Temat: Zrozumieć, przeanalizować i rozwiązać.

Szyfrowanie ma szerokie zastosowanie w społeczeństwach rozwiniętych technicznie; wykorzystuje się ją np. w rozwiązaniach zapewniających bezpieczeństwo kart bankomatowych, haseł komputerowych i handlu elektronicznego. Największe jednak „wzięcie" ma ta dziedzina w wojskowości i dyplomacji. To właśnie tu używa się najbardziej zaawansowanych technologii i protokołów bezpieczeństwa.

Kryptografia – **to nauka o szyfrach**, czyli sposób szyfrowania wiadomości, aby niepowołane osoby nie miały do nich dostępu. Słowo KRYPTOS = ukryty

Na przestrzeni wieków pojawiały się różne sposoby zapisu i szyfrowania wiadomości. Oto kilka z nich:

A	1	I	9	P	17
B	2	J	10	R	18
C	3	K	11	S	19
D	4	L	12	T	20
E	5	Ł	13	U	21
F	6	M	14	W	22
G	7	N	15	Y	23
H	8	O	16	Z	24

Matematyczny (**liczby**) — jedną z najprostszych metod jest przypisanie każdej literze alfabetu pewnej liczby i posługiwanie się tymi liczbami jak literami, na przykład w wersji najłatwiejszej **A** = **1**, **Z** = **24**. Niestety taki szyfr jest całkiem prosty do odczytania, zwłaszcza gdy tekst jest dłuższy. **Szyfr może zawierać litery z ogonkami: ś, ć, ń, ą, ę** – wystarczy tylko odpowiednio nadać im kolejną liczbę. Aby wyglądał na zadanie matematyczne wstawia się dodatkowo znaki +, -, nawiasy itp. **PRZYKŁADY:**

Zakodujmy znane uczniom słowo: „**P I E R D O N K A**" xD

KOD1: **17 9 5 18 4 16 15 11 1**

KOD2: **17+9+5-18-4+16-15+11-1**=20 lub jeszcze inaczej **KOD3**: $\overbrace{((17-9)*5)}^{40}*\overbrace{((18-4+16)/15)}^{2}/11-1 = 8$

Stosując nawiasy, znaki matematyczne uprawdopodabniamy działanie jednocześnie kodując ten sam wyraz.

Zobacz w każdym kodzie zastosowano te same liczby, które odpowiadają konkretnym literom alfabetu.

Szyfr Cezara — każdą literę tekstu, jaki chcemy utajnić, zastępuje się literą, która oddalona jest od niej w alfabecie o konkretną liczbę miejsc do przodu lub do tyłu. Z następną literą robi się tak samo. Na widocznym przykładzie zastosowano autentyczny szyfr stosowany przez **Juliusza Cezara**. W swej korespondencji do przyjaciół ***przesuwał on litery o 3 miejsca***. I tak litera **K** po zaszyfrowaniu to **H**, **O**=**M**, **Ń**=**Ł**. Wyraz **K O Ń** po zaszyfrowaniu wyglądać będzie tak: **H M Ł.** Acha! Możesz stosować dowolne kombinacje. Najprostsze przesunięcie o 1 literę lub może trudniejszą opcję np. przesunięcie **o 6 liter**.

Tekst jawny: **BĄDŹ MĘŻNY**

Tekst zaszyfrowany: **DĆFĄ OHBÓŻ**

A	Ą	B	C	Ć	D	E	Ę	F	G	H	i	J	K	L	Ł	M	N	Ń	O	Ó	P	R	S	Ś	T	U	V	W	Y	Z	Ź	Ż	Alfabet
Z	Ź	Ż	A	Ą	B	C	Ć	D	E	Ę	F	G	H	i	J	K	L	Ł	M	N	Ń	O	Ó	P	R	S	Ś	T	U	V	W	Y	Szyfr

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

Szyfr Polibiusza (**tabliczka mnożenia**) — Grecki historyk **Polibiusz** wymyślił prosty szyfr nazwany od jego imienia. Kluczem do szyfru jest tabela z umieszczonym w niej alfabetem. (bez polskich liter). Szyfrowanie polega na znalezieniu w kluczu odpowiednich liter a następnie zapisanie ich w formie mnożenia. (*Widoczna obok tabela została trochę zmodyfikowana na potrzeby lekcji*). Na przykład litera **A, Ą** = **1**x**1** | **C, Ć** = **1**x**3** | W = **5**x**2** | N = 4x4 |

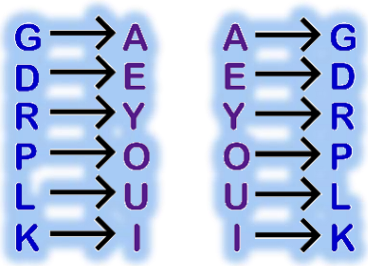
numer wiersza

numer kolumny

Słowo **OGAR** (ogarnij się – neologizm taki… xD) będzie wyglądać tak: **3x4 2x2 1x1 4x3**

Szyfr komórkowy - Szyfr ten powinien przypaść do gustu osobom nierozstającym się ze swoimi telefonami 😁. Szyfrując wiadomości można posłużyć się znakami umieszczonymi na klawiaturze telefonu komórkowego (klawiatury starych telefonów). Szyfrujemy tak jakbyśmy pisali sms'a tzn. jeśli chcemy zaszyfrować słowo **R O B O T** będzie ono wyglądało tak: **777 666 22 666 8**. Dla wyjaśnienia **R** zapisujemy jako **777** ponieważ jest na **3** pozycji na klawiszu **7**, a **T** jako **8** ponieważ jest na 1 pozycji klawisza 8.

Szyfry sylabowe — Zasada działania szyfru jest prosta, wystarczy podstawiać za literkę w szyfrowanym wyrazie literkę, która jest w parze. Jeśli zaś literka, w szyfrowanym wyrazie nie występuje w szyfrze przepisujemy ją. Słowo klucz: **GA-DE-RY-PO-LU-KI**. Słowo do zaszyfrowania: **BLOOPERS** (gafa, wpadka) po zaszyfrowaniu będzie wyglądać tak: **BUPPODYS**



B – przepisujemy **B**, bo nie ma tej litery w kodzie
L - jest w sylabie LU więc robimy podmiankę na **U**;
O - jest w sylabie PO więc podmianka na **P**;
O – tak jak powyżej jest w sylabie PO więc podmianka na **P**;
P – Jest w sylabie PO stąd zamiana na **O**;
E – też zmieniamy tym razem na **D**;
R – istnie w szyfrze sylaba RY więc podmiana na **Y**
S – tej litery również nie ma w naszym kodzie, więc przepisujemy **S**;

Inne ciekawe słowa klucze:
MA-LI-NO-WE-BU-TY
PO-LI-TY-KA-RE-NU
BI-TW-AO-CH-MU-RY
KU-LO-PE-RY-ZA-GI
HA-LO-JU-PI-TE-RY
MO-TY-LE-CU-DA-KI
NO-WE-BU-TY-LI-SA
GI-TA-RO-WE-NU-TY (mój xD)

Alfabet Morse'a — Stworzony w 1832 przez Samuela Morse'a sposób reprezentacji alfabetu, cyfr i znaków specjalnych za pomocą dźwięków, błysków światła, impulsów elektrycznych lub znaków popularnie zwanych kreską i kropką. Wszystkie znaki reprezentowane są przez kilkuelementowe serie sygnałów – krótkich (kropek) i długich (kresek). Kreska powinna trwać co najmniej tyle czasu, co trzy kropki. Odstęp pomiędzy elementami znaku powinien trwać jedną kropkę. Odstęp pomiędzy poszczególnymi znakami – jedną kreskę (3 kropki jak kto woli). Odstęp pomiędzy grupami znaków – trzy kreski (7 kropek).

Enigma — niemiecka przenośna, elektromechaniczna maszyna, oparta na zasadzie obracających się wirników, opracowana przez Artura Scherbiusa. Po raz pierwszy szyfrogramy zakodowane za pomocą Enigmy udało się rozszyfrować polskim kryptologom w grudniu 1932 roku

Zadanie 1
Zaszyfruj wyrazy „**ALE BEKA**" (ubaw, zabawa, coś śmiesznego) dwoma różnymi sposobami. Zarówno tekst otwarty (Ale beka) – jak i zaszyfrowany wpisz w zeszycie.

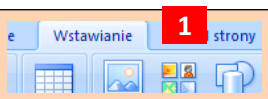
Zadanie 2
Na wykonanie zadania macie 5 minut. Kolejne 5 na deszyfrację tekstu, który otrzymacie od innej grupy. Niech każda grupa zaszyfruje wybraną metodą słowo lub krótkie zdanie zaproponowane przez nauczyciela. Wymieńcie się zaszyfrowanymi tekstami i rozszyfrujcie je. Wygrywa grupa, która najszybciej odgadnie metodę szyfrowania i rozszyfruje tekst.

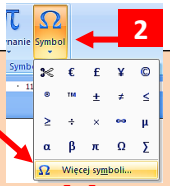
Hieroglify — Teksty można nie tylko szyfrować, ale też pisać pismem obrazkowym. Zestaw czcionek zawierających znaki graficzne zależy od oprogramowania zainstalowanego na komputerze. Na większości komputerów działających pod kontrolą systemu Windows znajdziesz czcionki graficzne. Są to **Wingdings**, **Wingdings2**, **Wingdings3** (czytaj: łindings) i **Webdings** (czytaj: łebdings).

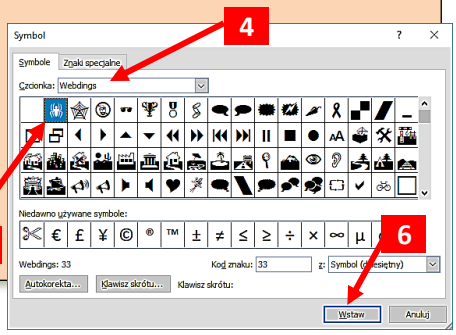
Sposób 1. Napisz tekst podany przez nauczyciela, a następnie zastąp wybrane słowa odpowiednimi symbolami, na przykład słowo klucz — obrazkiem , a książki — obrazkiem . Aby symbole były bardziej czytelne powiększ je. Na przykład jeśli tekst ma 12pkt to symbol może mieć 20pkt.

Sposób 2. Wstaw wybrane symbole, a później metodą przeciągnij i upuść lub wytnij – wklej ustaw je w odpowiednim miejscu w tekście , , , , , .

Wskazówka!!!
- Aby wstawić symbol:
- Wybierz zakładkę ***WSTAWIANIE [1]***
- w grupie ***SYMBOLE*** wybierz ***symbol[2]/Więcej Symboli[3]***
- W otwartym oknie Symbol odszukaj ***czcionkę [4]*** obrazkową
- i ***właściwy obrazek [5]***.
- Na koniec użyj przycisku ***Wstaw [6]***.







Zadanie 3
Przepisz poniższy tekst. Zastąp wyrazy oznaczone kolorem niebieskim symbolami obrazkowymi. Znajdziesz je w czcionce Webdings

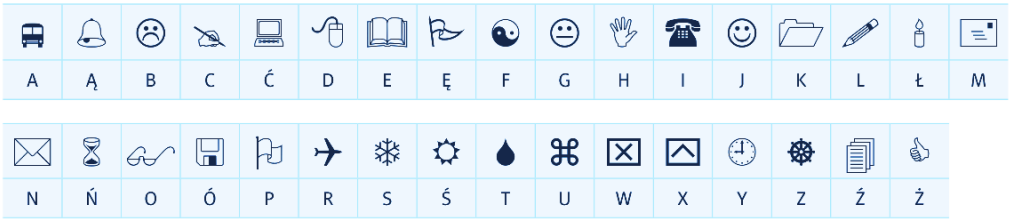
Dostaniesz ***medal***, gdy napiszesz: „Jedzie ***pociąg*** z daleka…"

Praca domowa: Pracę domową znajdziesz na kolejnej stronie…

Praca domowa

- **Wymień** (4 wyrazy – to nie książka) w zeszycie nazwy czcionek graficznych, które można znaleźć w systemie Windows. *(Jeszcze się nam przydadzą).* Oczywiście wstaw tytuł np.: Czcionki graficzne to:
- **Wklej** materiały otrzymane na zajęciach
- Jedna z ważnych zasad pracy z aplikacjami została zaszyfrowana. **Odszyfruj** ją, a następnie zapisz w zeszycie i odczytaj.

Kod szyfru:



Celujemy

Korzystając z informacji odszukanych w internecie na wybranych stronach WWW, przygotuj dokument tekstowy na temat **Moja porcja zagadek**. Dokument powinien dotyczyć wiedzy na temat **komputerów**, **urządzeń cyfrowych** i **sieci komputerowych** i być napisany z myślą o młodszych uczniach (trzeciej i czwartej klasy). Powinien mieć formę zagadek. Prześlij dokument na e-mail nauczyciela. Pracuj etapami:

- **Zaplanuj** — zastanów się, o czym będą Twoje zagadki.
- **Wykonaj** — wykorzystując posiadane umiejętności, przygotuj dokument tekstowy.
- **Przetestuj i sprawdź** — sprawdź, czy dokument odpowiada wymaganiom oraz czy nie ma błędów.
- **Działaj** — zakończ pracę prześlij nauczycielowi jej efekty.

Klasa 5 zobowiązuje. Wykorzystajcie poznane w klasie 4 zasady. (Rozstrzelenia, justowania itp.)