Włodzimierz Gogłoza

Kryptograficzne metody ochrony prywatności- przewodnik dla laików

I. Wprowadzenie

Klasyczna ekonomia upatrywała źródła bogactwa narodów w trzech czynnikach - zasobach naturalnych, pracy i kapitale. Obecnie na pierwsze miejsce tej listy wysuwa się informacja[1]. Dzięki globalnej sieci teleinformatycznej dane zapisane w postaci zerojedynkowej obiegają cały świat w ciągu kilku sekund, przekraczając granice państwowe, prawne i celne, bez przeszkód i przy braku jakiejkolwiek kontroli. *Nowa gospodarka* różni się od swego pierwowzoru nie tylko znacznie większą swobodą i szybkością transakcji, ale także naturą przedmiotu podlegającego obrotowi.

W przeciwieństwie do przedmiotów materialnych, informacja nie podlega dwóm podstawowym zasadom newtonowskiej fizyki - zasadzie zachowania materii i wynikającej z niej zasadzie wykluczania[2]. O ile korzystanie przez jedną osobę np. z książki uniemożliwia wykorzystanie jej w tym samym momencie do innych celów przez inną osobę, o tyle zawarta w niej informacja może być powielana dowolną ilość razy bez utraty jej jakości i jednocześnie wykorzystywana przez nieograniczoną liczbę osób. Właściwość ta w połączeniu z nieustającym rozwojem transparentnych sieci komputerowych rodzi dwa rodzaje problemów prawnych - konieczność zweryfikowania pojęcia tzw. własności intelektualnej lub zmiany metod jej ochrony[3] oraz kwestię zapewniania poufności, integralności i autentyczności danych przekazywanych drogą elektroniczną, bez których wykorzystanie nowoczesnych technik komunikacji w obrocie prawnym staje się niemożliwe.

Wymiana informacji za pośrednictwem sieci teleinformatycznych związana jest z szeregiem zagrożeń bądź to o charakterze losowym (np. zmianą treści wiadomości wynikłą na skutek błędów w transmisji), bądź też celowej ingerencji intruza mogącej przyjmować postać podsłuchu pasywnego, naruszającego poufność wiadomości (przeglądanie, przenikanie i wnioskowanie z danych) lub podsłuchu aktywnego, wymierzonego w jej autentyczność i integralność (zaprzeczenie nadania, zniekształcanie, przetwarzanie, wstawianie i niszczenie danych)[4]. Dla uchronienia się przed niekorzystnymi konsekwencjami wspomnianych wyżej działań stosuje się szereg zabezpieczeń, których podstawą są techniki kryptograficzne[5].

---

[1] F. Machlup, *Knowledge: It's Creation, Distribution and Economic Significance*, Princeton NJ 1980, *passim*.
[2] J. J. Szymona, *Wolność i własność w Internecie*, [w:] *Internet, problemy prawne*, red. R. Skubisz, Lublin 1999.
[3] A. Thierer, C. W. Crews Jr., *Copy Fights. The Future of Intellectual Property in the Information Age*, Washington DC 2002, *passim*.
[4] D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, *passim*, oraz J. McNamara, *Arkana szpiegostwa komputerowego*, Gliwice 2003, *passim*.
[5] B. Schneier, *Kryptografia dla praktyków. Protokoły, algorytmy i programy źródłowe w języku C*, wyd. II zmienione i rozszerzone, Warszawa 2002, *passim*.

II. Podstawy kryptografii

Szyfrowanie, czyli takie przekształcanie tekstu jawnego (P), by dla osoby trzeciej, innej niż nadawca i odbiorca, stanowił on jedynie przypadkowy ciąg znaków (C), na podstawie którego nie jest możliwe odtworzenie żadnej użytecznej informacji, wykorzystywane jest dla ochrony poufności komunikacji od przeszło trzech tysięcy lat[6]. Początkowo było ono oparte na systemie tzw. kryptografii symetrycznej, w której jeden, tajny dla osób postronnych klucz (k) służył zarówno do szyfrowania (E), jak i odszyfrowywania (D) treści wiadomości[7]. Jej przykładem jest prosty szyfr podstawieniowy przypisywany Juliuszowi Cezarowi, opierający się na przesunięciu alfabetu tekstu tajnego wobec alfabetu tekstu jawnego o trzy litery, w skutek czego zamiast litery „A" dla ochrony treści wiadomości pisano „D", zamiast „B"-„E", „C"-„F" itd. Dzięki zastosowaniu tego prostego systemu, tylko osoby znające tajny klucz wiedziały, iż pozornie chaotyczny ciąg „QLH XIDM EUXWXVRZL" w rzeczywistości oznacza „nie ufaj Brutusowi"[8].

Nowoczesne odpowiedniki klasycznych szyfrów symetrycznych realizowane są za pomocą odpowiednich programów komputerowych przetwarzających zapisane w postaci zerojedynkowej dane wejściowe, tj. tekst jawny i klucz kryptograficzny. Wiadomość reprezentowana jest w postaci tzw. kodu ASCII, w którym każdy znak klawiatury ma przypisany określony ciąg bitów, np. A to 01000001, B – 01000010, C – 01000011 itd. Kluczem jest sekwencja bitów, zaś samo szyfrowanie, to w zależności od tego czy mamy do czynienia z szyframi strumieniowymi lub blokowymi - dodawanie bitów parami (pierwszy bit tekstu jawnego dodawany jest do pierwszego bitu klucza, drugi bit tekstu jawnego do drugiego bitu klucza, itd.), bądź też niezależne przekształcenia bloków danych w bloki szyfrogramu i ich wiązanie (wyniki szyfrowania poprzednich bloków są danymi wyjściowymi operacji szyfrowania następnego bloku)[9].

Niewątpliwą zaletą szyfrów symetrycznych jest łatwość ich implementacji, oraz w wielu przypadkach bardzo wysoka odporność na kryptoanalizę (tj. siłowe łamanie)[10], ich mankamentem jest jednakże konieczność utrzymania klucza szyfrującego w tajemnicy przed osobami trzecimi. By dwie osoby mogły się ze sobą poufnie komunikować muszą najpierw uzgodnić i wymienić między sobą tajny klucz kryptograficzny, w sposób uniemożliwiający jego przechwycenie przez osoby trzecie (tzw. intruzów). Tymczasem, już z samej potrzeby stosowania kryptografii dla ochrony treści informacji przekazywanych między dwiema osobami wynika, iż nie dysponują one poufnym kanałem łączności, za pośrednictwem którego mogłyby one takiej wymiany dokonać (gdyby takowym kanałem dysponowały szyfrowanie wiadomości byłoby zbędne). W epokach poprzedzających powstanie globalnej sieci telekomunikacyjnej, gdy

---

[6] Zob. zwłaszcza *D. Kahn, Łamacze kodów. Historia kryptologii,* Warszawa 2004*, passim*. Wśród opracowań popularno-naukowych na zainteresowanie zasługują R. Kippenhahn, *Tajemne przekazy. Szyfry, Enigma i karty chipowe*, Warszawa 2000 oraz S. Singh, *Księga szyfrów. Od Starożytnego Egiptu do kryptografii kwantowej*, Warszawa 2001.

[7] Szyfrowanie - $E_K(P) = C$; deszyfrowanie - $D_K(C) = P$.

[8] R. Kippenhahn, *op. cit.*, s. 74-75.

[9] D. E. Denning, *op. cit.*, s. 326-330. Dla przykładu, prosty szyfr strumieniowy:

tekst jawny	C	A	B
tekst jawny w ASCII	01000011	01000001	01000010
klucz szyfrujący	11010001	01111001	00101011
tekst zaszyfrowany	10010010	00111000	01101001

[10] Najbezpieczniejszy znany obecnie system kryptograficzny, szyfr z kluczem jednorazowym (*one time pad*), jest właśnie szyfrem symetrycznym. B. Schneier, *op. cit.,* s. 44-47.

większość kontaktów miała charakter bezpośredni, problem ten nie był jeszcze tak silnie odczuwalny - dwie osoby mogły spotkać się w jakimś ustronnym miejscu i upewniwszy się, iż nie są podsłuchiwane uzgodnić, że od tej pory wszystkie wymieniane między sobą informacje będą szyfrować np. systemem J. Cezara. Obecnie, gdy wiele osób, z którymi utrzymujemy kontakty znamy wyłącznie z „sieci", wymóg zachowania klucza w tajemnicy istotnie ogranicza możliwość stosowania kryptografii symetrycznej. Transparentność komunikacji sieciowej wyklucza bowiem Internet jako poufny kanał wymiany informacji.

Problem ten został rozwiązany przez dwóch amerykańskich matematyków W. Diffie'go i M. Hellmana, którzy w 1976 r. opracowali system szyfrowania, którego bezpieczeństwo nie zależy od utrzymania klucza szyfrującego w tajemnicy[11]. Stworzona przez nich kryptografia asymetryczna, zwana też kryptografią w systemie klucza publicznego opiera się na rozdzieleniu zadań kryptograficznych między dwa komplementarne klucze. Jeden z nich służy wyłącznie do szyfrowania danych, drugi do ich odszyfrowywania. Klucze te wzajemnie się uzupełniają, jednak łączący je związek matematyczny został dobrany tak, by na podstawie znajomości klucza szyfrującego nie było możliwe obliczenie wartości klucza deszyfrującego. W tym celu Diffie i Hellman wykorzystali jednokierunkowość pewnych działań matematycznych[12]. Dla przykładu, mnożenie liczb pierwszych[13] jest stosunkowo łatwe, bez problemów obliczymy, iż iloczyn liczb 273 i 329 to 89817. Jednak działanie odwrotne, tzw. faktoryzacja, tj. ustalenie jakie dwie liczby pierwsze pomnożone przez siebie dają wynik 89817, jest dużo trudniejsze, zaś stopień trudności takiego zadania wzrasta wraz z wielkością liczby podlegającej rozkładowi. Szacuje się, że przy wykorzystaniu najszybszych znanych nam algorytmów faktoryzujących[14], faktoryzacja liczby pierwszej składającej się z 300 cyfr zajęłaby 3×10^{11} mips-lat [15].

Właśnie to założenie, iż nikt nie będzie w stanie odnaleźć w rozsądnym czasie dwóch liczb pierwszych ukrytych w innej wielkiej liczbie pierwszej, zwane obliczeniowym bezpieczeństwem, leży u podstaw systemu kryptografii asymetrycznej[16]. W uproszczeniu wygląda on następująco: Alicja[17] wybiera

[11] W. Diffie, M. Hellman, *New Directions in Cryptography,* "IEEE Transactions on Information Theory", IT-22(6) November 1976, s. 644-655. Należy zaznaczyć, iż w literaturze przedmiotu zgłaszany jest też pogląd, iż twórcami tej metody byli pracownicy brytyjskiej agencji wywiadu elektronicznego *Communications Electronics Security Group*. Dowodem potwierdzającym ich pierwszeństwo są trzy artykuły zamieszczone na początku lat 1970. w wewnętrznym biuletynie agencji - J. H. Ellis, *The Posibility of Secure Non-Secret Digital Encryption*, „CESG Report", January 1970; C. Cocks, *A Note on Non-Secret Encryption*, „CESG Report" November 1973 oraz M. J. Williamson, *Non-Secret Encryption Using a Finite Field*, „CESG Report" January 1974. Ponieważ prace te zostały odtajnione dopiero w kilkanaście lat po publicznym ogłoszeniu odkrycia Diffiego i Hellmana, to właśnie ich a nie brytyjskich kryptografów uznaje się za twórców kryptografii asymetrycznej. S. Levy, *Rewolucja w kryptografii*, Warszawa 2002, s. 314-331.

[12] Za jednokierunkowe uznaje się takie działania, w których znając x możemy łatwo obliczyć $f(x)$, ale działanie odwrotne, tj. obliczenie z danej wartości $f(x)$ wartości x, jest niezwykle trudne (w wielu przypadkach praktycznie niewykonalne). N. Ferguson, B. Schneier, *Kryptografia w praktyce*, Gliwice 2004, s. 147-159.

[13] Liczbami pierwszymi nazywamy liczby, które mają wyłącznie dwa dzielniki: 1 i samą siebie. Liczba a jest dzielnikiem liczby b, kiedy b dzieli się przez a bez reszty. Liczbami pierwszymi są np. 2, 3, 5, 7, 11 itd. Zgodnie z twierdzeniem Euklidesa istnieje nieskończenie wiele takich liczb.

[14] Tj. wielokrotnego wielomianowego sita kwadratowego i ogólnego sita ciała liczbowego. B. Schneier, *op. cit.,* s. 332.

[15] Moc obliczeniową komputerów mierzy się w tzw. mips-latach, 1 mips-rok to 1 rok nieustannej pracy komputera z prędkością miliona operacji na sekundę. *Ibid*., s. 216 – 227.

[16] Z tym jednakże zastrzeżeniem, iż w praktyce wykorzystywane jest nie mnożenie i dzielenie liczb pierwszych lecz potęgowanie w arytmetyce modularnej (potęgowanie modulo jest łatwe, logarytmowanie dyskretne trudne). Zob. N. Ferguson, B. Schneier, *op. cit.*, s. 150-159.

[17] Znaczny stopień skomplikowania protokołów kryptograficznych powoduje, iż ich prezentacji dokonuje się zazwyczaj poprzez odwołanie do działań tzw. postaci kanonicznych. W polskiej literaturze przedmiotu są nimi Alicja i Bartek, (ew.

dwie losowe, duże i różniące się od siebie liczby pierwsze (*p* i *q*), a następnie oblicza ich iloczyn, *p* x *q* = *N*. Wynik tego działania (liczba *N*) będzie stanowił klucz publiczny Alicji (K1). Osoby, którym zostanie on udostępniony, będą nim mogły szyfrować dane (np. listy) przeznaczone dla Alicji[18]. Sposób, w jaki przekaże ona swój klucz publiczny osobom trzecim nie ma znaczenia. Ponieważ klucz ten służy do szyfrowania, jego ew. przechwycenie przez intruza nie stanowi zagrożenia dla bezpieczeństwa komunikacji. Liczby *p* i *q* Alicja zachowuje do swojej wyłącznej wiadomości, będą one stanowiły jej klucz prywatny (K2)[19]. Za pomocą tego klucza, Alicja będzie mogła odszyfrować wszystkie wiadomości zakodowane (zarówno przez nią samą, jak i przez osoby trzecie) jej kluczem publicznym[20].

Jeśli jakiś znajomy Alicji, np. Bartek, będzie chciał wysłać jej zaszyfrowaną wiadomość, treść swojego listu wraz z otrzymanym od niej kluczem publicznym wstawi do specjalnego wzoru matematycznego (tzw. algorytmu szyfrowania) będącego funkcją jednokierunkową[21]. Wynikiem przeprowadzonego działania (stanowiącego łatwiejszą cześć funkcji jednokierunkowej) jest szyfrogram. Od tego momentu zawartość wiadomości jest skutecznie chroniona przed osobami trzecimi, albowiem by zapoznać się z jawną treścią szyfrogramu, intruz musiałby wykonać trudniejszą część funkcji jednokierunkowej, to zaś mogłoby mu zająć nawet kilkaset tysięcy lat. Alicja może szybko odszyfrować wiadomość przesłaną jej przez Bartka, gdyż jako jedyna osoba na świecie dysponuje dodatkową informacją, w postaci liczb *p* i *q*, za pomocą których może ona odwrócić jednokierunkową funkcję matematyczną, tak by ponownie stała się ona łatwym zadaniem[22].

W celu wykluczenia możliwości ustalenia przez intruza wartości *p* i *q* w oparciu o znajomość *N*, klucz publiczny musi być bardzo dużą liczbą pierwszą nie poddającą się łatwej faktoryzacji. Początkowo zalecana długość tego klucza wynosiła minimum 232 cyfry (768 bitów), dziś zaleca się, aby wynosiła ona co najmniej 617 cyfr (2048 bitów)[23]. Teoretycznie istnieje możliwość sfaktoryzowania nawet tak dużego klucza publicznego drogą tzw. ataku wyczerpującego (*brute force*) tj. sprawdzenia jego wszystkich możliwych kombinacji, jednak jak głosi słynne w kręgach kryptografów powiedzenie, osoba która usiłowałaby to zrobić przy obecnej mocy obliczeniowej komputerów, winna najpierw zaopatrzyć się w odpowiedni zapas świec,

---

Bolek) w publikacjach anglojęzycznych Alice i Bob. Imiona te nie opisują poszczególnych stron, a jedynie ich role w protokole. N. Ferguson, B. Schnieier, *op. cit.*, s. 185.

[18] Szyfrowanie - $E_{K1}(P) = C$.

[19] W celu zapewnienie wyłącznego dostępu do klucza prywatnego, w praktyce jest on dodatkowo chroniony specjalnym hasłem, numerem PIN, bądź też jedną z technik identyfikacji biometrycznej.

[20] Deszyfrowanie - $D_{K2}(C) = P$.

[21] Najpowszechniej używanym jest algorytm Rivesta, Shamira i Adlemana, znany szerzej jako *RSA*. Zob. N. Ferguson, B. Schneier, *op. cit.*, s. 171-184, oraz RSA Laboratories, *Frequent Asked Questions About Today's Cryptography*, version 4.1, 2000, Bedford: RSA Security Inc., s. 73-86. W praktyce wszystkie opisywane tu czynności wykonuje się przy pomocy specjalnych aplikacji komputerowych, np. darmowego programu *Pretty Good Privacy (PGP).* Listę najpopularniejszych programów kryptograficznych wraz z adresami serwerów, z których można je pobrać, można znaleźć m.in. na stronie http://www.pgpi.org.

[22] Jeśli Alicja chce w sposób równie bezpieczny odpowiedzieć Bartkowi, szyfruje swoją wiadomości jego kluczem publicznym. Wówczas tylko Bartek będzie mógł zapoznać się z treścią odpowiedzi, albowiem tylko on dysponuje odpowiednim kluczem prywatnym. Wszystkie pozostałe osoby (włącznie z Alicją) w celu odszyfrowania informacji musiałyby rozwiązać niezwykle trudne (w praktyce niewykonalne) zadanie matematyczne.

[23] B. Schneier, *op. cit,* s. 220. Zob. też R. Silverman *A Cost Based Security Analysis of Symmetric and Asymetric Key Lenghts*, "RSA Laboratories Bulletin" 13 (2000), oraz *Id*., *Has the RSA Algorithm Been Compromised as a Result of Bernstein's Paper?*, "RSA Laboratories Technical Notes and Reports", 4 (2002).

gdyż nim uda jej się osiągnąć swój cel zgaśnie Słońce[24].

Niestety, obok swych niewątpliwych zalet kryptografia asymetryczna ma też wady. Zastosowanie obliczeniowo bezpiecznych algorytmów szyfrowania w istotny sposób zwiększa poufność danych przekazywanych drogą elektroniczną, jednak bezpieczeństwo to ma swoją cenę – stosowane w nich działania matematyczne są tysiąckrotnie wolniejsze od tych wykonywanych przy konwencjonalnych algorytmach szyfrowania[25]. Dlatego też, w praktyce są one wykorzystywane jedynie do bezpiecznej wymiany klucza szyfrującego, samo zaś szyfrowanie wiadomości jest realizowane, jednym z algorytmów symetrycznych[26].

III. Ochrona anonimowości użytkowników sieci teleinformatycznych

Szyfrowanie danych przekazywanych drogą elektroniczną w istotny sposób zwiększa prywatność komunikacji internetowej, jednak nie gwarantuje ono użytkownikom sieci pełnego bezpieczeństwa. Analogicznie, jak w przypadku komunikacji telefonicznej, wiele informacji na temat kontaktujących się za pośrednictwem Internetu osób można pozyskać w oparciu o dane o ruchu[27]. Analiza nagłówka listu elektronicznego, wskaże intruzowi m. in. adres IP nadawcy, datę nadania wiadomości, jej numer identyfikacyjny, rodzaj programu użytego do jej nadania, ścieżkę przekazywania danych i szereg innych podobnych informacji. Zestawienie wielu takich nagłówków pozwala intruzowi na ustalenie, z kim i jak często kontaktuje się dana osoba, na jakie (jeśli w ogóle) listy dyskusyjne jest ona zapisana, jakie wątki dyskusji internetowych ją absorbują, a więc pośrednio - czym się interesuje, jakich informacji poszukuje w Internecie, jakie ma poglądy itp.. Podobne informacje użytkownicy Internetu ujawniają przy korzystaniu z innej popularnej usługi sieciowej, serwisów WWW. W ramach tzw. odwołań (*calling card*) udostępniają oni

[24] Istnieje wprawdzie wielomianowy algorytm faktoryzacji liczb (zwany od nazwiska jego twórcy algorytmem Shora), za pomocą którego można bardzo szybko odszyfrować wszelkie dane utajniane przy pomocy algorytmów, których bezpieczeństwo tkwi w problemie faktoryzacji, jednak jego praktyczne zastosowanie wymaga użycia komputerów kwantowych, które jak dotąd pozostają na etapie projektów. P. W. Shor, *Polynomial-Time Algoriths for Prime Factorization and Discrete Logarithms on a Quantum Computer*, referat wygłoszony na *35th Annual Symposium on Foundations of Computer Science*, Santa Fe, 22-09-1994, dostępny pod adresem http://www.arxiv.org/abs/quant-ph/9508027. Powstanie komputerów kwantowych zniweczy obliczeniowe bezpieczeństwo kryptografii asymetrycznej, nie jest ono jednak równoznaczne z końcem kryptografii jako takiej, albowiem teoria kwantów stanowi nie tylko fundament dla komputerów, które mogłyby złamać wszystkie współczesne szyfry, ale również podstawę nowego absolutnie bezpiecznego systemu kryptograficznego, tzw. kryptografii kwantowej. Bezpieczeństwo tego systemu opiera się na tym, iż na poziomie kwantowym, każda próba obserwacji układu wpływa na jego zmianę, co w przypadku kryptografii kwantowej oznacza, iż nie jest możliwe przeprowadzenie podsłuchu pasywnego (nie naruszającego treści komunikatu), albowiem zgodnie z zasadami mechaniki kwantowej, intruz próbując dokonać odczytu wiadomości zaburzyłby jej przekaz. Zob. S. Singh, *op. cit.*, s. 339-372. Po ujawnieniu istnienia systemu *Echelon*, Unia Europejska wystosowała 11 mln Euro na badania nad projektem SECOQC (*Secure Communication Based on Quantum Cryptography*), tj. praktycznymi zastosowaniami kryptografii kwantowej. Zob. *European Parliament's Report on the Existence of a Global System for the Interception of Private and Commercial Communications – Echelon Interception System*, 2001/2098 INI, 11 July 2001.

[25] D. E. Denning, *op. cit.*, s. 344.

[26] Alicja generuje jednorazowy klucz sesji (K) i posługuje się nim do zaszyfrowania treści wiadomości. Następnie za pomocą klucza publicznego Bartka (K1) Alicja szyfruje klucz sesji (K) i wysyła go wraz z zaszyfrowaną wiadomością Bartkowi. Po otrzymaniu wiadomości Bartek używa własnego klucza prywatnego (K2) do odszyfrowania klucza sesji (K), po czym za pomocą klucza K deszyfruje otrzymaną wiadomość.

[27] B. Schneier, *Ochrona poczty elektronicznej. Jak chronić prywatność korespondencji w sieci Internet?*, Warszawa 1996, s. 26-28.

osobom monitorującym ruch sieciowy dane na temat adresu IP ich komputera, rodzaju przeglądarki internetowej i jej rozszerzeń, adresów ostatnio odwiedzanych stron, dokładnych danych dostawcy usług sieciowych (siedziba, adresy kontaktowe, nazwiska administratorów, itp.), rozdzielczości monitora, a w niektórych przypadkach także zawartości pamięci podręcznej komputera. By ustrzec się przed niekorzystnymi konsekwencjami ujawnienia tych informacji, należy poszerzyć wachlarz opisywanych tu technik kryptograficznych, o protokoły anonimizacji, a w szczególności o skorygowanie ścieżki przekazywania danych przy użyciu tzw. anonimowych serwerów proxy i wykorzystanie serwerów przeadresowania poczty zwanych remailerami[28].

Anonimowy serwer proxy pełnieni rolę pośrednika pomiędzy klientem (osobą wywołującą usługę sieciową) i serwerem (podmiotem realizującym usługę sieciową), który zapewnia anonimowość poszczególnych zapytań i odpowiedzi, poprzez modyfikację odwołań. Odpowiednie skonfigurowanie opcji internetowych sprawi, iż każde wysłane przez klienta żądanie nawiązania połączenia zanim trafi do docelowej maszyny (serwera), zostanie przechwycone przez wskazany przez niego anonimowy serwer proxy, który podmieni jego dane identyfikacyjne (adres IP, nazwę domenową, *etc*.) i prześle je dalej jako własne. Dla zwiększenia bezpieczeństwa, a zwłaszcza utrudnienia inwigilacji w oparciu o dane o ruchu, całość komunikacji zachodzącej na linii klient-proxy winna być dodatkowo zaszyfrowana z użyciem silnej kryptografii. Zastosowanie opisywanego tu systemu anonimizacji sprawi, iż jedynymi osobami, które mają bezpośredni dostęp do informacji na temat nawyków sieciowych użytkownika Internetu, będzie on sam i operatorzy wybranego przez niego anonimowego serwera proxy[29]. Jeśli użytkownikom sieci Internet zależy na dalszym zawężeniu liczby podmiotów mających dostęp do tych danych, mogą skorzystać ze zdecentralizowanych metod anonimizacji, których skuteczność nie zależy od uczciwości administratorów serwerów proxy. Najszerzej obecnie stosowanym systemem tego rodzaju jest tzw. trasowanie cebulowe[30]. Działanie systemu Tor (będącego kaskadą zaufanych serwerów proxy z warstwowym szyfrowaniem) polega na tym, iż wysłany przez klienta zaszyfrowany pakiet danych zanim trafi do docelowej maszyny (np. serwera WWW) zostanie przesłany przez 3 losowo wybrane serwery pośredniczące, z których każdy zna tylko swojego poprzednika i następcę, nie dysponuje natomiast informacjami na temat początku i końca trasy[31].

Osoby wysyłające listy elektroniczne w celu uniemożliwienia ustalenie ich tożsamości mogą z kolei skorzystać z systemu anonimowych serwerów przeadresowania poczty. Wyróżniamy dwa ich podstawowe rodzaje, tzw. remailery I stopnia (określane często pseudo-anonimowymi) i remailery II stopnia, zwane

[28] Zgodnie z Rekomendacją 3/97 KE o anonimowości w Internecie, pozostawienie jednostce decyzji w sprawie zachowania anonimowości przy korzystaniu z sieci komputerowych ma zasadnicze znaczenie dla zapewnienia jej prywatności w systemie *on-line*. W dokumencie tym wskazano, iż należy osobom zainteresowanym umożliwić zachowanie anonimowości przy przesyłaniu poczty elektronicznej, pasywnym przeglądaniu zawartości sieci, oraz nabywaniu większości towarów i usług w Internecie. European Commission, Directorate General XV, Working Party of the Protection of Individuals with regard to the Processing of Personal Data, *Recommendation 3/97: Anonimity on the Internet*, Brussels 3 XII 1997, DG Markt D/5060/97.

[29] Pozostałe osoby mogą uzyskać takie informacje dokonując analizy czasowej ruchu sieciowego, tego rodzaju działanie jest jednak pracochłonne i kosztowne albowiem wymaga stałego monitorowania ruchu wchodzącego i wychodzącego z serwera proxy.

[30] Ogólne informacje na temat systemu *Tor*, wraz z oprogramowaniem niezbędnym do skorzystania z niego można znaleźć na stronie internetowej https://www.torproject.org/

[31] Zob. R. Dingledine, N. Mathewson, P. Syverson, *Tor: The Second-Generation Onion Router*, [w:] *Proceedings of the 13th USENIX Security Symposium*, San Diego CA 2004 s. 303-320.

mixmasterami[32]. Oba rodzaje remailerów usuwają z nagłówków listów elektronicznych dane identyfikujące ich nadawców, jednakże różnią się sposobem obsługi i stopniem bezpieczeństwa jakie oferują.

Działanie anonimowych remailerów I stopnia jest podobne do działania wyżej omówionych anonimowych serwerów proxy i polega na podmianie nagłówka każdego przesyłanego przez nie listu. Dla przykładu przyjmijmy, iż Alicja chce wysłać anonimowo list elektroniczny Bartkowi (tj. nie chce, by Bartek poznał jej tożsamość na podstawie informacji zawartych w nagłówku wysyłanego przez nią e-maila). W tym celu szyfruje wiadomość kluczem publicznym Bartka i wysyła ją wraz z instrukcją przeadresowania na adres wybranego przez nią remailera, np. anon@nemo.com (adres fikcyjny). Remailer wykonuje jej instrukcje, usuwając z nagłówka listu Alicji wszystkie identyfikujące ją dane i przesyła go Bartkowi jako własny. W ten sposób do Bartka dociera list Alicji, pozbawiony jednak identyfikującego ją nagłówka RFC[33].

Ta metoda anonimizacji jest jednak dalece niedoskonała, albowiem istnieje możliwość ustalania tożsamości korzystających z niej osób w oparciu o analizę bądź to *logów* systemowych remailera, przechowujących zapis każdej operacji przeadresowywania wykonywanej przez remailer[34], bądź też o analizę zachodzącego na nim ruchu sieciowego (porównywanie wiadomości przychodzących do- i wychodzących z serwera)[35]. Stąd też przy wysyłaniu szczególnie sensytywnych danych, Alicja celem uzyskania większego bezpieczeństwa winna skorzystać z systemu mixmasterów - anonimowych remailerów II stopnia wyposażonych w dwa dodatkowe mechanizmy anonimizacji – system opóźnień gwarantujący, iż listy przesyłane przez użytkowników na adres remailera nie będą wysyłane w kolejności ich nadejścia oraz system zmiany formatu wiadomości, sprawiający iż przeadresowywane przez remailer listy są trudne do odróżnienia.

Mixmastery korzystają z potrójnego szyfrowania algorytmem symetrycznym (dla ochrony treści wiadomości) oraz ze specjalnie zmodyfikowanego algorytmu kryptografii asymetrycznej RSA, dzięki któremu wszystkie wychodzące z remailera wiadomości mają taki sam format i tę samą wielkość (np. 35,1 kilobajtów). Dodatkowo w celu dalszego utrudnienia śledzenia ruchu przechodzącego przez remailer ich użytkownicy, za pomocą specjalnych komend (Latent-Time: + XX:XX, gdzie XX:XX to czas opóźnienia) mają możliwość wstrzymania na określony czas operacji przeadresowania listów i tym samym ukrywania ich w grupie innych przesyłanych przez remailer wiadomości. Protokół anonimizacji wygląda w tym przypadku

[32] Powoli wdrażany jest też eksperymentalny system remailerów III stopnia zwanych *mixminion*. Więcej na ten temat na stronie http://mixminion.net.

[33] Oznacza to także, iż Bartek nie będzie mógł w sposób bezpośredni odpowiedzieć Alicji, gdyż nie zna jej adresu e-mail. (Skorzystanie z opcji „Replay to" w programie pocztowym spowoduje, iż jego wiadomość zostanie wysłana nie na adres Alicji, lecz na adres remailera). Nie oznacza to jednak, iż Alicja i Bartek nie mogą się komunikować w sposób anonimowy. Zamiast przesyłać informacje na adres Bartka, Alicja może wysłać ją za pośrednictwem anonimowego remailera na adres jednej z wielu, specjalnie w tym celu stworzonych grup dyskusyjnych, zwanych „zbiornikami wiadomości" (*message pools*), np. *alt.anonymous.messages*. Jeśli zależy jej na tym by treść listu poznał wyłącznie Bartek winna ją dodatkowo zaszyfrować jego kluczem publicznym (dzięki temu zabiegowi nawet jeśli wiadomość zobaczy dziesiątki tysięcy osób - dostęp do archiwum tego typu list jest wolny od wszelkich ograniczeń - tylko Bartek będzie mógł odczytać jej jawny tekst). Jeśli z kolei Bartek zechce odpisać na list Alicji wystarczy, że za pośrednictwem anonimowego remailera wyśle zaszyfrowaną jej kluczem publicznym odpowiedź na adres tej samej grupy dyskusyjnej.

[34] W ten sposób została np. zidentyfikowana osoba, która za pośrednictwem nieistniejącego już remailera *anon.penet.fi* przesłała na grupę Usenet *alt.religion.scientology*, szereg tajnych dokumentów Kościoła Scjentologicznego. Zob. A. M. Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, „Journal of Law and Commerce" 15 (1996), s. 395-515.

[35] Usunięcie nagłówka zawierającego dane identyfikacyjne nadawcy nie wpływa na format i właściwą treść wysłanej przez niego wiadomości.

następująco:

1) Alicja przygotowuje wiadomość dla Bartka stosując się do instrukcji otrzymanej od administratora wybranego przez siebie remailera (np. mixmaster.it) -

```
::
Anon-To: testriot@o2.pl
Latent-Time: +02:00

##
Subject: test remailera

Nie ufaj Brutusowi
```

Gdzie

`::` to początek pola komend remailera,
`Anon-To:` to adres, na który ma zostać przesłana wiadomość – w analizowanym przykładzie testriot@o2.pl

`Latent-Time:` to czas opóźnienia (w analizowanym przykładzie 2 h od otrzymania listu)
to początek pola anonimizowanej wiadomości
`Subject:` to tytuł listu wyświetlany u docelowego odbiorcy
W analizowanym przykładzie treść wiadomości przeznaczonej dla docelowego odbiorcy to „Nie ufaj Brutusowi". W celu uniemożliwienia jej odczytania przez operatorów remailera należy ją zaszyfrować kluczem publicznym adresata (Bartka).

2) Alicja szyfruje powyższą wiadomość (zarówno pole komend, jak i samą treść wiadomości) kluczem publicznym mixmastera.
3) Alicja wysyła zaszyfrowaną wiadomość na adres remailera mix@mixmaster.it
4) Operator remailera odszyfrowuje własnym kluczem prywatnym otrzymaną wiadomość, w celu odczytania pól `Anon-to:` i `Latent-Time:`
5) Remailer usuwa z nagłówka listu Alicji jej dane identyfikujące a następnie wykonując przekazane przez nią instrukcje wysyła jej wiadomość w grupie innych nadesłanych na jego adres wiadomości.
6) Wiadomość Alicji dociera do Bartka.

Przedstawiony wyżej protokół anonimizacji poczty elektronicznej znacznie utrudnia monitorowanie ruchu sieciowego, a tym samym i ustalanie tożsamości korespondujących ze sobą osób[36], nadal istnieje jednak możliwość identyfikacji nadawcy wiadomości w oparciu o analizę *logów* systemowych remailera[37].

[36] Jak obrazowo stwierdza T. C. May, działanie anonimowych remailerów II stopnia można porównać do sposobu, w jaki w popularnych filmach sensacyjnych protagoniści gubią śledzące ich osoby. Bohater zorientowawszy się, iż podąża za nim jakaś osoba wchodzi wraz z grupą innych przechodniów do wielkiego kompleksu handlowego, w przebieralni jednego ze znajdujących się w nim butików przebiera się w najmodniejszy rodzaj ubioru (np. żółty płaszcz przeciwdeszczowy – właśnie zaczął padać deszcz) a następnie, gdy po kilku chwilach zgromadzi się grupa podobnie do niego ubranych osób, wychodzi wraz z nimi ze sklepu innymi drzwiami. T. C. May, *True Nyms and Crypto Anarchy,* [w:] J. Frenkel (red.) *True Names, and the Opening of the Cyberspace Frontier*, New York NY 2001, s. 39.

[37] O ile takowe w ogóle są przez ich administratorów przechowywane, wielu administratorów regularnie je kasuje celem

By zapobiec ujawnieniu jej tożsamości, Alicja może przesłać swą wiadomość za pośrednictwem całego szeregu anonimowych remailerów[38]. Wówczas jedynie operator pierwszego remailera będzie w stanie ustalić tożsamość Alicji, on jednak nie będzie znał docelowego adresata (w polu `Anon-To:` zamiast adresu Bartka znajdzie adres kolejnego remailera). Z kolei operator ostatniego remailera będzie znał adres docelowego odbiorcy, nie będzie jednak w stanie ustalić adresu Alicji (w nagłówku otrzymanej wiadomości w miejscu jej danych będą widnieć dane wcześniejszego remailera). Bartek zaś będzie mógł ustalić wyłącznie adres ostatniego serwera przeadresowywania[39].

Alicja przesyłając przez łańcuch anonimowych remailerów wiadomość zaszyfrowaną kluczem publicznym docelowego odbiorcy zyskuje niemal stuprocentową pewność, iż 1) żaden z operatorów remailerów nie odczyta jawnej treści jej szyfrogramu, 2) ani adresat wiadomości, ani operatorzy remailerów (inni niż operator pierwszego serwera przeadresowania) nie będą w stanie ustalić jej tożsamości jeśli nie podejmą współpracy z wszystkimi pozostałymi operatorami remailerów, 3) a tym samym, iż jest praktycznie niemożliwym, by końcowy odbiorca wiadomości mógł poznać jej dane osobowe inaczej niż poprzez skłonienie (np. w drodze nakazu sądowego) wszystkich administratorów remailerów do ujawnienia *logów* operowanych przez nich serwerów przeadresowywania[40]. Z uwagi na fakt, iż większość operatorów remailerów kasuje je regularnie, zadanie to może być niewykonalne[41].

---

uniemożliwienia identyfikacji, a tym samym ochrony prywatności ich użytkowników.

[38] Dla przykładu, *W* to jawna treść listu, [W, K] – wiadomość zaszyfrowana kluczem *K*, *Ko* – klucz publiczny docelowego odbiorcy, *Eo* – adres e-mail docelowego odbiorcy. Korzystam z łańcucha 3 anonimowych remailerów, o kluczach publicznych K1, K2, K3 i adresach e-mail E1, E2, E3:

1) Do pierwszego remailera wysyłam wiadomość [([([([W,Ko]+Eo),K3] +E3),K2] +E2),K1];
2) I remailer korzystając z własnego klucza prywatnego odszyfrowuje „wierzchnią" warstwę szyfrowania otrzymując wynik [([([W,Ko]+Eo),K3] +E3),K2] +E2. Odczytuje adres E2 i przesyła wiadomość do wskazanego remailera;
3) II remailer otrzymuje wiadomość [([([W,Ko]+Eo),K3] +E3),K2], korzystając z własnego klucza prywatnego odszyfrowuje „wierzchnią" warstwę szyfrowania otrzymując wynik [([W,Ko]+Eo),K3] +E3. Odczytuje adres E3 i przesyła wiadomość do wskazanego remailera;
4) III remailer otrzymuje wiadomość [([W,Ko]+Eo),K3], korzystając z własnego klucza prywatnego odszyfrowuje „wierzchnią" warstwę szyfrowania otrzymując wynik [W,Ko]+Eo, odczytuje Eo i przesyła wiadomość pod adres docelowego odbiorcy;
5) Docelowy odbiorca otrzymuje wiadomość [W,Ko], korzystając z własnego klucza prywatnego odszyfrowuje ostatnią warstwę szyfrowania i uzyskuje dostęp do jawnej treści wiadomości - W.

[39] Gdyby Bartek i wszyscy operatorzy remailerów, przez które Alicja przesłała swój list podjęli współpracę, mogliby wspólnymi siłami ustalić całą ścieżkę przeadresowywania i w ten sposób zdemaskować ją jako nadawcę. Wystarczy jednak, by choć jeden z nich odmówi pomocy, a łańcuch umożliwiający wyśledzenie Alicji zostanie zerwany. By zatem Alicja zyskała niemalże stuprocentową gwarancję anonimowości wystarczy, by na ścieżce przeadresowywania znalazł się remailer operowany przez nią samą (jego uruchomienie nie jest ani szczególnie trudne, ani kosztowne gdyż niezbędne oprogramowanie wraz z odpowiednimi instrukcjami jest dostępne w Internecie za darmo, zob. np. http://mixmaster.sourceforge.net).

[40] Jedyną znaną obecnie i co istotne nie zawsze skuteczną metodą ustalania tożsamości autorów listów elektronicznych wysyłanych za pośrednictwem łańcucha anonimowych remailerów II stopnia, jest analiza językowa treści wiadomości. Przy wykorzystaniu m.in. tej metody został zidentyfikowany słynny *Unabomber*, eko-terrorysta który w ciągu 18 lat swojej przestępczej działalności, rozsyłając anonimowo (tradycyjną pocztą) listy z bombami zabił 3 osoby i zranił 29 innych. W oparciu o analizę ogłoszonego przez niego manifestu lingwiści współpracujący z FBI ustalili m.in., iż jego autorem jest osoba, która studiowała, bądź też wykładała matematykę w drugiej połowie lat 1960. na University of California w Berkeley, będąca introwertykiem i prowadząca proste życie w odosobnieniu. Wszystkie te domniemania potwierdziło przeprowadzone w tej sprawie śledztwo.

[41] Nawet gdyby wszyscy operatorzy remailerów stale przechowywali informacje na temat przeadresowywanych listów ich pozyskanie i analiza mogłoby okazać się zbyt kosztowne, albowiem remailery działają na terenie kilkunastu krajów.

IV. Ochrona integralności i autentyczności danych

Omawiane wyżej systemy anonimizacji, zostały stworzone celem zapewnienia użytkownikom Internetu pełnej kontroli nad zakresem ujawnianych przez nich danych osobowych. W konsekwencji, o tożsamości osób korzystających z serwerów przeadresowania poczty wiemy jedynie tyle, ile one same zdecydują nam się wyjawić. Kierując się własnym uznaniem mogą one nie podawać żadnych danych identyfikacyjnych, bądź też np. w celu odróżnienia się od innych korespondujących z nami osób, korzystać z jakiegoś pseudonimu. Jeśli jednak nie istnieje możliwość ustalania tożsamości nadawców anonimowych listów elektronicznych, jak stwierdzić, iż „Alicja", która właśnie przysłała nam jakąś wiadomość, jest tą samą „Alicją", która skontaktowała się z nami tydzień temu[42]?

Ponieważ klucze stosowane w kryptografii asymetrycznej stanowią wzajemnie uzupełniającą się parę, wiadomość zaszyfrowana dowolnym z nich może być odszyfrowana przy pomocy drugiego komplementarnego z nim klucza. Dla potwierdzenia autorstwa wysyłanej przez siebie wiadomości wystarczy zatem, by Alicja zaszyfrowała ją własnym kluczem prywatnym Eκ2(P) = C. Jeśli Bartkowi uda się otrzymaną wiadomość odszyfrować jej kluczem publicznym Dκ1 (C) = P zyska pewność, iż pochodzi ona właśnie od Alicji, albowiem tylko i wyłącznie ona dysponuje kluczem prywatnym umożliwiającym stworzenie takiego szyfrogramu. Pomyślna weryfikacja szyfrogramu potwierdza autorstwo przesyłającej go osoby, stąd też ten rodzaj kryptosystemu określany jest mianem podpisu elektronicznego[43].

Tożsamość zweryfikowana podpisem elektronicznym, jest jednak tożsamością szczególnego rodzaju. Jeśli bowiem nie otrzymaliśmy klucza publicznego służącego do jego weryfikacji bezpośrednio od osoby składającej podpis (np. w drodze fizycznego przekazania dyskietki z jego zapisem) możemy mieć jedynie pewność, iż osoba, od której otrzymaliśmy szyfrogram rzeczywiście dysponuje tajnym kluczem osoby, za którą się podaje. Nie jesteśmy jednak w stanie określić, czy jej tożsamość elektroniczna pokrywa się z jej rzeczywistą tożsamością[44]. Cecha ta sprawia, iż w połączeniu z omawianymi w poprzednim punkcie

[42] Z tego samego pseudonimu może wszak korzystać nieograniczona liczba osób.

[43] Przedstawiony powyżej teoretyczny schemat podpisu elektronicznego, ze względów praktycznych ulega w codziennych zastosowaniach pewnym modyfikacjom. Ponieważ szyfrowanie całej wiadomości jest procesem uciążliwym dla odbiorcy (rozmiar powstałego w ten sposób szyfrogramu jest co najmniej dwukrotnie większy od ukrytego w nim tekstu), zamiast kodowania całej treść wiadomości programy kryptograficzne szyfrują tylko jej skrót (*message digest*) uzyskany dzięki zastosowaniu algorytmu tzw. funkcji mieszającej (*hash function*). Zaszyfrowany przy użyciu klucza prywatnego nadawcy skrót wiadomości (*hash*) jest załączany do przesyłki wraz z kluczem publicznym umożliwiającym jego identyfikację. Po otrzymaniu tak sporządzonej wiadomości odbiorca odszyfrowuje przy pomocy klucza publicznego nadawcy jej skrót, w wyniku czego otrzymuje pewien ciąg bitów. Następnie sam skraca wiadomość przy użyciu tej samej funkcji mieszającej co nadawca i porównuje otrzymane w ten sposób ciągi (w praktyce wszystkie te czynności wykonuje za niego odpowiedni program). Jeśli są one identyczne uzyskuje gwarancję, iż do złożenia podpisu elektronicznego użyto klucza prywatnego komplementarnego z posiadanym przez niego kluczem publicznym nadawcy. B. Schneier, *Kryptografia....,* s. 67-78.

[44] Z technologicznego punktu widzenia nic nie stoi na przeszkodzie, by osoba generująca za pomocą odpowiednich programów parę kluczy kryptograficznych wskazując dane osobowe ich użytkownika podała bądź to dane fikcyjne, bądź też dane osoby trzeciej. Dlatego też w obrocie prawnym wykorzystywane są certyfikowane podpisy elektroniczne. Certyfikaty stosowane w systemie kryptografii asymetrycznej są elektronicznymi zaświadczeniami potwierdzającymi, iż dana osoba, ma przypisany klucz publiczny o określonej w certyfikacie wartości. Co do zasady podmiotem uwierzytelniającym, zwanym w literaturze przedmiotu urzędem certyfikacyjnym (*certification authority*) może być dowolna osoba, organizacja lub instytucja ciesząca się zaufaniem obu stron korespondencji, w praktyce jednak jest nim zwykle wyspecjalizowana firma świadcząca usługi certyfikacyjne bądź też odpowiedni organ państwowy. Podmiot ten

systemem anonimowych remailerów, podpis elektroniczny może służyć do potwierdzania przez jednostkę autorstwa anonimowych wiadomości (np. listów), bez konieczności ujawniania przez nią jej danych osobowych[45]. Tego rodzaju elektroniczna tożsamość, określa się w literaturze przedmiotu *prawdziwym nimem* (*true nym,* w odróżnieniu od prawdziwego nazwiska - *true name*)[46].

V. System anonimowych płatności elektronicznych

Dokonując codziennych płatności możemy skorzystać z kart płatniczych (kredytowych), czeków bądź też gotówki. Dzięki dwóm pierwszym metodom możemy bezpiecznie przeprowadzić kosztowne zakupy, bez konieczności noszenia przy sobie dużych sum, dzięki trzeciej, chronić własną prywatność. Przy płatnościach gotówkowych sprzedawca nie musi wiedzieć o swych klientach nic ponad to, że mają oni czym zapłacić za jego towary bądź usługi. By uzyskać pewność, iż klient wywiąże się z umowy, nie musi sprawdzać czy jest on tym za kogo się podaje, czy korzysta z własnych środków finansowych, czy jest wypłacalny, czy jego konto bankowe nie jest obciążone spłatą wcześniej zaciągniętych długów, *etc*., wystarczy mu widok gotówki wyłożonej na ladę. Co więcej, nie mają dostępu do danych osobowych klientów nie może wykorzystać ich wbrew ich woli. Tak więc, gotówka nie tylko umożliwia zawieranie umów przez nieznające się (nie ufające sobie) osoby, ale i zapewnia, iż pozostaną one anonimowe tak długo, jak długo sobie tego życzą.

W Internecie sprzedaż towarów i usług ma bardzo często charakter ponadnarodowy, międzykontynentalny, wymykający się jurysdykcji[47]. Brak efektywnych mechanizmów egzekucji należności sprawia, iż transakcje muszą się opierać bądź to na zaufaniu/reputacji stron, bądź też kosztownych mechanizmach audytu. Nawet gdy wymiana towarów czy usług odbywa się lokalnie, biorące w niej udział podmioty nie mogą mieć pewności co do uczciwości kontrahenta, gdyż spełniwszy własne zobowiązanie mają znikomy wpływ na zachowanie drugiej strony. Problemem stanowi również zapewnianie poufności transakcji, albowiem każda płatność elektroniczna pozostawia po sobie elektroniczny ślad (*audit trail*),

---

po okazaniu mu dokumentów stwierdzających tożsamość osoby występującej o nadanie jej certyfikatu generuje pod jej kluczem publicznym podpis elektroniczny uwierzytelniający jego użytkownika. Do weryfikacji tego podpisu służy powszechnie dostępny klucz publiczny urzędu. Jeśli zatem pojawią się wątpliwości, co do pochodzenia przesłanej nam wiadomości należy sprawdzić czy podpis elektroniczny złożony pod służącym do jej odszyfrowania kluczem zgadza się z podpisem uwierzytelniającego go urzędu certyfikacyjnego. Pomyślna weryfikacja (przy spełnieniu dodatkowego założenia, iż nadawca wiadomości należycie chroni swój klucz prywatny i że nie dostał się on w ręce niepowołanej osoby) potwierdza tożsamość autora otrzymanej drogą elektroniczną przesyłki. Szerzej na temat skutków prawnych stosowania podpisu elektronicznego zob. W. Gogłoza, R. Kosieradzki, *Forma i skutki prawne podpisu elektronicznego*, „Studia Iuridica Lublinensia" 4 (2004), s. 78-89, oraz cytowana tam literatura.

[45] Dla przykładu, Alicja może występować w sieci nie pod własnym imieniem i nazwiskiem, lecz jako „siostra Brutusa". Jeśli wszystkie sygnowane tym pseudonimem wiadomości wysyła za pomocą anonimowych remailerów, nie istnieje możliwość połączenia jej tożsamości elektronicznej z tożsamością prawdziwą, (tj. nikt nie jest w stanie ustalić iż „siostra Brutusa" to w rzeczywistości Alicja). Jeśli „siostrze Brutusa" zależy na tym by inne osoby nie mogły się pod nią podszywać (np. wysyłając listy w „jej imieniu"), powinna wygenerować dla siebie parę (niecertyfikowanych) kluczy kryptograficznych. Prywatny zachować wyłącznie do własnej dyspozycji, zaś publiczny udostępnić każdemu zainteresowanemu. W ten sposób podpisując elektronicznie przesyłane za pośrednictwem anonimowych remailerów wiadomości, Alicja będzie w stanie wykazać wobec osób trzecich, iż jest tą samą „siostrą Brutusa", z którą kontaktowali się wcześniej, nie wyjawiając przy tym swojej prawdziwej tożsamości.

[46] T. C. May, *op. cit.*, s. 42-44.

[47] A. Thierer, C. W. Crews Jr., *Who Rules the Net? Internet Governance and Jurisdiction*, Washington DC 2003, *passim*.

stanowiący cenną informację nie tylko dla konkurencji czy firm marketingowych, ale także dla przestępców komputerowych.

Rozwiązaniem dla tej sytuacji mógłby być właśnie elektroniczny ekwiwalent gotówki, gwarantujący z jednej strony pewność transakcji, z drugiej zaś anonimowość obu jej podmiotom[48]. Zdaniem T. Okamoto i K. Ohta idealny system płatności elektronicznych musi spełniać łącznie sześć wymogów: 1) niezależność - bezpieczeństwo pieniędzy cyfrowych nie może być uzależnione od ich rzeczywistej lokalizacji; 2) odporność na fałszerstwa – środki nie mogą być kopiowane, ani wielokrotnie wydawane przez tę samą osobę; 3) prywatność - nikt nie może ustalić powiązań pomiędzy stronami transakcji; 4) autonomia - osoby dokonujące płatności nie muszą korzystać z usług centralnego komputera; 5) mobilność – środki można swobodnie przesyłać za pośrednictwem sieci do innych użytkowników; 6) podzielność - dana kwota może być podzielona na mniejsze, a wszystkie jej części muszą się poprawnie sumować[49].

Niewątpliwie najistotniejszym z wszystkich warunków stawianych przez Okamoto i Ohtę jest odporność na fałszerstwa. „Jak wie każdy kto, kopiował program z dyskietki na dysk twardy, w technice cyfrowej sporządzenie dokładnej kopii jest zadaniem banalnie łatwym. Co miałoby powstrzymać [kogoś] przed wykonaniem miliona lub nawet miliarda kopii cyfrowego dolara, metodą kopiuj/wklej? Gdyby [każdy] był w stanie tak uczynić, [wszystkie komputery] stałby się mennicami, a nieograniczona hiperinflacja uczyniłaby wkrótce tę postać waluty całkowicie bezwartościową”[50]. Oczywistym rozwiązaniem tego problemu wydaje się być nadanie każdemu cyfrowemu dolarowi (złotówce) niepowtarzalnego numeru identyfikacyjnego i jego weryfikacja za pomocą podpisów elektronicznych, jednak byłoby to równoznaczne z możliwością śledzenia i archiwizowania każdej, nawet najdrobniejszej transakcji internetowej.

Istnieje jednak protokół umożliwiający przesyłanie wiarygodnych, a jednocześnie niemożliwych do wyśledzenia płatności (tzw. *anonymous digital cash*)[51]. Jego opracowanie stało się możliwe dzięki stworzonym przez D. Chauma tzw. ślepym podpisom cyfrowym (*blind digital signature*) umożliwiającym zaciemnianie (tj. utajnianie przed podpisującym) treści sygnowanych dokumentów[52]. Skomplikowany matematycznie proces zaciemniania najłatwiej zrozumieć, wyobrażając sobie podpisywanie przez kalkę dokumentu ukrytego w kopercie. Jeśli do koperty wraz z naszym listem włożymy także kalkę, a następnie poprosimy osobę trzecią o podpisanie się na kopercie, to jej podpis odbije się także na niewidocznym dla niej dokumencie. W cyberprzestrzeni analogiczny efekt można uzyskać za pomocą funkcji mnożącej przemiennej z funkcją podpisującą[53]:

---

[48] Zob. np. Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Working Party on Information Security and Privacy, *Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks*, DSTI/ICCP/REG(98)12/Final, s. 54.

[49] T. Okamoto, K. Ohta, *Universal Electronic Cash*, “Advances in Cryptology – Crypto’91 Proceedings” 1992, s. 324-337.

[50] S. Levy, *Rewolucja...,* s. 220.

[51] D. Chaum, *Security Without Identification, Transaction Systems to Make Big Brother Obsolete*, “Communications of the ACM” 10 (1985), s. 1030-1044.

[52] *Id*., *Blind Signatures for Untraceable Payments*, “Advances in Cryptology Proceedings of Crypto ‘82”, 1983, s. 199-203.

[53] B. Schneier, *Kryptografia...,*s. 672.

1) Alicja przygotowuje dokument i mnoży go przez liczbę losową zwaną czynnikiem zaciemniającym (*blinding factor*).
2) Alicja przekazuje zaciemniony dokument do podpisania Bartkowi.
3) Bartek podpisuje zaciemniony dokument i oddaje go Alicji.
4) Alicja dzieli otrzymany wynik przez czynnik zaciemniający, uzyskując kopię oryginalnego dokumentu podpisanego przez Bartka.

Jak nie trudno zauważyć, w przedstawionym wyżej protokole osoba podpisująca zaciemniony dokument, co do znajomości jego treści jest zdana wyłącznie na dobrą wolę autora. Ponieważ nieuczciwość tego ostatniego może prowadzić do całego szeregu wyrafinowanych oszustw, całkowicie ślepe podpisy elektroniczne w praktyce wykorzystywane są bardzo rzadko. Zamiast nich stosuje się protokół ślepych podpisów wzbogacony o technikę zwaną *podziel-i-wybierz*. W tym wariancie tego protokołu Bartek otrzymuje od Alicji wielki plik zaciemnionych dokumentów, odczytuje dowolne z nich i podpisuje ostatni. Ponieważ Alicja nie wie, które dokumenty przeczyta Bartek wysokie ryzyko wykrycia oszustwa winno skłonić ją do zachowania uczciwości[54].

W podobny sposób działa protokół płatności anonimową cyfrową gotówką:

1) Alicja przygotowuje *n* (np. 100) anonimowych przekazów pieniężnych na kwotę np. 100 USD. Każdy z nich poza wskazaniem kwoty, na którą został wystawiony zawiera inny, niepowtarzalny ciąg losowy (NCL) – musi on być dostatecznie długi, by wyeliminować możliwość jego powtórzenia.
2) Alicja zaciemnia wszystkie przekazy, używając protokołu ślepych podpisów cyfrowych i przekazuje je własnemu bankowi.
3) Bank prosi Alicję o ujawnienie wybranych przez siebie *n - 1* przekazów pieniężnych (w omawianym przykładzie 99), a następnie sprawdza kwotę indywidualnych przekazów oraz ich NCL (w celu sprawdzenia czy są one różne).
4) Jeżeli bank nie stwierdzi żadnej próby oszustwa, podpisuje jedyny pozostały przekaz i pomniejsza konto Alicji o 100 USD.
5) Alicja usuwa zaciemnienie podpisanego przekazu, w skutek czego uzyskuje podpisany przez bank dokument potwierdzający, iż w banku tym zdeponowano kwotę 100 USD.
6) Alicja płaci przekazem za zakupy w wybranym przez siebie sklepie (dla uproszczenia przyjmijmy, iż cena zakupionych towarów wynosi dokładnie 100 USD).
7) W celu sprawdzenia autentyczności przekazu pieniężnego wręczonego mu przez Alicję, sprzedawca sprawdza widniejący pod nim podpis elektroniczny banku, a następnie prosi Alicję o wygenerowanie na przekazie losowego ciągu identyfikacyjnego (LCI).
8) Alicja generuje LCI.
9) Sprzedawca przesyła przekaz do banku.
10) W celu sprawdzenia, czy przekaz ten nie został już wcześniej zrealizowany, bank weryfikuje podpis elektroniczny, a następnie sprawdza zawartość swojej bazy zrealizowanych przekazów, poszukując przekazu z identycznym NCL.

[54] *Ibid*., s. 195.

11) A) Jeżeli nie stwierdzi żadnych nieprawidłowości[55], wypłaca sprzedawcy 100 USD, a NCL zrealizowanego przekazu umieszcza w odpowiedniej bazie.

B) Jeżeli w bazie danych banku znajduje się już przekaz z identycznym NCL, to bank odmawia jego realizacji i przystępuje do procesu identyfikacji oszusta próbującego ponownie zrealizować już wykorzystany przekaz pieniężny. W tym celu porównuje LCI z przekazu pieniężnego z odpowiednim ciągiem przechowywanym w bazie. Jeśli są one identyczne oszustem jest sprzedawca, jeśli są one różne oszustem jest osoba, która przygotowała przekaz[56].

Obecnie, pomimo liczny prób wdrożenia anonimowej cyfrowej gotówki, nie funkcjonuje jeszcze w Internecie żaden powszechnie akceptowany środek płatności, który spełniałby wszystkie warunki stawiane przez Okamoto i Ohtę[57]. Należy jednak spodziewać, iż korzyści jakie ona za sobą niesie - bezpieczeństwo transakcji, anonimowość stron, poufność płatności i efektywność międzynarodowych transferów [58] - skłonią wkrótce banki do jej wprowadzenia do obrotu[59].

VI. Steganografia

Obok technik służących do utajniania treści komunikacji, istnieją też metody ukrywania samego faktu jej istnienia[60]. Steganografia sięga swoimi korzeniami czasów starożytnej Grecji. Herodot relacjonuje w *Dziejach*, iż Demaratos, Grek mieszkający w Sparcie, chcąc ostrzec swych rodaków o ataku szykowanym przez Kserksesa, „wziął podwójną tabliczkę, zeskrobał z niej wosk, a następnie na drzewie tabliczki wypisał zamiar króla; uczyniwszy to, polał znowu litery woskiem, aby niosącemu próżną tabliczkę nie przyczyniła jakiego kłopotu ze strony straży strzegącej drogi. Kiedy tabliczka istotnie dotarła do Lacedemonu, nie mogli Lacedemończycy zgadnąć, co ona oznacza, aż (jak słyszę), córka Kleomenesa, a żona Leonidasa, Gorgo, jedyna ich pouczyła. Ona to po namyśle kazała im zeskrobać wosk, mówiąc że odnajdą litery na drzewie. Usłuchali, znaleźli i odczytali, a następnie dali znać reszcie Hellenów”[61].

---

[55] Tj. nie znajdzie w bazie zrealizowanych przekazów, przekazu o identycznym NCL.

[56] B. Schneier, *Kryptografia...,,* s. 197. Istnieją także bardziej złożone protokoły anonimowych płatności, pozwalające na ustalanie nie tylko tego, która ze stron transakcji jest oszustem (jak w powyższym przypadku), ale także jej danych osobowych. *Ibid.,* s. 198-200.

[57] Poza Internetem jest ona wykorzystywana w systemach płatności obsługujących karty chipowe *Octopus* (Hong Kong) *Ezlink* (Singapur) i *Interac* (Kanada). Licencjobiorcami systemu D. Chauma są także banki DeutscheBank AG, Credit Suisse oraz Bank Austria. T. Targosz, *Pieniądz elektroniczny*, [w:] P. Podorecki (red.), *Prawo Internetu*, Warszawa 2004, s. 291.

[58] Ponieważ cyfrowa gotówka jest pewnego rodzaju informacją, może być ona przesyłana pocztą elektroniczną (w tym także przez anonimowe remailery). W najdoskonalszym z obecnie znanych systemów tego rodzaju (realizującym wszystkie wymogi stawiane przez Okamoto i Ohtę), całkowita wielkość płatności wynosi ok. 20 KB, zaś cały protokół można zrealizować w ciągu kilku sekund. B. Schneier, *Kryptografia...,* s. 203.

[59] Jak żartobliwie stwierdza K. Kelly, jedyną przewagą tradycyjnej gotówki, nad jej cyfrowym odpowiednikiem, jest to, iż przy użyciu tej ostatniej nie jest możliwe rzucanie monetą. *Id*., *Out of Control. The New Biology of Machines, Social Systems, and the Economic World*, New York NY 1995, cytat za wersją elektroniczną dostępną na stronie http://www.kk.org/outofcontorl/, brak paginacji. Zob. też, K. L. Macintosh, *The New Money*, “Berkeley Technology Law Journal” 14 (1999), s. 659 i n. oraz *Id.*, *How to Encourage Global Electronic Commerce: The Case For Private Currencies on the Internet*, „Harvard Journal of Law and Technology” 11 (1998), s. 733-796.

[60] D. E. Denning, *op. cit.*, s. 355-359.

[61] Herodot, *Dzieje*, ks. VIII, 8-9, tłum. S. Hammer, Warszawa 1959.

Współcześnie efekt ukrycia wiadomości, w innej nie wzbudzającej podejrzeń przesyłce uzyskuje się wykorzystując technologie komputerowe. Dla przykładu, popularne metody zapisu obrazów cyfrowych charakteryzują się nadmiarowością informacji wizualnej[62], którą można wykorzystać do ukrycia w grafice dodatkowych danych, poprzez podmianę najmniej znaczących bitów (*least significant bit*). Standardowo w „czarno-białych" zdjęciach występuje 256 odcieni szarości, z których ludzkie oko jest w stanie dostrzec jedynie 64. Podmieniając za pomocą specjalnego oprogramowania jeden bit w każdym 1 bajtowym pikselu (tj. najmniejszym elemencie dwuwymiarowej grafiki), jesteśmy w stanie niepostrzeżenie ukryć w zdjęciu inny, osiem razy mniejszy (1 bajt to 8 bitów) plik (np. tekstowy). Dzięki zastosowaniu tej metody dostęp do ukrytych w danym zdjęciu informacji będzie miała wyłącznie osoba, która została poinformowana o fakcie ich istnienia i która dysponuje odpowiednim oprogramowaniem oraz hasłem dostępowym umożliwiającym ich wydobycie z nośnika (dla pozostałych osób zdjęcie to będzie zwykłym plikiem graficznym).

[62] Większość standardów graficznych zapewnia znacznie większą rozdzielczość skali kolorów, niż wynika to z możliwości percepcyjnych ludzkiego oka. B. Schneier, *Kryptografia*..., s. 37.