DOI: 10.24425/academiaPAN.2023.147608

# Czym jest szyfrowanie

W dzisiejszym świecie przesyłanie informacji to kluczowa forma naszej aktywności. Informacje możemy kodować po to, żeby nikt postronny nie miał do nich dostępu.

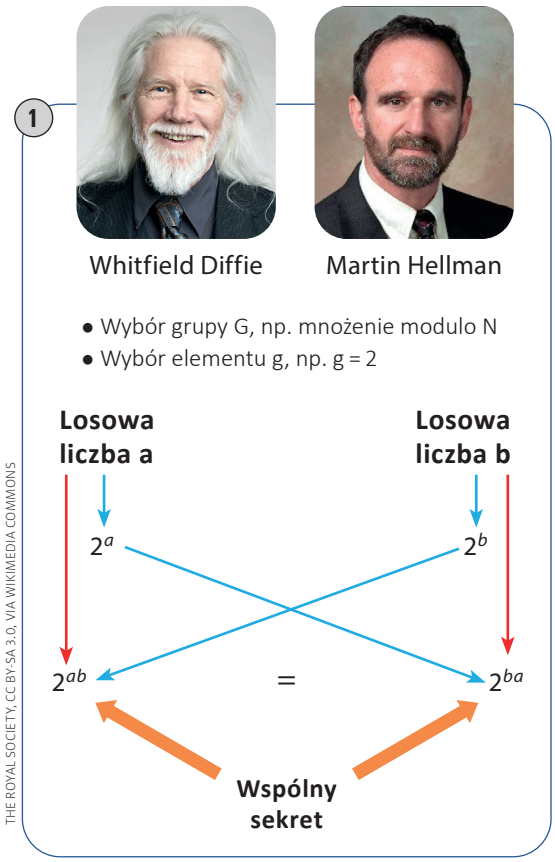
**dr Bartosz Naskręcki**
Matematyk, specjalizuje się w geometrii arytmetycznej, jest ekspertem teorii liczb i entuzjastą krystalografii matematycznej. Aktywny popularyzator wiedzy o polskich kryptologach. W życiu prywatnym jest szczęśliwym ojcem i mężem oraz notorycznym hodowcą awokado.
nasqret@gmail.com

**Bartosz Naskręcki**
Uniwersytet im. Adama Mickiewicza w Poznaniu
Instytut Matematyczny PAN w Warszawie

Wiek XXI to era informacji. Zalewa nas strumień danych, który jest niepo-równywalny do czegokolwiek widzianego wcześniej w historii. Żeby skutecznie i bezpiecznie przesyłać te dane, używamy niezwykle wyrafinowanych metod szyfrowania, których podstawowe idee sięgają cza-sów starożytnych.

Żeby zilustrować idee szyfrowania, posłużmy się przykładem. Chcemy przekazać komunikat osobie znajdującej się w innym pomieszczeniu, jedno krótkie zdanie, np. „Jestem w drugim pokoju". Ta informacja ma trafić tylko do jednej osoby. Każdy posługujący się językiem polskim bez trudu zrozumie sens tego zdania i wyciągnie oczywiste wnioski. Potrzebujemy pewnego sposobu zapisania tekstu w inny sposób, który w dodatku pozwala się odwrócić, czyli z kodu odzyskać wiadomość oryginalną. Zastosowanie pro-stej metody pozwala na zaszyfrowanie wiadomości.

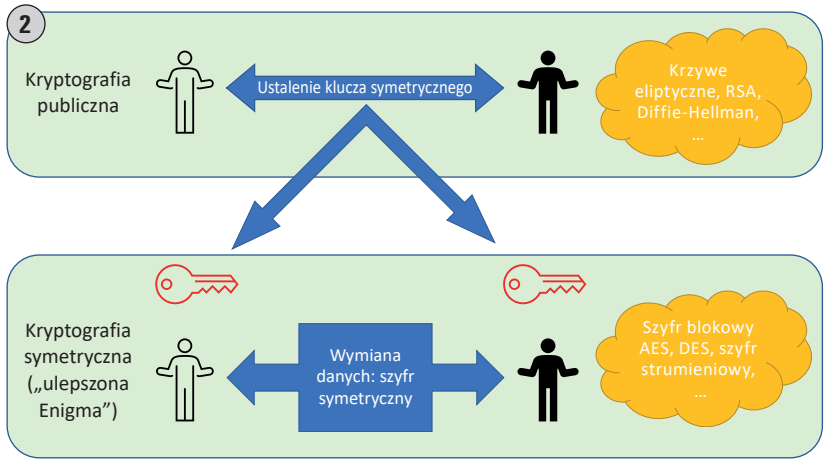

LENSCAP PHOTOGRAPHY/SHUTTERSTOCK.COM




Rys. 1
**Wymiana Diffiego-Hellmana**

## Wymiana Diffiego-Hellmana

Dwie osoby ustalają pewną liczbę, np. 2. Każda z nich wybiera pewną sekretną liczbę całkowitą, np. a i b. Obliczają $2^a$ i $2^b$ i wysyłają do siebie wynik. Obliczają teraz $(2^a)^b$ oraz $(2^b)^a$. Wynik jest równy $2^{a*b}$ i jest to ich wspólny sekret. Gdy wykonujemy operację potęgowania w arytmetyce zegarowej, czyli reszt z dzielenia przez N, otrzymamy wynik, w którym odtworzenie wykładnika a i b jest niezmiernie skomplikowane. Problem odzyskania liczb a z ($2^a$ modulo N) jest znany jako problem logarytmu dyskretnego. Generowanie w ten sposób wspólnych sekretów jest szalenie proste i skuteczne zarazem. Jest to rozwiązany problem tworzenia wspólnego klucza dla wymiany szyfrem blokowym (rys. 2).




Rys. 2
**Szyfrowanie stron WWW**

Literę A zastępujemy literą B, literę B literą C itd. Załóżmy dla uproszczenia, że mamy alfabet łaciński, który składa się tylko z 26 wielkich liter. Litera Z przejdzie na literę A. Usunięcie spacji nie stanowi dużego wyzwania przy czytaniu. W efekcie uzyskamy tekst: „KFTUFNXESVHJNQPLPKV". Nie wygląda zrozumiale, prawda? Jeśli przekażemy tekst, w obecności osób postronnych w pokoju, wówczas nikt nie będzie w stanie szybko tej wiadomości odczytać bez zanotowania jej na papierze. Jak nasz rozmówca odkoduje wiadomość? Po prostu przesunie litery o jedną pozycję w lewo. Otrzyma informacje: „JESTEMWDRUGIMPOKOJU".

Taki sposób zakodowania informacji nazywamy szyfrem Cezara. Rzymski przywódca Juliusz Cezar stosował ten prosty zabieg do ukrywania informacji przed osobami postronnymi. Najważniejsze cechy, które posiada ta metoda, to: szybkość zakodowania wiadomości, odwracalność procesu, ukrycie informacji przed osobą postronną, niewielka ilość informacji potrzebna do jej zakodowania.

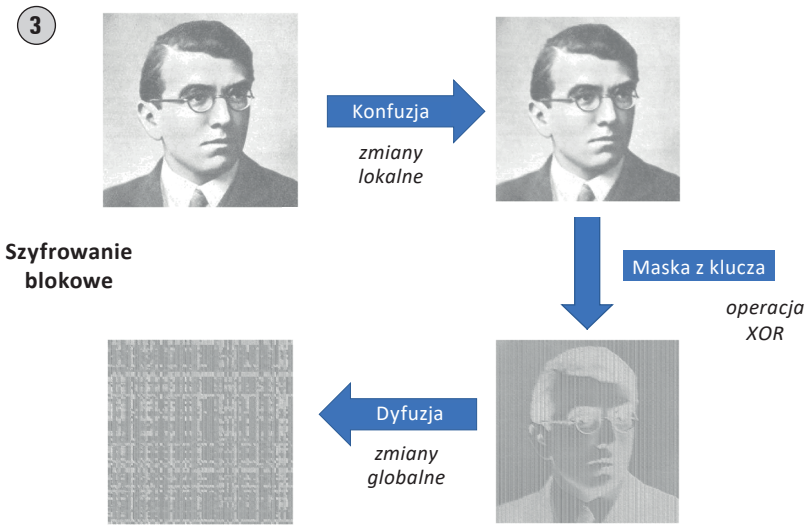
Te cztery cechy to postulaty naszego bezpieczeństwa informacyjnego. Istotą współczesnej kryptologii, czyli nauki o tworzeniu i łamaniu szyfrów, jest dostarczanie procedur, które spełniają te wymagania i gwarantują nam wysoki poziom bezpieczeństwa – odczytanie oryginalnej wiadomości bez znajomości sekretnego klucza jest w praktyce niemożliwe.

W internecie nikt z nas nie wysyła pasków papieru, na których odnotowujemy niezrozumiałe symbole, lecz przesyłanie danych musi spełniać opisane wyżej postulaty.

Procedury przetwarzania danych tak samo jak wymieniony wcześniej szyfr Cezara pozwalają wysyłać ogromną liczbę „pasków z wiadomościami". Informacji jest tak dużo, że możemy je mierzyć liczbą symboli sięgającą $10^{20}$ elementów. To trudna do wyobrażenia ilość informacji. Zwykły szyfr Cezara jest za prosty, by zakodować bezpiecznie taką ilość danych.

## Kodowanie wiadomości

W sukurs przychodzi nam idea, którą przypisuje się Blaise'owi de Vigenère, francuskiemu uczonemu żyjącemu w XVI wieku. Szyfr Cezara, polegający na przesunięciu liter, jest bardzo prosty do złamania. Mając dany ustalony język, wystarczy zrobić tabelę występowania częstości liter i porównując w oryginalnym alfabecie i zakodowanym, zestawić najczęściej występujące litery. Takie działanie bardzo często da nam prawidłową informację o przesunięciach potrzebnych do rozkodowania wiadomości. Nowy pomysł Vigenère'a polegał na tym, że możemy ustalić nieznanej długości słowo kodowe – klucz, którego litery będą decydować, o ile pozycji przesuwamy dany znak.






Rys. 3
Szyfrowanie blokowe. Na zdjęciu Henryk Zygalski – jeden z trójki poznańskich kryptologów, którzy złamali Enigmę

Na przykład używamy klucza:
ABC (zamieniamy litery na przesunięcia);
A –> 0; B –> 1; C –> 2.
Tekst jawny: ALAMAKOTA.
Używamy klucza: ABCABCABC, otrzymujemy w ten sposób szyfrogram: AMCMBMOUC.

Mając dostatecznie długie słowo kodowe, możemy spowodować, że złamanie takiego szyfru stanie się bardzo trudne. Gdy długość klucza jest równa długości wiadomości, otrzymujemy szyfr doskonały, zwany *one-time pad*.

Tak trudne, że w praktyce niemożliwe bez specjalnych metod. Takim szyfrem Vigenère'a „do potęgi" była maszyna szyfrująca Enigma, w której praktycznie każda litera jest szyfrowana innym alfabetem. Jednakże ten kod po raz pierwszy złamał w 1932 roku Marian Rejewski, absolwent Uniwersytetu Poznańskiego. Istotną rolę w tym przełomie odegrali również Jerzy Różycki i Henryk Zygalski, koledzy Rejewskiego z Biura Szyfrów. Zidentyfikowali i wykorzystali pewne regularności w sposobie szyfrowania Enigmy.

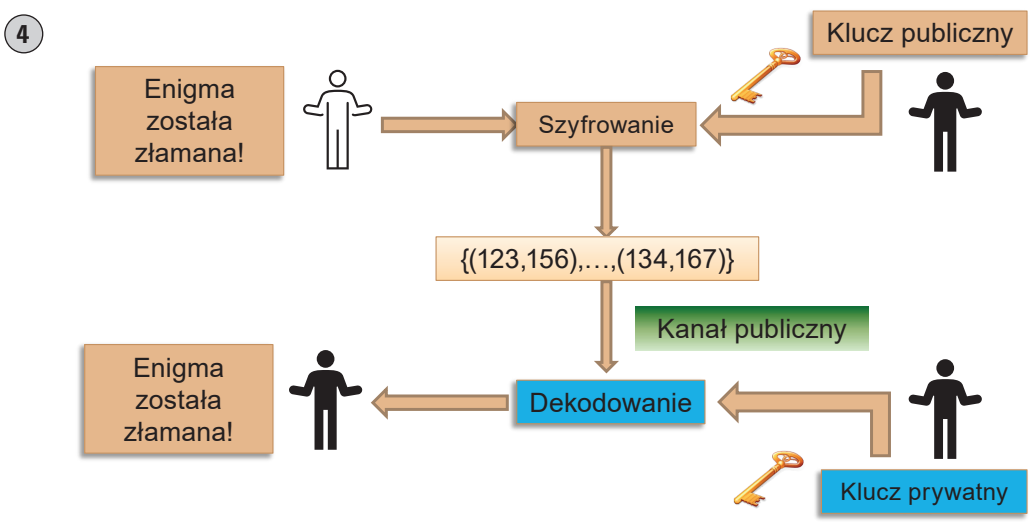
## Wyrafinowane szyfry blokowe

Lata I i II wojny światowej oraz powojenne to stopniowa transformacja szyfrowania z klasycznej domeny lingwistyki w to, co dziś nazywamy nowoczesną kryptografią. Ogromny rozwój nastąpił w latach 70., gdy zastąpiono tradycyjne szyfrowanie znakowe bardziej wyrafinowanymi szyframi blokowymi.

Szyfry blokowe można porównać do tasowania kart. W każdej rundzie wykonujemy operacje, które są z pozoru trywialne: konfuzja, maska z klucza, dyfuzja (rys. 3). Powtarzane wielokrotnie powodują olbrzymie skomplikowanie szyfru. Wymyślony w 1975 roku system Data Encryption Standard i jego następca Advanced Encryption Standard z 2001 roku jest obecnie używanym podstawowym szyfrem do bezpiecznego kodowania wiadomości o bardzo dużych rozmiarach. Praktycznie cały ruch w internecie jest szyfrowany standardem AES.

Co ciekawe, ten szyfr opiera się w swej istocie na jednej nieskomplikowanej obliczeniowo operacji, obliczania odwrotności elementu w ciele skończonym (tu konkretnie – 256-elementowym). A zatem mamy nasz ulepszony szyfr Cezara, który idealnie nadaje się do zaszyfrowania filmu lub innego olbrzymiego zbioru danych.

Żeby szyfry mogły być używane z sukcesem, nadawca i odbiorca wiadomości muszą znać klucz do szyfrowania. W połowie lat 70. w kryptografii pojawiły się dwa rozwiązania tego problemu. Pierwszy pomysł polega na generowaniu wspólnej tajemnicy tzw. protokołem Diffiego-Hellmana. Drugi pomysł polegał na stworzeniu procedury, w której mamy dwa klucze (rys. 4): publiczny, służący tylko do szyfrowania wiadomości, i prywatny, służący tylko do ich dekodowania. Potrzebujemy jeszcze procedury, która wytworzy




Rys. 4
Kryptografia z kluczem publicznym

taką parę kluczy i pozwoli nam udostępnić publicznie tylko klucz oznaczony jako „publiczny". W ten sposób każda osoba może nam wysłać sekret, ale nikt niepowołany nie może go odczytać bez klucza prywatnego. W konkretny sposób pomysł ten został wcielony w życie przez Rona Rivesta, Adiego Shamira i Leonarda Adlemana i jest znany jako algorytm RSA.

## Tajemnicze splątanie kwantowe

Stopniowo od lat 90. kryptografia stała się absolutną domeną matematyków zajmujących się liczbami i algebrą. Największymi zdobyczami ostatnich lat jest zastąpienie poczciwego podnoszenia liczb do potęg bardziej wyrafinowaną operacją algebraiczną zwaną dodawaniem na krzywej eliptycznej. Krzywe eliptyczne są obiektami z zakresu algebry i geometrii, który niezwykle przysłużył się nauce w dziedzinach tak różnorodnych jak fizyka wysokich energii, geometria różniczkowa, analiza czy teoria liczb. Słynne wielkie twierdzenie Fermata udowodnione w 1994 roku przez Andrew Wilesa wykorzystuje w kluczowych miejscach argumentu właśnie krzywe eliptyczne. Kryptografowie odkryli dla siebie te obiekty dość późno, ale z wielkim skutkiem. Każdy aspekt naszego życia „internetowego" wykorzystuje krzywe eliptyczne dla zagwarantowania wysokiego poziomu bezpieczeństwa przed złamaniem haseł.

W latach 80. XX wieku pojawiło się zagrożenie dla bezpieczeństwa algorytmu RSA i protokołu Diffiego-Hellmana w związku z użyciem algorytmu faktoryzacji Petera Shora. Przy obecności dużego komputera kwantowego algorytm ten lamałby bez trudu kody oparte na mnożeniu.

Coraz prężniejszy rozwój komputerów kwantowych i teorii informacji kwantowej spowodował pewną ucieczkę do przodu kryptografów zajmujących się RSA, krzywymi eliptycznymi i faktoryzacją. W ostatnich latach jesteśmy świadkami narodzin zupełnie nowej, tzw. postkwantowej kryptografii. O palmę pierwszeństwa obecnie walczy kilka algorytmów szyfrowania, mających zastąpić protokoły, które w przyszłości przy użyciu dużych komputerów kwantowych będziemy łamać bez trudu. Rozwój jest bardzo dynamiczny i dramatyczny. Spośród kilkudziesięciu kandydatów zgłoszonych do konkursu Post-Quantum Cryptography, ogłoszonego w 2016 roku przez amerykański National Institute of Standards and Technology, zostało już złamanych większość szyfrów i wyścig trwa dalej ze zwycięzcami czwartej rundy konkursu, ogłoszonymi w 2022 roku: CRYSTALS-Kyber – do generowania wspólnego sekretu, CRYSTALS-Dilithium, FALCON i SPHINCS+ – algorytmami do uzyskania podpisu elektronicznego.

Alternatywą jest również tzw. kryptografia kwantowa. Niezwykle prężnie rozwijający się dział fizyki i teorii obliczeń kwantowych, który pozwala zbudować oparte na laserach układy do bezpiecznego – na poziomie praw fizyki – przesyłania informacji na duże odległości. Podstawową ideą, którą się tu wykorzystuje, jest możliwość wygenerowania wspólnego sekretu, stosując tajemnicze splątanie kwantowe cząstek. W rozwoju tej technologii ponownie swój wkład mają Polacy, m.in. w osobie prof. Artura Ekerta, fizyka teoretycznego, który za swój wkład w tę dziedzinę otrzymał niedawno Nagrodę Milnera.

Współczesna cywilizacja jest oparta na informacji i wymaga silnych certyfikatów bezpieczeństwa przesyłania danych. Postulaty bezpieczeństwa są tak wyśrubowane, że aby im sprostać, wykorzystuje się niezwykle zaawansowany aparat matematyczny algebry, teorii liczb, kombinatoryki i statystyki. Można więc z pełnym przekonaniem powiedzieć, że matematyka pojawiła się już praktycznie wszędzie dzięki globalnej sieci internetowej. Jest ona cichym i dobrze naoliwionym, tajemniczym mechanizmem, który w ukryty sposób, jak w książce Umberto Eco „Wahadło Foucaulta", rządzi naszym światem i pozwala nam spać spokojnie, w czasie gdy maszyny obliczeniowe pracują na nasze bezpieczeństwo i dobrobyt (rys. 2). ■

### Szyfrowanie RSA

polega na wyborze dwóch bardzo dużych liczb pierwszych. Obliczamy ich iloczyn N = p*q. Znalezienie z liczby N wartości p i q jest ekstremalnie trudne (ryc. 5). Wiadomość wysyłana algorytmem RSA to liczba, np. m. Za pomocą liczb p i q przygotowujemy klucz prywatny i publiczny. Losujemy liczbę e, która jest względnie pierwsza z (p-1)*(q-1). Obliczamy liczbę d, która ma tę własność, że e*d = 1 modulo (p-1)*(q-1). Otrzymaliśmy klucz prywatny (N, d) oraz klucz publiczny (N, e). Wiadomość można bezpiecznie przesyłać, wykonując potęgowanie modularne: $c = m^e$ modulo N. Osoba postronna bez znajomości liczb p i q nie jest w stanie odtworzyć wiadomości m. Żeby zdekodować wiadomość, należy: $m = c^d$ modulo N. RSA polega na potęgowaniu zegarowym (modularnym) liczb całkowitych.

5


Ron RIVEST


Adi SHAMIR


Leonard ADLEMAN

- Wybieramy dużą liczbę całkowitą N. Ustalamy dwie liczby całkowite e i d, które dają odwracalne operacje na zegarze.
- Szyfrowanie RSA: wiadomość m kodujemy jako $c = m^e$.
- Dekodowanie RSA: szyfrogram c dekodujemy za pomocą $c^d$.
- Obliczenia wykonujemy na zegarze, czyli „modulo N".