Kryptografia i skomplikowane szyfry, które upraszczają życie

23 lutego 2018

Za każdym razem, gdy używamy przeglądarek internetowych, płacimy kartą, rozmawiamy przez komórkę czy oglądamy kablówkę, korzystamy z zabezpieczeń kryptograficznych. O tym, jak szyfrowane są nasze poufne informacje mówi PAP dr hab. Aleksander Wittlin.

Aby informacja nie dostała się w niepowołane ręce, można ją zaszyfrować. Sprawić, że stanie się niezrozumiała dla kogoś, kto wiadomość przechwyci. Dawniej szyfrów używano stosunkowo rzadko – np. przy wymianie poufnych listów wojennych lub… miłosnych.

Teraz, w erze telekomunikacji, z technik kryptograficznych korzystamy na każdym kroku: kiedy logujemy się do komputera, wpisujemy PIN w bankomacie, korzystamy z przeglądarki internetowej, rozmawiamy przez komórkę, a wreszcie – kiedy korzystamy z walut kryptograficznych… O szyfrowaniu, które stosujemy na co dzień – często bezwiednie, opowiada w rozmowie

z PAP popularyzator kryptografii, dr hab. Aleksander Wittlin z Instytutu Fizyki PAN w Warszawie.

Jak mówi, w kryptologii są trzy główne klasy algorytmów, które służą do ochrony poufności, integralności informacji. To algorytmy asymetryczne, funkcje skrótu i algorytmy symetryczne.

SYMETRIA NIEKONIECZNIE ESTETYKĄ GŁUPCÓW

„Ogromną większość bitów informacji, które współcześnie szyfrujemy, szyfruje się szyframi symetrycznymi" – mówi fizyk. Jak dodaje, jest to najstarsza znana klasa algorytmów.

Za pomocą jednego, tego samego klucza jedna strona szyfruje wiadomość, a druga – odszyfrowuje. Prostym przykładem jest chociażby tzw. szyfr Cezara (każdą literę zastępuje się literą odległą od niej w alfabecie o określoną, zadaną liczbę miejsc. Aby odszyfrować wiadomość, trzeba znać tę liczbę).

Obecnie techniki szyfrowania są zdecydowanie trudniejsze do rozgryzienia. Ale zasada jest podobna.

TELEFONY, KABLÓWKA, WOJSKO

„Algorytmem symetrycznym szyfrowane są np. płatne programy w telewizji" – opowiada prof. Wittlin. Hasło do szyfru dostajemy od operatora.

Naukowiec wyjaśnia, że również telefonia komórkowa oparta jest o kryptografię symetryczną. „Klucz do szyfrowania korespondencji, przekazywany drogą radiową, jest za każdym razem obliczany na podstawie przypadkowej liczby i tajnego klucza, który jest w chipie telefonu. Ten tajny klucz jest znany tylko użytkownikowi i firmie, u której kupiło się kartę" – powiedział dr hab. Wittlin.

Algorytmów symetrycznych praktycznie zawsze używa się też w kartach zbliżeniowych (z tagiem RFID).

JEDYNY SZYFR NIE DO ROZGRYZIENIA

Wśród algorytmów symetrycznych jest jeden wyjątkowy: szyfr Vernama. To jedyny znany dotąd algorytm kryptograficzny nie do złamania. Każda litera (lub znak tworzący wiadomość) szyfrowana jest osobno, w losowy sposób. Klucz może być użyty tylko raz i musi być przynajmniej tak długi, jak wiadomość. Ten algorytm ma jednak poważną wadę: obie strony muszą dostać wcześniej, przed zaszyfrowaniem wiadomości, ten sam klucz. A jego trzeba przekazać bezpiecznym kanałem – bezpośrednio z rąk do rąk.

Jednorazowymi kluczami rządy zabezpieczają np. personalia szpiegów – opowiada naukowiec.

„W PRL wszystkie sukcesy związane z łapaniem szpiegów nie polegały na łamaniu szyfrów – tylko na tym, że SB włamało się do kogoś i znalazło jednorazowe klucze. Fakt posiadania takiego klucza gwarantował w pewnym okresie historycznym dożywocie. Albo i gorzej" – opowiada popularyzator.

OTWORZĄ INNYM KLUCZEM, NIŻ TY ZAMKNIESZ

W algorytmach symetrycznych elementem newralgicznym jest moment przekazywania klucza. Nie zawsze bowiem dysponujemy kanałem bezpiecznym do jego dystrybucji. Właśnie dlatego popularność zyskała kryptografia z kluczem publicznym, a więc algorytmy asymetryczne. Tam zaszyfrować wiadomość może każdy, używając udostępnionego przez odbiorcę klucza publicznego. A odczytanie wiadomości możliwe jest tylko przy użyciu innego klucza – klucza prywatnego, który posiada tylko odbiorca. „Taki system pozwala komunikować się dwóm stronom, nie posiadającym bezpiecznego kanału do uzgodnienia klucza" – opowiada Aleksander Wittlin. Jednym z bardziej znanych algorytmów tego typu jest RSA.

W algorytmach asymetrycznych stosuje się problemy matematyczne, uznane powszechnie za trudne do rozwiązania. Obliczenia łatwo jest przeprowadzić w jedną stronę, ale trudno

do nich wrócić, znając tylko wynik. Np. łatwo mnoży się dwie liczby pierwsze – załóżmy 67 i 149. Trudniej jednak – mając iloczyn dwóch liczb pierwszych (np. 9983) – odnaleźć dwa jego dzielniki. „Jeśli liczby są dostatecznie duże, np. mają 500-600 cyfr, nasza cywilizacja nie potrafi ich szybko rozłożyć" – zauważa naukowiec.

Kiedy szyfruje się wiadomość algorytmem RSA, trzeba – w dużym uproszczeniu – użyć iloczynu, czyli dużej liczby, ujawnionej publicznie przez adresata. Aby jednak odczytać taką wiadomość, trzeba znać czynniki pierwsze tej liczby.

BANKI, GŁOWICE NUKLEARNE, CHIPY

Obecnie na RSA opiera się uwierzytelnianie transakcji bankowych, ale też np. – w pewnym miejscu – system uwiarygodnienia liczby głowic nuklearnych między Rosją i USA – opowiada Aleksander Wittlin. „To skomplikowany system, który polega na tym, żeby nie dawać żadnej ze stron informacji, która pozwoliłaby uzyskać przewagę, ale za to daje obu państwom pewność, że liczba rakiet nie przekracza tego, co zapisane w porozumieniach" – dodaje.

RSA stosuje się też np. w systemie międzynarodowych przekazów bankowych SWIFT. Albo np. w przeglądarkach internetowych. Również certyfikaty bezpieczeństwa stron HTTPS bazują właśnie na tego typu algorytmie.

LICZĄC NA KARTĘ

Oprócz RSA, którego bezpieczeństwo oparte jest na trudności faktoryzacji, używane są także algorytmy asymetryczne oparte na innych problemach matematycznych, które łatwo przeprowadzić w jedną stronę, ale trudno odwrócić. To np. problemy związane z logarytmami dyskretnymi, grupami multiplikatywnymi czy arytmetyką punktów na krzywych eliptycznych.

I tak np. kryptografia oparta na krzywych eliptycznych jest stosowana w kartach chipowych (np. bankowych), bo nie wymaga

dużej mocy obliczeniowej. „Procesor znajdujący się w karcie ma bardzo małą wydajność, bo nie ma własnego zasilania” – zwraca uwagę badacz.

Dzięki kryptografii asymetrycznej uwierzytelniane są też m.in. łatki systemów operacyjnych czy częściowo – podpis elektroniczny, a także uwierzytelniane są transakcje między użytkownikami walut kryptograficznych.

W SKRÓCIE O FUNKCJI FUNKCJI SKRÓTU

Trzecią z głównych klas algorytmów szyfrujących jest funkcja skrótu.

„Funkcja skrótu to funkcja, która – jak wierzymy – jest jednokierunkowa. Możemy sobie więc wyobrazić, że mamy 'młynek’, wrzucamy do niego wiadomość, kręcimy korbką i wypada liczba. Ta liczba ma teraz zwykle 256 bitów. Wierzymy, że to działa w jedną stronę i że z tej liczby nie da się odczytać oryginalnej wiadomości” – tłumaczy badacz z IF PAN.

Jeśli więc w oryginalnej wiadomości zostanie zmieniony choćby przecinek, skrót tej wiadomości również ulegnie zmianie.

Do oryginalnej wiadomości odbiorca może więc dodać poświadczenie w postaci odpowiednio uwierzytelnionego, na przykład podpisem elektronicznym skrótu. Dzięki temu może mieć większą pewność, że oryginalna wiadomość, którą otrzymał, nie została zmieniona.

„Funkcja skrótu jest używana między innymi w wielu protokołach podpisu elektronicznego, ale także w hasłach logowania do komputerów – np. w systemie Windows. Na takiej kryptografii opiera się też tworzenia łańcucha bloków w blockchainie (znanego chociażby posiadaczom bitcoinów)” – wymienia naukowiec.

MIKS METOD

Popularyzator dodaje jednak, że w obecnych rozwiązaniach

kryptograficznych, aby utrudnić rozgryzienie szyfru, stosowane są zabezpieczenia hybrydowe. Tak więc np. banki, kiedy wykonujemy przelew, wykorzystują drugi kanał uwierzytelniający. I transakcje potwierdza się dodatkowo, np. jednorazowym hasłem (choćby z SMS-a). Nie wystarcza więc samo logowanie i korzystanie z wiarygodnej strony HTTPS. Podobnie jest w przypadku niektórych portali społecznościowych, które wysyłają SMS-a, kiedy logujemy się do serwisu z nowego urządzenia lub z niestandardowej lokalizacji.

A te wszystkie nowe możliwości – które zależą od rozwoju kryptografii – zwiększają pewność użytkownika, że jego poufne dane nie zostaną wykorzystane przez niepowołane osoby.

Autorstwo: Ludwika Tomala
Zdjęcie: flyerwerk (CC0)
Źródło: NaukawPolsce.PAP.pl