujemy literę M i odczytujemy pierwszą literę kolumny, w której jest M, czyli N. Dalej wiersz rozpoczynający się od Y zawiera K w kolumnie, której pierwszą literą jest I, itd. A więc:

Szyfrogram	W	M	K	B	V	A
Klucz	s	z	y	f	r	a
Tekst jawny	E	N	I	G	M	A

Szyfr Beaufort'a

Do szyfrowania używamy zwykłego 26-literowego alfabetu, którego litery numerujemy od 0 do 25, kluczem jest dowolna liczba całkowita od 0 do 25.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Aby zaszyfrować literę na pozycji np. 8 z użyciem klucza 4, najpierw odejmujemy ją od 26, a do otrzymanej różnicy dodajemy wartość klucza, czyli 26 – 8 = 18,18 + 4 = 23, co odpowiada literze x. Podobnie odbywa się szyfrowanie litery c: mamy kolejno 26 – 2 = 24, 24 + 4 = 28, a liczbie 28 odpowiada ta sama litera, co różnicy 28 – 26 = 2, czyli c. Dla lepszego zrozumienia zaszyfrujemy słowo *wichura* kluczem $k = 7$.

Tekst jawny	w	i	c	h	u	r	a
n nr litery w alfabecie	22	8	2	7	20	17	0
$(26 - n) + k \mod 26$ nr litery w szyfrogramie	11	25	5	2	13	16	7
Szyfrogram	L	Z	F	C	N	Q	H

Deszyfrowanie odbywa się w taki sam sposób jak szyfrowanie. Słowo *burza*, po zaszyfrowaniu kluczem $k = 12$, ma postać LSYNM. Aby otrzymać tekst jawny, należy zaszyfrować LSYMN, używając tego samego klucza.

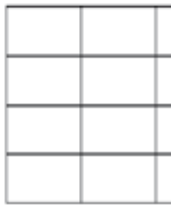
Tekst jawny	L	S	Y	N	M
n nr litery w alfabecie	15	8	5	13	14
$(26 - n) + k \mod 26$	27	20	17	25	26
Szyfrogram	b	u	r	z	a

Nasza przygoda z kryptografią dopiero się rozpoczęła. Poznamy kolejne metody szyfrowania, częściej będziemy korzystali z arkusza kalkulacyjnego. Planujemy też zorganizowanie kolejnych zawodów w szyfrowaniu i deszyfrowaniu. Zadania konkursowe z Pierwszych Mistrzostw Szkoły prezentujemy poniżej.

Rozwiąż jak największą liczbę zadań. Możesz korzystać z dodatkowych narzędzi przygotowanych do poszczególnych problemów. Dla ułatwienia posługujemy się alfabetem bez „ogonków" oraz znaków interpunkcyjnych (przecinki, kropki, itp.).

Zadanie 1. Szyfrem płotkowym o wysokości 3 utworzono szyfrogram: aslanruzaklcjykkuy. Odczytaj zaszyfrowaną treść.

Odpowiedź 1:



Zadanie 2. Szyfrogram ywkcpenewylo sianotrzymano za pomocą kwadratu 4×4 oraz klucza 2413. Odczytaj zaszyfrowany tekst.

Odpowiedź 2:

Zadanie 3. Używając szyfru Cezara (klucz k=3), zakoduj zdanie: SZYFROWANIE ZAPEWNIA BEZPIECZEŃSTWO.

S	Z	Y	F	R	O	W	A	N	I	E	Z	A	P	E	W	N	I	A	B	E	Z	P	I	E	C	Z	E	N	S	T	W	O

Odpowiedź 3:

Zadanie 4. Poniższy kryptogram został otrzymany za pomocą szyfru Cezara z kluczem jednocyfrowym. Odgadnij ten klucz i odczytaj treść ukrytą w szyfrogramie: hydeamihdepitwdetvdcwdpswg

Odpowiedź 4:

Zadanie 5. Przyjmując klucz szkoła,zbuduj kwadrat szyfrujący i zaszyfruj hasło: ARYTMETYKA MODULO

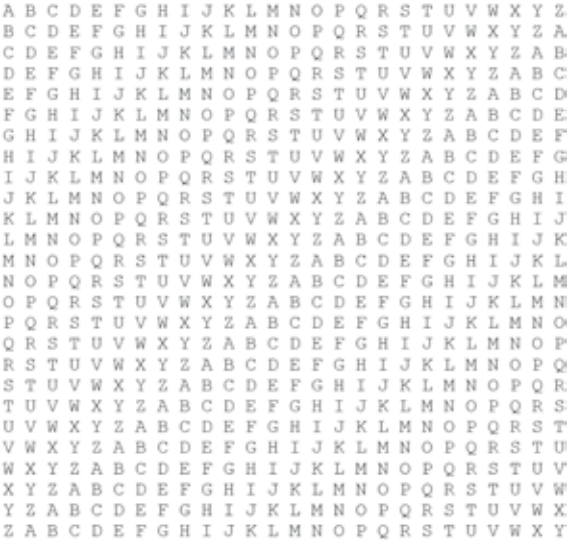
Odpowiedź 5:

Zadanie 6. Odczytaj poniższy szyfrogram, wiedząc, że powstał on przy pomocy kwadratu szyfrującego z kluczem duże drzewo: mbupovfchbsxmbflihdi

Odpowiedź 6:

Zadanie 7. Zaszyfruj stwierdzenie: JEST TYLKO PIĘĆ WIELOŚCIANÓW FOREMNYCH, klucz: *księga liczb.*

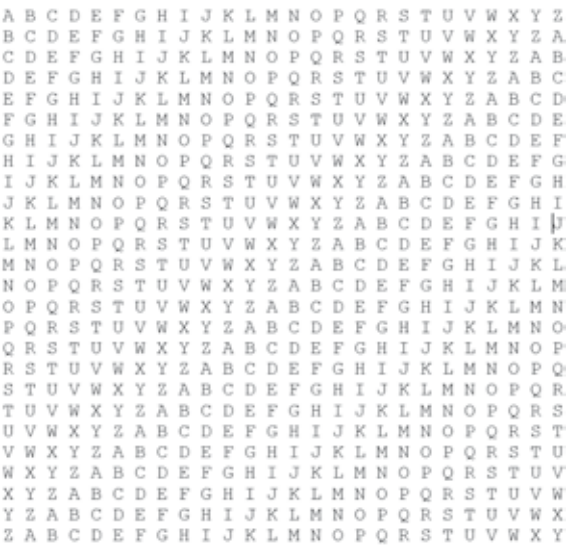
Odpowiedź 7:



J	E	S	T	T	Y	L	K	O	P	I	E	C	W	I	E	L	O	S	C	I	A	N	O	W	F	O	R	E	M	N	Y	C	H
k	s	i	e	g	a	l	i	c	z	b	k	s	i	e	g	a	l	i	c	z	b	k	s	i	e	g	a	l	i	c	z	b	k

Zadanie 8. Odczytaj szyfr, otrzymany za pomocą klucza *smakołyk:* larebdbswbiofygua

Odpowiedź 8:



s	m	a	k	o	l	y	k	s	m	a	k	o	l	y	k	s