Rejent * rok 11 * nr 10(126)
październik 2001 r.

Jerzy Jacyszyn
Sebastian Zakrzewski

Podpis elektroniczny jako element systemu zabezpieczenia danych w sieci (część pierwsza)*

Truizmem byłoby prowadzenie rozważań o tym, jak wielką rolę odgrywają w naszym życiu nowoczesne media komunikacyjne. Jest to faktem i nie trzeba chyba nikogo przekonywać o ich dużym wpływie na ekonomię, kulturę, sztukę, a także taką dziedzinę, jaką jest prawo. Prawo bowiem, by pozostawać dziedziną żywą, musi reagować na wszelkie zmiany rzeczywistości społecznej, gdyż nic innego jak panujące stosunki społeczne znajdują swoje odbicie w obowiązującym prawie. Co więcej, przemiany technologiczne, które możemy obserwować, dają także prawnikom do ręki nowe narzędzia, które pozwolą dostosować prowadzenie praktyki prawniczej – nie tylko w jej aspekcie merytorycznym, ale także rozwiązań administracyjnych i technicznych – do potrzeb współczesnego rynku usług. Poniższe opracowanie kładzie nacisk na wprowadzenie czytelnika w aspekty technologiczne, których znajomość może okazać się pomocna w dostosowaniu nowych technologii do specyfiki wykonywanego zawodu prawniczego[1].

---

* Część druga artykułu zostanie opublikowana w numerze 11(127) Rejenta.

[1] O zasadach etyki prawniczej w konfrontacji z Internetem zob. M. L u d w i k, *Dziesięć przykazań radcy prawnego w Internecie*, Radca Prawny 2001, nr 1, s. 65 i nast.

I. Podpis elektroniczny czy cyfrowy?

W związku z globalizacją światowego handlu oraz ciągłym rozwojem sieci Internet pojawił się problem ustanowienia ram dla potwierdzenia autentyczności informacji przekazywanych z wykorzystaniem technik komputerowych. Dla skutecznego rozwiązania tego zagadnienia należy wykorzystać wiedzę z zakresu co najmniej dwóch dyscyplin: prawa oraz bezpieczeństwa systemów informatycznych (lub szerzej – informacji). Narzędziem, które może posłużyć do zapewnienia bezpieczeństwa i nienaruszalności przesyłanych w formie elektronicznej informacji, jest podpis cyfrowy (elektroniczny). Należy jednak zauważyć, że obok elementów natury technicznej z podpisem cyfrowym wiążą się także trudności natury prawnej – np. sposób regulacji czy choćby stosunek do podpisu tradycyjnego (własnoręcznego). Idąc za przykładem USA, Unii Europejskiej, jak i jej krajów członkowskich, należy przyjąć, że dla zapewnienia należytej rangi podpisowi cyfrowemu konieczna jest regulacja ustawowa.

Gwałtowny rozwój handlu elektronicznego na świecie spowodował konieczności stworzenia odpowiedniej infrastruktury prawnej w postaci regulacji krajowych, opierających się na wspólnotowej Dyrektywie Unii Europejskiej (opublikowanej w Dz.Urz. Wspólnot Europejskich z dnia 19 stycznia 2000 r. L. 13/12). Ma ona szczególną misję do spełnienia, stanowi bowiem model i kierunkowskaz, jakim mają się posługiwać legislatorzy tych państw, które starają się o przyjęcie do Unii Europejskiej. Dyrektywa o wspólnotowej infrastrukturze podpisów elektronicznych jest efektem długoletnich prac nad przystosowywaniem europejskiego prawa wspólnotowego do rozwoju technologii informatycznej. Zgodnie z nią, podpis elektroniczny to elektroniczne dane służące weryfikacji autentyczności innych danych elektronicznych. Jest to pojęcie ogólne, które odrywa się od technologii. Do kategorii podpisów elektronicznych należą tzw. **podpisy cyfrowe**. Jest to technologia, która odgrywa obecnie największą rolę pośród podpisów elektronicznych. Zastępowanie bowiem dokumentów papierowych dokumentami elektronicznymi wymaga, ze względu na szczególny charakter tych ostatnich, przyjęcia i standaryzacji nowych technik uwierzytelniania dokumentów i potwierdzania ich integralności. Jedną z tych technik, powszechnie stosowaną, jest właśnie podpis cyfrowy w jego różnych odmianach i związane z nim usługi kryptologiczne. Można przyjąć zało-

żenie, że zastosowanie podpisu elektronicznego bez technologii asymetrycznej będzie praktycznie niemożliwe, dlatego też nie można rozdzielić pojęcia podpisu elektronicznego od terminu podpisu cyfrowego; są one „skazane" na siebie w sensie technologicznym i merytorycznym.

W doktrynie i legislaturze używa się często zamiennie obu tych terminów. Pojęcie „podpis cyfrowy" z uwagi na to, iż jest bez wątpienia szersze, uwzględniające nie tylko elektroniczny charakter danych czy sposób jego wykorzystania – elektroniczne przesyłanie informacji, ale także takie procesy, jak szyfrowanie czy deszyfrowanie informacji przy użyciu technik kryptograficznych, matematycznych itp.

W funkcjonujących już lub projektowanych w innych państwach aktach prawnych możemy zauważyć różne stosowanie tych pojęć, np. pierwszy tego typu akt na świecie, ustawa stanu Utah w USA, nazywa się ustawą o podpisie cyfrowym; Parlament Unii Europejskiej uchwalił Dyrektywę o wspólnotowej infrastrukturze podpisów elektronicznych, z kolei ustawodawca niemiecki odpowiedni akt z 1997 r. nazwał ustawą o podpisie cyfrowym. Nie oznacza to jednak, że istnieje w tym zakresie pewien uporządkowany i ujednolicony katalog pojęć i terminów, dotyczący tzw. gospodarki elektronicznej.

II. Funkcje podpisu elektronicznego

W raporcie American Bar Association *Digital Signature Guidelines Tutorial* wymienia się następujące generalne funkcje podpisu tradycyjnego, zamieszczonego na dokumencie:

• poświadcza autentyczność podpisanego dokumentu – poprzez identyfikowanie podpisującego z podpisywanym dokumentem;

• podkreśla prawne znaczenie oświadczenia, jakie składa podpisujący – ze względu na pewną „ceremonialność" tej czynności;

• jest traktowany jako wyraz oświadczenia woli złożonego przez podpisującego – jednakże w określonych przez obowiązujące prawo przypadkach;

• może być uznany za zakończenia rokowań i dojście przez podpisujących do porozumienia – takie założenie podlega każdorazowo badaniu przez sąd.

Podpis elektroniczny w systemach prawnych państw, w których wprowadzono odpowiednie regulacje prawne, pełni określone funkcje; zwykle

wymienia się trzy główne z nich, a mianowicie;

1) finalizacyjną – spełnia się ona w ostatecznej konkretyzacji oświadczenia woli lub wiedzy następującej przez złożenie podpisu;

2) ostrzegawczą – względem podpisującego, że przez dokonanie tej czynności wiąże się on z treścią oświadczenia zawartą w dokumencie;

3) dowodową – w postępowaniu sądowym dokument zapatrzony w podpis ma określoną moc dowodową, co w istocie podnosi jego rolę jako oświadczenia woli, a także stanowić może dowód w sprawie[2].

Funkcje podpisu elektronicznego wskazują na wielostronność w zastosowaniu e-podpisów w obrocie prawnym i gospodarczym; zwracają bowiem uwagę na szerokie i nowe możliwości uczestnikom transakcji handlowych. Nie można jednak powiedzieć, że transakcje zawierane za pośrednictwem nowoczesnych środków przekazu, jakim jest np. Internet, zmieniły się co do swej istoty, tak się oczywiście nie stało, lecz zmianie uległa jedynie technika ich zawierania. Z tego powodu regulacje prawne muszą uwzględniać ten stan, a co za tym, idzie stawać się bardziej odporne na szybką dezaktualizację, która cechuje obecnie zaawansowane technologie. Dlatego też nie chodzi o wymyślenie zupełnie nowej konstrukcji, takiej jak podpis cyfrowy, ale raczej o stworzenie norm prawnych o takiej budowie, która umożliwiałaby wykorzystanie nowych technologii do osiągnięcia celów istniejących już instytucji. W tym przypadku chodziłoby o spełnienie przez podpis cyfrowy wszystkich zadań, jakie stoją przed podpisem tradycyjnym plus zwiększenie bezpieczeństwa podmiotów posługujących się nim dzięki jego unikalnym, technicznym możliwościom.

Aby osiągnąć podstawowe funkcje tradycyjnej sygnatury, podpis elektroniczny powinien posiadać następujące atrybuty:

– indywidualizacja podpisującego, tzn. podpis cyfrowy powinien wskazywać konkretnie na osobę, która go używa;

– potwierdzenie autentyczności dokumentu, dzięki zastosowaniu podpisu cyfrowego odbiorca dokumentu powinien mieć możliwość sprawdzenia za jego pomocą, czy treść dokumentu nie uległa zmianie (zniekształceniu) w czasie przesyłu, tj. czy nie nastąpiła ingerencja osób trzecich.

---

[2] Zob. m.in. A. A m b r o z i e w i c z, *Podpis elektroniczny – pojęcie i funkcje w obrocie*, Przegląd Sądowy 2001, nr 1, s. 95 i nast.

Obecne możliwości technologiczne pozwalają na takie skonstruowanie podpisu cyfrowego, aby przewyższał on poziom bezpieczeństwa, który gwarantowała sygnatura tradycyjna; te atrybuty to:

• system certyfikacji – umożliwia potwierdzenie autentyczności podpisu przez niezależny organ, przewidziany w ustawie;

• trudność sfałszowania – dzięki użyciu najnowszych systemów kryptograficznych.

III. Sposób działania podpisu cyfrowego

1. Definicja podpisu cyfrowego

Specyfika i możliwości, jakie stwarza sieć Internet, zdeterminowały konstrukcję podpisu cyfrowego jako techniki służącej autentyfikacji osób komunikujących się za jego pomocą. Podpis taki występuje zawsze w parze z dokumentem elektronicznym, który jest formą przesyłania zdigitalizowanych informacji.

Podpis cyfrowy jest unikatową wartością przypisaną do dokumentu, która umożliwia stwierdzenie, że dokument został wysłany przez określoną osobę i nie został później zmodyfikowany. Podpis taki występuje w postaci sekwencji bitów dołączonej do podpisywanego dokumentu. Sekwencja ta jest zintegrowana z tekstem podpisywanej wiadomości, tworząc w ten sposób nową jakość – przetworzoną unikatową wiadomość, której nowa forma jest równocześnie jej cechą indywidualizującą i zabezpieczającą.

Aby zrozumieć sposób działania podpisu, należy zapoznać się z podstawowymi pojęciami z zakresu technologii informatycznej i kryptografii, gdyż implikuje to zrozumienie aspektów bezpieczeństwa stosowania podpisów cyfrowych.

2. Podstawowe pojęcia

Komputer – jego działanie polega na wykonywaniu operacji według ściśle określonych procedur. Jednostką sterującą pracą komputera jest **procesor**. W tym celu wykonuje on działania oparte na określonych algorytmach i języku wewnętrznym – kodzie maszynowym. Działania te są zaprogramowane przez człowieka i do ich przeprowadzania wykorzystywane są informacje **(dane)** wprowadzane do pamięci komputera przez operatora.

Pamięć – w uproszczeniu to zespół elektronicznych komórek wypełnionych danymi i wskazaniami dla komputera. Każda z komórek ma własne oznaczenie (adres), gdzie zapamiętana jest podstawowa jednostka informacji, jaką jest bajt.

Bajt – to najkrótszy adresowalny ciąg bitów traktowanych przez komputer jako niepodzielna całość w procesie przetwarzania, przechowywania i przesyłania informacji, składający się z ośmiu mniejszych jednostek – bitów.

Bit (ang. *binary digit* – cyfra dwójkowa) – to jednostka ilości informacji mogąca przybierać jedną z dwóch wartości: 0 lub 1.

Tak więc każda informacja, jaką zapisujemy w pamięci komputera za pomocą tekstu, grafiki, ruchomego obrazu czy też dźwięku, zostaje zapisana w systemie binarnym i mówimy, że ma postać zdigitalizowaną, czyli cyfrową.

Kryptologia – dziedzina badań obejmująca zagadnienia bezpiecznej komunikacji. W jej skład wchodzi kryptografia i kryptoanaliza.

Kryptografia – dziedzina wiedzy zajmująca się zagadnieniami utajniania informacji poprzez jej szyfrowanie, oznacza także zbiór technik służących takiemu utajnianiu.

Kryptoanaliza – dziedzina zajmująca się łamaniem szyfrów, tzn. odczytywaniem wiadomości utajnionej przez szyfrowanie bez znajomości tzw. klucza bądź kluczy, czyli informacji pozwalających na jej bezpośrednie odtajnienie.

3. Ogólne zasady i techniki szyfrowania

Aby utajnić treść informacji zawartych w oryginalnym dokumencie, zwanym **tekstem jawnym,** tworzy się jego zaszyfrowaną wersję, zwaną **kryptogramem**. Szyfrowanie i deszyfrowanie odbywa się za pomocą specjalnie wygenerowanego klucza. Zaszyfrowanie umożliwia zabezpieczenie transmisji pocztowej przed podejrzeniem przez kogokolwiek poza adresatem. Dokument po zaszyfrowaniu zmienia się z czytelnego tekstu w serię liczb, które może odszyfrować tylko ten, kto ma odpowiedni do tego klucz.

Proces szyfrowania oparto o dwa elementy:

1) **algorytm** – to przekształcenie matematyczne, przy pomocy którego tekst jest zamieniany w kryptogram;

2) **klucz kryptograficzny** – który wprowadzono w drugiej połowie XX wieku, jest to pewna liczba używana z algorytmem i powodująca odmienną

jego pracę, co jest dodatkowym utrudnieniem dla dokonania kryptoanalizy.

Na poziomie przekształceń kryptograficznych wyróżnia się obecnie dwie klasy szyfrów. Do pierwszej z nich należą ***szyfry blokowe***. Ich działanie polega na tym, że szyfrują one równocześnie w całości bloki informacji (porcje danych) o określonej długości (blok podstawowy). Wiadomości dłuższe od długości bloku podstawowego są wstępnie dzielone na bloki odpowiedniej długości. Jeśli ostatni fragment wiadomości lub cała wiadomość jest krótsza od bloku podstawowego, następuje jej dopełnienie do długości będącej wielokrotnością długości podstawowego bloku w taki sposób, by można było po jej odbiorze jednoznacznie odróżnić wiadomość od jej dopełnienia. Drugą klasę reprezentują **szyfry strumieniowe**, które szyfrują, każdy kolejny, pojawiający się na wejściu do urządzenia szyfrującego, znak wiadomości poprzez połączenie go w pewien nieodwracalny sposób z wygenerowanym wewnątrz urządzenia każdym kolejnym znakiem klucza. Dzięki temu strumień znaków wiadomości zostaje zaszyfrowany przy pomocy strumienia znaków klucza. Po stronie odbiorczej wiadomość jest odszyfrowywana przy pomocy wygenerowanego strumienia znaków klucza, który jest zsynchronizowany z tym po stronie nadawczej. Dla bezpieczeństwa szyfru strumieniowego istotne jest, by znaki wchodzące w skład klucza były nieprzewidywalne i niepowtarzalne, tzn. aby jego okres był dostatecznie długi.

Zazwyczaj sama formuła przekształcenia matematycznego służącego do szyfrowania i deszyfrowania jest powszechnie znana[3]. W takiej sytuacji bezpieczeństwo szyfrowania zapewnia dodatkowy parametr, zwany kluczem, który w przeciwieństwie do algorytmu jest znany tylko osobom upoważnionym. Zasadniczo wyróżniamy obecnie dwie techniki szyfrowania: tradycyjną tzw. kryptografię symetryczną i kryptografię asymetryczną. Rozróżnienie to jest wynikiem stosowanego algorytmu – odpowiednio symetrycznego lub asymetrycznego.

Kryptografia symetryczna (szyfrowanie z kluczem tajnym)

Metoda ta opiera się na współdzieleniu tajemnicy, którą jest klucz deszyfrujący, przez obie strony biorące udział w szyfrowanej transmisji.

[3] Do wyjątków zaliczyć można dwa algorytmy symetryczne RC2 i RC4 autorstwa Rona Rivesta. Są to algorytmy o zmiennej długości klucza szyfrowania, szczegóły ich konstrukcji nigdy nie zostały oficjalnie opublikowane.

Rodzi to potrzebę ustalenia wspólnego sekretu w postaci hasła bądź klucza szyfrującego i jego wymiany. W tym celu nieodzowne jest dojście do fizycznego spotkania się przez zainteresowane strony bądź też ustanowienie bezpiecznego sposobu wymiany informacji o tym wspólnym sekrecie.

Przykładem szyfrowania symetrycznego może być szyfrowanie dokumentu za pomocą przesunięcia liter – nieskomplikowany system szyfrujący z pojedynczym kluczem mógłby powodować przesunięcie każdej litery w wiadomości o trzy litery do przodu w alfabecie, przy czym znak spacji następowałby zaraz po literze Z. Inaczej mówiąc, słowo PIES zostanie przekształcone na SLHV. Po otrzymaniu wiadomości adresat odszyfruje ją, przesuwając wszystkie litery o trzy do tyłu w alfabecie. Inaczej mówiąc, przekonwertuje słowo SLHV z powrotem na PIES.

Zalety powyższej metody to szybkość działania, wydajność, odporność na łamanie. Podstawową wadą jest natomiast wymóg, aby obie strony znały klucz przed każdą transmisją, ponadto obie strony muszą mieć do siebie zaufanie, że żadna z nich nie przekaże klucza w niepowołane ręce. Co więcej, ponieważ nikt poza adresatem nie powinien mieć możliwości odszyfrowania transmisji, trzeba tworzyć różne klucze dla wszystkich osób, grup lub firm, do których są przesyłane informacje. Niewygoda związana z koniecznością przechowywania dużej liczby tajnych kluczy jest oczywista.

Kryptografia asymetryczna (szyfrowanie z kluczem publicznym)

Punktem przełomowym było opublikowanie przez Whitfielda Diffiego i Martina Hellmana w 1976 r. artykułu pod tytułem „Nowe kierunki w kryptografii", gdzie po raz pierwszy opisano mechanizm pozwalający dwóm stronom ustanawiać bezpieczną komunikację, bez potrzeby utrzymywania oddzielnego kanału wymiany informacji tajnej w postaci klucza deszyfrującego, co eliminuje możliwość jego przechwycenia drogą podsłuchu kanału komunikacyjnego. Mechanizm ten nazwano **PKC** – *Public Key Cryptography* i jest on uznawany za najbardziej rewolucyjny w całej historii kryptografii.

Diffie i Hellman po raz pierwszy wprowadzili podstawową koncepcję nowoczesnego szyfrowania z arytmetyką modularną. Sam algorytm Diffiego-Helmana nie może być bezpośrednio wykorzystany do szyfrowania danych. Pozwala on, aby nadawca i adresat informacji mogli wyznaczyć jeden, tajny klucz szyfrowania bez konieczności wcześniejszej wymiany

jakichkolwiek poufnych informacji. Twórcy algorytmu podali, że używając bardzo dużej liczby pierwszej do szyfrowania informacji, można z tej liczby wyprowadzić drugą, bardzo dużą liczbę pierwszą. Za pomocą tej drugiej liczby pierwszej, mimo że różnej od oryginalnej, szyfrującej liczby pierwszej, można odszyfrować informację. System szyfrowania z kluczem publicznym wymaga dwóch wzajemnie uzupełniających się kluczy. Proces nie jest symetryczny, gdyż klucz stosowany do szyfrowania wiadomości nie pozwala na jej odszyfrowanie. Każda wiadomość zaszyfrowana kluczem publicznym może zostać odszyfrowana tylko za pomocą powiązanego z nim klucza prywatnego, jednocześnie znajomość jednego z kluczy nie pozwala na odtworzenie drugiego, mimo iż klucze uzupełniają się, tworząc parę. Nazwa „klucz publiczny" wzięła się stąd, iż podawany jest on do publicznej wiadomości (publikowany w gazecie, na stronie www, lub w innym ogólnodostępnym miejscu), dzięki czemu może zostać pobrany przez nadawcę i służy mu do zaszyfrowania przekazu. Klucz prywatny, służący do odszyfrowania przekazu, pozostaje w rękach adresata i powinien być przechowywany w bezpiecznym miejscu, niedostępnym dla nikogo poza adresatem. Pozostaje tylko jeden problem – uwierzytelnienia nadawcy komunikatu, wszak metoda ta nie daje żadnej pewności, że osoba, która korzysta z klucza publicznego adresata, jest tą, za którą się podaje.

Jedną z pierwszych implementacji tej techniki był system oparty na algorytmie **RSA**, opracowanym w 1978 r. w Massachusetts Institute of Technology, a nazwanym tak od nazwisk jego twórców: Rivesta, Shamira i Adelmana. Bazuje on na istnieniu funkcji matematycznych, które łatwo jest przeprowadzić w jedną stronę, lecz niezwykle trudno jest odwrócić. Funkcja taka jest zwana także **funkcją-zapadnią działającą w jedną stronę,** ponieważ, jak łatwo zauważyć, można ją obliczyć szybko w jedną stronę, ale nie w drugą. Funkcja jest zwana zapadnią, gdyż można łatwo obliczyć funkcje odwrotne, jeśli tylko zna się pewną tajną informację (klucz). Przykładowo – łatwo jest pomnożyć przez siebie dwie duże liczby pierwsze, nie jest jednak tak prosto rozłożyć dużą liczbę na czynniki, których się nie zna. Korzystając właśnie z tej prawidłowości, możliwe jest stworzenie dwóch matematycznie powiązanych ze sobą kluczy, z których każdy umożliwia odwrócenie operacji dokonywanych za pomocą drugiego, przy czym znajomość tylko jednego z kluczy nie pozwala na odtworzenie drugiego

i nieautoryzowane posługiwanie się nim. Algorytm ***RSA*** umożliwia zarówno szyfrowanie informacji, jak i tworzenie podpisów cyfrowych.

Protokół klucza publicznego skutecznie eliminuje potrzebę zabezpieczania kanałów, czego wymagały standardowe systemy z pojedynczym kluczem. Stosowanie tego systemu ma jeszcze jeden podstawowy aspekt, mianowicie odpowiedzialność za bezpieczeństwo tajnego klucza (prywatnego) spoczywa tylko na jednej ze stron – adresacie, który jest jednocześnie właścicielem kluczy, odpada więc konieczność zabezpieczania wielu kluczy tajnych, po jednym dla każdego korespondenta.

Technologia **PKC** szczególną rolę odegrać powinna w handlu elektronicznym, ponieważ daje możliwość ustanowienia prawnie uznawanej praktyki podpisywania kontraktów i innych porozumień w formie elektronicznych dokumentów. Wydaje się, że technologia podpisów cyfrowych bardziej niż jakakolwiek dziedzina techniki przyczynia się do urealnienia wizji bezpiecznego, globalnego biznesu elektronicznego.

4. Tworzenie podpisu cyfrowego

Generowanie podpisu cyfrowego polega na wykorzystaniu wyżej opisanych własności protokołu szyfrowania z kluczem publicznym, ale odwraca kolejność czynności dokonywanych w ramach tego protokołu. Aby podpisać dokument, należy w odwrotnej kolejności użyć kluczy kryptograficznych:

1. Dokument wysyłany do odbiorcy nadawca podpisuje przy pomocy **swojego klucza tajnego.**
2. Następnie szyfruje go **kluczem jawnym odbiorcy.**
3. Odbiorca otrzymany przekaz odszyfrowuje **swoim kluczem tajnym.**
4. Podpis sprawdza **kluczem jawnym nadawcy.**

Wyróżnić możemy trzy rodzaje czynności związanych z podpisami:

1. Czynności wstępne – wyznaczenie niezbędnych parametrów, za pomocą których generowany będzie podpis.
2. Generowanie podpisu – podpisujący „dokonuje" obliczeń, w wyniku których powstaje ciąg bitów będący podpisem konkretnego dokumentu[4].

[4] Do generowania podpisów cyfrowych i posługiwania się nimi służy oprogramowanie kryptograficzne. Istnieje wiele różnych aplikacji i systemów kryptograficznych pozwalających na zarządzanie kluczami i szyfrowaną korespondencją. Wszystkie obliczenia matematyczne są realizowane automatycznie przez aplikacje, zaś ich wyniki są komunikowane użytkownikowi.

3. Weryfikacja podpisu – czynności dokonywane przez osobę, która pragnie przekonać się o autentyczności podpisu i jego autorze, jak i podpisywanym dokumencie. Weryfikacja ma postać testu, który powinny przechodzić jedynie poprawnie utworzone podpisy.

Jeśli weryfikacja jest pozytywna, to znaczy odszyfrowany dokument ma sens, oznacza to, że nikt pod nadawcę się nie podszył, ponieważ tylko rzeczywisty nadawca jest w posiadaniu swojego klucza tajnego, którego użyto to podpisania wiadomości.

5. Algorytm szyfrujący

Oprócz algorytmu RSA, o którym była już mowa, naukowcy zaproponowali wiele algorytmów asymetrycznych. Wszystkie one bazują na technikach, które wywodzą się z różnych obserwacji matematycznych. Jednym z ważniejszych takich algorytmów jest algorytm El Gamala. Dr El Gamal zauważył, że przykład przedstawiony przez Diffiego i Hellmana zawierał elementy pełnego systemu z kluczem publicznym. Dodał on do oryginalnego pomysłu wymiany klucza Diffiego-Hellmana funkcję podpisu cyfrowego. W 1994 roku National Institute of Standards and Technology (NIST) zaadaptował standard DSS (*Digital Signature Standard*), oparty na wariancie podpisu cyfrowego El Gamala. Jest to o tyle istotna informacja, iż DSS jest amerykańskim standardem podpisów cyfrowych.

My skupimy się na krótkim omówieniu algorytmu RSA, jako najbardziej obecnie popularnego. Podczas szyfrowania wiadomości komputer wykonuje z pomocą klucza publicznego szereg operacji matematycznych. Są to operacje arytmetyczne, polegające na podnoszeniu liczb do dużych potęg. Muszą one zostać zaimplementowane w efektywny sposób. Zespół tych operacji jest powszechnie zwany algorytmem szyfrowania. Algorytm RSA jest uważany za jeden z najlepszych algorytmów szyfrowania z kluczem publicznym. Cechą charakterystyczną RSA jest przemienność. Klucze kryptograficzne mogą ulec przestawieniu w zależności od woli właściciela. Każdy z nich może pełnić funkcje szyfrujące lub deszyfrujące. Dlatego też ma on dwa zastosowania: szyfrowanie korespondencji i jej uwierzytelnianie.

Generowanie kluczy

Aby wygenerować klucze, należy losowo wybrać dwie duże liczby pierwsze. Do odróżniania liczb pierwszych od liczb złożonych stosuje się

testy pierwszości liczb – specjalnego rodzaju testy, mówiące jedynie, że liczba jest złożona bez podawania rozkładu. W przypadku algorytmów asymetrycznych, klucze są długie i wymagają wygenerowania większej ilości losowych bitów niż te, które ostatecznie znajdą się w kluczu, dlatego też generuje się je elektronicznie przez generator ciągów losowych lub pseudolosowych.

Działanie algorytmu RSA

Klucz szyfrowania, oznaczony jako *E,* jest związany z pewną stałą *n.* Stała ta określa limit długości szyfrowanego bloku (czyli jak wiele bajtów danych może zawierać pojedynczy szyfrowany blok). Szyfrowanie jest wykonywane w trzech prostych krokach, omówionych poniżej.

1. Program wdrażający algorytm RSA przekształca wiadomość tekstową w liczbę całkowitą z przedziału między *0* a *(n-1)*. Metoda używana do konwertowania tekstu na liczbę zależy od konkretnego programu. Duże wiadomości (takie, które nic mogą być reprezentowane przez liczbę mniejszą od *n-1)* są dzielone przez program na kilka bloków, z których każdy jest określony przez osobną liczbę całkowitą, mniejszą od *n-1*.

2. Program szyfruje wiadomość podnosząc każdą liczbę całkowitą do potęgi E-tej (czyli blok E). Następnie program wykonuje działanie modulo (szczególny rodzaj działania, które podaje tylko resztę z operacji dzielenia) na powstałej wartości, dzieląc ją przez M i zapisując resztę jako szyfrowaną wiadomość. Wiadomość ma teraz postać zaszyfrowanego dokumentu tekstowego C.

3. Aby odszyfrować wiadomość C, jej odbiorca podnosi ją do potęgi *D,* a następnie wynik dzieli przez modulo *n.* Powstaje seria wartości, reprezentująca bloki w odszyfrowanym pliku, które program konwertuje z powrotem na tekst za pomocą tej samej metody, co użyta poprzednio do konwersji tekstu.

Powyżej przedstawiono podstawowe kroki, które wykonuje algorytm RSA. Jednak należy zdawać sobie sprawę, że algorytm ten jest bardziej złożony.

6. Metody generowania krótkich podpisów

Wadą opisanej wyżej metody jest to, że podpis jest bardzo długi, co najmniej tak długi, jak podpisywany dokument. Ma to znaczenie o tyle, że podstawową wadą algorytmów asymetrycznych jest powolność działania. Algorytm RSA wymaga wielu operacji arytmetycznych, więc jego pręd-

kość szyfrowania bądź deszyfrowania jest dużo niższa niż algorytmów symetrycznych (od 100 do 1000 razy). Na szybkość pracy algorytmu ma przede wszystkim wpływ wielkość szyfrowanego dokumentu. Problem długich podpisów można rozwiązać przez zastosowanie jednokierunkowej funkcji hashującej, dzięki czemu unika się szyfrowania całości uwierzytelnianego dokumentu. W efekcie zamiast dokument podpisywać będziemy wartość hashującą na tym dokumencie. W ten sposób otrzymuje się tzw. krótki podpis cyfrowy, który dołączany jest do oryginalnego dokumentu przesyłanego w postaci jawnej lub zaszyfrowanej algorytmem symetrycznym przy użyciu tzw. klucza sesyjnego, co umożliwia zrealizowanie funkcji poufności. Dodatkowym skutkiem tego zabiegu jest to, że można prezentować podpis, nie zdradzając treści dokumentu.

Podpis cyfrowy z jednokierunkową funkcją skrótu

Narzędziem, które służy do tworzenia krótkich podpisów, jest algorytm matematyczny o odpowiednich właściwościach. Nazywany jest on funkcją skrótu, gdyż w wyniku jego działania otrzymujemy skrót wiadomości lub – mówiąc inaczej – ekstrakt dokumentu. Ekstrakt ten podobny jest do sumy kontrolnej, mianowicie umożliwia powiązanie wiadomości o dowolnej długości z charakterystyczną dla tej wiadomości liczbą z ustalonego zakresu, to znaczy o ustalonej długości reprezentacji liczby w przyjętym systemie zapisu – dziesiętnym lub binarnym. Dane z pliku poddanego działaniu funkcji są przetwarzane na „wartość zhashowaną" – inaczej mówiąc, obliczenie skrótu to podanie informacji w postaci argumentu funkcji skrótu. Protokół podpisywania ekstraktu wiadomości i weryfikacji podpisu przebiega następująco:

1. Dla dokumentu *X* oblicza się wartość *h(X)*, gdzie *h* oznacza ustaloną funkcję hashującą. Funkcja hashująca generuje jedną wartość na podstawie całej zawartości pliku, przy czym na podstawie wartości funkcji hashującej nie można odtworzyć zawartości pliku.

2. Wartość *h(X)* zostaje zaszyfrowana za pomocą klucza prywatnego nadawcy. Dodatkowo na koniec program podpisujący zapisuje podpisaną wersję pliku, która zawiera informacje o programie podpisującym oraz znaczniki końca i początku podpisanego pliku. Zaszyfrowana wartość *h(X)* jest następnie odszyfrowywana za pomocą klucza publicznego nadawcy.

3. Weryfikacja podpisu przebiega następująco. Adresat oblicza dla dokumentu *X*, który zostaje mu przesłany wraz z podpisem (dokument może

zostać zaszyfrowany, jeśli nadawca chce, by jego treść została poufna), wartość *h(X)'* dla tej samej funkcji hashującej. Następnie *h(X)'* jest porównywana z *h(X)*, jeżeli obie wartości są identyczne, to program informuje o autentyczności podpisu nadawcy.

Podstawy teoretyczne i działanie jednokierunkowych funkcji haszujących

Aby stosowanie funkcji skrótu nie obniżało poziomu bezpieczeństwa podpisu cyfrowego, funkcje te muszą posiadać odpowiednie właściwości. Pierwszą z nich jest cecha jednokierunkowości, która gwarantuje, że nie ma możliwości wyznaczenia treści wiadomości na podstawie jej skrótu, gdyż zadanie to należy do kategorii problemów trudnych obliczeniowo. Mówimy, że *h* jest jednokierunkową funkcją hashującą, gdy spełnione są następujące warunki:

– dla każdego *x* łatwo jest obliczyć *h(x)*;

– *h(x)* ma ustaloną długość dla wszystkich tekstów *x* (w ten sposób długość *h(x)* nie zdradza żadnych informacji o tekście *x*);

– dla zadanego *y* znalezienie *x* takiego, że *h(x) = y*, jest praktycznie niemożliwe (dotyczyć to ma w szczególności metody systematycznego przeszukiwania wszystkich możliwych tekstów).

Jeżeli funkcja spełnia te warunki, to dla losowo wybranej wartości o odpowiednio dużej długości odwrócenie funkcji jest niewykonalne, bo żaden efektywny algorytm nie jest w stanie dostarczyć prawidłowego rozwiązania. Przykładowo, gdy wartości funkcji składają się z 128 bitów, to istnieje 2 do 128-mej potęgi możliwych wartości. Liczba ta jest ogromna (dla porównania według niektórych teorii całkowity okres trwania wszechświata bywa szacowany na 2 do 61-ej potęgi sekund), co czyni próby złamania ekstraktu za pomocą metody systematycznego przeszukania praktycznie beznadziejnymi. Aby mówić o jednokierunkowości funkcji, funkcje muszą spełniać warunek **bezkonfliktowości**[5]. Drugą ważną cechą funkcji jest hashowanie. W wyniku zastosowania funkcji hashującej otrzymujemy skrót będący przetworzeniem tekstu oryginalnego w ciąg bitów, który nie ujawnia treści dokumentu. Hashowanie zapewnia, że skrót wiadomości jest unikalny i nie jest możliwe stworzenie dwóch różnych wiadomości dających takie same skróty. Dzięki temu możliwe jest zapewnienie kontroli

[5] M. K u t y ł o w s k i, W.B. S t r o t h m a n n, *Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych*, Warszawa 1999, s. 83.

integralności dokumentu przez możliwość stwierdzenia, czy dokument został w świadomy lub przypadkowy sposób zmodyfikowany. Jeżeli w dokumencie dokonana zostanie jakakolwiek zmiana, choćby o jeden bit, to wartość skrótu zmieni się, co zostanie odkryte w procesie weryfikacji podpisu. Uniemożliwia to podstawienie innego dokumentu w miejsce oryginalnego lub dokonywanie zmian w podpisanym już dokumencie, a więc wyklucza możliwość przerobienia wytworzonego już dokumentu w celu posługiwania się nim jako dowodem zajścia faktów, które nigdy nie miały miejsca.

Szyfrowanie z kluczem sesyjnym

Ostatnim elementem, jaki został do omówienia przy okazji posługiwania się krótkimi podpisami, jest szyfrowanie za pomocą klucza sesyjnego. Stosujemy je, gdy chcemy, aby treść podpisanego dokumentu pozostała poufna. Nie stosuje się do tego szyfrowania asymetrycznego, gdyż właśnie potrzeba uniknięcia szyfrowania długich tekstów była jedną z przyczyn stosowania krótkiego podpisu. Technika klucza publicznego służy nam natomiast do zaszyfrowania i przesłania np. 128-bitowego klucza sesyjnego, który jest jednorazowy dla każdej sesji. Klucz sesyjny służy do zapewnienia bezpieczeństwa transmisji za pomocą szyfrowania symetrycznego. Dzięki temu zasadnicza część przekazu jest szyfrowana przez szybszą metodę symetryczną, natomiast zastosowanie szyfrowania asymetrycznego ogranicza się do małej, lecz najistotniejszej części transmisji, tj. przekazania klucza szyfru symetrycznego.