„Istota matematyki zawiera się w jej wolności „

Georg Cantor

SZYFRY

Bartłomiej Zajda

klasa II a

Gimnazjum Nr 3 w Wadowicach

Tel. 338232480

zsp2wadowice@poczta.onet.pl

W roku 2012 minęła 80 rocznica złamania szyfru Enigmy , więc chciałbym rozszerzyć informacje związane z szyframi . W tej pracy spróbuję przybliżyć wiadomości , o tym jak szyfrowano dawniej , a jak szyfruję się obecnie .

Enigma (z greckiego zagadka) była to przenośna, niemiecka, elektromechaniczna maszyna szyfrująca oparta na zasadzie obracających się wirników. Enigma wyglądała jak zwykła maszyna do pisania . Tylko wpisując jakąś literę wyskakiwała całkiem inna , nawet jeśli 2 razy z rzędu użyliśmy tej samej litery, to Enigma zamieniała tę literę na jeszcze inną . Maszyna ta opracowana została przez Artura Scherbiusa, a następnie produkowana przez wytwórnię Scherbius & Ritter. Artur Scherbius nie był pierwszym inżynierem, który skonstruował maszynę szyfrującą opartą na wirnikach. Poza nim i Hugonem Kochem prace nad podobnymi urządzeniami prowadzili także Edward Hebern (USA, 1917) i Arvid Gerhard Damm (Szwecja, 1919), ale tylko Scherbius ze swoją Enigmą osiągnął sukces wprowadzając ją najpierw na rynek cywilny, a później do instytucji państwowych. Enigma była używana komercyjnie od lat dwudziestych XX wieku, a później została zaadaptowana przez instytucje państwowe wielu krajów. Podczas II wojny światowej maszyna ta była wykorzystywana głównie przez siły zbrojne oraz inne służby państwowe i wywiadowcze Niemiec a także innych państw głównie do szyfrowania informacji z frontu. Po raz pierwszy szyfrogramy zakodowane przy pomocy Enigmy udało się rozszyfrować polskim kryptologom na początku lat trzydziestych. Marian Rejewski, Jerzy Różycki i Henryk Zygalski z Uniwersytetu Poznańskiego wyniki swoich prac, wraz ze zrekonstruowanymi egzemplarzami Enigmy przekazali po wybuchu II wojny Brytyjczykom, którzy skwapliwie skorzystali z dokonań naszych naukowców przy deszyfrowaniu informacji w czasie Bitwy o Atlantyk. Centrum kryptologiczne w Wielkiej Brytanii znajdowało się wtedy w Betchley Park, zwanym Stacją X, gdzie 12 tysięcy ludzi zaangażowanych było w prace nad deszyfrowaniem tajnych wiadomości. Działalność Stacji X oraz całego sztabu specjalistów zajmujących się Enigmą utajniono, dokumenty zaś związane z tamtymi wydarzeniami ujrzały światło dzienne dopiero w latach siedemdziesiątych XX wieku. Rozszyfrowanie Enigmy miało ogromne znaczenie dla świata. Niektórzy uważają , że rozpracowanie Enigmy pozwoliło skrócić wojnę o 2 a nawet 3 lata , oraz ocalić życie 20 mln ludzi . Wielu uważa, że dzisiejszy kształt Europy to także pośredni efekt rozszyfrowania Enigmy.

Zacznę od najprostszego szyfru , a mianowicie od szyfru Cezara. Czasem można się spotkać z inną nazwą tego szyfru – szyfr przesuwający , co jest rzadkością , bo nazwa tego szyfru jest zaczerpnięta od jego „wynalazcy" , gdyż w czasach Cezara wszystkie dobre rzeczy były przypisywane jemu . Polega on na przesuwaniu wiadomości , o pewną umówioną liczbę liter w przód lub w tył . Chodzi o to , że np. jeżeli umówimy się na liczbę 3 , to wówczas (a = d), (b = e) itd.

Więc spróbujmy zaszyfrować coś tym sposobem . Załóżmy , że naszą wiadomością jest zdanie : **NIC Z TEGO NIE ROZUMIEM** , a naszą umówioną cyfrą będzie 1 czyli: n = o , i = j , c =d itd. Szyfrując tym oto sposobem widomość , uzyskujemy ciąg liter : OJD A UFHP OJF SPAVNJFN . Jak można zauważyć, wybierając nawet bardzo małą cyfrę do przesunięcia , można bardzo zmienić treść wiadomości .

Większość szyfrów nie jest wynalazkiem nowoczesności i stosowane były we wszystkich epokach. Nawet w Zakonie Krzyżackim , kodowanie było na porządku dziennym , gdyż przejęcie ważnych informacji przez wroga mogło zmienić losy bitwy a nawet wojny . Więc chcąc zapobiec takim wypadkom Wilki Mistrz Krzyżacki wybierał sobie „służbę specjalną" , która szyfrowała korespondencję wojenną . Na każdą wojnę była taka służba brana i to ona rozszyfrowywała wiadomości od i do Mistrza . Może jest to zabawne , ale ich szyfr polegał tylko na 3 literach : S , K , L , są to odpowiedniki trzech pierwszych liter do niemieckich czasowników : S – swigen = milczeć , K – keren = obracać i L – lesen = czytać . S oznaczało pominięcie danego wyrazu , K obrócenie wyrazu np. okelm znaczyłoby mleko, i L oznaczało czytać bez zmieniania niczego . Przed każdym wyrazem stawiano , S , K lub L i od razu odszyfrowywano tekst . Może teraz ten szyfr budzi uśmiech na naszych twarzach , ale nie było to głupie . W czasach średniowiecza mało kto umiał czytać , a gdy nawet osoba , która odnalazła wiadomość i umiała czytać, to musiała przysporzyć sobie dużo trudu , aby to rozszyfrować . Spróbujmy pójść śladem Wielkiego Mistrza Krzyżackiego i zaszyfrujmy zdanie : **NIC Z TEGO NIE ROZUMIEM** . Będzie to wyglądało tak : KCIN SE LZ LTEGO KIEN KMEIMUZOR , w pierwszym wyrazie pierwszą literą jest K , więc obracamy wyraz i wychodzi NIC , w drugim słowie jest litera S , więc pomijamy ten wyraz , w 3 i w 4 wyrazie jest L , więc bez zmieniania niczego czytamy słowo, w 5 i w 6 jest K czyli obracamy wyrazy i odczytujemy zaszyfrowane zdanie.

Następnym szyfrem , jaki chciałbym przybliżyć jest szyfr Bacona . Nie jest on trudny , a był używany już w Renesansie . Polega on na zakodowaniu wiadomości za pomocą 5 literowych „wyrazów" składających się tylko z liter **a** lub **b** , ale w pewniej kolejności przedstawionej na tej o to tablicy :

A = aaaaa
B = aaaab
C = aaaba
D = aaabb
E = aabaa
F = aabab
G = aabba
H = aabbb
I/J = abaka
K = abaab
L = ababa
M = ababb
N = abbaa
O = abbab
P = abbba
Q = abbbb
R = baaaa
S = baaab
T = baaba
U/V = baabb
W = babaa
X = babab
Y = babba
Z = babbb

Mając taką tabelę spróbujmy zaszyfrować wiadomość :
NIC Z TEGO NIE ROZUMIEM

abbaa abaaa aaaba babbb baaba aabaa aabba abbab abbaa abaaa aabaa baaaa abbab babbb baabb ababb abaaa aabaa ababb

Tak wygląda wiadomość zaszyfrowana , a jej odkodowanie jest bardzo proste , wystarczy poszukać w tabeli ciągu liter i zamienić je na odpowiadające im litery.

Kolejnym szyfrem jaki chciałbym opisać jest szyfr Vigenera . Jest to jeden z dość powszechnych szyfrów średniowiecznych . Działanie szyfru jest oparte na następującej tablicy :

	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

Jak można zauważyć , każdy z poniższych wierszy odpowiada szyfrowi Cezara . W pierwszym wierszu liczba o którą mamy przesuwać litery wynosi 0 , ale już w 2 rzędzie można zauważyć , że B odpowiada A , czyli „przesunięcie” jak to sobie umownie nazwę wynosi 1 , a z każdym następnym wierszem „przesunięcie” wynosi o jeden więcej , więc w 3 wierszu litera A będzie zastąpiona literą C , a w jeszcze następnym literą D i tak dalej … Do zakodowania wiadomości z użyciem tego szyfru potrzebne nam jest także słowo klucz, które składa się z takiej liczby liter aby ona była mniejsza od liczby liter szyfrowanej wiadomości.

Załóżmy , że chcemy zaszyfrować wiadomość : **NIC Z TEGO NIE ROZUMIEM** , a naszym słowem kluczem będzie wyraz : MLEKO. Jeżeli mamy już słowo klucz , oraz wiadomość do zaszyfrowanie , to musimy podpisać słowo klucz pod wiadomością , tyle razy , aby zapełnić całe zdanie :

NIC Z TEGO NIE ROZUMIEM

MLE K OMLE KOM LEKOMLEK

Z połączenia dwóch liter stojących pod sobą ,na tablicy możemy odszukać literę szyfrującą , czyli z połączenia N i M wyjdzie nam litera Z , z połączenia liter I oraz L wyjdzie nam litera T i tak dalej . Nasza cała zakodowana wiadomość brzmi :

ZTG J GQRS XWQ CSJIYTIW

Odszyfrowanie wiadomości jest bardzo proste chociaż bardzo pracochłonne . Mając słowo klucz znów podpisujemy je pod wiadomością , ale tym razem zaszyfrowaną :

ZTG J GQRS XWQ CSJIYTIW

MLE K OMLE KOM LEKOMLEK

I mając już gotową wiadomość do rozszyfrowania szukamy na tablicy litery M , i w kolumnie w której jest M, znajdujemy literę Z i wtedy w tym samym wierszu gdzie znaleźliśmy Z odczytujemy literę wiadomości N .

Pomimo pracochłonności w kodowaniu wiadomości tym szyfrem , jest on bardzo dobry . Zostało udowodnione , że mając spełnione pewne 3 warunki , ten klucz jest nie do złamania . Znalazłem informacje, że tymi warunkami są:

- klucz użyty do szyfrowania wiadomości był krótszy lub równy szyfrowanej wiadomości,
- klucz musi być wygenerowany w sposób całkowicie losowy (nie może istnieć sposób na odtworzenie klucza na podstawie znajomości działania generatorów liczb pseudolosowych),
- klucz nie może być użyty do zaszyfrowania więcej niż jednej wiadomości

Jak widać szyfrowanie było bardzo powszechne w przeszłości jednak dzisiaj też używa się szyfrowania . Nawet w codziennie używanej poczcie elektronicznej stosowane jest kodowanie . Mamy własne hasło i własny login , ale do bazy danych nie są one przekazywane w ten sam sposób jak wpisaliśmy . Następuje tam szyfrowanie pomiędzy zalogowaniem się a przejściem informacji do bazy danych .

Kolejnym przykładem instytucji gdzie istnieje stała potrzeba szyfrowania danych w obecnych czasach są banki . Szyfruje się tam za pomocą rozkładu liczb na czynniki pierwsze , a fachowo nazywa się to szyfrem RSA od pierwszych liter wynalazców . W roku 1977 trzej profesorowie z MIT w USA, Ronald L. Rivest, Adi Shamir i Leonard Adleman, opublikowali nowy rodzaj szyfrowania danych. Jest to niesymetryczny algorytm szyfrujący, którego

zasadniczą cechą są dwa klucze: publiczny do kodowania informacji oraz prywatny do jej odczytywania. Klucz publiczny (można go udostępniać wszystkim zainteresowanym) umożliwia jedynie zaszyfrowanie danych i w żaden sposób nie ułatwia ich odczytania, nie musi więc być chroniony. Dzięki temu firmy dokonujące transakcji poprzez sieć Internet mogą zapewnić swoim klientom poufność i bezpieczeństwo. Drugi klucz (prywatny, przechowywany pod nadzorem) służy do odczytywania informacji zakodowanych przy pomocy pierwszego klucza. Klucz ten nie jest udostępniany publicznie. System RSA umożliwia bezpieczne przesyłanie danych w środowisku, w którym może dochodzić do różnych nadużyć. Bezpieczeństwo oparte jest na trudności rozkładu dużych liczb na czynniki pierwsze. Warto zauważyć , że nawet znając liczbę , którą trzeba rozłożyć na czynniki pierwsze , to jest to na tyle pracochłonne i trudne, że złodzieje jeżeli chcą okraść bank wolą wyciągać pieniądze przez napad , a nie przez rozpracowywanie szyfrów .

Myślę , że podając tyle przykładów szyfrowania pokazałem , że kryptografia to ciekawa dziedzina wiedzy i warto się jest nią zainteresować . Informacje o szyfrach zgłębiam głównie przeszukując zasoby Internetu, do którego mamy w dzisiejszych czasach nieograniczony dostęp. Dzisiejsza kryptografia ma silne podstawy w wiedzy matematycznej i informatycznej którą chciałbym w przyszłości poznać i zgłębić.

Literatura:

pl.wikipedia.org

alehistoria.blox.pl