TAJNE ŻYCIE TEORII LICZB

Zuzanna Balon

SP 54 IM JULIANA TUWIMA W KRAKOWIE

Nauka o przekazywaniu informacji w bezpieczny sposób nazywa się kryptologią. Można ją podzielić na dwie części. Kryptografia zajmuje się opracowywaniem, doskonaleniem i badaniem sposobów szyfrowania a jej celem jest zabezpieczenie informacji. Natomiast kryptoanaliza to nauka o łamaniu szyfrów. Kryptoanalitycy starają się odczytać treść wiadomości bez dostępu do klucza albo odkryć zasadę działania szyfru mając dostęp do klucza i zaszyfrowanej (lub nie) wiadomości.

Prawdopodobnie największą i najbogatszą instytucją zajmującą się kryptologią jest amerykańska National Security Agency. Skrót NSA bywa także tłumaczony jako No Such Agency (nie ma takiej agencji). Przez długi czas rząd USA zaprzeczał istnieniu NSA. NSA jest jednym z największych (prawdopodobnie największym) pracodawcą zatrudniającym matematyków.

Szyfry są wszędzie

Za każdym razem, gdy robisz zakupy online lub korzystasz z banków, robisz to w bezpiecznym środowisku chronionym przez kryptografię. Teoretyczne podstawy ostatnich postępów w kryptografii opierają się na teorii liczb w matematyce, ponieważ podstawowe szyfrowanie obejmuje arytmetykę modularną, liczby pierwsze i teorię prawdopodobieństwa. Szyfrowanie to metoda przekształcania danych w taki sposób, aby nie zostały przed nikogo odczytane, z wyjątkiem osób upoważnionych. Proces szyfrowania zmienia zwykły tekst do tekstu szyfrowanego za pomocą klucza kryptograficznego. Klucz kryptograficzny jest zbiorem wartości liczbowych znanych i ustalanych przez jego nadawcę i odbiorcę. Odszyfrowanie (lub translacja) zaszyfrowanych danych jest możliwe dla każdego, kto taki klucz posiada. To dlatego specjaliści dzisiejszej kryptografii rozwijają coraz to nowsze i bardziej skomplikowane klucze. Jeśli komputer wykonuje miliony lub nawet miliardy prób złamania hasła lub klucza deszyfrującego, mowa jest o ataku typu brute force, czyli siłowym. Współczesne

komputery potrafią wykonywać takie obliczenia niezwykle szybko. Obecne metody szyfrowania muszą być odporne na tego rodzaju atak.

Najbardziej popularnym, dostępnym za darmo narzędziem kryptograficznym jest program GPG (GNU Privacy Guard), bezpłatny odpowiednik aplikacji PGP (Pretty Good Privacy). Wykorzystuje on szyfry z kluczem asymetrycznym (takie, w których klucz prywatny jest różny od klucza publicznego) DSA oraz ElGamal. Szyfry z kluczem asymetrycznym działają w ten sposób, że każdy użytkownik generuje dwa klucze: publiczny i prywatny. Klucz publiczny może być ujawniony wszystkim. Używając go można zaszyfrować wiadomość, która zostanie rozszyfrowana tylko przy pomocy klucza prywatnego. Szyfrów z kluczem publicznym można używać także do podpisywania dokumentów.

Kryptografia jest polem nieustannej rywalizacji między tymi, którzy opracowują szybsze sposoby łamania zabezpieczeń, oraz tymi, którzy wymyślają bardziej złożone metody szyfrowania. Różne organizacje od czasu do czasu informują, że opracowały zupełnie nowy rodzaj szyfru, całkowicie odporny na łamanie. Mając w rękach tak doskonałe narzędzie odmawiają przekazania informacji o zasadach działania. Zazwyczaj źle to wróży. Bezpieczny jest tylko taki szyfr, którego zasadę działania znają wszyscy a mimo tego nikt nie potrafi odczytać zaszyfrowanej wiadomości, o ile nie ma odpowiedniego klucza.

Szyfrowanie

Zacznę od najprostszego szyfru czyli szyfru Cezara. Szyfr ten to technika szyfrowania, w którym każda litera tekstu niezaszyfrowanego, jest zamieniana na literę oddalona od niej o ustalona liczbę miejsc w alfabecie. Chodzi o to, że jeżeli ustalimy sobie, że przesuwamy liczbę o 3 miejsca do przodu to: a = d, b = e itd. Kierunek zmiany musi być zachowany, nie ma znaczenia czy jest to litera duża czy mała. Autorem tego szyfru jest Juliusz Cezar, stąd też nazwa szyfru. Jednak

czasami możemy się jednak spotkać z inną nazwa – szyfr przesuwający. Obecnie nie używa się już tego szyfru, ponieważ jest on zwyczajnie za prosty i dla współczesnych komputerów odszyfrowanie go zajęło by zaledwie sekundę. Spróbujmy coś zaszyfrować tym sposobem. Uznajmy ze chcemy wysłać wiadomość: ANIA MA KOTA. Gdy będziemy wszystkie cyferki przesuwać o 1 pole do przodu wyjdzie nam: BOJB NB LPUB.

Następnym szyfrem, jaki chciałabym pokazać jest szyfr Bacona, który był już używany w Renesansie . Polega on na zakodowaniu wiadomości, gdzie każdą literkę zapisujemy jako 5 literowe „wyrazy" składające się tylko z liter a lub b , ale w pewniej kolejności przedstawionej poniżej:

A = aaaaa

B = aaaab

C = aaaba

D = aaabb

E = aabaa

F = aabab

G = aabba

H = aabbb

I/J = abaaa

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

Teraz zaszyfrujmy wiadomość: ANIA MA KOTA,

aaaaa abbaa abaaa aaaaa ababb aaaaa abaab abbab baaba aaaaa.

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 o którym chciałabym opowiedzieć jest Szyfr Vigenere'a. Jest to jeden z powszechnych szyfrów średniowiecznych. Działanie szyfru jest oparte na tablicy. Każdy z wierszy tablicy odpowiada już wcześniej poznanemu szyfrowi Cezara, przy czym w pierwszym wierszu przesunięcie wynosi 0, w drugim 1 itd. Czyli A w pierwszym wierszu będzie A, w drugim B, w trzecim C, itd. Do zakodowania wiadomości będzie nam potrzebny tak zwane słowo klucz, które składa się z takiej liczby liter aby ona była mniejsza od liczby liter szyfrowanej wiadomości. Spróbujmy zakodować wiadomość:

	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

ANIA MA KOTA.

Naszym słowem kluczem będzie:

KWIATEK.

Jeżeli mamy już słowo klucz, oraz wiadomość do zaszyfrowania, to musimy podpisać słowo klucz pod wiadomością, tyle razy, aby zapełnić całe zdanie:

ANIA MA KOTA.

KWIA TE KKWI.

Z połączenia dwóch liter stojących pod sobą, na tablicy możemy odszukać literę szyfrującą, czyli z połączenia A i K wyjdzie nam litera K, z połączenia liter N oraz W wyjdzie nam litera J i tak dalej. Nasza cała zakodowana wiadomość brzmi:

KJQA FE UYPI.

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

KJQA FE UYPI.

KWIA TE KKWI.

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

Pomimo pracochłonności kodowania tym szyfrem. Zostały podane trzy warunki, przez które ten szyfr jest nie do złamania. Oto warunki które znalazłam:

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

Teoretycznie najsilniejszym, gwarantującym 100% bezpieczeństwa sposobem szyfrowania jest metoda z bloczkami kluczy jednorazowych. Osoba szyfrująca wiadomość i osoba, która ją odczyta muszą mieć identyczne zestawy liczb losowych. Często były one drukowane albo pisane na maszynie na niewielkich karteczkach. Szyfrowanie polegało na tym, że najpierw zamieniano litery jawnego tekstu na liczby (przy pomocy tabeli kodowej, jeszcze nie szyfru) a następnie dodawano do nic, albo odejmowano liczby losowe odczytane z jednorazowego bloczka. W rezultacie otrzymywano szereg liczb, które wyglądały na całkowicie losowe a więc odporne na kryptoanalizę. Ta metoda jest bezpieczna

do dzisiaj pod warunkiem, że użyje się wystarczająco długiego klucza losowego, klucz nigdy nie zostanie użyty więcej, niż raz i klucz nie zostanie nigdy ujawniony.

Kolejnym ciekawym przykładem jest Enigma. Enigma była to przenośna, niemiecka, maszyna szyfrująca. Enigma wyglądała jak zwykła maszyna do pisania. Tylko wpisując jakąś literę wyskakiwała całkiem inna , nawet jeśli kilka razy z rzędu użyliśmy tej samej litery, to Enigma zamieniała tę literę na jeszcze inną . Maszyna ta opracowana została przez Artura Scherbiusa. Poza nim i Hugonem Kochem prace nad podobnymi urządzeniami prowadzili także Edward Hebern i Arvid Gerhard Damm, ale tylko Scherbius ze swoją Enigmą osiągnął sukces wprowadzając ją najpierw na rynek cywilny, a później do instytucji państwowych. Podczas II wojny światowej maszyna ta była wykorzystywana głównie przez siły zbrojne. Jako pierwsi rozszyfrowali ją Polacy: Marian Rejewski, Jerzy Różycki i Henryk Zygalski. Wyniki swoich prac przekazali po wybuchu II wojny Brytyjczykom, którzy skorzystali z dokonań naukowców przy deszyfrowaniu informacji w czasie Bitwy o Atlantyk. 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.

Szyfrowanie ma przyszłość

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.

Bardzo ważne tez w szyfrowaniu i w całej kryptografii są liczby pierwsze. Bezpieczeństwo informacji w Internecie zapewniają różne systemy szyfrujące, których podstawę ich stanowią liczby pierwsze. Im większa jest liczba pierwsza, tym trudniej jest złamać klucz szyfrujący. Jesienią 2008 roku została podana kolejna liczba pierwsza odkryta przez Edisona Smith'a. Ma ona około 13 milionów cyfr. Osiągnięcie to przyniosło mu popularność w świecie naukowym i 100 tysięcy dolarów zapłaconych przez amerykańską fundacje Electronic Frontier Foundation. Jest to organizacja mająca na celu walkę o wolności obywatelskie w elektronicznym świecie.

Połączenie liczb pierwszych z kryptografią nabrało szczególnego znaczenia w 1978 roku, za sprawą trzech profesorów: Ronalda Rivesta, Adiego Shamera i Leonarda Adelmana. Stworzony przez nich system szyfrowania danych, określany jest skrótem R.S.A. (od nazwisk autorów). Szyfr ten ma za zadanie umożliwić np. bankom czy przedsiębiorstwom transmisję informacji w bezpieczny sposób. Algorytm RSA jest aktualnie jednym z najpopularniejszych asymetrycznych algorytmów kryptograficznych. Jego zastosowanie można znaleźć w szyfrowaniu wiadomości, w operacjach między bankami oraz w komunikatorach internetowych. Dane można zaszyfrować, gdy są w spoczynku (przechowywane) lub „w drodze" (przesyłane). Istnieją dwie główne klasyfikacje szyfrowania: symetryczna i asymetryczna. Szyfrowanie symetryczne wykorzystuje tylko jeden klucz, a wszystkie osoby upoważnione używają tego samego tajnego klucza. Określenie „szyfrowanie asymetryczne" pochodzi od wykorzystania wielu kluczy: jednego do zaszyfrowania i jednego do odszyfrowania danych. Chociaż klucz szyfrujący jest publiczny, a deszyfrujący - prywatny.

Szyfrowanie hybrydowe - ta metoda łączy zarówno szyfrowanie asymetryczne, jak i symetryczne, dzięki czemu korzysta z zalet obydwu.

Całym algorytm RSA można podzielić na kilka części:

1. Wygenerowanie klucza publicznego oraz prywatnego.

2. Zaszyfrowanie danych przy użyciu klucza publicznego oraz wysłanie zaszyfrowanych danych do adresata.
3. Deszyfracja wiadomości za pomocą klucza prywatnego przez odbiorcę.

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. W 2009 roku grupie naukowców udało się złamać klucz o długości 768 bitów co trwało aż 2 lata, a wynik pracy algorytmów deszyfrujących zajął aż 5 TB danych!

Aktualnie standardem jest klucz 2048 bitowy. Cała siła tego algorytmu tkwi w matematycznym problemie znalezienia dwóch podzielników dużej liczby, które po przemnożeniu dają w wyniku tę bardzo dużą liczbę. Dla komputerów mnożenie jest procesem szybkim, ale dzielenie już nie. Najsłabszym ogniwem algorytmu RSA jest konieczność ochrony klucza prywatnego. Nie ważne jak bardzo matematycznie będzie skomplikowany klucz prywatny, jeżeli hackerowi uda się uzyskać do niego dostęp przy pomocy przejęcia kontroli nad serwerem to będzie w stanie przejąć i bez problemu odszyfrować zaszyfrowaną wiadomość. Jednak przy odpowiednich zabezpieczeniu wysłania klucza prywatnego rozszyfrowanie jest praktycznie niemożliwe.

Współczesne szyfry kryptograficzne są tworzone w taki sposób, aby ich deszyfracja trwało nieskończenie długo i na tym polega siła. I tutaj pojawiają się komputery kwantowe. Komputery kwantowe są dużo szybsze niż domowe komputery. Aby stworzyć silny klucz prywatny potrzebujemy 2 dużych liczb pierwszych oraz pewności, że te liczby pierwsze są bardzo trudne do odgadnięcia. Należy stworzyć dużą liczbę losową i sprawdzić, czy jest ona liczbą pierwszą. Jak możemy sprawdzić, czy liczba jest liczbą pierwszą, czy też nie? Najbardziej bezpośrednim podejściem jest podzielenie liczby przez każdą liczbę, która jest od

niej mniejsza. Jeśli nie jest podzielna przez żadną z nich, jest wówczas z pewnością liczbą pierwszą. Jest to jednak procedura dość długa. Istnieją dwie procedury sprawdzania czy podana liczba jest liczbą pierwsza. Jednym z nich jest użycie algorytmu deterministycznego, czyli takiego jakby próbnego dzielenia. Chodzi w tym o to, że dzielimy nasza liczbę przez wszystkie liczby przed nią, aby sprawdzić, czy przeprowadzenie dzielenia jest możliwe, jeżeli ni to znaczy że liczba jest pierwsza. Deterministyczny sposób oznacza, że będziemy w stanie stwierdzić, czy liczba jest liczbą pierwszą ze 100% dokładnością. Algorytmy deterministyczne są jednak wyjątkowo nieefektywne obliczeniowo i wymagają dużo czasu i obliczeń.
Procesowanie sprawdzenia twierdzeniem Wilsona wymaga również dużo energii. Działa to w następujący sposób: biorąc pod uwagę liczbę naturalną n> 1, jest ona liczbą pierwszą wtedy i tylko wtedy, gdy iloczyn wszystkich dodatnich liczb całkowitych mniejszych od n jest o jeden mniejszy od wielokrotności n. Metoda Millera-Rabina jest metodą probabilistyczną, tzn. nie jest w 100% dokładna, ale jest wystarczająco dokładna dla większości algorytmów kryptograficznych.

Wielkie losowanie

Bardzo ważna dla kryptografii jest możliwość wytwarzania bardzo dużej ilości liczb losowych. Są one potrzebna na przykład do produkcji kluczy jednorazowych. W czasie II Wojny Światowej i wkrótce po niej używano w tym celu maszyn losujących z bębnem poruszanym korbą. Do bębna wrzucano zestaw ponumerowanych kul. Po pokręceniu korbą pracownik wyjmował kulę, zapisywał umieszczony na niej numer, wrzucał ją z powrotem i powtarzał całą procedurę.
Komputery nie potrafią wytwarzać liczb losowych, a jedynie pseudolosowe. To znaczy, że jeśli będziemy wystarczająco długo zapisywali liczby, w końcu zauważymy, że ich kolejność się powtarza. Taka losowość nie jest wystarczająca, dlatego w kryptografii stosuje się generatory liczb losowych wykorzystujące

zjawiska fizyczne, np. rozpad izotopu promieniotwórczego, szum wytwarzany przez element półprzewodnikowy (diodę) itp.

Ciekawym zastosowaniem kryptografii są jednokierunkowe funkcje skrótu. Jeśli weźmiemy dużą ilość danych, np. treść grubej książki i obliczymy dla niej taką funkcję, to otrzymamy ciąg znaków (np. 60). Jeżeli dokonamy najmniejszej zmiany w długim tekście, to po ponownym obliczeniu wartości funkcji skrótu będzie ona zupełnie inna. Dzięki temu można wykorzystać funkcje skrótu do sprawdzenia, czy mamy do czynienia z oryginalnym dokumentem, czy też ktoś wprowadził zmiany.

Tej metody korzystają często producenci oprogramowania. Umieszczając w Internecie plik z nową wersją programu publikują też wartość funkcji skrótu. Jeśli po pobraniu programu obliczymy dla niego funkcję skrótu to musi być identyczna z opublikowaną. Jakakolwiek różnica jest sygnałem, że ktoś manipulował przy programie np. dodał do niego wirusa albo inny złośliwy kod.

Funkcji skrótu używa się też do przechowywania haseł do serwisów internetowych. W bazie danych nie ma prawdziwego hasła, tylko jego skrót. Kiedy użytkownik loguje się do serwisu na podstawie hasła obliczana jest wartość funkcji skrótu. Dwie jednakowe wartości oznaczają, że hasło jest zgodne.

Bardzo dużą rolę w kryptoanalizie odgrywa analiza statystyczna. Umożliwia ona odgadywanie znaczenia znaków i wyrazów w zaszyfrowanym tekście. Przynajmniej w starszych szyfrach. Pomagają w tym słowniki frekwencyjne. Są to słowniki, które zawierają informację: jak często w danym języku występują poszczególne litery albo słowa. Jeśli w zaszyfrowanej treści zauważymy znak który występuje tak samo często, jak litera np. „a” w języku, którego się spodziewamy, to w wielu łatwiejszych szyfrach rzeczywiście będzie ona oznaczała literę „a”.

Większość szyfrów można złamać. Konstruktorzy algorytmów o tym wiedzą, dlatego nie tracą czasu na opracowanie idealnego, doskonałego algorytmu. Wystarczy, jeśli będą mieli pewność, że zaszyfrowanej wiadomości

nikt nie odczyta w ciągu kilkudziesięciu albo np. stu lat bez względu na to, jak będzie wzrastała moc obliczeniowa dostępnych komputerów.
Metoda brutalnego łamania szyfru polega na używaniu kolejno wszystkich możliwych kluczy. Dla człowieka jest nudna i męcząca, ale komputery radzą sobie z nią doskonale. Dlatego ważne jest stosowanie haseł na tyle długich, żeby ich odgadnięcie metodą brutalną było bardzo trudne i długotrwałe. Zapięcie do roweru z czterema pierścieniami zawierającymi po 10 cyfr (od 0 do 9) ma 104 możliwych kombinacji. Gdyby na każdym z pierścieni umieścić wszystkie litery małe i wielkie, specjalne znaki pisarskie oraz cyfry to przy czterech pierścieniach mielibyśmy 26+26+10+30=924=71 639 296 kombinacji. Gdybyśmy użyli jako hasła ciągu 256 znaków wybieranych spośród takiego zestawu, to możliwych kombinacji byłoby 71256.

Bez matematyki ani rusz

Kryptografia jest doskonałym przykładem zmiany podejścia do matematyki i jej praktycznych zastosowań. Przez długi czas teorię liczb uważano za interesującą, ale czysto abstrakcyjną gałąź matematyki. Później, na początku XX wieku okazało się, że teoria liczb dostarcza teoretycznych podstaw kryptografii. Nauki o wielkim znaczeniu dla losów świata, ale jednak ograniczonym zastosowaniu, korzystali z niej dyplomaci, wojsko, wielcy przedsiębiorcy. Pod koniec XX wieku, między innymi za sprawą Internetu kryptografia stała się niezbędna dla każdego. Szyfrowane są połączenia przeglądarek WWW z serwerami banków, rozmowy telefoniczne, numery PIN kart kredytowych przesyłane do centrów rozliczeniowych, telewizja satelitarna. A to tylko niewielka część zastosowań kryptografii.
Skoro nie możemy obyć się bez kryptografii, a kryptografia jest naturalnie związana z matematyką, to znaczy, że poznawanie matematyki ma głęboki sens.

Dzięki niej potrafimy zrozumieć świat i narzędzia, których używamy. A kiedy je zrozumiemy będziemy mogli używać ich skutecznie i bezpiecznie.

Źródła:

https://www.cryptomuseum.com/manuf/mils/files/mils_otp_proof.pdf
https://www.cryptomuseum.com
https://home.agh.edu.pl/~zobmat/2021/rzepka_radoslaw/zastosowania.html
https://bithub.pl/kryptowaluty/blockchain/liczby-pierwsze-w-kryptografii/
https://rcin.org.pl/dlibra/doccontent?id=2054
https://pl.wikipedia.org/wiki/Wikipedia:Strona_g%C5%82%C3%B3wna