Tomasz Sowiński jest fizykiem na Wydziale Biologii i Nauk o Środowisku UKSW i w Centrum Fizyki Teoretycznej PAN. W 2005 roku skończył studia na Wydziale Fizyki Uniwersytetu Warszawskiego w zakresie fizyki teoretycznej, a trzy lata później uzyskał tam stopień naukowy doktora. Od lat zajmuje się popularyzacją nauk przyrodniczych. W roku 2008 otrzymał tytuł Mistrza Popularyzacji Nauki „Złoty Umysł" w konkursie Prezesa Polskiej Akademii Nauk.

Nasz dzisiejszy świat zdominowany jest przez wszelkiego rodzaju łączność na odległość. Rozwój Internetu sprawił, że dziś kontrahenci nie muszą się już spotykać, aby podpisać umowę, przekazać pieniądze czy prowadzić negocjacje. Rozkazy wojskowe mogą być wydawane poszczególnym żołnierzom przez dowódców znajdujących się tysiące kilometrów od teatru działań wojennych na podstawie obrazowego przedstawienia sytuacji wygenerowanej ze zdjęć satelitarnych. Szybka komunikacja na odległość całkowicie zmieniła nasz sposób patrzenia na świat, który rzeczywiście stał się globalną wioską.

Tomasz Sowiński

Kryptografia klasyczna i kwantowa cz. I

TEKST ŚREDNIO TRUDNY

KOMUNIKACJA NA ODLEGŁOŚĆ

Wiele aspektów przekazywania informacji na odległość opiera się na zaufaniu, że informacja dotrze do adresata szybko i bezpiecznie. Bezpiecznie, czyli: niezmieniona pod względem treści i, jeśli jest to konieczne, zabezpieczona tak, że nikt niepowołany jej nie odczyta. Cóż bowiem znaczyłyby internetowe banki i sklepy, gdyby prostym sposobem było można przechwycić numer karty kredytowej czy zmienić numer konta, na które mają trafić pieniądze wysłane internetowym przekazem. Z tego zapotrzebowania na bezpieczną komunikację na odległość bezpośrednio wynika zainteresowanie różnymi metodami kryptograficznymi wszystkich podmiotów świadczących usługi elektroniczne.

JAK ZAKODOWAĆ WIADOMOŚĆ?

Wszystkie problemy związane z bezpieczną komunikacją na odległość można sprowadzić do jednego, bardzo dobrze określonego problemu. Aby to zrozumieć, wyobraźmy sobie, że dwie osoby rozmawiają ze sobą przez telefon i chcą mieć pewność, że informacje, które sobie przekazują, nie zostaną przez nikogo przechwycone lub, jeśli coś takiego niestety się zdarzy, to dla podsłuchującego będą bezużyteczne. Załóżmy, że osoba A chce przekazać osobie B ciąg znaków: TAJNE. Może to zrobić mówiąc przez telefon kolejne litery tego ciągu: T–A–J–N–E. Jednak taką wiadomość jest bardzo łatwo podsłuchać. Dlatego osoba A powinna w jakiś sposób zakodować swoją wiadomość i dopiero ją przesłać. Jak może to zrobić? Takim sposobem może być np. użycie tajnego klucza (losowego ciągu liczb), który mówi o ile miejsc należy przesunąć każdą literę w alfabecie. Dla przykładu załóżmy, że tajnym kluczem jest ciąg liczb: 2–7–1. Wtedy zakodowana informacja ma postać: V–H–K–P–L. Jak ona powstała? Bierzemy pierwszą literę wiadomości (T) i przesuwamy ją w alfabecie o tyle liter, ile wskazuje pierwsza liczba klucza (2). Czyli T zamienia się w V. Następnie drugą literę zamieniamy, wykorzystując drugą liczbę z klucza. Tym sposobem

Bezpieczny transfer pieniędzy

A zamienia się w H. Trzecia litera wiadomości to J i przesuwa się ją o jeden, czyli zamienia na K. Klucz się skończył, więc wracamy do jego początku i kolejne litery zamieniamy znów wg tego samego schematu. Czyli N przesuwa się o 2 i zamienia na P, a E przesuwa się o 7 i zamienia się na L. Aby algorytm ten zawsze dał się zastosować, musimy się umówić, że po literze Z w alfabecie jest znów litera A. Tym sposobem, jeśli dojdziemy do końca alfabetu, wiemy, co oznacza przesuwanie się dalej w prawo.

Tak przygotowaną wiadomość V–H–K–P–L osoba A przesyła do osoby B, mówiąc przez telefon kolejne litery. Nawet jeśli tę wiadomość ktoś podsłucha, to nic to mu nie da. Bez klucza ta wiadomość jest bezużyteczna. Osoba B natomiast, jeśli tylko dysponuje tajnym kluczem, wiadomość może bez trudu odszyfrować. W tym celu wystarczy, że zastosuje taki sam algorytm, jaki stosowała osoba A przy kodowaniu, ale zamiast przesuwać litery w prawo, będzie je przesuwała w lewo. Tym sposobem odzyska wiadomość zakodowaną przez osobę A.

BEZPIECZEŃSTWO KLUCZA

Warto w tym miejscu zatrzymać się i powiedzieć, że przy takim algorytmie najbardziej bezpieczny jest oczywiście klucz, który ma taką samą długość, jaką długość ma wiadomość. Wtedy nie ma żadnej korelacji pomiędzy przesunięciami kolejnych liter wiadomości i bez znajomości klucza niemożliwe jest odczytanie zakodowanej informacji. Aby zrozumieć, że kodowanie z krótkim kluczem może zostać złamane, zobaczmy, co dzieje się z naszą wiadomością, jeśli zakodujemy ją prostym kluczem jednoliczbowym, np. 3. Po zakodowaniu wiadomość ma postać: W–D–M–R–H. Osoba, która podsłuchała taką wiadomość, może próbować przesuwać wszystkie litery naraz o tyle samo miejsc. Najpierw o jedno, później o dwa, itd... W tych przypadkach będzie widziała, że litery układają się w bezsensowne słowa. Gdy jednak dojdzie do przesunięcia „o 3", to zauważy, że litery układają się w napis T–A–J–N–E i tym samym odczyta zaszyfrowaną wiadomość. Gdy klucz byłby dwuliczbowy, byłby trudniejszy, ale również możliwy do sforsowania. Gdy bowiem uda się odgadnąć w jakiś sposób dwie pierwsze litery wiadomości, to pozostała część jest już praktycznie jawna. Gdy natomiast każdy znak wiadomości jest zakodowany innym przesunięciem, to, aby odczytać całą wiadomość, trzeba jakby złamać klucz dla każdego znaku osobno. A to oczywiście jest bardzo czasochłonne.

PODSTAWOWY PROBLEM KRYPTOGRAFICZNY

Przedstawiony wyżej sposób kodowania wiadomości jest zarówno bardzo prosty pod względem idei, jak i bezpieczny. Jedyny problem, jaki się pojawił, to sposób w jaki osoba A może przekazać osobie B tajny klucz, którego użyła do zakodowania wiadomości. Nie może oczywiście go przekazać przez telefon, bo ktoś, kto podsłuchałby ten tajny klucz, mógłby odszyfrować zakodowaną nim wiadomość. Najprościej jest, gdy osoby A i B mogą się ze sobą wcześniej spotkać bezpośrednio. Na takim spotkaniu osoba A może dyskretnie przekazać osobie B swój tajny klucz zapisany na kartce papieru i powiedzieć, że następną wiadomość wyśle jej przez telefon, szyfrując ją wcześniej tym właśnie kluczem. W takiej sytuacji jest stuprocentowa pewność, że klucz, i tym samym zaszyfrowana za jego pomocą wiadomość są bezpieczne. Tajny klucz posiadają bowiem tylko dwie zainteresowane osoby A i B.

Co jednak można zrobić, gdy osoby, które chcą przesłać sobie wiadomości, nie mogą się spotkać twarzą w twarz? Jest to przecież sytuacja najczęstsza z jaką mamy do czynienia, korzystając z usług elektronicznych. Przecież po to właśnie zakładamy konto w banku internetowym, żeby nie było potrzeby spotykać się z pracownikiem banku. My nie mamy ochoty tam iść w celu założenia konta, a co dopiero mówić o odebraniu jakiegoś tajnego klucza.

Dyskretne przekazanie tajnego klucza

Podstawowym problemem kryptograficznym jest zatem ustalenie tajnego klucza pomiędzy osobami A i B. Najlepiej, gdyby było to można zrobić na odległość, bez konieczności spotykania się. Można oczywiście pomyśleć o specjalnym tajnym kanale komunikacji pomiędzy osobami A i B, co do którego mamy pewność, że nie jest podsłuchiwany. Problem polega jednak na tym, że takiego kanału nie ma, bo medium, którego używamy, to globalna sieć teleinformatyczna, do której dostęp ma praktycznie każdy mieszkaniec Ziemi. Poza tym, gdybyśmy mieli taki kanał, to nie trzeba byłoby nim przesyłać tajnego klucza, a od razu wiadomość, którą chcemy przekazać. Zatem prawdziwy problem to ustalenie tajnego klucza pomiędzy osobami A i B, na odległość, przy wykorzystaniu ogólnodostępnego medium (np. Internetu albo telefonu).

JAK TO SIĘ ROBI?

Wydaje się, że przedstawiony przed chwilą problem nie ma dobrego rozwiązania. Bardzo trudno jest sobie wyobrazić, że można ustalić tajny klucz szyfrujący wiadomość za pomocą medium, do którego każdy ma dostęp. Obejście tego problemu w dzisiejszych systemach łączności jest oparte o pewną bardzo cie-

Tajny klucz przekazujemy kanałem

kawą obserwację matematyczną. Otóż, jak każdy łatwo może się przekonać, dużo łatwiej jest mnożyć liczby przez siebie niż rozkładać je na czynniki pierwsze. Na przykład jeśli wybierzemy dwie liczby pierwsze 7 i 13, to łatwo jest je przez siebie przemnożyć. W wyniku otrzymamy 91. Gdybym jednak zadał pytanie odwrotne: jakie liczby trzeba przez siebie pomnożyć, aby otrzymać 91, to podanie odpowiedzi nie byłoby takie proste. Trzeba po prostu sprawdzać, czy 91 dzieli się przez kolejne liczby pierwsze. Przypomnę tylko, że rozkład każdej liczby na jej czynniki pierwsze jest jednoznaczny. W związku z tym 91 jest równe $7 * 13$ i nie ma innej możliwości.

Jeśli nadal nie wierzysz mi, Drogi Czytelniku, że problem rozłożenia liczby na jej czynniki pierwsze jest dużo trudniejszy niż pomnożenie dwóch, nawet bardzo dużych liczb, to mam dla Ciebie prostą zagadkę. Proszę, powiedz mi, jakie liczby trzeba przez siebie pomnożyć, aby otrzymać 325573? Dla ułatwienia powiem Ci, że pomnożyłem przez siebie dwie liczby, które są pierwsze. Zadanie dość trudne prawda? A teraz sprawdź, że podana liczba to nic innego jak iloczyn liczb 1543 i 211.

Ta ciekawa obserwacja, że mnożyć liczby jest dużo łatwiej, niż je rozkładać na czynniki pierwsze, jest podstawą genialnego algorytmu RSA, który został wymyślony w 1978 roku i jest dziś powszechnie używany do szyfrowania wszelkich poufnych wiadomości w komunikacji przez Internet. Skrót RSA pochodzi od pierwszych liter nazwisk twórców tego algorytmu: Ronalda Rivesta, Adi Shamira i Leonarda Adlemana.

IDEA ALGORYTMU RSA

Sam algorytm RSA wymaga pewnej wiedzy matematycznej wykraczającej poza szkołę średnią i dlatego nie będziemy wchodzili tutaj w szczegóły. Przedstawimy tylko samą koncepcję na jakiej opiera się ten algorytm. Załóżmy, że osoba A chce wysłać osobie B tajną wiadomość, np. tajny klucz, którym będą się posługiwali podczas swojej komunikacji. Aby to zrobić, dzwoni do osoby B, która tajną wiadomość ma odebrać i prosi o wygenerowanie tzw. klucza publicznego.

Osoba B poproszona o wygenerowanie klucza publicznego robi to następująco: otwiera tablicę liczb pierwszych i całkowicie losowo wybiera dwie z nich. Załóżmy, że te liczby to X i Y. Następnie mnoży je przez siebie i w ten sposób powstaje liczba $P_1 = X * Y$. Następnie mnoży przez siebie liczby o jeden mniejsze od wylosowanych, otrzymując w ten sposób liczbę R, tzn. $R = (X–1) * (Y–1)$. Teraz wybiera (zupełnie dowolnie) liczbę P_2, która jest względnie pierwsza z wyliczoną przed chwilą liczbą R. Przypomnijmy, że liczby względnie pierwsze to takie, które nie mają wspólnych dzielników. Osoba B dysponuje więc następującymi liczbami: X, Y, P_1, P_2 i R, przy czym liczby P_1 i R w prosty sposób powstają z liczb pierwszych X i Y. Ów klucz publiczny to nic innego jak para liczb (P_1, P_2). I to właśnie te dwie liczby osoba B przesyła do osoby A.

I trochę tajnej matematyki

Osoba A za pomocą klucza publicznego może zakodować swoją tajną wiadomość. Aby to zrobić, zamienia najpierw swoją wiadomość na liczbę W wg powszechnie znanych reguł (np. kodu ASCII). Jak pewnie pamiętacie z lekcji informatyki, każdą wiadomość można zapisać za pomocą liczby i dlatego to nie jest nic trudnego. Kodowanie wiadomości W to nic innego jak wykonanie pewnej, dobrze określonej operacji matematycznej na trzech liczbach P_1, P_2 i W. W wyniku tej operacji otrzymuje się czwartą liczbę K, która jest właśnie zakodowaną wiadomością W. To znaczy za pomocą klucza publicznego osoba A zakodowała wiadomość W do postaci K. To co jest bardzo ważne to fakt, że operacja ta jest nieodwracalna. To znaczy, że znając liczbę K oraz liczby P_1 i P_2 stanowiące klucz publiczny nie można odzyskać wiadomości W. Klucz publiczny może tylko wiadomość zakodować, ale odkodować już nie może. Jest to tzw. kodowanie asymetryczne.

Tak zakodowaną wiadomość K osoba A przesyła do osoby B. Cały algorytm jest tak przemyślany, że choć odkodowanie wiadomość jest niemożliwe przy znajomości klucza publicznego, czyli liczb P_1 i P_2, to można ją bez problemu odkodować, znając klucz publiczny wraz z początkowymi liczbami pierwszymi X i Y (prawdę mówiąc, wystarczą do tego jedynie liczby P_1 P_2 i R). Ponieważ osoba B generowała klucz publiczny to zna liczby X i Y, dlatego wiadomość może bez kłopotu odszyfrować. Ponieważ liczby te zna tylko ona, to tylko ona może to zrobić. A ponieważ ich nigdzie nie przesyłała ani nie publikowała, to algorytm jest w praktyce bezpieczny. Niebezpieczeństwo tego, że ktoś uzyska dostęp do informacji umożliwiającej odkodowanie wiadomości nie istnieje. Informacji tej bowiem nigdzie nie przesyłamy.

BEZPIECZEŃSTWO OPARTE NA WIERZE

Tak jak już wcześniej powiedziałem, bezpieczeństwo algorytmu RSA opiera się na obserwacji, że bardzo trudno liczby rozkłada się na czynniki pierwsze. Zauważmy bowiem, że jednym z elementów klucza publicznego jest liczba P_1, czyli iloczyn tajnych liczb X * Y. Gdyby ktoś umiał rozłożyć szybko liczbę P_1 na czynniki pierwsze, to mógłby wygenerować liczbę R = (X–1) * (Y–1) i tym samym miałby wszystkie potrzebne informacje do odzyskania wiadomości W z szyfrogramu K. Bezpieczeństwo RSA jest zatem oparte na naszej wierze w to, że nikt nie potrafi sprawnie rozkładać liczb na czynniki pierwsze. I zapewne ta wiara jest jak na razie uzasadniona. Prawdopodobnie żaden dzisiejszy komputer, nawet najlepszy z najlepszych, nie potrafi rozkładać szybko liczb na czynniki. Jeśli dodamy do tego fakt, że największe dziś znane liczby pierwsze składają się z (UWAGA!) ponad dziesięciu milionów cyfr, to łatwo sobie wyobrazić, jak rozkład iloczynu dwóch takich liczb na czynniki jest czasochłonny. Odkrycie nowej dużej liczby pierwszej jest bardzo często świetnym towarem, za który duże firmy, a nawet rządy państw, są w stanie zapłacić miliony dolarów. Używanie bowiem w algorytmie RSA dużych liczb pierwszych, których dodatkowo nikt inny nie zna, wydaje się najlepszym zabezpieczeniem tajnej komunikacji.

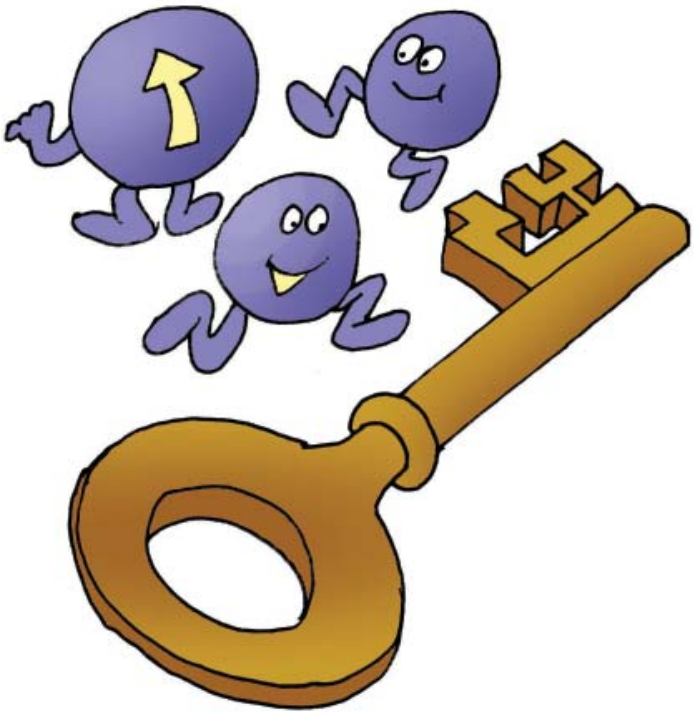
Podkreślmy to jeszcze raz: bezpieczeństwo algorytmu RSA oparte jest na WIERZE. Wierze w to, że ktoś, kto chciałby podsłuchać naszą wiadomość, nie potrafi czegoś zrobić. Czy to nie straszne? Przecież może być tak, że już dawno ktoś wie, jak łatwo i szybko rozkładać liczby na ich czynniki pierwsze, ale nie dzieli się tą informacją z resztą świata, tylko na tym nieuczciwie zarabia, podrabiając nasze przelewy bankowe. A może obecny kryzys gospodarczy to wcale nie skutek napompowania jakiejś tam bańki finansowej w Stanach Zjednoczonych, ale sabotaż terrorysty, który wykorzystując swój tajny sposób rozkładania liczb na czynniki pierwsze, potrafił sfałszować miliardy operacji na światowych giełdach. Wszędzie tam używany jest bowiem algorytm RSA, który opiera się na wierze, że żaden terrorysta nie potrafi rozkładać liczb na czynniki pierwsze.

BEZPIECZEŃSTWO OPARTE NA FIZYCE

Po takich słowach od razu cisną się na usta pytania. Czy nie można oprzeć naszego bezpieczeństwa na czymś lepszym niż tylko ślepa wiara? Czy naprawdę nie istnieje sposób na ustalenie klucza na odległość, który byłby bezpieczny z samej zasady?

Mam dobrą wiadomość. Taki sposób istnieje. Istnieje, a jego bezpieczeństwo jest gwarantowane nie wiarą w to, że ktoś czegoś nie potrafi zrobić, ale opiera się na prawach Przyrody. To sama Przyroda gwarantuje, że jest on bezpieczny. Wystarczy w tym celu wykorzystać własności fotonów – kwantów promieniowania elektromagnetycznego. To właśnie ich zdumiewające własności wynikające wprost z praw mechaniki kwantowej, czyli teorii fizycznej opisującej zjawiska subatomowe, pozwala opracować całkowicie bezpieczny algorytm ustalania klucza kryptograficznego. ●

cdn.



Algorytm ustalania klucza kryptograficznego