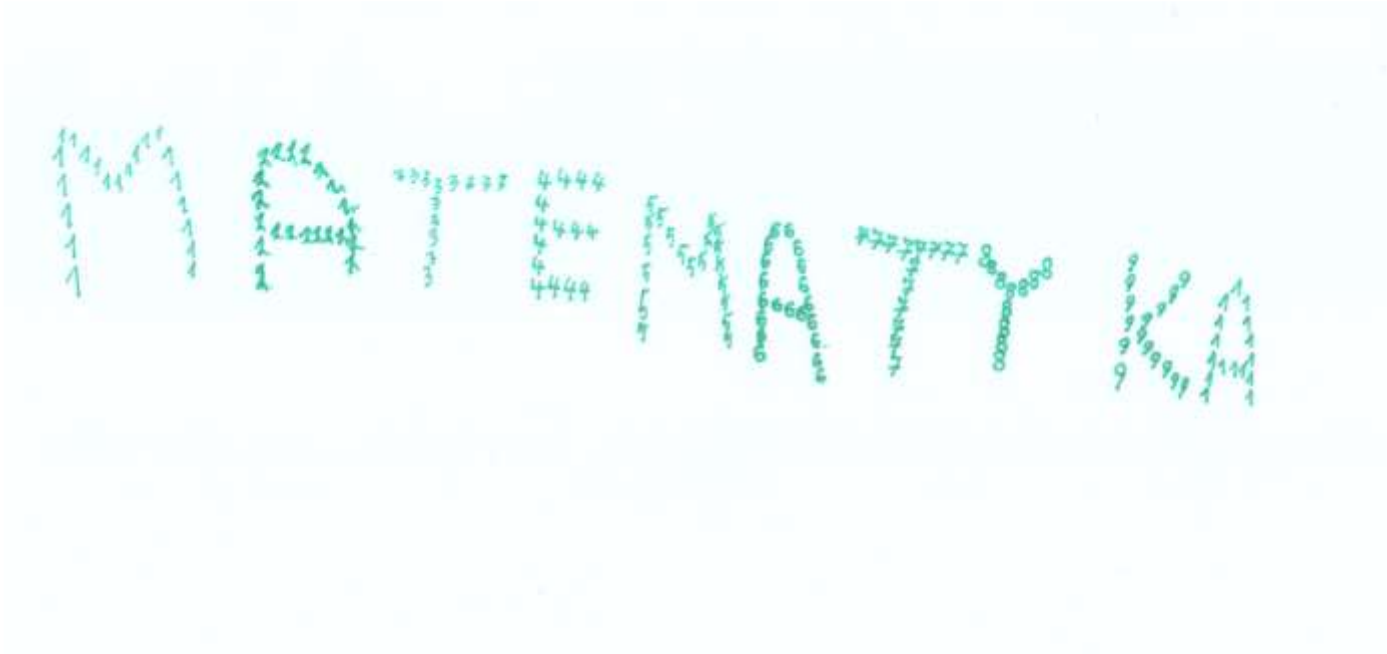


Autorki : Julia Taborska , Urszula Wolska

klasa 5a, Szkoła Podstawowa Nr 1 z Oddziałami Integracyjnymi w Chrzanowie

ul. Borelowskiego 1, 32 – 500 Chrzanów

tel/fax 32623 28 44

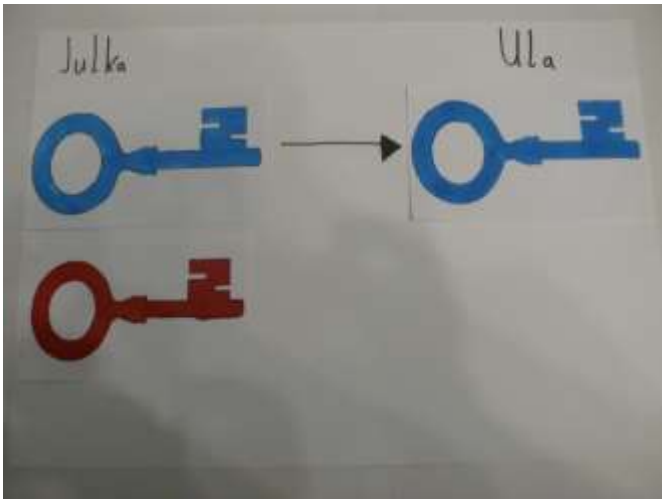
opiekun: Anna Szwancyber

Kryptograficzny algorytm szyfrujący pospolicie nazywamy szyfrem . Jest to funkcja matematyczna, która służy do szyfrowania lub deszyfrowania tekstu jawnego . Tekst jawny to zrozumiała informacja przed zaszyfrowaniem. Algorytm może być :

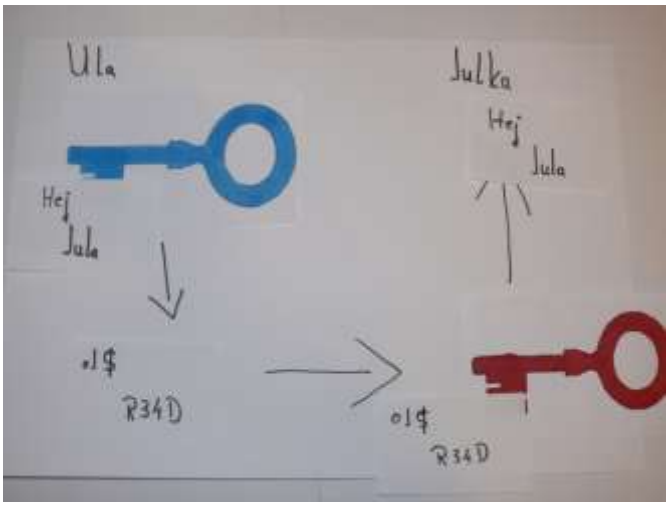
1. ograniczony - bezpieczeństwo szyfrogramu jest zapewnione wtedy kiedy nie jest znana postać algorytmu
2. algorytm z kluczem – bezpieczeństwo wiadomości oparte jest na kluczu (określa on przede wszystkim porządek liter w alfabecie szyfrowym, ustawienia na maszynie szyfrującej, wzorzec dokonywania zmian w przestawieniu)
   a) algorytmy symetryczne – klucz szyfrujący może być określony z klucza deszyfrującego a klucz deszyfrujący wyznaczony z klucza szyfrującego

Możemy wyróżnić algorytmy strumieniowe oraz blokowe . W tych pierwszych informacja przetwarzana jest po jednym bicie , natomiast w drugich wiadomość przetwarzana jest blokami bitów (bit to najmniejsza ilość informacji potrzebna do określenia , który z dwóch równie prawdopodobnych stanów przyjął układ) **.** Przykłady szyfrów blokowych : DES, AES , BLOWFISH, DESX , IDEA, LUCIFER , MARS , SERPENT .

   b) algorytmy z kluczem publicznym – nie można określić klucza deszyfrującego z klucza szyfrującego , klucz publiczny (szyfrujący) nie jest taki sam jak klucz prywatny (deszyfrujący)



Julka przesyła swój klucz publiczny do Uli (klucz niebieski – klucz publiczny , klucz czerwony – klucz prywatny) .



Ula zaszyfruje wiadomość do Julki kluczem publicznym. Julka po otrzymaniu zaszyfrowanej informacji rozszyfruje ją swoim kluczem prywatnym.

Historia szyfrowania jest bardzo długa. Początkowo trzeba było stworzyć taki szyfr , który mógł być zaszyfrowany i deszyfrowany przez człowieka. Aktualnie większość tajnych wiadomości jest rozszyfrowywana przy pomocy komputerów. Przykładami szyfrów, które można używać do dzisiaj , bez zastosowania informatyki , z zapewnieniem jakiegokolwiek bezpieczeństwa są np. :

1. Szyfr z kluczem jednorazowym . Przykładem jest reguła Vernama . Wywodziła się z kodu Baudota, gdzie każdej literze odpowiadało pięć jednostek (impulsów) Zasugerował on wydziurkowanie na taśmie znaków klucza szyfrującego i elektromechaniczne dodawanie odpowiadających mu impulsów do tych ,które odpowiadają znakom tekstu jawnego. Szyfrogram powstawał w wyniku procesu sumowania znaków :

tekst jawny	***klucz***	***szyfrogram***
plamka	+ plamka	= odstęp
plamka	+ odstęp	= plamka
odstęp	+ plamka	= plamka
odstęp	+ odstęp	= odstęp

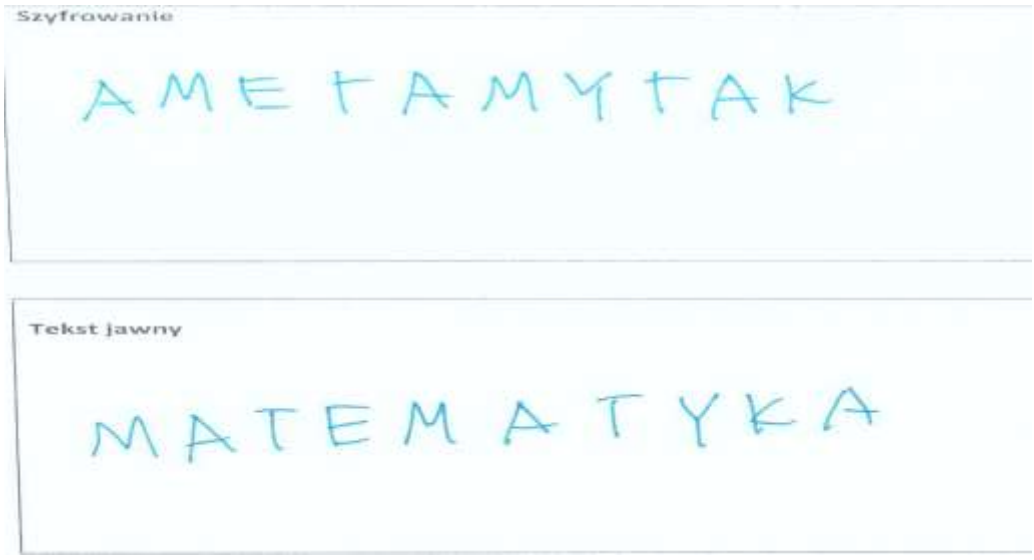
Celem prostszego posługiwania się szyfrem plamce przypisano cyfrę 1 , a odstępowi 0 .

		tekst jawny		
		1	0	
klucz	1	0	1	szyfrogram
	0	1	0	

Vernam , aby uzyskać pięć impulsów dla znaków szyfrogramu połączył pięć impulsów odpowiadających znakom tekstu jawnego z pięcioma znakami klucza. Np.

tekst jawny	1	1	0	0	0
klucz	1	0	0	1	1
szyfrogram	0	1	0	1	1

2. Szyfry podstawieniowe . W wiadomości zaszyfrowanej znajdują się wszystkie znaki tekstu jawnego , ale w zmienionej kolejności np. (troszkę własnej twórczości) :



Szyfry , które miały znaczenie w przeszłości :

a. Enigma

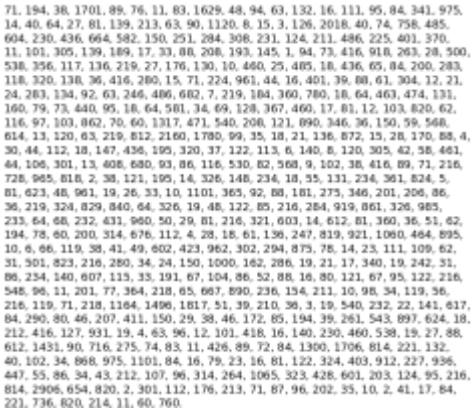
Maszyna wynaleziona na początku XX wieku przez doktora Arthura Scherbiusa. Urządzenie działało dzięki wirnikom. Miało tak wiele kluczy, że w razie potrzeby nie udałoby się przetestować na czas wszystkich możliwości . Dużą zasługą w rozszyfrowaniu urządzenia mieli Polscy uczeni : Marian Rejewski, Henryk Zygalski , Jerzy Różycki . Stworzyli metodę

określenia położenia wirników zestawiając pary liter i ustalili pozycje startową wirników . Rekonstruowali klucze dzienne dzięki czemu mogli rozszyfrowywać informację z danego dnia.

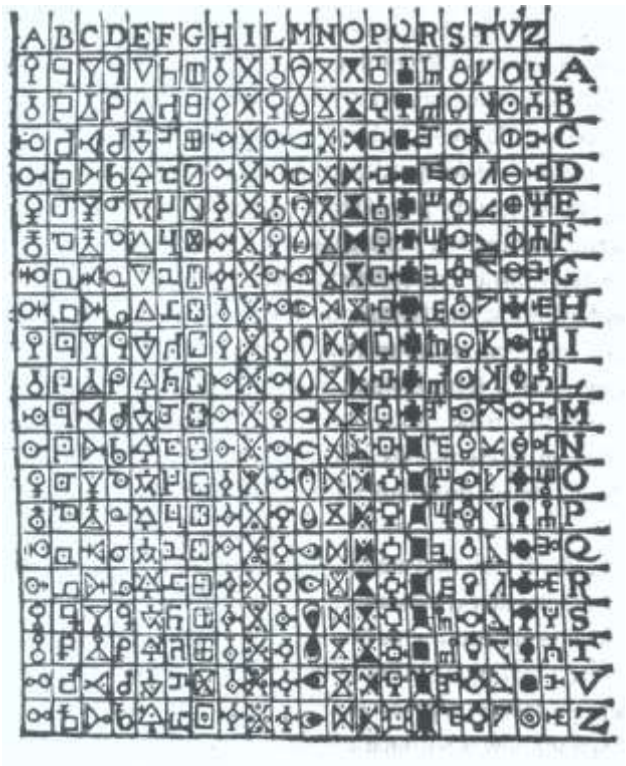
b. Szyfr podstawieniowy (polegał na zastępowaniu każdego znaku tekstu jawnego innym znakiem szyfrogramu) . Wyróżniamy :
- prosty szyfr podstawieniowy (każdy znak tekstu jawnego zastępowany jest przez jeden znak szyfrogramu)
Przykładem jest szyfr Cezara . Litery tekstu jawnego były zastępowane literami znajdującymi się o 3 miejsca dalej w alfabecie :

alfabet jawny	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
alfabet szyfrowy	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

- homofoniczny szyfr podstawieniowy (poszczególny znak tekstu jawnego zastępowany jest odpowiadającym mu znakiem szyfrogramu) , np. szyfr Beale'a



- poligramowy szyfr podstawieniowy (szyfrowane są grupy znaków zamiast pojedynczych)
Szyfr Giovanni Battisty Porty , w którym zastąpił każdą parę liter znakiem w miejscu przecięcia się wierszy i kolumn.



- polialfabetyczny szyfr podstawieniowy (powstaje w wyniku złożenia kilku szyfrów monoalfabetycznych)

Szyfr Vigenera . Podobny jest do szyfru Cezara. Przesunięcie kolejno wynosi 0, 1, 2 itd. Do zaszyfrowania wiadomości potrzebne jest słowo kluczowe, które jest tajne.

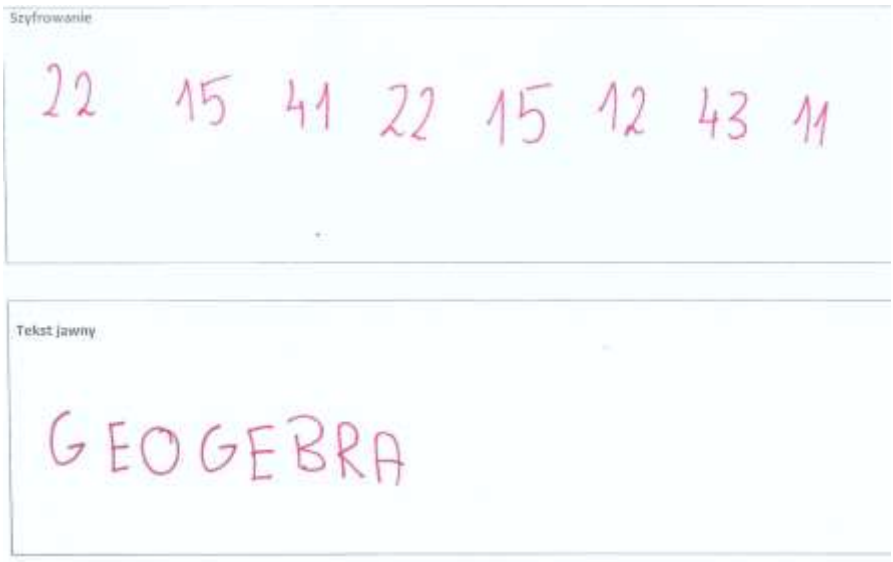
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

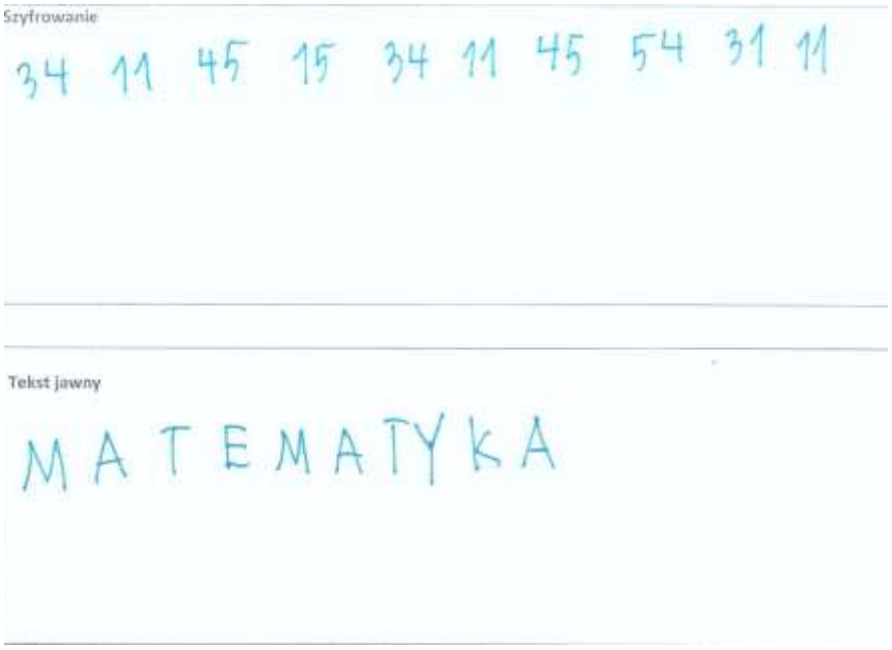
c. Szachownica Polibiusza

Grecki pisarz Polibiusz poukładał litery w kwadrat. Ponumerował wiersze i kolumny . Jedna litera była odpowiednikiem dwóch cyfr . Modyfikacja dla polskiego alfabetu .

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

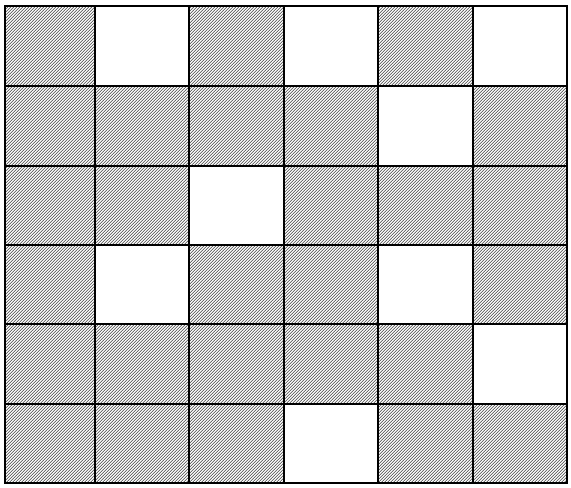
Nasze zaszyfrowane wiadomości :





e) maskownica obrotowa Cardana

Był to zazwyczaj kawałek kartonu. Został on podzielony na małe pola – kwadraty, z których ¼ została wycięta tworząc szablon. w puste pola wpisywano hasło. Następnie obracano 3 razy o 90 stopni , za każdym razem wpisując litery. Wiadomość zazwyczaj odczytywano wierszami.



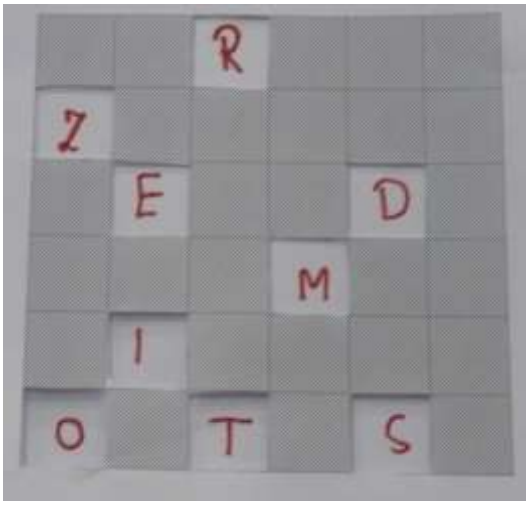
Wspólnie wymyśliłyśmy zaszyfrowaną wiadomość :

A	M	R	A	T	T
Z	O	Z	S	E	K
V	E	M	O	D	P
L	A	E	M	T	N
R	I	Y	P	!	Y
O	!	T	K	S	!

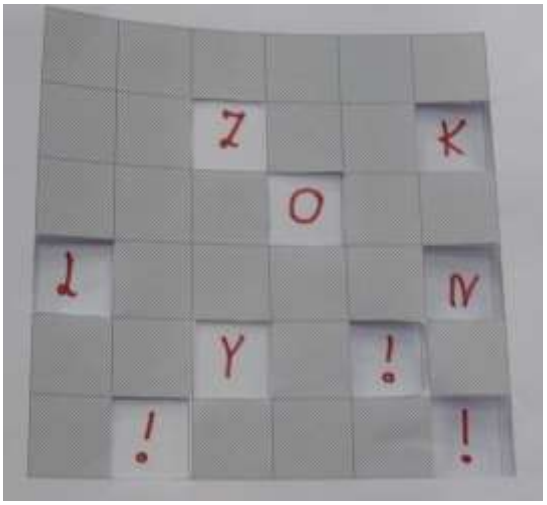
W czasie szyfrowania …

MATEMATYK

A TO SUPER P



RZEDMIOT S



ZKOLNY !!!

Rozszyfrowana wiadomość : MATEMATYKA TO SUPER PRZEDMIOT SZKOLNY !!!

Podsumowanie:

W tej prezentacji przedstawiłyśmy dużo szyfrów z wielu epok. Chciałyśmy pokazać, iż szyfrowanie było tak naprawdę od zawsze i towarzyszy nam do dzisiaj w różnych celach. Kilka kodów wypróbowałyśmy same, co miało udowodnić , iż czasami poufne wiadomości można przedstawić w prosty sposób , a do ich rozwiązania nie trzeba używać komputera. Pragniemy również zaznaczyć , że szyfrowanie jest bardzo atrakcyjną , logiczną rozrywką dla naszych młodych umysłów .

Bibliografia:

- ,,Łamacze szyfrów'' – David Kahn
- Wikipedia (przede wszystkim) :
  https://pl.wikipedia.org/wiki/Szyfr
  https://pl.wikipedia.org/wiki/Algorytm_symetryczny
  https://pl.wikipedia.org/wiki/Szyfr_strumieniowy
  https://pl.wikipedia.org/wiki/Szyfr_blokowy
  https://pl.wikipedia.org/wiki/Kryptografia_klucza_publicznego
  https://pl.wikipedia.org/wiki/Enigma
  https://pl.wikipedia.org/wiki/Szyfr_podstawieniowy
  https://pl.wikipedia.org/wiki/Szyfr_monoalfabetyczny
  https://pl.wikipedia.org/wiki/Szyfr_homofoniczny
  https://pl.wikipedia.org/wiki/Szyfr_poligramowy
  https://pl.wikipedia.org/wiki/Szyfr_polialfabetyczny
  https://pl.wikipedia.org/wiki/Szyfr_przestawieniowy
  https://pl.wikipedia.org/wiki/Szachownica_Polibiusza