Aleksander Tudruj
Wydział Matematyki, Informatyki i Mechaniki

Bezpieczna Przyszłość — O upadku klasycznej kryptografii

Przyszłość niesie za sobą wiele niebezpieczeństw. Godzinami można rozprawiać, jakież to ludzkość napotka przeszkody w dalszym rozwoju naszej kultury. Nie sposób wymieniać możliwe katastrofy natury politycznej, społecznej czy naturalnej. Zastanówmy się jednak nad niebezpieczeństwem wynikającym z właśnie owego rozwoju. Co, jeżeli to właśnie on będzie jednym z czynników upadku cywilizacji, którą znamy?

Zacznijmy od podstaw bezpiecznego przekazywania informacji. Wraz z rozwojem technologii oraz rozrostem sieci naukowcy napotkali następujący problem. W jaki sposób bezpiecznie porozumiewać się w sieci narażonej na podsłuchy? Jak wykryć, czy przekazana wiadomość nie została zmieniona w drodze? Te problemy wcale nie były nowe. Ludzkość już wiele setek lat wcześniej[12] formułowała takie problemy. Jednak wraz z upowszechnieniem komputerów łamanie prostych szyfrów podstawieniowych stało się błahostką. Potrzebny był bardziej wymagający, ale zarazem prosty obliczeniowo sposób na szyfrowanie informacji. Opublikowany w 1977 roku asymetryczny algorytm kryptograficzny RSA wydawał się rozwiązać ten problem. Algorytm ten jest bardzo prosty w obsłudze i nie wymaga skomplikowanych obliczeń. Jednak czy na pewno jest bezpieczny?

RSA bazuje swoje działanie na następującym założeniu: istotnie łatwiej jest dwie liczby pomnożyć, niż otrzymać je z iloczynu. Jest to oczywiście uproszczenie istnienia łatwo obliczanej funkcji odwrotnej do operacji mnożenia dwóch liczb pierwszych. Przez łatwo obliczanej rozumiemy, że funkcja odwrotna ma być klasy nie gorszej niż funkcja pierwotna. Gdybyśmy potrafili rozłożyć liczbę na czynniki pierwsze, to będzie to równoważne z umiejętnością złamania RSA. Jest jednak jeden haczyk — nie potrafimy szybko faktoryzować liczb naturalnych. Wiele zależy od doboru długości klucza, lecz już klucz o długości 2048 bitów wydaje się być niezłamywalny przez współczesne komputery. Jednak RSA korzysta z jeszcze jednego założenia, o którym nie słyszy się tak często. Mianowicie zakładamy, że nie istnieje inny sposób na złamanie RSA niż owa faktoryzacja. Co, jeżeli się mylimy? Co, jeżeli istnieje inny, sprytny sposób wykorzystujący zaawansowane właściwości teorii liczb, który pozwala na łamanie tego szyfru? Tę gałąź pozostawmy jednak kryptoanalizie. Skupmy się na faktoryzacji.

Istnieje algorytm `szybkiego` rozkładu liczby na czynniki pierwsze. Jednak ma on jeden mankament — do swojego działania wymaga działającego bez zakłóceń komputera kwantowego o przyzwoitej mocy obliczeniowej. Nosi on nazwę algorytmu Shora i został opublikowany już w 1994 roku. Od tamtej pory trwają prace nad coraz to bardziej wydajnym komputerem kwantowym, który potrafi faktoryzować coraz to więcej liczby naturalne. Moim zdaniem powstanie odpowiedniego komputera kwantowego, to tylko kwestia czasu, o ile już teraz, gdzieś w tajnej bazie Area 51, nie stoi uruchomiona właśnie taka jednostka.

[1] https://www.journals.uchicago.edu/doi/10.1086/698861
[2] http://bcs.fltr.ucl.ac.be/FE/07/CRYPT/Intro.html

Co tak właściwie jest zagrożone? Otóż nie tylko algorytm RSA. Protokół Diffiego-Hellmana oraz wymiana kluczy oparta o krzywe eliptyczne nie powinny czuć się bezpiecznie, a co za tym idzie wszelkiego rodzaju bankowość[3] czy inna poufna wymiana informacji. Boję się nawet wysławiać, co złego może stać się, jeżeli narzędzie do łamania tych szyfrów trafi w ręce nieodpowiednich ludzi.

Z tyłu głowy nasuwa się myśl: „a może zaprzestać dalszemu rozwojowi nauki nad komputerami kwantowymi?". Niewątpliwie, gdyby cały świat zalecił się do tego postanowienia, to problem wygląda na rozwiązany. Jest to jednak idea zgubna z przynajmniej dwóch powodów. Po pierwsze nie jesteśmy w stanie sprawić, aby każdy zaprzestał takowych prac — jest to po prostu awykonalne. Po drugie i co ważniejsze nie możemy zaprzestać badań nad tak zaawansowanym rozwiązaniem, jak komputery kwantowe. Poza niebezpieczeństwem w rejonie szyfrowania niosą one za sobą wiele rozwiązań innych problemów. Zamiast popadać w panikę, zastanówmy się jak rozwiązać ten nowy problem. I tutaj wkrada się zaskoczenie o nazwie BB84. Już w 1984 dwójka naukowców Charles Bennett i Gilles Brassard opublikowali kwantowy algorytm wymiany kluczy, który w przeciwieństwie do klasycznej kryptografii nie jest oparty o teorię liczb, a o zaawansowane właściwości fizyki kwantowej.

Mamy zatem w rękach rozwiązanie naszego problemu bezpieczeństwa. Jedyne co pozostaje, to wprowadzić je w życie. Banki czy inne podmioty tajnej komunikacji powinny być gotowe na przejście na alternatywne rozwiązanie szyfrowania. Niegdyś rewolucyjne było przejście z zeszytów z tabelkami i maszyn do pisania na współczesne komputery z arkuszami kalkulacyjnymi. Tym razem czeka nas podobna transformacja. Ludziom sto lat temu nie śniły się rozwiązania, które dla nas są dzisiaj codziennością. Głęboko wierzę, że za sto lat ludzie przyszłości będą posługiwać się równie bardziej zaawansowaną technologią, niż my dzisiaj.

Potrafię sobie wyobrazić, że komputer kwantowy będzie kiedyś dla człowieka tak podstawowym narzędziem, jak dla nas dzisiaj telefon komórkowy z dostępem do Internetu. Z tego właśnie powodu powinniśmy oswajać się z myślą przesiadki z klasycznej kryptografii na kwantową, bo to właśnie ona będzie gwarantem bezpiecznego przekazywania informacji zarówno przez wielkie korporacje, jak i małych szarych obywateli szukających pewnego i bezpiecznego sposobu na wysyłanie wiadomości.

[3] https://futureoffinance.biz/2021/07/13/why-every-bank-must-prepare-for-quantum-computers-now/