Piotr Górski

W okowach szyfrów

Fot. Braden Hays

Mało kto zdaje sobie sprawę, jak bardzo powszechne dzisiaj stały się sposoby komunikowania zapoczątkowane m.in. przez Gajusza Juliusza Cezara (100 p.n.e.-44 p.Chr.), a później wykorzystywane z różnym skutkiem przez osoby tak zapisujące się na kartach dziejów, jak: francuski mąż stanu, kardynał Armand Richelieu (1558-1642), czy – być może - szpiedzy Mata Hari (1876-1917) lub Richard Sorge (1895- 1941). Przecież wstukiwanie PIN-u nie bardzo nasuwa nam myśl, że oto właśnie pośrednio korzystamy z doświadczeń będących efektem skonstruowania, a następnie rozpracowania Enigmy - niemieckiej maszyny szyfrującej z czasów II wojny światowej.

Wchodząc na stronę internetową lub logując się hasłem, nie mamy świadomości, że w tej chwili skorzystaliśmy z szyfru, czyli metody poufnej korespondencji. Kryptologia, która ostatnio niezwykle się rozwija, to według Leksykonu PWN: „nauka o szyfrowaniu obejmująca metodykę szyfrowania (kryptografia) i łamania nieznanych szyfrów, tj. ustalenie sposobu szyfrowania w wyniku analizy zakodowanych tekstów (kryptoanaliza)". Kryptografia zaś to ogół metod utajniania informacji za pomocą szyfrowania, a słowo „szyfr" – według tego samego źródła- wywodzi się z języka arabskiego i oznacza kod stosowany w niektórych dziedzinach, np. przy przesyłaniu tajnych informacji.

Kodowanie informacji, to zadania głównie z dziedziny wielkich liczb (stosuje się kombinacje na liczbach zapisywanych w postaci 600 i więcej cyfr dziesiętnych, czyli od 0 do 9, a standardem są liczby ponad 200-cyfrowe). Naukowcy specjalizujący się w tej dziedzinie wiedzy to dzisiaj nie lingwiści czy historycy, ale głównie matematycy, informatycy i cybernetycy. Być może jednak już nie długo poszerzy się krąg naukowców zgłębiających metody tajnego lub poufnego porozumiewania się. Najbliżej dziedziny, ekscytującej przeciętnych obywateli, wydają się być dzisiaj fizycy. Trwają

Fachowcy od kryptoanalizy wykryli też, że wybitnym włamywaczom wystarczy sam pomiar czasu, by określić rodzaj klucza, a to już jest milowy krok do jego złamania.

prace nad kryptografią kwantową, ale jej zastosowanie jak dotąd nie wyszło z fazy eksperymentów. Wizjonerzy prognozują, że kiedyś dołączą do nich biolodzy, a także psycholodzy i psychoanalitycy. Nie powinno ulec jednak zmianie podstawowe pojęcie dla tej działalności, a mianowicie „algorytm". Ma ono dwa znaczenia: w cybernetyce jest to *dokładny opis wykonania w określonym porządku skończonej liczby operacji, pozwalający na rozwiązanie każdego zadania danego typu, a w matematyce: reguła przekształcania wyrażeń matematycznych przez powtarzanie tych samych działań na kolejno otrzymanych wynikach działań poprzednich.*

Szyfrowe słowa na „b"

Atrakcyjność komunikacyjna elektronicznego przekazu wynika z powszechności i ogólnej dostępności. Wystarczy prześledzić choćby rozwój płatności bezgotówkowej, by zdać sobie sprawę z masowości tego procesu. Przykładowo MasterCard rozpoczął swoją działalność na polskim rynku w 1995 r. Banki członkowskie wydały wówczas 200 tysięcy kart tego systemu. W tym czasie karty płatnicze były akceptowane głównie przez sklepy, hotele, restauracje obsługujące zagranicznych turystów – było to zaledwie 12,9 tys. punktów. Obecnie w portfelach Polaków jest 900 tys. kart obciążeniowych i kredytowych oraz 5,3 mln kart debetowych. Mogą z nich korzystać w 85 tys. punktach handlowo-usługowych i 7,9 tys. bankomatach w Polsce, a także w 24 mln punktów akceptacji na całym świecie - w tym w 7 mln w samej Europie. Zapewnienie bezpieczeństwa tylko tak dokonywanym transakcjom wydaje się przedsięwzięciem ogromnym. W dodatku dane, które tu przytoczyłem, dotyczą tylko Polski i tylko jednego systemu kart. Według „Rzeczpospolitej" w ubiegłym roku z usług finansowych przez Internet skorzystało 6 proc. Polaków kontaktujących się z bankiem. W tym samym czasie do takiej instytucji osobiście udało się 57 proc. rodaków. Widać więc, że w tej dziedzinie możliwy jest jeszcze wzrost. Bezpieczeństwo tego obrotu może mieć więc kluczowe znaczenie. W ten sposób mamy pierwsze słowo na „b" – czyli bezpieczeństwo – ważne dla współczesnych szyfrantów. Drugim kluczowym słowem na tę samą literę jest biznes. Można dużo zarobić już tylko na opracowaniu algorytmów, czyli procedury postępowania w szyfrowaniu i deszyfrowaniu informacji. Zwłaszcza, że straty w transakcjach wykonywanych w sieci bez zabezpieczeń mogą iść w miliony dolarów.

Matematyka przestępców?

Na niedawno organizowanym panelu zatytułowanym „Bezpieczeństwo bankowości elektronicznej" w poznańskiej Akademii Ekonomicznej, Krzysztof Jan Jakubki - kierownik Zespołu Ochrony Informacji Departamentu Bezpieczeństwa i Administracji Banku Polskiej Spółdzielczości SA – nie miał wątpliwości, że przestępstwa komputerowe są u nas możliwe i dla złoczyńców atrakcyjne. Utrzymywał, że mogą być one nawet trudno wykrywalne. Przytaczał taki przykład: w jednym z banków zachorował administrator sieci i dyrektor banku - tylko na ten krótki czas – zaproponował „opiekę" informatyczną nad swoją instytucją informatykowi obsługującemu „przybankowe" biuro maklerskie. Ten się zgodził, ale w trochę dziwnych godzinach. W poniedziałek chciał być w pracy przed 6. rano, a w piątek zostawać dłużej po południu. Warunki te zaakceptowano. Gdy tylko chory wrócił do pracy, zastępca zniknął. Właśnie tylko to „zaginięcie" było przyczyną wszczęcia śledztwa. Okazało się, że jednoczesna obsługa banku i biura maklerskiego może dać szanse na nielegalny zarobek. Jak wiadomo, środki na rachunkach inwestycyjnych w biurach maklerskich są nieoprocentowane. Od piątku do poniedziałku giełda nie działa. Jeśli ma się internetowy dostęp do kont i możliwość dysponowania nimi, to można niepostrzeżenie w piątek przelewać pieniądze na inne konto, a w poniedziałek z powrotem umieszczać je tam, gdzie być powinny. Ślad przeprowadzenia tej wirtualnej operacji można wykasować, tak by nie było wiadomo, że pieniądze „wędrowały". Tylko fakt naliczenia odsetek wynoszących ok. 1 mln dolarów na koncie informatyka oraz to, że po raz ostatni odnotowano jego pobyt na lotnisku we Frankfurcie nad Menem wskazało, że dokonano przestępstwa.

Trudno jednak powiedzieć, czy lepszy szyfr zapobiegłby tego typu machinacji. Specjaliści twierdzą, że nie ma kodu nie do złamania i przytaczają przykład pierwszego rozpowszechnianego systemu klucza tajnego, czyli DES (*Data Encryption Standard*). Został on opracowany – z wykorzystaniem algorytmu Lucifer Horsta Feistela – przez firmę IBM w latach 70. Po akceptacji przez Narodowe Biuro Standardów USA (ANSI) stał się standardem szyfrowania danych nie utajnionych przez agencje rządowe. W dwadzieścia lat później podjęto skuteczny atak na ten standard i szyfr został złamany. Dokonano tego dla klucza 52-bitowego, umożliwiającego łącznie ponad 72 kwadryliony kombinacji (aby mówić o bezpieczeństwie, dzisiaj należy mieć na myśli klucze o długości co najmniej 80 bitów a najlepiej 128 bitów). Grupa nazwana „Deschall" w ciągu pół roku przeprowadzała najprostszą z możliwych prób, czyli atak siłowy. Testowała każdy możliwy klucz i osiągnęła zakładany rezultat. Trzeba jednak przyznać, że przy dużej do-

zie szczęścia, bo na rozwiązanie trafiono już po sprawdzeniu ok. 25 procent możliwych kombinacji.
Fachowcy od kryptoanalizy wykryli, że wybitnym włamywaczom wystarczy sam pomiar czasu, by określić rodzaj klucza, a to już jest milowy krok do jego złamania.

Pojęcia nie do pojęcia, że strach

Niedawno świat obiegła informacja, że została udowodniona licząca 150 lat „Hipoteza Reimanna". Według tych samych źródeł oznaczać to miało ogromne kłopoty dla handlu w Internecie. Czy to prawda, czy tylko straszenie internautów? Podstawą odpowiedzi byłaby zapewne treść hipotezy. W najprostszej, według naukowców, wersji brzmi ona tak: „Hipoteza Riemanna dotyczy tzw. funkcji dzeta Riemanna. Funkcja ta pozwala na oszacowanie liczby liczb pierwszych, nie większych niż dana. W tym kontekście istotne znaczenie mają takie wartości, dla których funkcja twierdzenia przyjmuje wartość zero - tzw. miejsca zerowe. Hipoteza Riemanna mówi, iż wszystkie nietrywialne (tzn. „trudne do znalezienia") zera funkcji dzeta Riemanna są określonej postaci, tzn. są liczbami zespolonymi (tj. liczbami postaci a+bi, gdzie i oznacza pierwiastek kwadratowy z -1, natomiast a, b są rzeczywiste), o części rzeczywistej równej 1/2."
Czy to może być zrozumiałe dla przeciętnego użytkownika Sieci? Jeśli ktoś z czytelników nie pojął w czym rzecz, to... mam już towarzystwo. Nie drążąc więc matematycznego tematu i nie rozstrzygając, czy hipoteza została udowodniona, czy nie, przedstawię tylko to, co mi wytłumaczono. Hipoteza Riemanna jest trudna do udowodnienia prawdopodobnie z powodu „głębokiej nietrywialności samego zagadnienia, czyli badania rozmieszczenia liczb pierwszych". Wiadomo jednak, iż hipoteza Riemanna jest prawdziwa dla wszystkich (około 250 milionów) zer dotąd znalezionych metodami numerycznymi. To jest jedna z przesłanek przemawiających za prawdziwością tego założenia.
Jego konotacje z, np. e-handlem wynikają z tego, że najbardziej popularne algorytmy w szyfrowaniu danych stosowane w Sieci wykorzystują operacje na dużych liczbach pierwszych. Już samo określenie miejsca ewentualnego ich występowania mogłoby być dużym ułatwieniem dla działalności internetowych przestępców. Nie oznacza to jednak kresu kryptologii, ale jest nowym dla niej wyzwaniem. Tak samo, jak być może prawdziwa, informacja o złamaniu algorytmu SHA-1 przez chińskich naukowców z Shandong University. Nie będę jednak tu tłumaczył pojęcia algorytmu haszującego i opisywał konkretnej jego wersji nazwanej SHA-1 (*Secure Hash Algorithm*), której działanie ponoć udało się Chińczykom „rozgryźć". Podam tylko, że algorytm ten utworzony został w 1994 roku przez National Institute of Standards and Technology i był do tej pory uważany za bezpieczny pod względem kryptograficznym. Znajduje on zastosowanie, między innymi, w procesie generowania i weryfikacji podpisu cyfrowego. Jego ewentualne złamanie – według kryptologów - oznacza tylko to, że poprzeczka dla kryptoanalityków jest zawieszona na wyższym poziomie. Chińscy naukowcy prawdopodobnie przejdą do historii. Wysunięte zostaną propozycje funkcji haszujących, które będą stanowić nowe wyzwanie dla maszyn obliczeniowych oraz kryptoanalityków (np. SHA-512). Bardziej jeszcze uogólniając oznacza to także, że znowu na internetowym bezpieczeństwie będzie można zarobić. Większość matematycznych rozwiązań szyfrujących jest opatentowanych i za ich użycie, a także za programy je wykorzystujące, trzeba płacić.

Czy to konieczne i niezbędne?

Nie sposób wyobrazić sobie przesyłania danych bez ich kodowania. Pojawia się jednak podstawowe pytanie, czy tak zawsze być musi?

Odpowiedzi należy chyba szukać w rozwiązaniach, które towarzyszyły usługom pocztowym. Pierwotnie nikt nie dopuszczał, by była możliwość powszechnego czytania jakiejkolwiek czyjejś korespondencji (dzisiaj w dużej części zakaz jest etyczny) i obowiązywały koperty. Przełomem była kartka pocztowa. Dziś taka otwarta forma pisania jest bardzo popularna. Nadal jednak istnieje cały szereg informacji, których obieg jest poufny lub bardzo osobisty. Wydaje się, że i tak będzie w Internecie. Podział na jawną i zaszyfrowaną korespondencje wynikać będzie prawdopodobnie również z pewnych niedogodności (opłaty, czas transkrypcji itp.) towarzyszących tej drugiej. Niewykluczone jest jednak, że w przyszłości sposób kodowania, algorytm będzie związany bardziej z naszymi cechami psychicznymi i osobniczymi, a mniej z liczbami, które dzisiaj dominują.

Autor dziękuje wszystkim, którzy przyczynili się do powstania tego materiału. Szczególne wyrazy wdzięczności kieruje pod adresem dr Stanisława Gawiejnowicza z UAM za nad wyraz cierpliwe tłumaczenie skomplikowanych, dla wyżej podpisanego, zagadnień matematycznych i wyrozumiałość dla potrzeb dziennikarskich.