O bezpieczeństwie algorytmu RSA

dr WOJCIECH NOWAKOWSKI

Instytut Maszyn Matematycznych, Warszawa

Twórcy algorytmu RSA w 2003 roku. The RSA algorithm Autors in 2003 (http://www.usc.edu/dept/molecular-science/RSA-2003.htm)

Podstawowym elementem aplikacji i protokołów szyfrowania danych są algorytmy kryptograficzne. Tematem niniejszego artykułu jest bardzo szeroko obecnie stosowany algorytm RSA [1]. RSA jest algorytmem kryptograficznym z kluczem publicznym, który umożliwia zarówno szyfrowanie jak i podpisywanie cyfrowe (weryfikacja). Podstawową zaletą kryptografii z kluczem publicznym jest to, że klucze nie muszą być przekazywane lub ujawniane nikomu, w odróżnieniu od kluczy prywatnych (tajnych), które muszą być przekazywane, gdyż ten sam klucz służy do szyfrowania i deszyfrowania danych.

System RSA opracowali w 1977 r. Ronald Rivest, Adi Shamir i Leonard Adleman (*Fot.*). Algorytm RSA działa w następujący sposób:

- Wybieramy dwie duże liczby pierwsze:{*p, q*} oraz obliczamy ich iloczyn $n = pq$ oraz funkcję Eulera $\varphi = (p - 1)(q - 1)$. Wybieramy losowo liczbę $e < n$, względnie pierwszą* z liczbą φ. Liczba *e* będzie kluczem szyfrującym. Znajdujemy (korzystając z rozszerzonego algorytmu Euklidesa) liczbę *d* taką, że: $d \equiv e^{-1} \pmod{\varphi}$ lub $de \equiv 1 \pmod{\varphi}$, $d<\varphi$. Liczby *d* i *n* są także względnie pierwsze. Liczby {*e,n*} stanowią klucz publiczny, który ujawniamy, zaś liczby {*d,n*} stanowią klucz prywatny, który powinien być ściśle chroniony (liczba *d*) [2].

Szyfrowanie, deszyfrowanie, podpisywanie lub weryfikacja polega w systemie RSA na potęgowaniu *modulo***. Obliczenie to jest wykonywane jako seria mnożeń *modulo*. Całe grupy użytkowników mogą korzystać z tego samego wykładnika publicznego, każdy z innym *modulo*. To sprawia, że szyfrowanie i weryfikacja są szybsze niż deszyfrowanie i podpisywanie. W typowych algorytmach potęgowania *modulo* algorytmu RSA, operacje na kluczach publicznych wymagają

$O(k^2)$ kroków, operacje na kluczach prywatnych – $O(k^3)$ kroków, a generowanie klucza wymaga $O(k^4)$ kroków, gdzie *k* jest liczbą bitów w *modulo* (*O* oznacza *notację dużego O****). Szybkie techniki mnożenia, takie, jak metody oparte na szybkiej transformacie Fouriera (FFT) wymagają asymptotycznie mniej kroków. W praktyce jednak nie są one tak powszechne, ze względu na większą złożoność oprogramowania; poza tym mogą być one wolniejsze przy typowych wielkościach kluczy.

Bezpieczeństwo systemu RSA opiera się więc na założeniu, że faktoryzacja (rozkład na czynniki) dużych liczb całkowitych jest trudna. Odkrycie szybkiej metody faktoryzacji bądź radykalne przyspieszenie obliczeń sprawi, że algorytm RSA stanie się nieprzydatny. A szybkość i wydajność wielu dostępnych na rynku procedur programowych i sprzętowych algorytmu RSA dynamicznie rośnie.

W literaturze zaleca się, aby w parach kluczowych stosować tzw. mocne liczby pierwsze *p* i *q*. Liczby pierwsze *p* i *q* nazywamy *mocnymi liczbami pierwszymi*, gdy największy wspólny dzielnik *p-1* i *q-1* jest mały, *p-1* i *q-1* mają duże czynniki pierwsze i *(p-1)/2* oraz *(q-1)/2* są liczbami pierwszymi. Mocne liczby pierwsze mają pewne cechy, które sprawiają, że *n* jest trudne do faktoryzacji niektórymi metodami. Jednak postęp w metodach faktoryzacji

w ciągu ostatnich lat spowodował osłabienie tej zalety. Dlatego wybór mocnych liczb pierwszych nie zwiększa istotnie bezpieczeństwa algorytmu, najważniejszy jest wybór wystarczająco dużych liczb pierwszych.

Rozmiar klucza w algorytmie RSA odnosi się zwykle do wielkości modułu *n*. Liczby pierwsze, *p* i *q*, powinny mieć długości zbliżone. Faktoryzacja jest wtedy trudniejsza, niż w przypadku, gdyby jedna z liczb pierwszych byłaby znacznie mniejsza. Jeśli wybierzemy 768-bitowy moduł, to *p* i *q* powinny mieć długość około 384 bitów. Jeżeli dwie liczby pierwsze są bardzo bliskie sobie, to istnieje potencjalne zagrożenie bezpieczeństwa, ale prawdopodobieństwo, że dwie losowo wybrane liczby pierwsze są takie, jest znikoma. Im większy moduł, tym większe bezpieczeństwo, ale faktoryzacja wolniejsza.

Obecnie już ugruntowana jest świadomość, że użycie 512-bitowych kluczy nie zapewnia wystarczającego bezpieczeństwa. RSA Laboratories zaleca obecnie stosowanie kluczy o wielkości 1024 bitów dla firm i 2048 bitów dla instytucji certyfikujących.

Kilka ostatnich standardów określa 1024-bitowe minimum dla firm. Dotychczas największym kluczem RSA, jaki rozłożono na czynniki pierwsze, jest klucz 768-bitowy. Dokonano tego 12 grudnia 2009 r., a informację o przeprowadzonej faktoryzacji opublikowano 7 stycznia 2010 r. [3]. Wykorzystano klaster komputerów. Potencjalnym zagrożeniem dla RSA jest natomiast skonstruowanie komputera kwantowego [4].

Innym zagadnieniem jest, czy istnieje wystarczająca ilość liczb pierwszych. Już Euklides udowodnił ponad dwa tysiące lat temu, że istnieje nieskończenie wiele liczb pierwszych. Ponieważ

jednak algorytm RSA ma stałą długość klucza, liczba liczb pierwszych dla użytkownika algorytmu jest ograniczona. Mimo to liczba ta jest jednak bardzo duża i wynosi około 10^{150}. To więcej niż liczba atomów w znanym wszechświecie.

RSA jest obecnie stosowany w wielu produktach na świecie. Algorytm ten jest wbudowany w systemy operacyjne firmy Microsoft, Apple, Sun i Novell. Algorytm RSA można znaleźć np. w bezpiecznej telefonii, czy na kartach sieciowych. Jest on włączony do wszystkich głównych protokołów bezpiecznej komunikacji internetowej, w tym S/MIME, SSL, i S/WAN. Jest on również stosowany wewnętrznie w wielu instytucjach rządowych, wielkich korporacjach, laboratoriach i uniwersytetach. RSA jest najszerzej stosowanym na świecie systemem z kluczem publicznym i taktowany jest de facto jako standard. Fakt ten jest bardzo ważny dla rozwoju gospodarki cyfrowej. Powszechne używanie jednego systemu kryptograficznego z kluczem publicznym umożliwia, przynajmniej teoretycznie, uwierzytelnianie i podpisywanie dokumentów cyfrowych w różnych krajach za pomocą różnych programów na różnych platformach. W praktyce istnieje szereg ograniczeń lokalnych. Np. w UE podpis elektroniczny obwarowany jest przepisami i normami – nie musi więc być kompatybilny z podpisem składanym np w USA czy krajach azjatyckich (ponadto sama technologia złożenia podpisu to nie wszystko, istotna jest kompatybilność formatów tworzonych plików itp.).

Brak bezpiecznego uwierzytelniania był, a nawet jest nadal, główną przeszkodą w cyfryzacji obiegu dokumentów i rozwoju elektronicznych transakcji. Podpis cyfrowy jest narzędziem niezbędnym do zastąpienia dokumentów papierowych elektronicznymi. Postęp metod obliczeniowych wymusza postęp w algorytmach szyfrowania danych. Algorytm RSA, wspierany nowymi technikami jak np. kluczem kryptograficznym AES (ang. *Advanced Encryption Standard* – symetryczny szyfr blokowy przyjęty przez NIST jako standard FIPS-197 w wyniku konkursu ogłoszonego w roku 1997).

*) Liczbami względnie pierwszymi nazywamy liczby, których największym wspólnym dzielnikiem jest 1. Oznacza to, że żadna liczba naturalna większa od 1 nie dzieli jednocześnie tych liczb. Rozkłady na czynniki pierwsze liczb względnie pierwszych wyróżniają się brakiem dzielników pierwszych wspólnych dla wszystkich liczb. Najmniejszą wspólną wielokrotnością liczb względnie pierwszych jest ich iloczyn. Każde dwie kolejne liczby naturalne są względnie pierwsze. Każde dwie liczby parzyste nie są względnie pierwsze.

**) Potęgowanie *modulo* jest jednym z działań arytmetyki modularnej *(arytmetyki reszt)* – działań na liczbach całkowitych, w których liczby „skracają się" po osiągnięciu pewnej wartości nazywanej modułem. Arytmetyka modularna pojawia się wszędzie tam, gdzie występuje powtarzalność i cykliczność. Korzysta się z niej w teorii liczb, teorii grup, kryptografii, informatyce, przy tworzeniu sum kontrolnych, a nawet przy tworzeniu wzorów. Wyraz *modulo* w żargonie jest nazywany jako „z dokładnością do".

***) Notacja *dużego O* służy do opisu asymptotycznego tempa wzrostu, które jest miarą określającą zachowanie wartości funkcji wraz ze wzrostem jej argumentów. Stosowane jest w teorii obliczeń, w celu opisu złożoności obliczeniowej, czyli zależności ilości potrzebnych zasobów (np. czasu lub pamięci) od rozmiaru danych wejściowych algorytmu.

Notacja *dużego O* została zaproponowana po raz pierwszy w roku 1894 przez Paula Bachmanna. Później spopularyzował ją Edmund Landau, dlatego niekiedy nazywana jest notacją Landaua (http://pl.wikipedia.org/wiki/Asymptotyczne_tempo_wzrostu)

Autor dziękuje za cenne uwagi i poprawki panu mgr inż. Robertowi Poznańskiemu (IMM).

Literatura

[1] Rivest R.L., Shamir A., Adleman L.M.: A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM (2) 21 (1978), 120–126.

[2] Nowakowski W.: Algorytm RSA – podstawa podpisu elektronicznego. Elektronika, nr 6/2010, Warszawa

[3] Gaudry P., Kruppa A., Montgomery P.L., Osvik D.A., Riele H., Timofeev A., Zimmermann P.: Factorization of a 768-bit RSA modulus. http://eprint.iacr.org/2010/006.pdf

[4] Nowakowski W.: O kryptografii kwantowej. Elektronika, nr 2/2010, Warszawa.