Kryptografia a liczby pierwsze

Autor

Dariusz Kulma

Wstęp

Liczby pierwsze są absolutnie zadziwiające mimo swej prostoty. Rzadko sobie uświadamiamy, że mamy z nimi do czynienia wszędzie, a szczególnie jeśli dotyczy do ochrony danych - kart bankowych, systemów bezpieczeństwa komputerów czy ochrony prywatności rozmów mailowych czy telefonicznych. Jeden z nowoczesnych systemów kryptograficznych KRYPTOSYSTEM RSA opiera się właśnie na operacjach z wykorzystaniem liczb pierwszych. Można powiedzieć, że dzięki liczbom pierwszym możemy czuć się bezpieczni.

Po co znajdować kolejne liczby pierwsze?

Od wieków matematycy prześcigali się w znajdowaniu kolejnych liczb pierwszych. Chcieli znajdować coraz większe. Jak dotąd nikomu nie udało się podać wzoru, który pomógłby znajdować te liczby, takie jakbyśmy chcieli. Nieprzewidywalność liczb pierwszych spowodowała, że wielu ludzi wręcz poświęca swoje życie, by szukać kolejnych, już w tych czasach ogromych, liczb pierwszych. W tych czasach jest nie inaczej. Poszukiwania przybrały formę wyścigu, którego nagrodą jest sława i pieniądze. Tak, tak - pieniądze. **Electronic Frontier Foundation** ustanowiła nagrodę 100 tysięcy dolarów dla odkrywcy liczby pierwszej o więcej niż 10 milionach cyfr oraz nagrodę 150 tysięcy dolarów dla odkrywcy liczby pierwszej o więcej niż 100 milionach cyfr. Największa odkryta dotąd liczba pierwsza to 47 znana liczba pierwsza Mersenne'a: $2^{43112609}-1$ i liczy sobie 12978189 cyfr w zapisie dziesiętnym. Została ona odkryta 23 sierpnia 2008 roku przez Edsona Smitha – uczestnika projektu GIMPS. GIMPS (**Great Internet Mersenne Prime Search**) to projekt obliczeń rozproszonych, w którym biorą udział ochotnicy poszukujący właśnie liczb pierwszych Mersenne'a. Założycielem i autorem oprogramowania jest George Woltman.

Przykłady pokazują, że powstają nawet wielkie organizacje, które koordynują prace nad szukaniem liczb pierwszych. Dlaczego dla ludzi tak ważne są więc te nowe - ogromych już rozmiarów - liczby pierwsze?

Jedna z bezpośrednich przyczyn to związek liczb pierwszych z szyfrowaniem. Poczta elektroniczna, transakcje między bankami czy jakiekolwiek przesyłanie danych jest szyfrowane w oparciu o własności liczb pierwszych.

Szyfrowanie a wielkie liczby pierwsze

W 1975 roku Whit Diffe i Martin Hellman wpadli na pomysł szyfrowania asymetrycznego. Jest to system oparty na funkcjach matematycznych o specjalnych własnościach nazwanych funkcjami jednokierunkowymi. Pozwalają one bardzo dobrze zaszyfrować informację i nie ma praktycznie żadnych szans na złamanie tego szyfru bez odpowieniego klucza. Każdy użytkownik ma dwa klucze -

prywatny i publiczny. Jeśli wysyłamy jakąś zaszyfrowaną wiadomość używamy klucza publicznego, ale już aby odczytać wiadomość, należy użyć klucza prywatnego. Oczywiście przykład jest uproszczony, ale posłużmy się już liczbami pierwszymi i edytorem wyznaczania liczb pierwszych mniejszych od miliarda.

W 1977 roku zaprojektowano jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów z kluczem publicznym zwanym **RSA,** a wymyślonym przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Był to pierwszy algorytm, który może być stosowany zarówno do szyfrowania jak i do podpisów cyfrowych. Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych. Jego nazwa pochodzi od pierwszych liter nazwisk jego twórców.

Edytor wyznaczania liczb pierwszych mniejszych od miliarda

Edytor wyznaczania liczb pierwszych mniejszych od miliarda.

Dariusz Kulma - Matematyka innego wymiaru, Utworzony z GeoGebra

Próba szyfrowania

Dokładne zanalizowanie metody szyfrowania z wykorzystaniem liczb pierwszych jest dość skomplikowane do przedstawienia, ale spróbujmy omówić idę na uproszczonym przykładzie. Wyobraźmy sobie, że mamy jakąś liczbę np. 143, która jest szyfrem naszej wiadomości. By ją otworzyć, musimy odczytać czynniki pierwsze, na jakie rozkłada się ta liczba. Oczywiście po kilku obliczeniach uda się stwierdzić, że są to liczby 11 i 13. Czy jednak tak łatwo pójdzie nam z liczbą **4 056 187**?

Sprawdźmy za pomocą edytora, na jakie czynniki rozkłada się ta liczba. Okazuje się, że liczba ta to iloczyn **2011** i **2017**. Nie jest łatwo wpaść na to nawet przy pomocy kalkulatora, a obliczenia będą bardzo żmudne. A przecież liczby **2011** i **2017** to dopiero 305 i 306 liczba pierwsza, a każda jest tylko czterocyfrowa.

Liczba **99 890 710 929 007** rozkłada się na dwie wizualnie podobne do siebie liczby **99990001** i **999007**. Tu obliczenia za pomocą kalkulatora są absolutnie niemożliwe. A przecież liczb pierwszych mniejszych od 2 milionów jest blisko 150 tysięcy! Gigantyczna liczba możliwości. Biorąc pod uwagę, że największa liczba pierwsza ma 12 978 189 cyfr to szyfrowanie jest niemal doskonałe. Z takimi liczbami nie radzą sobie już komputery, ponieważ ich moc obliczeniowa nie jest wystarczająca. Obliczono, że złamanie szyfru o długości 1024 cyfr zajęłoby tyle, ile szacowany wiek wszechświata czyli 13,7 miliarda lat!

Jak widać liczby pierwsze są fantastycznym narzędziem kryptografii, broniąc nas przed nieoczekiwanymi próbami hakerów czy po prostu przed nieuczciwymi zachowaniami.