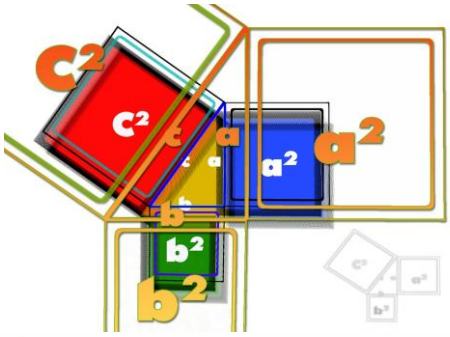
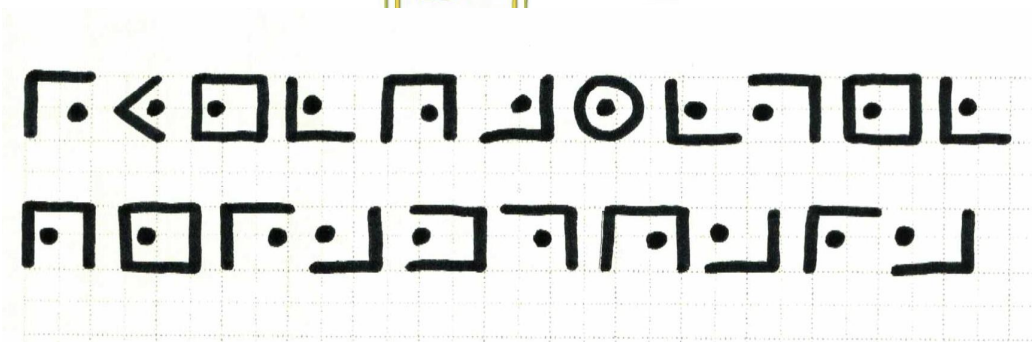
w Jawiszowicach
im. K. I. Gałczyńskiego

ZASZYFROWANA MATEMATYKA





PAWEŁ NAWROCKI

Klasa IV

Zespół Szkolno-Przedszkolny nr 6 w Jawiszowicach

Spis treści

Wstęp…… 3

Skytale …… 5

Szachownica Polibiusza …… 6

Szyfr Cezara …… 7

Alfabet Morse'a …… 8

Szyfr harcerski – czekoladka …… 10

Szyfr harcerski – ułamkowy …… 11

Alfabet semaforowy …… 12

Moje szyfry

Szyfr Minecraft'owy …… 13

Szyfr iloczynowy …… 18

Podsumowanie …… 21

Bibliografia …… 22

Rozwiązania szyfrów …… 23

Opinia o uczniu …… 25

Wstęp

Czy zastanawialiście się kiedyś, jak przekazać komuś poufną wiadomość, by osoby postronne - nawet po przechwyceniu jej - nie odczytały treści? Albo jak wytłumaczyć fakt, że jedni od razu odczytują zaszyfrowane informacje, a inni głowią się nad tym przed długi czas i to bez rezultatu? Takie pytania zrodziły się w mojej głowie po obejrzeniu filmu „Kod Merkury", w którym dziewięcioletni Simon – chłopiec z autyzmem – z łatwością odczytał „najbardziej skomplikowany i najbezpieczniejszy kod Ameryki". Zaciekawiony tematem szyfrowania zacząłem szukać informacji w Internecie i przeglądać książki o kryptologii z biblioteki miejskiej.

Czym jest szyfrowanie?

Jedna z definicji wyjaśnia, że szyfrowanie to po prostu metoda zapisu tekstu jawnego w taki sposób, by stał się on nieczytelny dla osób trzecich. Proces ten nazywany jest szyfrowaniem, a proces odwrotny, czyli zamiana tekstu zaszyfrowanego w możliwy do odczytania, deszyfrowaniem. Do zaszyfrowania i odszyfrowania informacji potrzebny jest algorytm, czyli sposób działania lub klucz, od którego zależy wynik obu procesów.

Okazało się, że nad problemem szyfrowania zastanawiano się od wielu tysięcy lat, a poszukiwanie możliwych rozwiązań stało się bodźcem do rozwoju kryptologii, czyli dziedziny wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem.

Kilka faktów z historii…

Pierwsze zapiski na temat metod szyfrowania znaleziono już w ok. 1500r.p.n.e. w Mezopotamii, na tabliczkach z pismem klinowym. Jednak dopiero Grecy i Rzymianie zrobili z nich pełny użytek, ponieważ w ich kulturach tajna komunikacja stanowiła kluczowy element sukcesu militarnego. Przez kolejne wieki kryptografia rozwijała się powoli, nierównomiernie i przybierała różne formy. Można ją porównać do pewnego rodzaju bitwy na szyfrowanie i deszyfrowanie, gdzie przeciwnikami są strażnicy sekretu (czyli kryptografowie) oraz ci, co mają nadzieję na złamanie szyfru (czyli kryptoanalitycy).

Współcześnie kryptologia jest uznawana za gałąź zarówno matematyki, jak i informatyki; jest także związana z teorią informacji, statystyką, kombinatoryką, teorią liczb, inżynierią oraz bezpieczeństwem komputerowym.

Z punktu widzenia ucznia, także w szkole podczas lekcji używamy czasami znanego tylko sobie szyfru do zakodowania jakiejś informacji lub rozwiązania jakiegoś problemu. Mogą to być szyfry obrazkowe, blokowe, literowe lub cyfrowe, które dla innych są nieczytelne.

W pierwszej części mojej pracy przedstawię krótko najbardziej znane szyfry: np. skytale, szyfr Cezara, szachownicę Polibiusza, alfabet Morse'a i alfabet semaforowy oraz dwa szyfry harcerskie.

Natomiast w drugiej części chciałbym zaprezentować propozycje własnych szyfrów: dwa dla fanów popularnej gry komputerowej Minecraft oraz szyfr iloczynowy. Mam nadzieję, że odszyfrowywanie zakodowanych przeze mnie informacji stanie się nie tylko okazją do ćwiczenia logicznego myślenia, lecz także świetną rozrywką matematyczną.

Życzę miłej lektury!

Paweł Nawrocki

SKYTALE

W V wieku p.n.e. w księgach Herodota pojawiają się fragmenty dotyczące sztuki szyfrowania, stosowane przez starożytnych Spartan. Używano w niej pręta o podstawie wielokąta, na który nadawca nawijał skórzany pas. Tekst pisano na stykających się brzegach, więc po rozwinięciu pasa widać było tylko bezsensowną kombinację liter. Owijano go wokół bioder posłańca, literami do wewnątrz, więc jako przepaska nie wzbudzał żadnych podejrzeń. Aby odczytać zaszyfrowaną wiadomość, potrzebny był skytale o takiej samej grubości, jaką miał pręt nadawcy.

https://pl.wikipedia.org/wiki/Skytale

https://commons.wikimedia.org/wiki/File:Skytala%26EmptyStrip-Shaded.png

Odpowiednikiem spartańskiego skytale może być dzisiaj „wąż literowy”, w którym ukryte jest hasło. Po wykreśleniu niepotrzebnych liter, pozostaną nam te tworzące zaszyfrowaną wiadomość.

Zad. 1

Jaką wiadomość mógłby przekazać Spartanin współczesnemu uczniowi?

AKDROUPKETNCOKEYBZWMQAISMAUKWICSGERĘBRAWOME

TNAWAKOTSETZELANMOSTIKYSZKLQURENDRCEKNDOZLAM

EWBPLASZOASTPLMWERNIAKALKOTBUZNEMSENKPARZOJS

TADGKWOWKLTUWDJVROIWQNCDEKLANPDZAWDLZSEKBDY

DOBWLKSARNALQORNHULASPECPOLFBZWENTA*

* Uwaga: W oryginalnym skytale litery powinny być ułożone pionowo, jedna pod drugą. Tutaj w celu łatwiejszego deszyfrowania są położone koło siebie.

SZACHOWNICA POLIBIUSZA

W II w. p.n.e. grecki pisarz Polibiusz wymyślił stosowany do dziś sposób szyfrowania. Ułożył litery w kwadrat, a rzędy i kolumny ponumerował. Numer wiersza i kolumny, czyli współrzędne, kodowały konkretną literę.

	1	2	3	4	5
1	**A**	**B**	**C**	**D**	**E**
2	**F**	**G**	**H**	**I/J**	**K**
3	**L**	**M**	**N**	**O**	**P**
4	**Q**	**R**	**S**	**T**	**U**
5	**V**	**W**	**X**	**Y**	**Z**

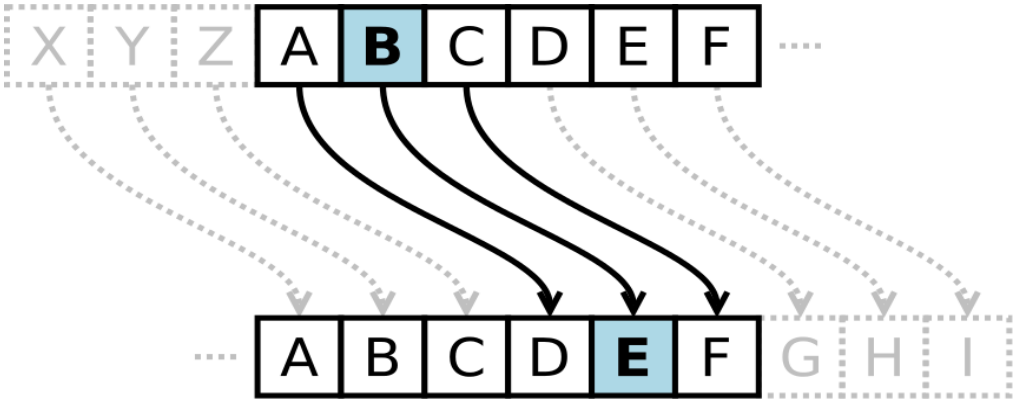
Zad. 2

Jaką myśl zapisaną szyfrem Polibiusza chciałby przekazać autor niniejszej pracy?

32-11-44-15-32-11-44-54-25-11-44-34-32-34-24-11-35-11-43-24-11

SZYFR CEZARA

Kolejny sposób szyfrowania pochodzi od Juliusza Cezara, który szyfrował swoją korespondencję z przyjaciółmi. Jest to technika polegająca na przesunięciu liter o stałą wartość. Cezar, zamiast danej litery, wpisywał literę występującą w alfabecie o trzy miejsca dalej, dlatego metoda ta nazwana została szyfrem przesuwającym, kodem Cezara lub przesunięciem Cezariańskim.



https://commons.wikimedia.org/wiki/File:Caesar3.svg

Samo przesunięcie liter byłoby jednak zbyt proste, dlatego Cezar dodatkowo układał swoje wiadomości tak, aby liczba liter w wiadomości była pełnym kwadratem. Potem zapisywał je właśnie w taki kwadrat, pisząc w pionie n liter w n rzędach. Następnie wiadomość przepisywał normalnie, ale rzędami, nie kolumnami. Odbiorca stosował procedurę odwrotną.
Współcześnie szyfru Cezara używa się z przesunięciem 13 (ROT 13).

Zad. 3
Co jest potrzebne do rozwiązywania zagadek, szyfrów i łamigłówek matematycznych?

Hasło przed wpisaniem do kwadratu Cezara:

O	**R**	**J**	**L**	**N**	**D**	**P**	**D**	**W**	**H**	**P**	**D**	**W**	**B**	**N**	**D**

Hasło zapisane w kwadracie Cezara:

O	**N**	**W**	**W**
R	**D**	**H**	**B**
J	**P**	**P**	**N**
L	**D**	**D**	**D**

Hasło po całkowitym zaszyfrowaniu:

O	**N**	**W**	**W**	**R**	**D**	**H**	**B**	**J**	**P**	**P**	**N**	**L**	**D**	**D**	**D**

ALFABET MORSE'A

Ten specjalny sposób szyfrowania został stworzony przez Samuela Morse'a i Alfreda Vaila w 1840 roku. Stosowany był w telekomunikacji radiowej, w prowadzeniu międzynarodowej korespondencji, przy użyciu linii telegraficznych, podwodnych kabli i obwodów radiowych.

Każda litera alfabetu jest reprezentowana w zapisie przez specjalny, stały układ kropek i kresek. W telekomunikacji znaki są przekazywane za pomocą dźwięków, błysków światła, impulsów elektrycznych, przy czym sygnał krótki odpowiada kropce, a długi kresce.

Alfabet Morse'a najlepiej zapamiętać za pomocą haseł, które dzielimy na sylaby. Kreska odpowiada sylabie zawierającej samogłoskę „O" lub „Ó", a kropka – sylabie zawierającej każdą inną samogłoskę. Odstęp pomiędzy poszczególnymi znakami zaznaczamy jedną kreską ukośną (/), a odstęp pomiędzy grupami znaków – dwiema kreskami (//).

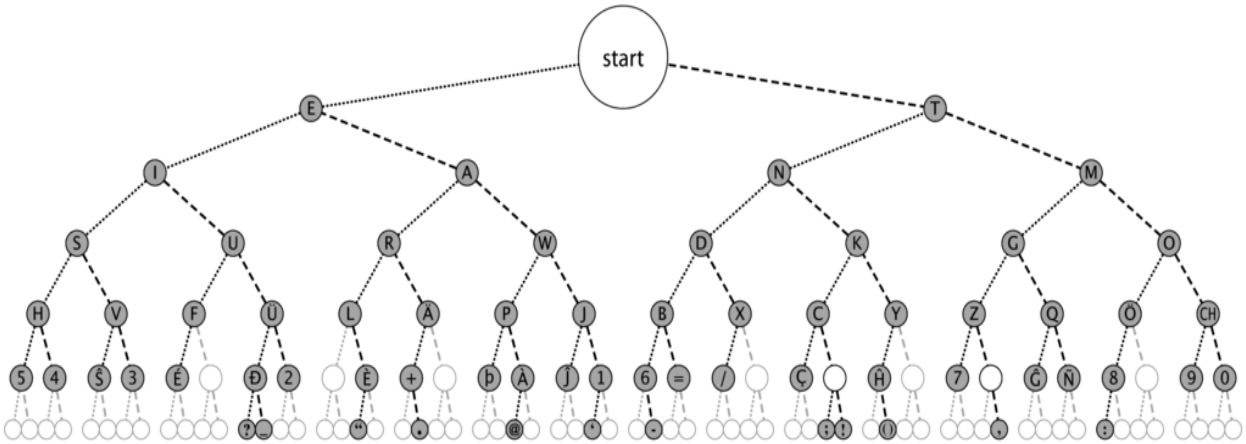
Obecnie alfabet Morse'a używany jest przez radioamatorów i harcerzy☺

LITERA	KOD	**HASŁO** ułatwiające zapamiętanie
A	● —	A-ZOT
B	— ● ● ●	BO-TA-NI-KA
C	— ● — ●	CO-MI-ZRO-BISZ
D	— ● ●	DO-LI-NA
E	●	EŁK
F	● ● — ●	FI-GA-SŁOD-KA
G	— — ●	GO-SPO-DA
H	● ● ● ●	HA-LA-BAR-DA
I	● ●	I-GŁA
J	● — — —	JED-NO-KON-NO
K	— ● —	KO-LA-NO
L	● — ● ●	LE-O-NI-DAS
M	— —	MO-TOR
N	— ●	NO-GA
O	— — —	O-POCZ-NO
P	● — — ●	PE-LO-PO-NEZ
Q	— — ● —	
R	● — ●	RE-TOR-TA
S	● ● ●	SA-HA-RA
T	—	TOM
U	● ● —	UR-SY-NÓW
V	● ● ● —	
W	● — —	WI-NO-ROŚL
X	— ● ● —	YORK-HULL-OX-FORD
Y	— ● — —	YO-GUR-TO-WO
Z	— — ● ●	ZŁO-TO-RY-JA

CYFRY	
1	● — — — —
2	● ● — — —
3	● ● ● — —
4	● ● ● ● —
5	● ● ● ● ●
6	— ● ● ● ●
7	— — ● ● ●
8	— — — ● ●
9	— — — — ●
0	— — — — —

POLSKIE ZNAKI	
Ą	● — ● —
Ć	— ● — ● ●
Ę	● ● — ● ●
Ł	● — ● ● —
Ń	— — ● — —
Ó	— — — ●
Ś	● ● ● — ● ● ●
Ż	— — ● ● — ●
Ź	— — ● —

Pomocą przy odczytywaniu znaków może też być poniższy diagram. Należy poruszać się w dół diagramu w zależności od tego, czy odbierana jest kropka, czy kreska.



https://commons.wikimedia.org/wiki/File:Morse_code_tree3.png

Zad. 4

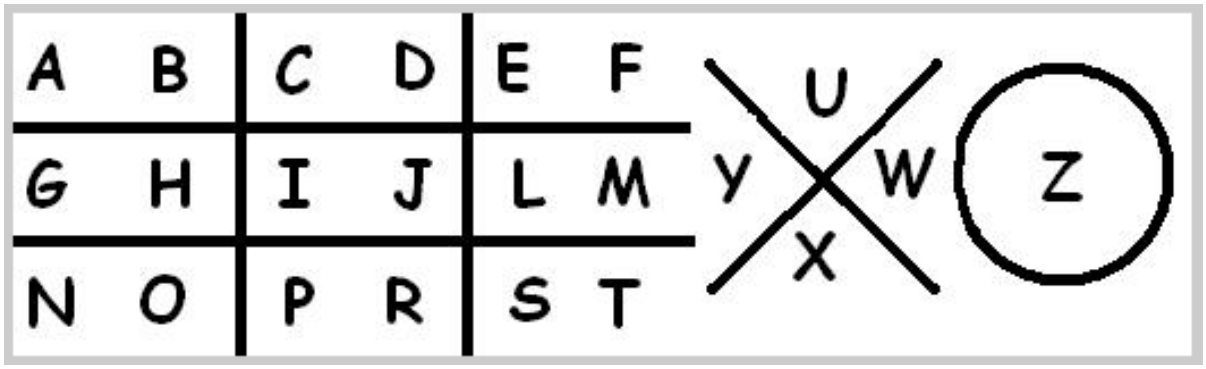
Co sprawia uczniom trudność na lekcjach matematyki?

// • — — / — • — — / • — • / • — / — — • • — • / • / — • / • • / • — //

// • — / • — • • / — — • / • / — • • • / • — • / • — / • • / — • — • / — — • • / — • / • //

SZYFR HARCERSKI - CZEKOLADKA

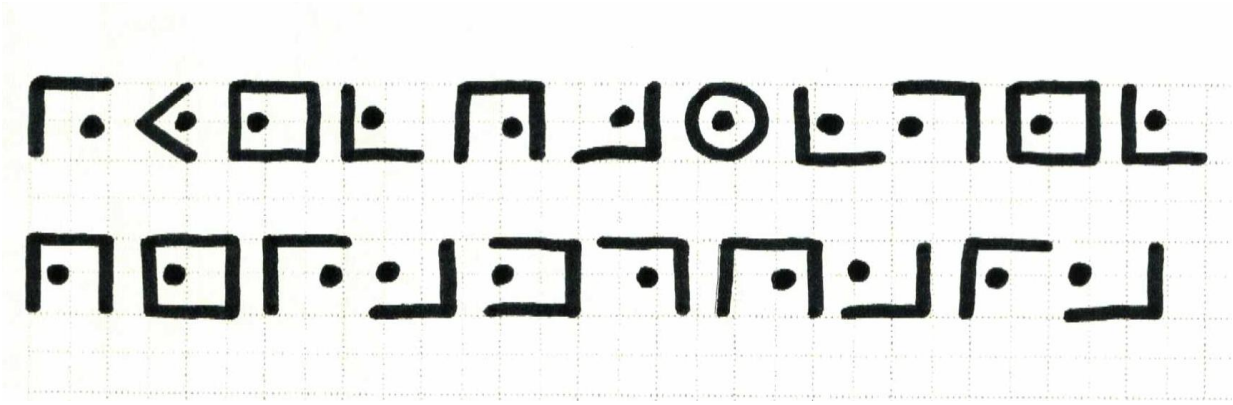
Szyfr ten w odróżnieniu od prostych szyfrów różni się tym, że literę zastępuje się obrazkiem, a nie inną literą. Szyfrując - w miejsce litery wstawiamy kropkę. Kluczem do tego szyfru są literki powpisywane w ramkę w następujący sposób:



http://pisdh.sopot.zhp.pl/poradnik-harcerski/szyfry/

Zad. 5

Jakie znane twierdzenie dotyczące trójkątów prostokątnych przedstawia wzór: $a^2+b^2=c^2$?

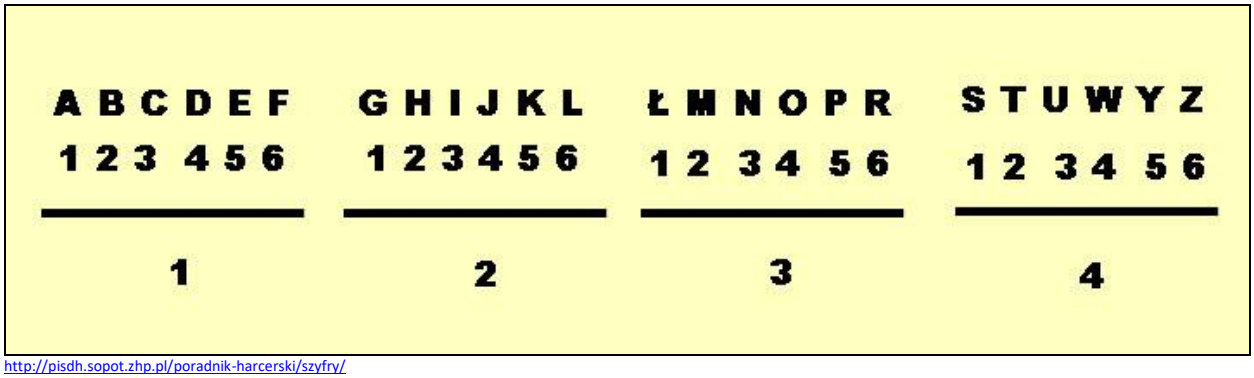


SZYFR HARCERSKI – UŁAMKOWY

Litery szyfru zapisane są w formie ułamka. Aby szyfr był regularny, w każdym ułamku musi być tyle samo liter, więc istnieją wersje, gdzie są: 1, 3, 4, 6, 8, 12, 24 grupy ułamków. Najpopularniejszymi są grupy 4 i 6.

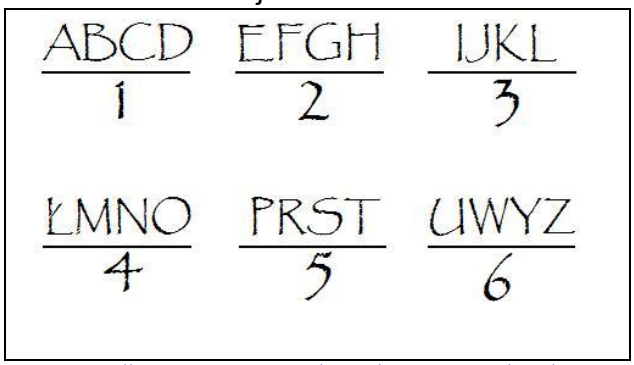
Aby zaszyfrować słowo, wyszukujemy konkretną literę i zapisujemy ją w formie ułamka. Licznik wskazuje na kolejność litery w danej grupie, a mianownik - która jest to grupa.

Wersja 4-ułamkowa



http://pisdh.sopot.zhp.pl/poradnik-harcerski/szyfry/

Wersja 6-ułamkowa



https://6pdhdziupla.wordpress.com/druzyna/techniki-harcerskie/szyfry/

Zad. 6

Do jakiego wspólnego zbioru należą kwadrat, prostokąt, trójkąt, romb, trapez i koło?

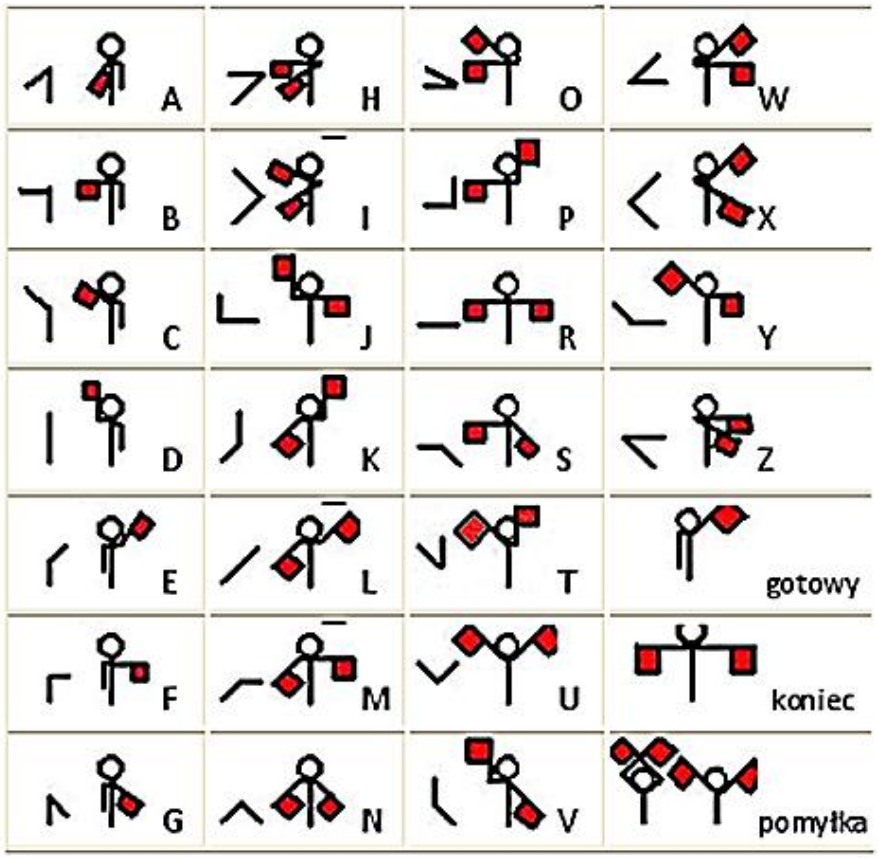
6 3 1 3 6 5 1 5 4 2 5 2 6 5 3 6 3 5 wersja 4-ułamkowa
1 2 2 4 3 4 2 1 3 3 1 4 3 4 1 4 3 1

2 1 3 1 2 3 3 1 4 2 1 4 2 3 3 4 3 1 wersja 6-ułamkowa
2 3 2 6 5 6 2 2 4 4 2 5 5 6 1 6 4 2

ALFABET SEMAFOROWY

Alfabet semaforowy stosowany był dawniej w żegludze. Jest to kod naśladujący alfabet, złożony ze znaków nadawanych przez marynarza przy pomocy trzymanych w rękach chorągiewek. Każde ułożenie obu rąk z chorągiewkami oznacza inną literę, cyfrę lub znak specjalny.

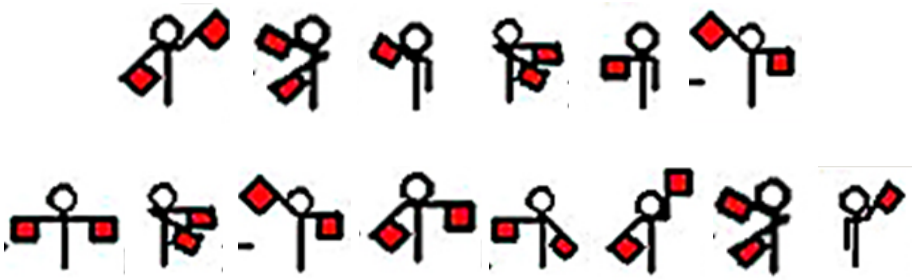
Do sygnalizacji używa się chorągiewek o wymiarach 40 x 40 cm w dwóch kontrastujących kolorach, które łączy się po przekątnej albo tarcz sygnalizacyjnych o wymiarach 40 x 40 cm z uchwytami pośrodku.



http://www.zhppgk.org/organizacja_harcerek/egazetka_6/gazetka_6_technika.htm

Zad. 7

Liczby zapisywane za pomocą liter, używane przez mieszkańców starożytnego imperium?



MOJE SZYFRY

SZYFR MINECRAFT'OWY

Minecraft – to popularna gra komputerowa, w której świat zbudowany jest z obiektów 3D, głównie sześcianów. Gracz buduje konstrukcje składające się z bloków (np. trawa, kamień, drewno, lawa, ogień itp.), które umieszcza w trójwymiarowej siatce; może je też rozbijać i tworzyć inne bloki lub przedmioty. Można tworzyć wszystko, a jedynym ograniczeniem jest wyobraźnia - tutaj trzeba wyobrazić sobie całą strukturę i nauczyć się szukać w niej powtarzających się wzorców. Budowanie w Minecraft pozwala ćwiczyć wyobraźnię przestrzenną, uczy obliczać potrzebną ilość bloków do zbudowania jakiegoś obiektu czy świata. W Internecie można znaleźć wiele stron, gdzie z pomocą tej gry komputerowej można świetnie uczyć się matematyki.

Szyfr Minecraft'owy stworzyłem z myślą o wszystkich fanach tej gry komputerowej. Najpierw wykorzystałem fakt, że każdy blok ma swoją ikonę i swoje ID. Potem, bazując na nazwach bloków lub podobieństwie ikon do liter, zestawiłem cały alfabet. W ten sposób powstał szyfr ikonowy i szyfr ID-blokowy.

Oryginalne ikony i ID poszczególnych bloków:

Ikona	Dec	Hex	Nazwa
	00	00	Powietrze
	01	01	Kamień
	02	02	Blok trawy
	03	03	Ziemia
	04	04	Bruk
	05	05	Deski
	06	06	Sadzonka
	07	07	Skała macierzysta
	08	08	Woda
	09	09	Stała woda
	10	0A	Lawa
	11	0B	Stała lawa
	12	0C	Piasek
	13	0D	Żwir
	14	0E	Ruda złota
	15	0F	Ruda żelaza
	16	10	Ruda węgla
	17	11	Drewno
	18	12	Liście

Ikona	Dec	Hex	Nazwa
	40	28	Czerwony grzyb
	41	29	Blok złota
	42	2A	Blok żelaza
	43	2B	Złączone płyty
	44	2C	Płyta
	45	2D	Cegły
	46	2E	TNT
	47	2F	Biblioteczka
	48	30	Zamszony bruk
	49	31	Obsydian
	50	32	Pochodnia
	51	33	Ogień
	52	34	Spawner potworów
	53	35	Schody
	54	36	Skrzynia
	55	37	Przewód z czerwonego kamienia
	56	38	Ruda diamentu
	57	39	Blok diamentu
	58	3A	Stół rzemieślniczy

Ikona	Dec	Hex	Nazwa
	80	50	Śnieg (blok)
	81	51	Kaktus
	82	52	Blok gliny
	83	53	Trzcina cukrowa
	84	54	Szafa grająca
	85	55	Płot
	86	56	Dynia
	87	57	Netherrack
	88	58	Piasek dusz
	89	59	Jasnogłaz
	90	5A	Portal do Netheru
	91	5B	Jack o'Lantern
	92	5C	Ciasto
	93	5D	Przekaźnik (Wyłączony)
	94	5E	Przekaźnik (Włączony)
	95	5F	Barwione szkło
	96	60	Klapa
	97	61	Blok z ukrytym potworem
	98	62	Kamienne cegły

Ikona	Dec	Hex	Nazwa
	120	78	Rama portalu Kresu
	121	79	Kamień Kresu
	122	7A	Jajo Smoka
	123	7B	Lampa (Wyłączona)
	124	7C	Lampa (Włączona)
	125	7D	Podwójna drewniana płyta
	126	7E	Drewniana płyta
	127	7F	Roślina kakao
	128	80	Schody z piaskowca
	129	81	Ruda szmaragdu
	130	82	Skrzynia Kresu
	131	83	Zaczep na linkę
	132	84	Linka
	133	85	Blok szmaragdu
	134	86	Drewniane schody
	135	87	Drewniane schody
	136	88	Drewniane schody
	137	89	Blok poleceń
	138	8A	Magiczna latarnia

https://minecraft-pl.gamepedia.com/Warto%C5%9Bci_danych

19	13	Gąbka
20	14	Szkło
21	15	Ruda lazurytu
22	16	Blok lazurytu
23	17	Dozownik
24	18	Piaskowiec
25	19	Blok dźwiękowy
26	1A	Łóżko
27	1B	Zasilane tory
28	1C	Tory z czujnikiem
29	1D	Lepki Tłok
30	1E	Pajęczyna
31	1F	Trawa
32	20	Uschnięty krzew
33	21	Tłok
34	22	Głowica tłoku
35	23	Wełna
36	24	Blok 36
37	25	Mniszek Lekarski
38	26	Mak
39	27	Brązowy grzyb
59	3B	Nasiona pszenicy
60	3C	Pole uprawne
61	3D	Piec
62	3E	Rozpalony piec
63	3F	Tabliczka postawiona na podłodze
64	40	Drewniane Drzwi
65	41	Drabina
66	42	Tory
67	43	Brukowe schody
68	44	Tabliczka postawiona na ścianie
69	45	Dźwignia
70	46	Kamienna Płyta naciskowa
71	47	Żelazne drzwi
72	48	Drewniana Płyta naciskowa
73	49	Ruda czerwonego kamienia
74	4A	Świecąca ruda czerwonego kamienia
75	4B	Wyłączona czerwona pochodnia
76	4C	Włączona czerwona pochodnia
77	4D	Kamienny Przycisk
78	4E	Śnieg (pokrywa)
79	4F	Lód
99	63	Wielki brązowy grzyb
100	64	Wielki czerwony grzyb
101	65	Kraty
102	66	Szyba
103	67	Arbuz (blok)
104	68	Łodyga dyni
105	69	Łodyga arbuza
106	6A	Pnącze
107	6B	Furtka
108	6C	Schody z cegły
109	6D	Schody z kamiennej cegły
110	6E	Grzybnia
111	6F	Lilia wodna
112	70	Blok netherowej cegły
113	71	Płot z netherowej cegły
114	72	Schody z netherowej cegły
115	73	Brodawka
116	74	Stół do zaklęć
117	75	Statyw alchemiczny
118	76	Kocioł
119	77	Portal Endu
139	8B	Brukowy murek
140	8C	Doniczka
141	8D	Marchewka (Zasadzona)
142	8E	Ziemniak (Zasadzony)
143	8F	Drewniany przycisk
144	90	Głowa
145	91	Kowadło
146	92	Skrzynia-pułapka
147	93	Wagowa płyta naciskowa (Złota)
148	94	Wagowa płyta naciskowa (Żelazna)
149	95	Komparator (Wyłączony)
150	96	Komparator (Włączony)
151	97	Detektor światła dziennego
25px	152	98 Blok czerwonego kamienia
153	99	Ruda Netherowego kwarcu
154	9A	Lej
155	9B	Blok netherowego kwarcu
156	9C	Schody z kwarcu
157	9D	Tory aktywujące
158	9E	Podajnik
159	9F	Barwiona glina

https://minecraft-pl.gamepedia.com/Warto%C5%9Bci_danych

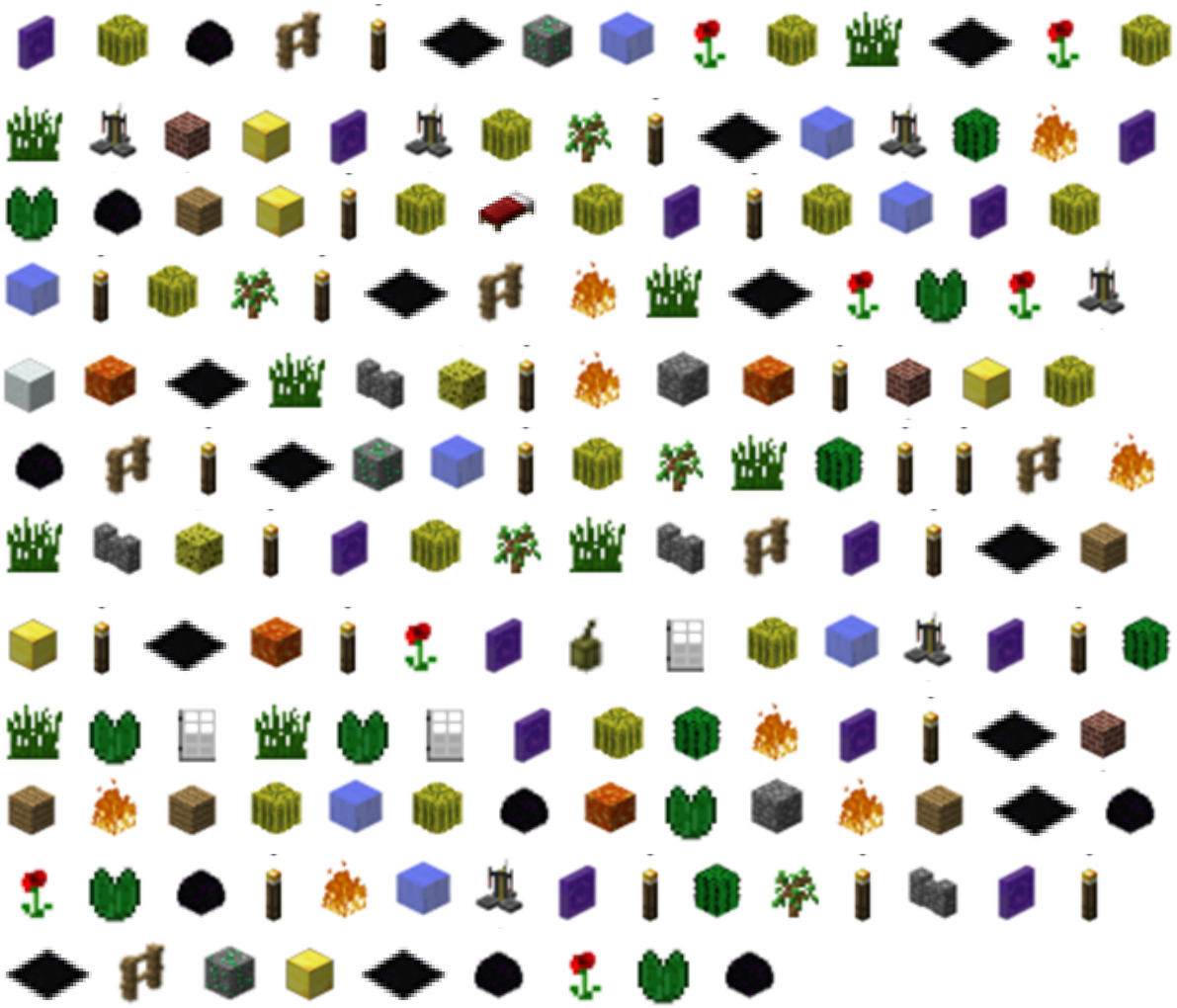
SZYFR MINECRAFT'OWY

LITERA	NAZWA BLOKU	SZYFR IKONOWY	SZYFR ID-BLOKOWY
A	ARBUZ		10367
B	BRUK		0404
C	CEGŁY		452D
D	DESKI		0505
E	END (PORTAL ENDU)		11977
F	FURTKA		1076B
G	GĄBKA		1913
H	TORY		6642
I	POCHODNIA		5032
J	JAJO SMOKA		1227A
K	KAKTUS		8151
L	LAWA		100A

M	MAK		3826
N	NETHER (PORTAL NETHERU)		905A
O	OGIEŃ		5133
P	PŁOT		8555
R	RUDA SZMARAGDU		12981
S	SADZONKA		0606
T	TRAWA		311F
U	LILIA WODNA		1116F
V	DREWNIANE SCHODY		13587
W	WODA		0808
X	DETEKTOR ŚWIATŁA DZIENNEGO		15197
Y	STATYW ALCHEMICZNY		11775
Z	BLOK ZŁOTA		4129
Ć	CZERWONY GRZYB		4028
Ś	ŚNIEG		8050
Ń	KRATY		10165
Ł	ŁÓŻKO		261A
Ż	ŻELAZNE DRZWI		7147
Ó	ROŚLINA KAKAO		1277F
Ę	BRUKOWY MUREK		1398B
Ą	USCHNIĘTY KRZEW		3220

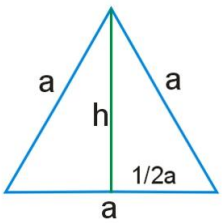
Zad. 8a

Jak zapamiętać kolejność wykonywania działań? Aby rozwiązać zagadkę, wykorzystaj szyfr ikonowy.



Zad. 8b

Jak zapamiętać prosty wzór na obliczanie pola trójkąta?
Aby rozwiązać zagadkę, wykorzystaj szyfr ID-blokowy.



85555133100A10367311F129811277F1227A81513220
311F10367905A503211977100A5032452D4129905A10
367513381515133382690 5A1277F714785551277F261
A855551330505060631 1F1036708081177512981103 6
741291177508081177506065133815151338050402 8☺

SZYFR ILOCZYNOWY

1. Pierwszym krokiem utworzenia szyfru iloczynowego jest zapisanie każdej litery jako liczby będącej wynikiem mnożenia przynajmniej trzech liczb pierwszych.

Przykład: A → 105 = 3 · 5 · 7

2. Następnie znajdujemy trzy dowolne kombinacje mnożenia, ale teraz dwóch czynników z podanej wcześniej liczby.

Przykład:		A → 105 = (3 · 5) · 7	czyli 15 · 7	albo	7 · 15
	lub:	A → 105 = 3· (5 · 7)	czyli 3 · 35	albo	35 · 3
	lub:	A → 105 = (3·7) · 5	czyli 21 · 5	albo	5 · 21

3. Kolejny krok - dopisujemy przed wybrany czynnik liczbę, która odpowiada ilości cyfr tego czynnika. Kasujemy też znak mnożenia.

21517	albo	17215
13235	albo	23513
22115	albo	15221

4. Na koniec stawiamy przed całością liczbę, która pokazuje, z ilu cyfr składa się cała liczba.

521517	albo	517215
513235	albo	523513
522115	albo	515221

W ten oto sposób powstaje szyfr – zapis litery A w sześciu różnych kombinacjach.

Podobnie postępujemy z każdą kolejną literą alfabetu oraz z cyframi. Jest to czasochłonne, wymaga logicznego myślenia, spostrzegawczości, umiejętności kombinacji, ale w wyniku tych operacji powstaje szyfr „nie do złamania”, ponieważ za każdym razem pisząc tą samą literę lub cyfrę, możemy wybrać jeden z 6 wariantów szyfru ☺

znak	iloczyn - 3 czynniki	wynik mnożenia	3 z 6 możliwości zapisu szyfru		
A	3·5·7	105	521517	513235	522115
Ą	11· 5·3	165	525513	6211215	523315
B	7·11·5	385	6235211	527715	525517
C	11·3·7	231	523317	527713	6221211
Ć	13·5·7	455	526517	6235213	529115
D	5·3·13	195	6215213	523915	513265
E	13·7·19	1729	6291219	73133213	6324717
Ę	13·11·7	1001	6211291	6213277	6314317
F	5·11·13	715	6255213	6265211	6153143
G	3·11·13	429	6213233	6239211	6314313
H	17·3·5	255	6215217	525115	513285
I	5·17·7	595	6217235	528517	6311915
J	3·7·17	357	6221217	517251	6133119
K	11·7·17	1309	6277217	73119211	6173187
L	5·11·17	935	6255217	6211285	6318715
Ł	11·17·3	561	6233217	6211251	6133187
M	13·17·11	2431	73221211	73143217	73187213
N	13·17·7	1547	6173221	6291217	72133119
Ń	3·13·17	663	6239217	6251213	6322113
O	13·5·17	1105	6265217	6322115	6285213
Ó	2·3·5	30	41615	521013	521512
P	5·2·7	70	521017	523512	521415
Q	2·7·3	42	521413	41617	522112
R	11·7·2	154	522217	6214211	512277
S	2·11·3	66	516211	523312	522213
Ś	2·5·11	110	6211210	512255	515222
T	2·13·3	78	522613	523912	516213
U	13·5·2	130	526512	6210213	522615
V	7·2·13	221	6214213	522617	512291
W	2·13·11	286	6123143	6226211	6222213
X	17·2·3	102	523413	516217	525112
Y	2·17·5	170	6210217	528512	523415
Z	17·7·2	238	6217214	523417	6123119
Ź	2·11·17	374	6222217	6218712	6211234
Ż	2·17·13	442	6123221	6226217	6234213

1	2·3·19	114	516219	523813	512257
2	2·7·19	266	6219214	517238	6313312
3	19·5·2	190	523815	6210219	512295
4	5·7·19	665	6235219	6313315	529517
5	3·19·5	285	6215219	529513	525715
6	7·19·3	399	6219221	525717	6133133
7	19·11·3	627	6233219	6211257	6320913
8	11·5·19	1045	6219255	6295211	6153209
9	19·2·13	494	6238213	6226219	6123247
0	19·11·13	2717	73247211	73143219	72133209

Zad. 9

Matematyki najlepiej uczyć się na wesoło, w formie zabawy, rymowanek, wierszyków, zagadek. Oto jedna z nich:

6213233513265528512621521362652175132655221155172516211
2916285213621521373133213622121773221211621021361331196
2132776213233613318741615612314361731875215175162116123
1195285125277157311921162852137322121162172355235125122
7751323552331762102136221217632471762262115162116123119
6210217523312522613627721763221155210176217235631431773
1192116173221631191563247175233126217235621129152221352
6512731432175265126221217731332137322121162652175172515
1323562222135285176291219621521352341752151752141552221
7632211552331762912197213311952261362102135172516291219
6291219627721762652176173221628521373221211528517522115
5234175132355222175234175255136215213621721452151762912
1762172356291219516213632211562552135285176173221522115
6291217523312521013622621161331196291219523312522613521
0176322115523417721331195215176291217621723573133213623
5211513235522217612314361732215221155235125122776217214
5285125222136217214613318762652176211210526517732212116
3119155233126217235621327752331262912176210213622121773
1332137314321752151751621373221211621327773119211513235
6123221621521352851251326562172145285175122555222135226
1362102136215213631191552651262212177313321 3

Podsumowanie

Kryptografia i bezpieczne przekazywanie poufnych wiadomości przez wieki były sprawą najwyższej wagi. Wraz z pojawieniem się pierwszych maszyn szyfrujących i maszyn służących do łamania szyfrów nastąpił punkt zwrotny w tej dziedzinie. Dziś, w dobie informacji, nie ma w zasadzie żadnego kanału przesyłania danych, który nie byłby zakodowany w ten czy inny sposób, zaś bezpieczeństwo i poufność komunikacji w cyfrowym świecie zależą od skomplikowanych szyfrów tworzonych przez matematyków. Kodowanie, szyfrowanie i odszyfrowywanie nie byłoby w ogóle możliwe bez matematyki oraz wybitnych matematyków.

Nie można tutaj nie wspomnieć o szyfrach wojny, np. szyfrantach z plemienia Nawaho czy maszynie szyfrującej Enigmie i związanych z nią polskich kryptologach: Marianie Rejewskim, Henryku Zygalskim i Jerzym Różyckim. To oni jako pierwsi złamali kod Enigmy, a dzięki temu znacznie przyczynili się do zwycięstwa aliantów podczas II wojny światowej. Ale to już temat na kolejną pracę…

Mam nadzieję, że lektura niniejszej pracy i deszyfrowanie zakodowanych wiadomości było dla Państwa przyjemnością i matematyczną zabawą.

Poprawność szyfrów testowali również: moja siostra gimnazjalistka, mój 10-letni kuzyn oraz moi rodzice.

Paweł Nawrocki

Bibliografia:

Gomez J.: *Matematycy, szpiedzy i hakerzy. Kody i szyfry*. Toruń, RBA, 2010.
Kahn D.: *Łamacze kodów; historia kryptologii.* Warszawa, WNT, 2004.
Singh S.: *Księga szyfrów.* Warszawa, Albatros, 2001.

Netografia:

http://home.agh.edu.pl/~zobmat/2016/3_rogowskipiotr/

https://mlodytechnik.pl/eksperymenty-i-zadania-szkolne/wynalazczosc/28431-szyfry

http://www.eszkola-wielkopolska.pl/eszkola/projekty/gimnazjum4szamotuly/enigmatyczny/php/11.php

https://education.minecraft.net/

https://github.com/BetaAndBit/MathCraft/wiki

http://di.com.pl/nauczyciele-uzywajacy-minecrafta-laczcie-sie-52542

http://maga.witrynaszkolna.pl/strona=wiersze

http://www.gazetka_matematyczna.republika.pl/wiersze_uczniow.htm

Rozwiązania szyfrów

Zad. 1

AKDROUPKETNCOKEYBZWMQAISMAUKWICSGERĘBRAWOME

TNAWAKOTSETZELANMOSTIKYSZKLQURENDRCEKNDOZLAM

EWBPLASZOASTPLMWERNIAKALKOTBUZNEMSENKPARZOJS

TADGKWOWKLTUWDJVROIWQNCDEKLANPDZAWDLZSEKBDY

DOBWLKSARNALQORNHULASPECPOLFBZWENTA

Hasło: Ucz się matmy, ucz – bo matma to wiedzy klucz!

Zad. 2

M	A	T	E	M	A	T	Y	K	A	T	O	M	O	J	A	P	A	S	J	A
32	11	44	15	32	11	44	54	25	11	44	34	32	34	24	11	35	11	43	24	11

Zad. 3

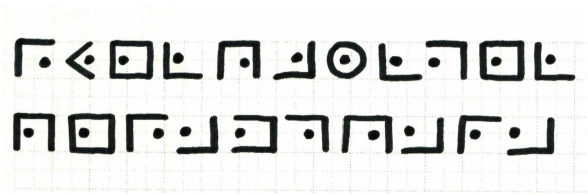
O	N	W	W	R	D	H	B	J	P	P	N	L	D	D	D
L	O	G	I	K	A	M	A	T	E	M	A	T	Y	K	A

Zad. 4 WYRAŻENIA ALGEBRAICZNE

// • — — / — • — — / • — • / • — / — — • • — • / • / — • / • • / • — //

// • — / • — • • / — — • / • / — • • • / • — • / • — / • • / — • — • / — — • • / — • / • //

Zad. 5 TWIERDZENIE PITAGORASA

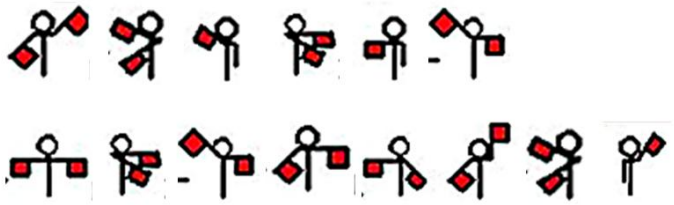


Zad. 6 FIGURY GEOMETRYCZNE

$$\frac{6}{1}\ \frac{3}{2}\ \frac{1}{2}\ \frac{3}{4}\ \frac{6}{3}\ \frac{5}{4}\ \frac{1}{2}\ \frac{5}{1}\ \frac{4}{3}\ \frac{2}{3}\ \frac{5}{1}\ \frac{2}{4}\ \frac{6}{3}\ \frac{5}{4}\ \frac{3}{1}\ \frac{6}{4}\ \frac{3}{3}\ \frac{5}{1}$$ wersja 4-ułamkowa

$$\frac{2}{2}\ \frac{1}{3}\ \frac{3}{2}\ \frac{1}{6}\ \frac{2}{5}\ \frac{3}{6}\ \frac{3}{2}\ \frac{1}{2}\ \frac{4}{4}\ \frac{2}{4}\ \frac{1}{2}\ \frac{4}{5}\ \frac{2}{5}\ \frac{3}{6}\ \frac{3}{1}\ \frac{4}{6}\ \frac{3}{4}\ \frac{1}{2}$$ wersja 6-ułamkowa

Zad. 7 LICZBY RZYMSKIE



Zad. 8a

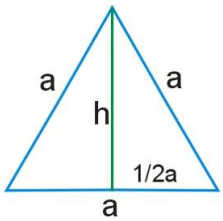
Najpierw matematyczny Asie,
wykonuj działania w nawiasie.

Potem umyśle tęgi,
obliczaj pierwiastki i potęgi.

Następnie dziel i mnóż,
a wynik tuż-tuż.

Na koniec dodawaj lub odejmuj,
i o wynik się nie przejmuj.

Zad 8b.



Pola trójkąta nie licz na oko, mnóż pół podstawy razy wysokość.

Zad. 9

Gdy dodaję, odejmuję,
Główka szybko mi pracuje
Wszystko pięknie się sumuje
Moja wiedza procentuje.

Ekonomia, zarządzanie
To finansów jest poznanie.
Barwna przyszłość mi się snuje
Matmę każdy dziś studiuje.

(Autor: Krystian Kamiński „Moje marzenie”)