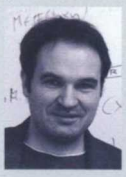
Kryptologia, czyli język szyfrów

Klucze i rozmowy z kartą



STEFAN DZIEMBOWSKI
Wydział Matematyki, Informatyki i Mechaniki
Uniwersytet Warszawski
crypto.edu.pl/Dziembowski
Dr hab. Stefan Dziembowski jest adiunktem na Wydziale Matematyki, Informatyki i Mechaniki UW oraz na Wydziale Informatyki Uniwersytetu La Sapienza w Rzymie. Pracował naukowo w Danii, we Włoszech i w Szwajcarii. Obecnie kieruje grupą zajmującą się badaniem bezpieczeństwa systemów komputerowych.

Academia: Zajmuje się pan kryptografią, ale też kryptologią. Jaka jest różnica między tymi pojęciami?

Stefan Dziembowski: Kryptologia składa się z kryptografii i kryptoanalizy. Kryptografia zajmuje się tworzeniem szyfrów i systemów kryptograficznych, a kryptoanaliza - ich łamaniem. Ten podział jest trochę sztuczny - wszyscy, którzy zajmują się jednym, zajmują się i drugim.

Porozmawiajmy więc o kryptografii.

To dziedzina rozwijana od czasów starożytnych - już Juliusz Cezar tworzył proste szyfry, żeby kontaktować się z wojskiem. Przez wiele wieków ludzie wymyślali jakiś szyfr, po czym inni go łamali, więc wymyślano nowy albo łatano stary, który ktoś znowu łamał... Ale dopiero w ciągu ostatnich dekad kryptografia stała się nauką. Jej eksplozja wiąże się z rozwojem informatyki - ona stworzyła język, który pozwolił formalnie mówić na temat bezpieczeństwa.

Właśnie. Czy istnieją szyfry niełamalne?

Każdy szyfr, w którym klucz jest krótszy niż wiadomość, daje się złamać, jeśli tylko ma się dostatecznie dużą moc obliczeniową. Pytanie tylko, czy wydajnie. Jeśli do złamania szyfru trzeba by używać wszystkich komputerów, jakie ma ludzkość, przez 1000 lat, to można uznać, że jest on dość bezpieczny.

Kryptografia służy zabezpieczeniu danych w procesie przesyłania lub gromadzenia. Podstawą tego zabezpieczenia jest szyfr.

Tak. Mamy algorytm szyfrujący i algorytm odszyfrowujący. Algorytm szyfrujący wykorzystuje tajny klucz i stosuje go do wiadomości. W ten sposób produkuje szyfrogram. Algorytm odcyfrowujący na podstawie szyfrogramu i klucza odczytuje wiadomość.
Z tym wszystkim wiążą się oczywiście problemy. Na przykład przy komunikacji przez Internet. Jaką właściwie mamy pewność, że wiadomość, którą otrzymaliśmy, pochodzi od osoby, która ją wysłała? Druga rzecz: skąd wziąć klucz? Jeśli się znamy, to możemy go ustalić, a potem go używać, ale w sieci nie ma takiej możliwości. Kiedy kupujemy w sklepie internetowym, musimy podać numer swojej karty kredytowej, a przecież nie spotkaliśmy się z właścicielem tego sklepu i nie wymieniliśmy wcześniej kluczy...

Jest na to jakaś rada?

Tak. Kryptografia klucza publicznego. Pomysł jest taki: robimy szyfr, w którym klucz do szyfrowania i klucz do odszyfrowania są inne. Co więcej, klucz do szyfrowania - mój klucz publiczny - mogę ujawnić każdemu. Jeśli ktoś chce wysłać mi wiadomość, szyfruje ją kluczem publicznym, a odtworzyć ją mogę tylko ja, bo tylko ja mam prywatny klucz do odszyfrowania. Oczywiście znajomość klucza publicznego nie może pozwalać na odgadnięcie, jaki jest klucz prywatny.
Podobnie można zrobić z uwierzytelnianiem - mogę wysłać wiadomość, podpisując ją moim kluczem prywatnym, i każdy, kto ma mój klucz publiczny, może sprawdzić, czy wiadomość rzeczywiście pochodzi ode mnie. To się nazywa podpis elektroniczny.

Dotychczas kryptografia kojarzyła mi się z Enigmą i Marianem Rejewskim...

Enigma była maszyną, w środku były rotory, a teraz techniki są zupełnie inne, wszystko

Dr hab. Stefan Dziembowski, magistrantka Katarzyna Jankiewicz i dr Tomasz Kazana z Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego

robi się komputerowo. Postęp wydajności jest ogromny. Musi tak być, bo z jednej strony zawsze jest ktoś, kto ma skomplikowany, szybko działający system szyfrujący, a z drugiej jest przeciwnik, który chce go złamać. I on również dysponuje dużą mocą obliczeniową. Poza tym wiele szyfrów jest znanych publicznie, a tajność dotyczy wyłącznie klucza. Chodzi o to, że szyfry powinny działać bezpiecznie, nawet jeśli przeciwnik zna ich opis.

Najbardziej znanym szyfrem, który powstał w latach 70., jest Digital Encryption Standard. DES był wykorzystywany przez IBM, przy nie do końca jasnym udziale amerykańskich służb specjalnych. Amerykańska Agencja Bezpieczeństwa Narodowego (National Security Agency; NSA) to instytucja zatrudniająca najprawdopodobniej najwięcej matematyków na świecie. DES, wymyślony przez IBM przy udziale NSA, został opublikowany i stał się standardem amerykańskim i światowym. Przez lata ludzie nie byli pewni, czy DES jest bezpieczny. Czy NSA nie ukryła jakichś „drzwiczek"? Wadą DES jest krótki klucz, oficjalnie długości 64, ale w praktyce 56 bitów. Oznacza to, że liczba kluczy potencjalnych wynosi 2^{56}. Przejrzenie wszystkich 2^{56} kluczy w latach 70. XX wieku wydawało się trudne każdemu, poza oczywiście NSA.

Niestety, już dobrą dekadę temu to 2^{56} stało się osiągalne nawet dla zwykłych ludzi. Teraz już za parę tysięcy dolarów można kupić urządzenie, które łamie DES.

Ale historia tego szyfru nie przestała być ciekawa. Ma on strukturę, która jest logiczna, za wyjątkiem pewnych tajemniczych szczegółów. To tzw. S-boksy. W latach 80. i na początku 90. naukowcy działający w sferze akademickiej opracowali tzw. kryptoanalizę różnicową, która złamała parę szyfrów, ale... z DES sobie słabo radziła, właśnie za sprawą S-boksów. Wtedy dopiero IBM i NSA przyznały, że znały kryptoanalizy różnicowe już w latach 70., tylko nie chciały ich ujawniać. Kryptografia to więc taka trochę dziwna dziedzina, bo coś odkrywamy - my, naukowcy działający na uniwersytetach - i nagle okazuje się, że już 20 lat temu amerykańskie służby specjalne to znały, tylko nie ujawniły.

Na nowy szyfr zrobiono otwarty konkurs światowy. Wygrał projekt belgijski, który jest standardem już od 10 lat - szyfr AES (Advanced Encryption Standard).

Brzmi trochę niepokojąco w kontekście terroryzmu - okazuje się, że zawsze można znaleźć klucz „odkodowujący". Czy tak?

Tak, ale do tego trzeba mieć albo dużo szczęścia, albo dużo czasu. Teraz najkrótszy klucz AES ma 128 bitów. A to strasznie dużo. Nikt nie wierzy, że ktokolwiek może w tej chwili złamać AES. Nad łamaniem go pracują na uniwersytetach tysiące bardzo mądrych ludzi. Ryzyko, że terroryści zechcą nam coś złego zrobić, łamiąc AES, jest niewielkie, bo w porównaniu z całą mocą mózgów ludzi na świecie, którzy próbują go złamać, mają niewielkie możliwości. Natomiast różni złoczyńcy mogą, zamiast koncentrować się na łamaniu szyfrów, atakować samo urządzenie.
Dla bezpieczeństwa systemów komputerowych kryptografia jest jednym z narzędzi. Natomiast wiele innych aspektów bezpieczeństwa nie należy do kryptografii. Jeśli szyfrujemy, używając komputerów osobistych, to o wiele łatwiej jest zainstalować nam jakieś złośliwe oprogramowanie, np. wirusa. Wtedy, niezależnie od tego, czy mamy AES, czy DES, przeciwnik może sobie przeczytać, co chce. Gdybym miał kogoś podsłuchać, na pewno nie próbowałbym łamać szyfru, tylko włamałbym się do jego komputera. W związku z tym do poważniejszych zastosowań używa się specjalnych, dodatkowo zabezpieczonych urządzeń szyfrujących.
Jak zatem tworzyć urządzenia bezpieczne? I kryptografię, która byłaby bezpieczna, nawet jeśli urządzenia nie do końca spełniają to wymaganie? To jest między innymi temat moich badań.

Kieruje pan całą grupą. Czym dokładnie się zajmujecie?

Głównie teoretycznym podejściem do ataków fizycznych na urządzenia. Zastanawiamy się, czy można zrobić system, który pozostanie bezpieczny, nawet jeśli wiemy z góry, że przeciwnik będzie miał częściowy dostęp do urządzenia, na przykład pozna jakąś część klucza. Próbujemy to rozegrać od strony matematycznej, teoretycznej. A praktycy chcieliby, żeby to działało. Dyskutujemy więc z praktykami, mając nadzieję, że w końcu wykrystalizują się jakieś jasne modele i bezpieczne systemy.

A czy potraficie skonstruować coś bezpiecznego?

Jest taki żart: jaka jest różnica między teorią a praktyką? W teorii żadna... W ostatnich latach pojawiło się sporo wyników teoretycznych pokazujących, że się da, natomiast praktycy kręcą nosem, że to nie jest dokładnie to, o co chodzi. Myślę, że na coś, co będzie stosowane w praktyce będziemy musieli poczekać jeszcze parę lat.

Współpracujecie z wieloma wiodącymi ośrodkami: z Izraela, z USA, z Niemiec. A kim są odbiorcy waszych rozwiązań? Banki, armia...?

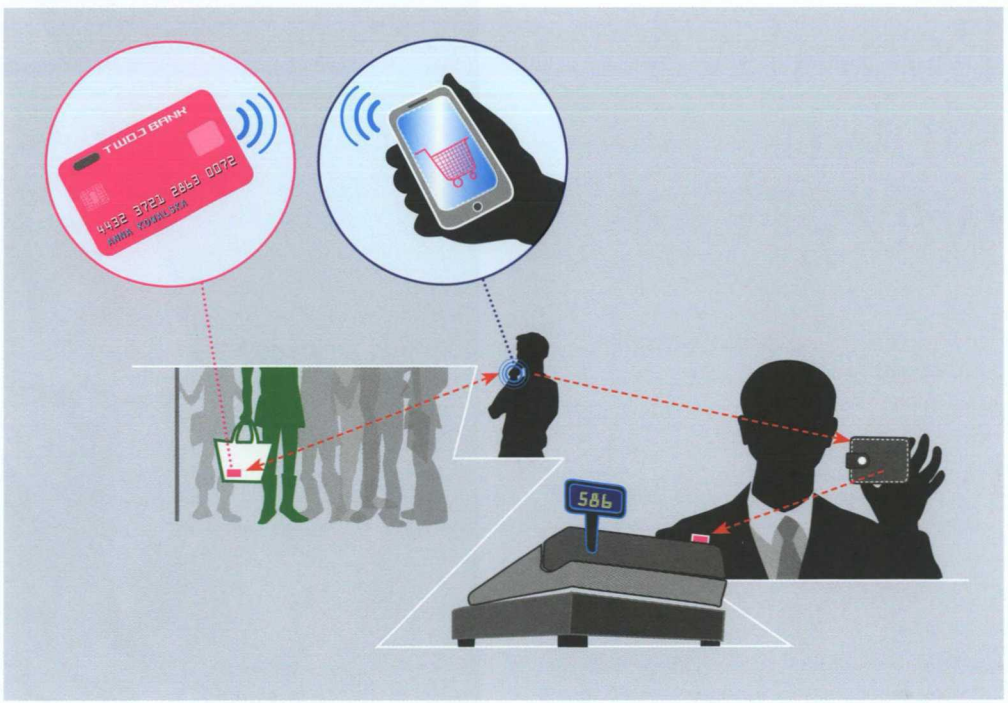
Na przykład banki. Ale nie jest to proste. Naukowiec myśli: mam rozwiązanie bezpieczniejsze, więc oczywiście powinienem nim zastąpić to mniej bezpieczne. A bank patrzy przede wszystkim na koszt wymiany wszystkich kart. Popatrzmy na karty dotykowe - z punktu bezpieczeństwa to po prostu tragedia.

Ja używam...

Ja też, ale jest z tym mnóstwo problemów. Choćby taki, że ktoś może do ciebie podejść - dajmy na to w tramwaju - i zacząć sobie z nią rozmawiać. Urządzenia do takiej komunikacji są tanie, nawet komórki to potrafią. (patrz infografika).

Do tej chwili czułam się z moją kartą bezpiecznie, teraz zaczynam się bać. Ale przecież są limity na kartach.

Są, ale na pojedyncze transakcje. W trybie offline nie ma limitu na sumę transakcji, o ile odbyły się w krótkim okresie, np. w czasie jednego dnia. Wystarczy, jeśli zacznę rano i wykonam sto transakcji, za każdym razem wydając 50 zł. I już masz na koncie mniej o 5000 zł.
Taki atak za pomocą zdalnego urządzenia jest zbyt wyrafinowany, żeby go wytłumaczyć czytelnikowi gazet - gazety wolą pisać o tym, że ktoś np. zgubił kartę lub mu ją ukradziono. Poza tym trzeba by zadać pytanie, dlaczego bankowcy lubią te karty? To proste: policzyli straty i zyski, i wyszło im, że mimo zagrożeń to się opłaca. Polska jest jednym z pierwszych rynków, na których to rozwiązanie jest wprowadzane, bo polscy konsumenci są mało uświadomieni. Banki de facto traktują nasz kraj jako poligon doświadczalny.
Generalnie gry komputerowe są o wiele lepiej zabezpieczone niż systemy bankowe. W przypadku gier komputerowych gracz zbiera miecze i zbroje, ma postać, która zabiła już ileś smoków i jeśli ktoś ukradnie mu hasło i nazwę, to gracz zostanie nagi, bez miecza



Rys. Paweł Kardyni

i zbroi... i dlatego w grach mamy bardzo poważne zabezpieczenia. Bankowcy mają zupełnie innych klientów i tam zabezpieczenia są do niczego.

Pozostaje nam więc bardzo uważać i często kontrolować transakcje. Ale wróćmy do pana. Jak to się stało, że zajął się pan kryptografią?

Przypadkiem. Wyjechałem do Danii pracować nad doktoratem i tam zetknąłem się z kimś, kto się zajmował kryptografią. Uznałem, że to najciekawsza część informatyki. W pewnym sensie działa wbrew niej. Generalnie informatyka zajmuje się wymyślaniem rozwiązań, które są najbardziej wydajne. Kryptografia to coś odwrotnego: szukamy problemów, które są trudne do rozwiązania. Dobra wiadomość dla algorytmików jest złą dla nas i na odwrót. To jest w pewnym sensie bycie po ciemnej stronie mocy. I w kryptografii intrygujące jest to, że stosuje się bardzo różne metody; właściwie wszystkie triki są dozwolone, jeśli prowadzą do celu.

Czyli wy, teoretycy, szukacie najlepszych metod zabezpieczania danych i metod ich łamania?

Nas, prawdę mówiąc, interesują publikacje. Jeśli wynikiem mojej pracy jest to, że coś można zrobić bezpiecznie, to dobrze. Jeśli wynikiem jest, że coś można złamać, to również dobrze - pod warunkiem że jest to ciekawe. Posuwamy naukę do przodu.

A czy etyczne jest łamanie publiczne znanych szyfrów?

Można zastosować argument, którego użyłem wcześniej: wiemy, że AES jest bezpieczny, bo tylu ludzi próbuje go złamać i nikomu się nie udało. Ktokolwiek go złamie, natychmiast to opublikuje - dla sławy. Poza tym są oczywiście służby specjalne... Może NSA wie, jak złamać AES - prawdopodobnie nikt inny na świecie takich możliwości nie ma. Myślę, że moc intelektualna amerykańskich służb specjalnych może przewyższać moc wszystkich naukowców razem wziętych. A i służby jakiegokolwiek innego kraju na pewno nie są na tym poziomie.

Rozumiem, że systemy, których używamy, np. karty chipowe, są absolutnie bezpieczne...

Cóż - kryptografia jest bezpieczna. W całej tej konstrukcji, którą nazywamy bezpieczeństwem systemów komputerowych, kryptografia jest najsilniejszym elementem. Największy problem to wirusy czy ataki fizyczne na urządzenia. ■

Rozmawiała **Anna Zawadzka**
Warszawa, 2013