Magazyn Elektroniki Użytkowej

dodatek do miesięcznika Elektronika dla wszystkich

Poznać i zrozumieć sprzęt

O tym się mówi

Bezpieczeństwo w świecie bitów

Znak naszych czasów - niepozorny kawałek krzemu na straży naszych pieniędzy.

A miało być tak pięknie

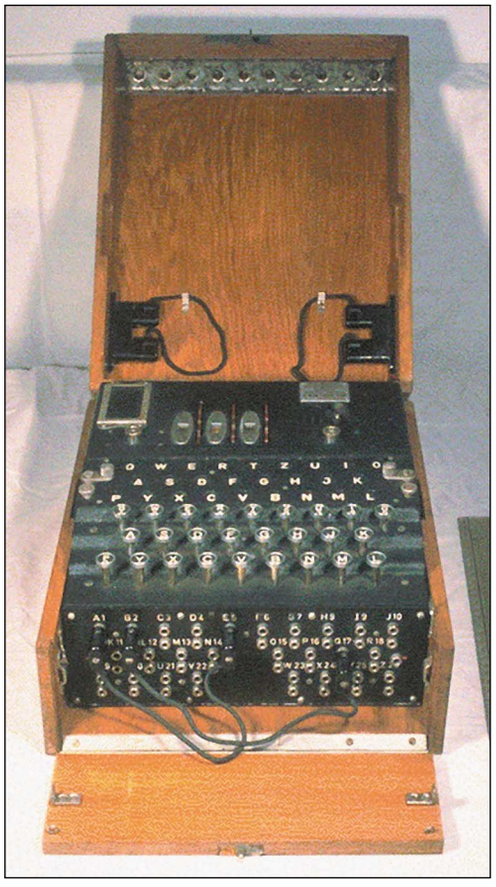
Technika cyfrowa zmieniła nasz świat szybciej niż się spodziewaliśmy. Prawdę mówiąc zdecydowana większość z nas, a zwłaszcza ci, którym dane było urodzić się nieco wcześniej (czyż czas nie jest bezlitosny?) za tempem owych zmian nadąża z – delikatnie mówiąc – pewnym trudem. Trzeba obiektywnie przyznać, że w wielu dziedzinach życia nowa technika okazała się niezwykle pomocna. Szczególnie zrewolucjonizowała szeroko pojęte zagadnienie przekazu informacji. Rewolucja ta polega, z grubsza rzecz biorąc, na tym, że w postaci cyfrowej przekazywanych może być coraz więcej informacji, w coraz dokładniejszej formie i w coraz krótszym czasie. Istotne jest również to, że tak zapisane dane mogą być wielokrotnie kopiowane bez szkody dla nich samych. Telefonia komórkowa, telewizja cyfrowa, Internet ze swoim e-handlem, e-pocztą i e-bankowością wydałyby się naszym pradziadkom prawdziwymi cudami. Nie wdając się w dywagacje na temat czy jesteśmy przez to szczęśliwsi czy nie, musimy przyznać, że niepostrzeżenie nadeszła epoka informacyjna, w której posiadanie i wymiana informacji zaczyna odgrywać zasadniczą rolę. Cały ten oszałamiający postęp techniczny ma jednak podstawową wadę. Nie podnosi niestety jednocześnie poziomu moralnego korzystających z niego ludzi. Zdezorientowany czytelnik może w tym miejscu zacząć zastanawiać się, czy aby na pewno ma w ręku kolejny numer EdW. Spokojnie nie ma obawy! Będzie o technice a nie o moralności, choć prawdę mówiąc artykuł ten nie byłby zupełnie potrzebny, gdyby nie paskudna strona natury ludzkiej, która powoduje, że wielu z nas albo ma szczególny apetyt na cudzą własność, albo przejawia nieodpartą chęć bezinteresownego nawet zaszkodzenia bliźniemu. Przed nastaniem epoki informacyjnej ludzie musieli myśleć głównie o tym, jak zabezpieczać swoje dobra materialne: domy, kosztowności itp. Oczywiście ten problem nadal spędza nam sen z oczu. Mamy więc coraz więcej coraz lepszych zamków w drzwiach, instalujemy drogie systemy alarmowe w samochodach, pieniądze trzymamy w sejfach. Bogatsi zamykają się w strzeżonych przez uzbrojonych po zęby ochroniarzy twierdzach otoczonych polami minowymi. Super! Ale prawdę mówiąc rzeczywistość może być gorsza niż przypuszczamy. Otóż w dzisiejszych czasach informacja przedstawia często większą wartość niż wymienione dobra materialne i to właśnie ona jest coraz częściej obiektem zainteresowania czarnych charakterów. Współczesny świat staje więc przed gigantycznym wyzwaniem jakim jest skuteczna ochrona informacji – cennego dobra, którego nie można zamknąć w sejfie, dobra które albo drzemie w formie zapisu magnetycznego na dysku twardym komputera, albo biegnie gdzieś po nitkach globalnej sieci w formie zero-jedynkowego bełkotu. A jest o co walczyć. W tzw. „dawnych czasach" mówiąc o wartości przedsiębiorstwa mieliśmy na uwadze głównie jego materialny majątek. Dziś już nie. Posłużę się przykładem pewnego potężnego koncernu amerykańskiego, który w latach dziewięćdziesiątych przejął inną firmę za 12,9 miliarda dolarów. Z kwoty tej zaledwie 1,3 miliarda przypadło na przedmioty materialne. Wspomniany koncern gotów był zapłacić pozostałe 11,6 miliarda dolarów za markę firmy, know-how i bazę danych klientów. Inny przykład ze świata wielkiego biznesu. Olbrzymie ilości danych o pomiarach sejsmograficznych, które pomagają w doborze miejsc pod platformy wiertnicze są warte dla każdego konkurenta grube miliony. Nic dziwnego, że chętnych do zdobywania i sprzedawania takich informacji nie brakuje, zwłaszcza gdy nie wymaga to wielkiego zachodu. Umieszczanie pluskiew, podsłuch przez superczułe mikrofony, szantażowanie pracowników czy też wtargnięcia do siedzib firm pod osłoną nocy są trudne i ryzykowne. A tu ktoś,

żaden tam superman tylko jakiś rachityczny, blady młodzieniec, który umie posługiwać się ledwie myszką, może - po złamaniu algorytmu szyfrującego (o tym później) - dostać się do najtajniejszych danych. Nie musi zadać sobie przy tym specjalnego trudu jako, że wykorzystywane dziś sieci są niezwykle łatwe do podsłuchania (łatwo podpiąć się pod magistralę danych komputera). Z reguły takie działanie nie pozostawia żadnych śladów. Poza tym inne osoby lub komputery równie łatwo mogą skorzystać z tego programu: skopiowanie oprogramowania jest nieporównanie tańsze od zakupu pluskwy. W 1998 roku w samych tylko Niemczech szkody spowodowane przez szpiegostwo przemysłowe wyniosły 4 miliardy euro.

Nie sposób też nie wspomnieć o tym, że nie brakuje szaleńców czy fanatyków próbujących włamać się do wojskowych systemów informatycznych i wykraść tajne informacje umożliwiające przejęcie kontroli nad śmiercionośnym arsenałem głowic nuklearnych. Problem, który dziś chcę przybliżyć znajduje stosowne odbicie w scenariuszach nowoczesnych filmów sensacyjnych. Coraz częściej „dobrzy" toczą zażartą walkę ze „złymi" o jakąś niepozorną dyskietkę komputerową. Do znudzenia oglądamy też, idiotyczne w istocie rzeczy, sceny „łamania" infantylnych haseł zabezpieczających dostęp do dysków twardych zawierających szczególnie cenne dane itd. itd. Niedługo dojdzie do tego, że najgroźniejsi bandyci będą po prostu cały czas przesiadywać w garniturach przed ekranem monitora, co ostatecznie wyeliminuje z rynku wirtuozów aktorstwa w rodzaju Arnolda Szwarcenegera czy Jean Claude Van Damma.

Czy mnie – szarego obywatela powinno to obchodzić?

Z pewnością zdecydowana większość z nas nie prowadzi wojny, nie kupuje przedsiębiorstw ani nie wierci w poszukiwaniu ropy. Nie zmienia to jednak faktu, że nasza osobista pomyślność finansowa, a także bezpieczeństwo zależą od odpowiedniego obchodzenia się z cyfrowo przechowywaną i przekazywaną informacją. Krótko mówiąc ani na chwilę nie można upubliczniać jej jawnej wersji. I tu jawi nam się cała groza świata informacji zaklętej w bitach. Dzięki coraz szybszym komputerom i coraz wymyślniejszemu oprogramowaniu może mieć do niej dostęp każdy, kto dysponuje odpowiednią wiedzą i pieniędzmi. Najczęściej nie zastanawiamy się nad tym, że przecież sieci GSM, elektroniczne systemy bankowe, bazy danych w różnych urzędach państwowych, firmach w których pracujemy, towarzystwach ubezpieczeniowych, szpitalach itd. są źródłami często bardzo poufnych informacji, które ktoś niepowołany może zdobyć i wykorzystać w bardzo nieprzyjemny dla nas sposób. Ale to tylko wierzchołek góry lodowej. Coraz częściej przy pomocy swego wspaniałego PC-ta łączymy się z Internetem. Żaden inny sposób komunikacji nie zrobił tak oszałamiającej kariery w tak krótkim czasie jak Internet. Jego globalność, taniość (mówimy o cywilizowanych krajach), interaktywność jest nie do pobicia. Większość z nas ma już swoje skrzynki pocztowe. Być może odwiedzaliśmy już sklepy internetowe i zastanawiamy się nad otwarciem – tak modnego ostatnio – bankowego konta internetowego. Ale uwaga! Nie traćmy czujności. Fala niesamowitego boomu internetowego sprzed dwóch lat, kiedy to wartość akcji firm oferujących cyberusługi rosła w oczach, odsłoniła też drugą, niezbyt miłą twarz globalnej sieci. W krajach Unii Europejskiej w 2000 roku o 50% (!) wzrosła ilość oszustw dokonywanych z użyciem kart płatniczych. Lwia część tego niechlubnego wzrostu przypadła na transakcje zawierane w Internecie. Ocenia się, że wartość nielegalnych operacji wyniosła 600 milionów euro. Amerykańscy specjaliści oceniają, że od 20 do 40% operacji zakupów on-line jest związanych z próbą oszustwa wymierzoną albo w kupującego (ktoś podszywa się pod inną osobę i dokonuje zakupów na jej konto), albo w sprzedającego (kupujący używając rożnych tricków płaci mniej za towar lub nie płaci wcale). Ujawniono wiele skandalicznych przypadków wycieku danych o numerach kart kredytowych klientów ze stron internetowych znanych firm. Jednym z najbardziej spektakularnych przykładów był „sukces" hakera przedstawiającego się jako Curador, który wykorzystując żenujące słabości w powszechnie stosowanym oprogramowaniu komputerowym dokonał ośmiu włamań na strony www w czterech krajach i ściągnął z nich dane 23000 kart kredytowych. Opublikował też list, w którym podziękował wszystkim naiwnym użytkownikom sieci za pozostawienie tak cennych informacji bez zabezpieczenia. „Chciałbym też pozdrowić mego przyjaciela Billa Gatesa. Facet, który sprzedaje systemy operacyjne z defaultowo ustawioną opcją swobodnego dostępu nie może być zły" zakończył swój list Curador. Ocenia się, że właśnie poważne problemy z bezpieczeństwem w sieci były przyczyną szybkiego ochłodzenia entuzjazmu dla biznesu internetowego. Czy od tego czasu coś się poprawiło? Ostatnio Gazeta Wyborcza zamieściła wiadomość, że w 2001 roku blisko 10 tysięcy Amerykanów zostało okradzionych w Internecie na łączną sumę 17,8 miliona dolarów. Osobną kategorią zagrożeń czyhających na nas w świecie bitów, to ataki mające na celu niszczenie cennych dla nas informacji lub uniemożliwianie dostępu do nich. Mam tu na myśli powstające jak grzyby po deszczu złośliwe programy komputerowe typu wirus bądź koń trojański. Wydaje się, że pomysłowość ludzka w bezinteresownym wyrządzaniu krzywdy drugiemu nie zna granic. Oto wraz z naszym wejściem w epokę informacji pojawiło się nowe zajęcie, któremu z lubością oddaje się wielu młodych i zdolnych ludzi – pisanie i puszczanie w obieg różnych programów destrukcyjnych. Każdy z nas wie, ile szkody mogą narobić. Kiedyś można było zainfekować swój system komputerowy przez jakąś trefną dyskietkę, dziś można to zrobić bezwiednie surfując sobie spokojnie po wirtualnej sieci. Z pełnej swobody poruszania się po cyber-przestrzeni



Słynna niemiecka mechaniczna maszyna szyfrująca Enigma używana przez Wermacht w czasie II wojny światowej. Uchodziła za całkowicie bezpieczną. Ocenia się, że w najbardziej zaawansowanej wersjii stosowanej w marynarce mogło istnieć jakieś 8 trylionów kluczy szyfrujących. Nad złamaniem szyfru Enigmy pracował przed wojną zespół polskich kryptoanalityków. Wykorzystując szereg błędów popełnionych przez niemieckich operatorów udało im się odkryć zasadę działania maszyny. Swoje odkrycia przekazali jeszcze przed rozpoczęciem wojny wywiadowi brytyjskiemu. Dziś wiemy na pewno, że złamanie kodów Enigmy miało ogromny wpływ na losy wojny.

korzystają też czarne charaktery, stąd jeśli naszym narzędziem do poruszania się po niej jest poczciwy pecet z systemem operacyjnym Windows bez żadnych dodatkowych zabezpieczeń, to nigdy nie możemy być pewni czy w czasie ściągania jakichś stron www nie przedostał się do naszego komputera podstępny wirus i czy nie przygotowuje się właśnie do sformatowania naszego dysku twardego. Mniej brzemienne skutki mają częste ataki na serwery obsługujące skrzynki pocztowe. Kończy się to odmową obsługi naszego konta przez zainfekowany serwer. Podobne efekty przynosi, praktykowana przez patologicznych użytkowników sieci, zabawa zapychania ograniczonych przestrzeni skrzynki odbiorczej tysiącami bezwartościowych wiadomości. Zwłaszcza aktywni uczestnicy dyskusji internetowych narażeni są również na inny rodzaj ponurego dowcipu. Chodzi mianowicie o to, że jakiś złośliwiec podszywając się pod nich zapisze ich na wiele list dyskusyjnych jednocześnie. W skrajnych przypadkach zdarzało się, że zaskoczeni użytkownicy sieci otrzymywali ok. 5000 listów dziennie co skutecznie utrudniało im życie.

Nie tylko ukradną nam pieniądze ale również tożsamość i prywatność

Puśćmy wodze negatywnym fantazjom. Nadawanie numerów ludziom kojarzy nam się jak najgorzej. Cały cywilizowany świat potępił uprzedmiotowienie ludzi w państwach totalitarnych. Minęło trochę czasu, nadeszła technika cyfrowa ze wszystkimi dobrodziejstwami i zagrożeniami. I co tak naprawdę określa dziś naszą tożsamość? Tak, tak nie mamy co się oszukiwać w świecie informacji cyfrowej jesteśmy numerem, który byle komputer jest w stanie odnaleźć wśród milionów innych w ciągu ułamka sekundy. W ciągu bardzo krótkiego czasu ktoś może ustalić kim jesteśmy i gdzie jesteśmy. Wszak mamy włączoną naszą wspaniałą komórkę. Bardzo jesteśmy z niej dumni, ale czy zdajemy sobie sprawę z tego, że dzięki połączeniom globalnej sieci GSM ktoś jest w stanie określić gdzie aktualnie przebywamy. Stwarza to kolejne zagrożenie tym razem dla naszej prywatności. Organy ścigania mają możliwości (zagwarantowane prawem) dostępu do tych danych. Może to być nieoceniona broń w walce ze światem przestępczym, ale może stać się narzędziem totalnej inwigilacji. Przykład: przewidziany do pomocy w ściganiu przestępców program „Promis" został wdrożony w niezliczonej ilości miejsc umożliwiając amerykańskiej służbie wywiadowczej NSA (National Security Agency) dostęp do niezwykle szerokiej gamy baz danych na całym świecie – mówi się nawet o dostępie do danych banków szwajcarskich. Służby wywiadowcze zbierają informacje często nielegalnie i na zapas, bo w zaawansowanej technice cyfrowej nie ma problemu z przechowywaniem i analizą danych. Należy więc liczyć się z tym, że za dziesięć lat ktoś zapyta nas co robiliśmy 1 lipca 2002 roku około godziny 13.00 na ulicy Lipowej w Pcimiu Dolnym. Upiorna wizja odartego z resztek prywatności człowieka z „Roku 1984" George'a Qrwella wydaje się całkiem możliwa do zrealizowania w możliwym do przewidzenia czasie. Świadczą o tym umowy zawarte niedawno między UE a FBI, które otwierają furtkę globalnemu systemowi podsłuchu. Mówi się już głośno o tym, że nawet przeciętny monitor komputerowy działa jak nadajnik. Dysponując odpowiednio czułą aparaturą nawet ze znacznej odległości można odfiltrować sygnał emitowany przez monitor i zrekonstruować zawartość ekranu. Nawiasem mówiąc wyświetlacz bankomatu też jest monitorem. Pięknie co? Ale jak straszyć to na całego. Jeśli naszą tożsamość w globalnej sieci określa numer, to łatwo można sobie wyobrazić, że ktoś może podając się za nas wyrządzać szkody, za które jednak my będziemy musieli odpowiadać. Czasem wystarczy tylko stanąć na drodze osoby pozbawionej skrupułów, która będzie miała odpowiednie zdolności i okazję ich wykorzystania. No i jak teraz podoba się wam nasz wspaniały cyfrowy świat? Może trochę stracił blask, ale to dobrze bo świadomość zagrożeń jest podstawowym czynnikiem poprawiającym bezpieczeństwo.

Zaszyfrowany świat, czyli kryptografia przychodzi z odsieczą

Prawdę mówiąc to straszę was trochę na wyrost. Ludzie od dawna szukali sposobów ochrony szczególnie ważnych informacji i nauczyli się robić to całkiem skutecznie. I tak już w starożytności narodziła się kryptografia. Dzięki niej możemy przekształcić normalny, zrozumiały tekst lub innego typu wiadomość tak, że stanie się ona niezrozumiała dla nieupoważnionego odbiorcy. Właściwy adresat wiadomości może po jej otrzymaniu zamienić ją z powrotem na postać czytelną. Właśnie wykorzystywanie na szeroką skalę kryptografii jest dziś podstawowym środkiem utrzymania bezpieczeństwa w świecie bitów. Prawie wszystkie wymienione wyżej operacje przetwarzania i przesyłania informacji wykorzystują jakieś procedury kryptograficzne. System kryptograficzny składa się z dwóch wzajemnie dopełniających się procesów: szyfrowania i deszyfrowania. Szyfrowanie to proces, w którym oryginalna wiadomość tekstowa (zwana w kryptologii tekstem jawnym) jest zamieniana na wiadomość zaszyfrowaną (kryptogram). Zobaczmy to na przykładzie prostego szyfru wykorzystywanego przez starożytnych Rzymian zwanego szyfrem Cezara (od tego przykładu zaczyna się większość książek o kryptologii). Polegał on na tym, że alfabet zapisywano na obwodzie koła tak, że po A następowało Z (czyli alfabet powtarzał się cyklicznie). Każda litera tekstu jawnego zamieniana była na występującą w alfabecie trzy miejsca za nią. Przebieg szyfrowania przebiegał następująco:

A = D
B = E
C = F
.....
W = Z
X = A
Y = C
itd.

Biorąc pod uwagę poziom intelektualny armii rzymskiej i jej przeciwników metoda ta była w owym czasie nie do złamania. Ale dla niezbyt pojętnego następcy Juliusza Cezara – Augusta nawet ona była zbyt skomplikowana. August zamieniał każdą literę na bezpośrednio po niej następującą, czyli A na B, B na C itd. W systemie szyfrowania Cezara kluczem jest 3. August wykorzystywał tę samą metodę, lecz z kluczem 1. Tak więc klucz jest tu liczbą kroków, o które trzeba przesunąć alfabet w przód, aby dokonać substytucji. Wobec tego istnieje 25 kluczy (klucz 0 nie zmienia tekstu). W języku matematyki mamy do czynienia ze znanym z teorii liczb dodawaniem stałej w klasie reszt modulo 26, czyli dodawaniem reszt z dzielenia przez 26. Oznaczmy przez p literę tekstu jawnego, przez c literę kryptogramu (tj. otrzymanego tajnego ciągu znaków), a przez s klucz (stałą). Wtedy możemy zapisać:

$c = p + s \bmod 26$

Pamiętajmy przy tym, że litery traktujemy jako liczby, to znaczy A = 0, B =1,.....Z = 25. Wyrażenie mod 26 oznacza tutaj: jeśli $p + s$ jest większe lub równe 26, to od sumy odejmujemy 26 (w szerszym sensie taką wielokrotność liczby 26, by wynik mieścił się w przedziale: 0....25). Osobom nie związanym profesjonalnie z matematyką taka definicja wyda się nieco osobliwa i trąci przerostem formy nad treścią, ale warto ją zapamiętać bo przyda nam się jeszcze przy omawianiu bardziej skomplikowanych metod szyfrowania. Oczywiście dziś nie stosuje się szyfru Cezara z prostej przyczyny. Dysponując komputerem można go dziecinnie łatwo złamać. Ale..... spróbujmy zrobić to bez komputera! Od razu poczujemy szacunek dla kryptoanalityków, którzy jeszcze kilkadziesiąt lat temu np. podczas drugiej wojny światowej pracowali z przysłowiowym ołówkiem w ręku. Nowoczesne procesy szyfrowania realizowane są z użyciem odpowiedniego algorytmu (który jest złożoną funkcją matematyczną) oraz specjalnego klucza szyfrującego. Deszyfrowanie przeprowadza się używając innej złożonej funkcji oraz klucza deszyfrującego. Aktualnie stosowane są dwa rodzaje algorytmów kryptograficznych. Pierwszy to algorytmy wykorzystujące **klucz symetryczny**. Znaczy to, że

klucz szyfrujący jest identyczny z deszyfrującym. Taki klucz bywa też nazywany prywatnym albo tajnym. Warto podkreślić, że symetria odnosi się do klucza a nie do metody. Najczęściej sposób w jaki szyfrujemy różni się od sposobu deszyfrowania. Nawet w metodzie Cezara szyfrowanie i deszyfrowanie były odmiennymi procedurami. Przypomnę, że przy szyfrowaniu do każdego znaku dodawaliśmy (modulo 26) określoną wartość, przy deszyfrowaniu – odejmowaliśmy. Mówiąc ściśle, w wypadku metod symetrycznych korzystamy, co prawda, zawsze z tego samego klucza, lecz niemal zawsze z dwóch procedur. Drugim rodzajem używanych obecnie algorytmów szyfrujących są algorytmy wykorzystujące tak zwany **klucz publiczny**. Stosuje się w nich dwa różne klucze: jeden do szyfrowania wiadomości, a drugi do jej deszyfrowania. Właśnie klucz używany do szyfrowania nazywa się kluczem publicznym, gdyż może on zostać udostępniony publicznie bez ryzyka ujawnienia zawartości szyfrowanych przy jego użyciu informacji. Klucz deszyfrujący jest w tym systemie kluczem prywatnym czyli tajnym, który zna tylko osoba uprawniona do odczytania wiadomości. Systemy oparte na kluczu publicznym są czasami nazywane algorytmami wykorzystującymi klucz asymetryczny. Niemożliwe (to znaczy nie można tego zrealizować przy zastosowaniu znanych środków w praktycznie akceptowalnym czasie) jest wyliczenie klucza prywatnego na podstawie klucza publicznego. Obydwa wymienione rodzaje algorytmów mają swoje zalety i wady. Algorytmy oparte na kluczach symetrycznych są głównym mechanizmem współczesnych systemów kryptograficznych. Są one znacznie szybsze i nieco łatwiejsze w zastosowaniu od algorytmów opartych o klucz publiczny. Niestety ich praktyczne zastosowanie wiąże się z jedną bardzo poważną przeszkodą. Mianowicie, aby dwie strony mogły bezpiecznie wymieniać informacje zaszyfrowane za pomocą algorytmu wykorzystującego klucz symetryczny, muszą najpierw w bezpieczny sposób wymienić między sobą sam klucz szyfrujący. Jeśli chodzi o zwykłe pogaduszki z przyjaciółmi za pośrednictwem Internetu wystarczy przekazać telefonicznie wspólne hasło. Ale jeśli chodzi o tajemnice ogromnego znaczenia? Można wysłać pocztą, ale konkurencja albo obcy wywiad mogą przekupić listonosza. Najlepiej odwiedzić przyjaciela osobiście. Delikatny problem wyłania się, gdy mieszka on powiedzmy w Nowej Zelandii. Sytuacja znacznie się komplikuje, gdy tą metodą chcemy przekazywać poufne informacje wielu osobom. Problem ten nie istnieje w algorytmach wykorzystujących klucz publiczny. Jest on bowiem dostępny dla wszystkich zainteresowanych. Jeśli osoba A chce wysłać osobie B zaszyfrowaną wiadomość, musi jedynie uzyskać jej klucz publiczny (klucz taki umieszcza się często na prywatnych stronach www). Dzięki temu A będzie mogła zaszyfrować przesyłaną do B wiadomość, którą tylko B będzie mogla odczytać, gdyż tylko ona posiada odpowiedni klucz prywatny, który – dodajmy - może nigdy nie opuszczać jej komputera. Nie ma potrzeby żadnego tajnego porozumienia między nadawcą a odbiorcą. W rzeczywistości nie muszą się oni przedtem w ogóle kontaktować. Algorytmy wykorzystujące klucz publiczny są więc niezwykle praktyczne i wydaje się, że powinny szybko wyprzeć metody symetryczne, ale mają jedną poważną wadę: są powolne. Z tego powodu stworzono trzecią grupę systemów – systemy hybrydowe, łączące zalety dwóch poprzednich. W systemach tych metody asymetryczne wykorzystywane są do uzgodnienia jednorazowego tzw. klucza sesji, który jest tajnym kluczem wykorzystywanym później w metodach symetrycznych. Niemal wszystkie używane w praktyce systemy oparte o klucz publiczny są systemami hybrydowymi. W tym miejscu musimy wprowadzić kolejne pojęcie zwane mocą kryptograficzną algorytmu. Krótko mówiąc jest to zdolność algorytmu do odparcia prób jego złamania. Zależy ona od wielu czynników:

- tajność klucza
- odporność klucza na odgadnięcie lub wypróbowanie wszystkich możliwych jego kombinacji (tzw. brute force attack). Zazwyczaj im dłuższy klucz, tym trudniej go odgadnąć lub wypróbować wszystkie możliwe kombinacje
- Trudność określenia algorytmu odwrotnego bez znajomości klucza szyfrującego (złamanie algorytmu)
- Istnienie lub brak tzw. tylnego wejścia, czyli alternatywnych sposobów umożliwiających prostsze rozszyfrowanie wiadomości bez znajomości klucza
- Możliwość odszyfrowania całej wiadomości poprzez odszyfrowanie jej części (tzw. atak znanym tekstem jawnym)

Moc kryptograficzna praktycznie nie daje się udowodnić. Istnieje co najwyżej możliwość udowodnienia jej braku. W chwili tworzenia nowego algorytmu jego autorzy mogą być przekonani, iż jest on idealny. Z upływem czasu opracowywane są jednak nowe metody przeprowadzenia ataków, które mogą doprowadzić do złamania szyfru. Warto zauważyć, że coraz szybsze komputery stanowią zagrożenie dla systemów szyfrowania. Nawet jeśli rozwiązanie wydaje się z początku niewyobrażalnie skomplikowane, może w niedługim czasie zostać znacznie uproszczone. Najlepszym dowodem potwierdzającym moc algorytmu szyfrującego jest poddanie go publicznej weryfikacji tzn. wystawienie na ataki kryptoanalityków.

Nie tak dawno temu w Ameryce

Narodziny wyżej omówionych systemów wiązały się ściśle z rozwojem technik obliczeniowych i rewolucji w dziedzinie komunikacji. Na początku lat 70 NBS (National Bureau of Standards) dostrzegło konieczność opracowania algorytmu kodowania, który byłby powszechnie dostępny i bezpieczny. Jak na Amerykę przystało rozpisano konkurs i tak oto w firmie IBM narodził się algorytm DES (Data Encryption Standard). Był on pierwszym publicznie przedstawionym algorytmem, który został zbadany przez NSA (National Security Agency) – amerykańską organizację rządową, która intensywnie zajmuje się kryptologią, ogólnoświatowym podsłuchem i zbieraniem danych (prawdopodobnie zatrudnia 40000 pracowników w tym 2000 wybitnych matematyków i ma dostęp do niewiarygodnie szybkiej techniki obliczeniowej, do jej istnienia przyznano się dopiero w związku z pojawieniem się DES-a). Nawiasem mówiąc, wciąż trwają kontrowersje na temat roli NSA w upublicznieniu DES-a. Niektórzy sugerują nawet, że NSA zredukowała długość klucza szyfrującego algorytmu ze 128 do 56 bitów (pojawiały się wówczas spekulacje, czy NSA jest w stanie złamać DES–a) lub pozostawiła w algorytmie tzw. „tylne drzwi" umożliwiające rozszyfrowywanie interesujących ją przekazów. Pod koniec 1976 roku DES stał się oficjalnym standardem szyfrowania. Metoda została pomyślana jako środek do ochrony „normalnej" informacji, nie zaś do ochrony danych najwyższej klasy bezpieczeństwa. Być może zdecydował o tym właśnie fakt jej upublicznienia. DES wykorzystywał symetryczny klucz 56 bitowy i był algorytmem mocnym. Ale jak mocnym? Wiemy już, że na powyższe pytanie nie istnieje oficjalna odpowiedź. Jedynym użytecznym praktycznie sposobem ataku na DES-a pozostawał „brute force" czyli sprawdzenie wszystkich 2^{56} możliwych kluczy. To ogromna liczba – dla około 72 000 000 000 000 000 kluczy trzeba deszyfrować kryptogram i testować pod kątem zawierania sensownej treści. W 1993 roku maszynę, która mogłaby tego dokonać w 3,5 godziny, oceniono na milion dolarów. W 1998 ukazały się informacje, że hipotetycznie czas ten można skrócić do 0,5 godziny przy zachowaniu ceny.

Rok 1998 Electronic Frontier Foundation Komputer Deep Crack kosztujący 220.000$ potrzebuje 4,5 dnia na złamanie jednego algorytmu DES.

Wszelkie spekulacje rozwiała amerykańska organizacja EFF (Electronic Frontier Foundation), która zbudowała nakładem „zaledwie" 250 000 dolarów komputer Deep Crack do łamania DES-a. Można już oczekiwać, że usługa kryptoanalizy DES-a oferowana jest „spod lady". Wniosek: w żadnym wypadku nie wolno przesyłać przez Internet zaszyfrowanych DES–em informacji, które są warte miliony. W każdym razie ta pierwsza publiczna prezentacja dobrego algorytmu, który mógł być zbadany przez cały świat, była olbrzymim krokiem naprzód. Okazało się też, że prawdopodobnie nie istnieją „tylne drzwi". Słabością DES–a była długość klucza. Przy dzisiejszych mocach obliczeniowych era 56-bitowych kluczy przeszła definitywnie do historii. W 1997 roku NIST (National Institute of Standards and Technology) - następca NBS - rozpoczął poszukiwanie następcy DES–a. Od tamtego czasu powstały algorytmy wykorzystujące klucz 128-bitowy, RC4 opracowany przez Ronalda Rivesta i firmę RSA Data Security – powszechnie wykorzystywany przez przeglądarki do szyfrowania danych przekazywanych przez sieć www - a także IDEA (International Data Encryption Algorithm} rodem ze Szwajcarii, który jest wykorzystywany przez popularny program PGP do szyfrowania poczty elektronicznej. Przy 128-bitowym kluczu istnieje 2^{128} różnych kombinacji. To naprawdę bardzo dużo. Gdyby komputer sprawdzał miliard kluczy na sekundę i gdyby atakujący dysponował miliardem takich komputerów, to nawet wówczas złamanie klucza 128-bitowego zajęłoby 10^{13} lat. Jest to prawie tysiąckrotnie więcej niż wiek wszechświata. Przy dzisiejszym stanie wiedzy takie ataki są, delikatnie mówiąc, niepraktyczne. Nie jest jednak tak zupełnie dobrze. Wiele czynników natury technicznej, prawnej i politycznej ogranicza używanie takich algorytmów. Poza tym szyfry łamie się nie tylko metodą siłową. Większość z nich ma jakieś słabe strony, co może wykorzystać jakiś zdolny kryptoanalityk i odszyfrować wiadomość bez znajomości klucza.

Trochę matematyki, czyli o algorytmach z kluczem publicznym

W roku 1976, tym samym, w którym za oficjalny standard uznano DES-a, narodziła się również metoda szyfrowania oparta o klucz publiczny i fakt ten odmienił całkowicie dotychczasowe oblicze kryptografii. Nowe metody wniosły zupełnie nową jakość – rozwiązywały problem przekazywania kluczy. Interesujące jest pytanie, dlaczego kryptografia wykorzystująca klucze publiczne musiała czekać na swe odkrycie tak długo, choć matematyczne narzędzia z teorii liczb potrzebne do jej wynalezienia były znane już w XVIII wieku. Jednym z powodów późnego rozwoju koncepcji kluczy publicznych było to, że dawniej (to znaczy do lat 70) kryptografii używano głównie do celów wojskowych i dyplomatycznych, do których szyfry z tajnymi kluczami świetnie się nadawały. Jednak wraz z komputeryzacją życia gospodarczego powstały nowe potrzeby zastosowania kryptografii. W przeciwieństwie do sytuacji w wojsku i dyplomacji, gdzie mamy do czynienia ze sztywną hierarchią, nie zmieniającymi się przez długi czas listami uprawnionych osób i zorganizowanym systemem kurierów, przy zastosowaniach w działalności gospodarczej i ochronie danych spotykamy się z szerszą i bardziej płynną grupą użytkowników systemu. Kryptografia z kluczem publicznym nie była wynaleziona wcześniej, bo po prostu nie było na nią zapotrzebowania. Poza tym, jak dowiemy się za chwilę, bezpieczne klucze publiczne opierają się na użyciu bardzo dużych liczb, których przeliczanie bez komputerów byłoby bardzo trudne. Właśnie wynalezienie metod szyfrowania z użyciem klucza publicznego ogromnie zwiększyło rolę algebry i teorii liczb w kryptografii. Podstawą tych metod jest zastosowanie do szyfrowania matematycznych funkcji jednokierunkowych. Co to takiego? Mówiąc nieformalnie, funkcja f:XY jest jednokierunkowa, jeśli dla danego xX łatwo jest obliczyć f(x), ale wyliczenie $f^{-1}(y)$ dla przypadkowo wybranego y jest trudne. O ile dobre algorytmy wykorzystujące klucz symetryczny modyfikują dane wejściowe na podstawie podanego klucza (opracowanie nowego algorytmu polega więc na stworzenie nowej metody modyfikacji), to algorytmy klucza publicznego opierają się na teorii liczb. W tym przypadku opracowanie nowego algorytmu wymaga rozwiązania nowego problemu matematycznego. Omówimy teraz dwa algorytmy asymetryczne. Pierwszym w historii był algorytm Diffiego- Hellmana. System ten nie służy do szyfrowania w klasycznym sensie. Jest to sposób tworzenia kluczy kryptograficznych i ich wymiany publicznymi kanałami. Bazuje on na poważnym problemie matematyki jakim jest logarytm dyskretny. Jak to działa? Oto A (Alicja) i B (Bob) chcą uzgodnić dużą liczbę naturalną, która będzie im potem służyć za tajny klucz w systemie z kluczami prywatnymi. Sposób ich postępowania można przedstawić tak:

1 Alicja i Bob wybierają wspólnie jakąś dużą liczbę pierwszą p (przypominam, że liczba pierwsza dzieli się tylko przez 1 i samą siebie) oraz, w zależności od p, jakiś generator g (tzn. takie g, że wszystkie liczby 1....p-1 można przedstawić jako reszty postaci g mod p. Liczby k i g nie są tajne.

2 Alicja wybiera dużą, tajną liczbę $x < p$ i wysyła Bobowi resztę X z równania: $X = g^x \bmod p$.

3 Analogicznie Bob wybiera dużą tajną liczbę $y < p$ i przesyła Alicji resztę Y z równania $Y = g^y \bmod p$

4 Alicja oblicza resztę: $s = Y^x \bmod p$

5 Bob oblicza $s' = X^y \bmod p$

Reszty s i s' są równe, gdyż zachodzi: $s = s' = g^{xy} \bmod p$.

Wartość s służy Alicji i Bobowi jako klucz sesyjny. Wprawdzie ktoś mógłby poznać wartości p, g, X i Y, jednak, aby obliczyć klucz s, musiałby wyliczyć dyskretny logarytm, tzn. wyznaczyć x z reszty $g^x \bmod p$. Choć dla laika brzmi to niepozornie, jest to z matematycznego punktu widzenia trudny orzech do zgryzienia. Prawdę mówiąc, jeszcze nikt tego nie dokonał. Obecnie absolutnym liderem na rynku algorytmów asymetrycznych jest algorytm RSA opracowany w 1978 roku przez późniejszych profesorów MIT (Massatchussets Institute of Technology) – Ronalda Rivesta, Adi Shamira i Leonarda Adlemana. Nazwa pochodzi od pierwszych liter ich nazwisk. System RSA nadaje się zarówno do szyfrowania informacji, jak i do tworzenia podpisów cyfrowych. Dla jasności przy podpisie elektronicznym użycie kluczy publicznego i prywatnego następuje w odwrotnej kolejności. Najpierw szyfruję wiadomość moim kluczem prywatnym. Odczytać ją może każdy, kto dysponuje moim kluczem publicznym. Jednakże dzięki temu zyskuje pewność, że to ja jestem autorem wiadomości, bo tylko ja (przynajmniej teoretycznie mam dostęp do swojego klucza prywatnego). Algorytm RSA opiera się na bardzo trudnym matematycznym problemie, mianowicie na faktoryzacji – czyli mówiąc po ludzku - rozkładaniu na czynniki pierwsze bardzo dużych liczb (obecnie co najmniej 300 miejsc w zapisie dziesiętnym). Żeby zrozumieć o co chodzi, powróćmy do definicji liczb pierwszych. Liczba naturalna nazywa się pierwszą, jeśli jest podzielna wyłącznie przez 1 i przez samą siebie. Przy czym umownie 1 nie nazywa się liczbą pierwszą. Pierwszymi są więc np. liczby: 2,3,5,7,11,13 .....itd. W tym miejscu musimy wprowadzić niestety jeszcze jedną matematyczną definicję, która będzie nam potrzebna za chwilę, mianowicie chodzi o liczby względnie pierwsze. Otóż liczbę m nazywa się względnie pierwszą z n, jeśli żadna liczba większa niż 1 nie dzieli równocześnie m i n. 12 i 7 są więc względnie pierwsze, ale 12 i 8 już nie. Dla matematyka liczby pierwsze to jak dla fizyka cząstki elementarne. Można z nich bowiem zbudować wszystkie liczby naturalne. Bo już w III wieku p.n.e. Euklides udowodnił fundamentalne twierdzenie arytmetyki, że każda liczba naturalna większa od 1 może być wyrażona jako iloczyn liczb pierwszych i to w jeden jedyny sposób. Np. 75 900 jest iloczynem siedmiu liczb pierwszych: 2,2,3,5,5,11,23. Nazywa się to rozkładem liczby na czynniki pierwsze. To właśnie na trudności w rozkładaniu dużych liczb na czynniki pierwsze opiera się moc kryptograficzna algorytmu RSA. Działa to następująco. Najpierw generujemy klucz szyfrujący. W tym celu każdy użytkownik systemu – nazwijmy go znów umownie A(Alicja) - wybiera dwie bardzo duże liczby pierwsze p i q (np. 512 bitowe) i mnoży je przez siebie uzyskując liczbę

n. Czyli $n = pq$. Następnym krokiem jest obranie kolejnej liczby $e1$, która jest względnie pierwsza z $(p-1)(q-1)$. Właśnie n i e tworzą klucz publiczny. Dalej Alicja oblicza wartość d, dla której $de = 1 \bmod (p-1)(q-1)$. Kluczem prywatnym jest d. Co robi użytkownik B(Bob), gdy chce przesłać Alicji wiadomość, której liczbową wartość określmy przez w? Znajduje na prywatnej stronie internetowej Alicji (albo w książce telefonicznej) jej klucz publiczny. Następnie szyfruje wiadomość w obliczając resztę z dzielenia w^e przez n. Wynik – nazwijmy go s, jest właśnie zaszyfrowaną wartością w. W języku matematycznym Bob wykonuje potęgowanie modularne: $s = w^e \pmod n$. Aby odszyfrować wiadomość, Alicja posługuje się swoim tajnym kluczem deszyfrującym d. Jak? Wylicza resztę z dzielenia s^d przez n. Wynik jest dokładnie równy w. Stosując zapis matematyczny $w = s^d \bmod n$. Uff!!

Jeśli jest to dla was niestrawne, to możecie – tak jak ja – poprosić o wyjaśnienie znajomego matematyka, który jeszcze nie stracił zupełnie kontaktu z rzeczywistością i umie mówić ludzkim językiem. Jeśli wam się nie uda i ciągle nie wiecie o co chodzi, nie przejmujcie się tak bardzo. Mówiąc najkrócej pomysł algorytmu RSA przedstawia się następująco: znając tylko wartość iloczynu $n = pq$ dwóch liczb pierwszych, niezwykle trudno jest znaleźć oba jego czynniki (tj. p i q). Wraz ze wzrostem długości liczby trudność faktoryzacji gwałtownie rośnie. Warto oczywiście podkreślić wyrażenie „niezwykle trudno" bo nikt na razie nie udowodnił, że to jest niemożliwe. Z tego wynika, że wybitni matematycy nie potrzebują obawiać się na razie braku pracy. Wszyscy próbują rozwiązać powyższe problemy matematyczne, na których oparto algorytmy z kluczem publicznym. Jeśli komuś się to uda, będziemy musieli zrezygnować z algorytmu RSA na rzecz innej, bardziej odpornej metody szyfrowania. Walka kryptografów z kryptoanalitykami trwa. A może niedługo ktoś zbuduje komputer kwantowy, dla którego dzisiejsze bariery obliczeniowe staną się śmieszne, bo wzrost prędkości obliczeniowej w stosunku do znanych dziś algorytmów będzie wykładniczy? Co to by znaczyło? Otóż obecnie uznaje się za teoretycznie możliwe złamanie nawet 512-bitowego klucza RSA przy użyciu konwencjonalnych komputerów (oczywiście nowszej generacji), ale złamanie 1024-bitowego klucza RSA tymi metodami jest czystą utopią. Gdybyśmy mieli jednak komputer kwantowy, to 1024 bity zajęłyby nam dwuewentualnie czterokrotnie więcej czasu niż 512 bitów. I możliwe, że chodziłoby o minuty czy nawet sekundy. Wtedy naprawdę dzisiejsze systemy szyfrowania danych trzeba będzie wyrzucić do śmieci. Ale wróćmy do rzeczywistości początku XXI wieku. Póki co, jednym z najsłynniejszych ataków na RSA był atak, w wyniku którego obliczono czynniki pierwsze liczby RSA-129 – jednej z dużych liczb wykorzystywanych jako klucz publiczny. Wartość RSA-129 opublikowano w 1977 roku w magazynie Popular Science. Jej czynniki wyliczyła w roku 1994 międzynarodowa grupa ochotników koordynowana przez czterech naukowców. Przez cały czas trwa poszukiwanie kolejnych dużych liczb pierwszych, co wcale nie jest łatwe bo nie istnieje matematyczny algorytm takiego wyszukiwania. Pozostaje więc metoda prób i błędów. Zachęcam do spróbowania swoich sił (można na tym nieźle zarobić). Dla porządku podaję, że największa znana dziś liczba pierwsza odkryta w lipcu 2001 przez Michaela Camerona i George'a Woltmana to $2^{13466917}-1$. Ma ona 4 miliony 53 tysiące 946 cyfr. A więc do dzieła i powodzenia!

Świat totalnie zaszyfrowany, ale czy bezpieczny?

Omówione wyżej nowoczesne metody szyfrowania wydają się na dzień dzisiejszy skutecznie chronić ważne informacje. Niedawno Bill McQuaide – wiceprezes firmy RSA Security, posiadającej praktyczny monopol na najpopularniejszy obecnie algorytm z kluczem publicznym – powiedział w wywiadzie dla Gazety Wyborczej: „Przeciętny użytkownik nie musi obawiać się, że ktoś będzie próbował złamać szyfr, którym szyfrowana jest sesja komunikacyjna z bankiem. Gdy ktoś inwestuje, dajmy na to 10 tys. dolarów to nie po to, by ukraść tysiąc. To niepraktyczne. A do złamania sesji SSL ze 128 bitowym kluczem potrzebna jest olbrzymia moc obliczeniowa. Gdy ktoś jest w stanie ją zgromadzić, nie będzie kradł pieniędzy z kont osobistych." Bill McQuaide powiedział też, że według jego wiedzy nawet wywiad amerykański nie ma szans na złamanie takich szyfrów. Ale pamiętajmy, że są one tylko jednym elementem w procedurach stosowanych przez użytkowników systemów przetwarzania i przesyłania danych np. banków, którym powierzyliśmy swoje pieniądze. Gdzieś, w którymś miejscu poufne dane mogą być przechowywane w formie niezaszyfrowanej. Hakerzy usiłują więc np. dostać się do systemu bankowego i po prostu ukraść hasła, numery kart kredytowych. Stosują różne sztuczki, np. dzwonią do użytkownika sieci bankowej, przedstawiają się jako administratorzy systemu i proszą o hasło. Wbrew pozorom, to bardzo często działa. Dlatego nawet dobre kryptologiczne algorytmy nie gwarantują niezawodnej ochrony. Bezpieczeństwo może zapewnić tylko łańcuch pozbawiony słabych ogniw. Każdy z nas musi więc mieć świadomość problemów bezpieczeństwa. Nie wolno zapisywać haseł na karteczkach przyklejonych do monitora, ani na spodniej stronie klawiatury. Nie wolno zezwalać innym na patrzenie na ręce przy wpisywaniu hasła, ani mamrotać hasła pod nosem przy wpisywaniu go, a już na pewno nigdy nie wydrapywać PIN-u na swojej karcie kredytowej. W praktyce niestety nieraz ma to miejsce. Poza tym nośniki zawierające niezaszyfrowane dane muszą być przechowywane w bezpiecznym miejscu, a pisane jawnym tekstem poufne wiadomości nie mogą swobodnie wędrować po sieciach komputerowych, w których mogłyby przechwycić je osoby trzecie. Komputery powinny być zabezpieczone przed dostępem niepowołanych osób fizycznie, ale przede wszystkim programowo. Przecież jak to wynika z omówionych wcześniej przykładów, włamanie do systemu komputerowego pracującego pod „gołym" Windowsem i np. edycja zawartości dysku twardego nie przedstawia dla zaawansowanego hakera większych trudności. I wreszcie na koniec najważniejszy warunek bezpieczeństwa: **Wszyscy współpracownicy muszą być godni zaufania**. Wynika z tego prosty wniosek, że najlepszą inwestycją w bezpieczeństwo, również w świecie bitów byłoby jednak trwałe podniesienie poziomu moralnego społeczeństwa. Ale to już materiał na zupełnie inny artykuł i raczej nie nałamach EdW.

Wojciech Turemka