NOWOCZESNE TECHNOLOGIE INFORMATYCZNE — BEZPIECZEŃSTWO DANYCH

Zbigniew Kotulski

1 Wstęp

Wiek XIX i prawie cały wiek XX, okres gospodarki tradycyjnej, nazwać możemy czasem energii (mówiono: wiek pary, wiek elektryczności, wiek atomu). Burzliwy rozwój dziedzin nowej gospodarki, opartej na technologiach informatycznych, sprawia, że okres od połowy XX. wieku nazwać możemy czasem informacji. Nie będziemy tu definiować energii i informacji. Wspomnijmy tylko, że oba te pojęcia, a raczej wielkości fizyczne nazywane energią i informacją, mają pewne cechy wspólne, mają też cechy różniące je. Spróbujmy podać tutaj te cechy analogiczne i cechy odmienne. Zacznijmy od energii.

Energia jest w fizyce podstawowym elementem modelowania świata. Występują tam różne rodzaje energii: kinetyczna, potencjalna, elektromagnetyczna, chemiczna, jądrowa. Energię można przesyłać w czasie i w przestrzeni. Można zaprojektować (lub przynajmniej odkryć!) procesy energetyczne: przemiany jednego rodzaju energii w inny (uwzględniając zasadę zachowania energii), sposoby przechowywania energii oraz metody przesyłania energii. Można wreszcie energię mierzyć, czyli wyrazić liczbowo jej ilość. Mimo tych wielu możliwości wykorzystania pojęcia energii do opisu fizycznej rzeczywistości, wobec skomplikowanej budowy świata (np. w jednym molu gazu jest liczba Avogadro, czyli $6{,}022 \cdot 10^{23}$ cząsteczek) nie wystarcza ono do tego celu. Dlatego też niezbędne było wprowadzenie pojęcia informacji jako uzupełnienia energetycznego opisania świata.

Wprowadzając pojęcie informacji zauważmy, że są wykorzystywane dwa jej typy. Pierwszy to entropia, czyli wielkość fizyczna opisująca naszą niewiedzę o zjawisku. Drugi to po prostu informacja, opisująca wiedzę o procesie lub zjawisku. Pojęcie entropii stanowi immanentny składnik termodynamiki i tam zostało po raz pierwszy wykorzystane (Boltzmann). Funkcjonuje tam druga zasada termodynamiki, która mówi, że w układzie izolowanym entropia jest niemalejącą funkcją czasu, co oznacza że stan tego układu oddala się, w coraz bardziej nieprzewidywalny sposób, od stanu początkowego. To intuicyjne w fizyce pojęcie entropii dostało się w ręce matematyków, którzy w różny sposób próbowali je sformalizować, korzystając z pojęć rachunku prawdopodobieństwa. Najbardziej spójną i najszerzej stosowaną (także, a może przede wszystkim, poza fizyką) jest teoria Shannona, w której entropia zjawiska, reprezentowanego przez zmienną losową, jest po prostu wartością średnią z logarytmu rozkładu prawdopodobieństwa (funkcji gęstości lub funkcji rozkładu) tej zmiennej, wzięta z przeciwnym znakiem. Teoria ta stała się fundamentem nowej dziedziny matematyki nazwanej teorią informacji.

W teorii informacji natychmiast wprowadzono w sposób formalny pojęcie informacji wzajemnej, czyli tej „pozytywnej" informacji, którą posiada jedno zjawisko (czytaj: zmienna losowa) o innym zjawisku. W ramach teorii informacji, podobnie jak to było w przypadku energii, mogą występować różne rodzaje informacji. Informacja może być przesyłana w czasie i przestrzeni.

Możliwe jest również projektowanie procesów informacyjnych, czyli przemian jednego rodzaju informacji w inny, przechowywania i przesyłania informacji. W procesach tych obowiązuje odpowiednik drugiej zasady termodynamiki mówiący, że w procesach informacyjnych informacja zawsze maleje w czasie (jest funkcją monotoniczną). W naturalny sposób można również informację, jako funkcję rzeczywistą rozkładów prawdopodobieństwa, wyrażać w pewnych jednostkach, czyli mierzyć.

Podsumowując to wprowadzenie do powstania matematycznego pojęcia informacji, warto zauważyć, że nastąpiło zamknięcie pewnego cyklu. Pochodzące od fizycznego pojęcia entropii, matematyczne sformułowanie informacji (czyli informacji pozytywnej, mierzącej naszą wiedzę o zjawisku) powróciło do fizyki, stanowiąc podstawę fizyki informacyjnej (nazywanej też, dla podkreślenia występowania przepływu informacji we wszystkich zjawiskach fizycznych i jej oddziaływania na te zjawiska, dynamiką informacyjną). Ta gałąź fizyki jest rozwijana w kilku ważnych ośrodkach naukowych na świecie, na przykład w MIT. W Polsce miejscem takim jest Toruń, gdzie w pracach R. Ingardena z zakresu termodynamiki szeroko wykorzystywano pojęcia dynamiki informacyjnej. Również w dynamicznych zagadnieniach mechaniki pojęcie entropii informacyjnej i informacji stało się bardzo owocnym narzędziem zarówno obliczeniowym (zasada maksymalnej entropii w aproksymacji rozkładów prawdopodobieństwa), jak i koncepcyjnym. Ważne wyniki w tej dziedzinie są rezultatem prac K. Sobczyka w IPPT.

Wróćmy jednak do głównego przedmiotu tego opracowania, czyli informacji. Wszelka informacja, przesyłana, zgromadzona i przechowywana, stanowi podstawę wiedzy. Oznacza to, że informację należy traktować nie tylko jako pewien obiekt matematyczny lub fizyczny, wyrażany liczbowo (ilościowo), lecz również jako klasę danych posiadających pewne cechy składające się na wartość użytkową informacji i stanowiące jej treść. Aby informacja miała wartość użytkową, nie może być w trakcie przesyłania, gromadzenia, przechowywania i przetwarzania zniekształcana. Tę stabilność własności informacji i wszelkich procesów informacyjnych prowadzonych przez człowieka mogą zagwarantować tylko usługi ochrony informacji. O nich też będziemy mówić w dalszej części tej pracy.

2 Współczesne zastosowania bezpiecznego przesyłania i przechowywania informacji

Zanim przejdziemy do opisu współczesnych sposobów zapewnienia bezpieczeństwa informacjom, przedstawmy nieco faktów historycznych dotyczących ochrony informacji. Przede wszystkim, w przeszłości wiadomości były na ogół zapisane tekstem na papierze (pergaminie, itp.), zatem ich ochrona polegała po prostu na odpowiednim zaszyfrowaniu tekstu. Szyfrowanie polegało na przekształceniu tekstu według tajnego algorytmu (polegającego na wymieszaniu liter lub podstawieniu w ich miejsce innych liter lub znaków) do takiej postaci, aby mogły go odczytać tylko osoby uprawnione, znające algorytm odwrotny do szyfrowania (czyli algorytm odszyfrowania). Tak pojęte bezpieczeństwo informacji stało się domeną nauki nazwanej kryptologią. W ramach tej nauki znaleźli sobie miejsce zarówno ci, którzy chcieli bezpiecznie przesyłać informacje (kryptografowie) jak i ci, którzy te informacje, mimo wszelkich zabezpieczeń, chcieli w sposób nieuprawniony odczytać (kryptoanalitycy).

Oczywiście, bezpieczeństwo informacji nie ograniczało się tylko do zachowania jej tajności. Dokument z zaszyfrowanym tekstem musiał być dostarczony do adresata; adresat powinien mieć pewność, że zaszyfrowana treść dokumentu nie została zmieniona lub uszkodzona, czyli że zachowana została jej integralność (mogła to zagwarantować jedynie jakość papieru i atramentu), że nadawcą jest znana mu osoba (to można było potwierdzić odpowiednimi podpisami i pieczęciami). Jak z tego wynika, istotne znaczenie miała ochrona fizyczna dokumentu, takżeświadectwo posłańca potwierdzającego nadawcy dostarczenie dokumentu do adresata.

Pozostaje jeszcze odpowiedź na naturalne pytanie o zastosowanie podanych wyżej metod ochrony informacji. Otóż w przeszłości korzystali z nich przede wszystkim wojskowi i dyplomaci, a więc przedstawiciele władzy, w zakresie dotyczącym wielkich spraw ówczesnegoświata. Inne grupy osób prawie nie korzystały z metod kryptograficznych ochrony informacji, a Galileusz strzegący wyników swych badań (czy raczej praw autorskich do tych wyników) używając anagramów, był tu raczej wyjątkiem. O przestępcach i członkach tajnych stowarzyszeń nie będziemy tu wspominać, bo takie grupy z natury nie chcą ujawniać swych tajemnic i zamiarów. Postawmy tu jeszcze jedno pytanie: czy od tamtych czasów coś się zmieniło w dziedzinie ochrony informacji? Odpowiedź, na pozór prosta, nie jest jednak tak całkiem jednoznaczna.

Współcześnie mamy do czynienia z wielką różnorodnością przesyłanych informacji. Poza tradycyjnym tekstem przesyłany bywa obraz, głos oraz wielka ilość danych cyfrowych powstających we wszystkich dziedzinach życia gospodarczego i społecznego. Dodatkowym faktem mającym wpływ na bezpieczeństwo danych jest to, że, poza nielicznymi wyjątkami, są one przesyłane kanałami otwartymi: w Internecie, przez łącza telefoniczne lub w otwartej przestrzeni niesione przez fale elektromagnetyczne. Mimo całej różnorodności rodzajów przesyłanych danych i dróg ich przesyłania istnieje element wspólny, mający zasadnicze znaczenie dla metod ochrony informacji. Otóż, po odpowiednim zakodowaniu, każdy z rodzajów przesyłanych informacji może być sprowadzony do postaci cyfrowej, czyli zapisany w postaci ciągu bitów. Wszelkie algorytmy chroniące informacje mogą zatem przekształcać jeden ciąg bitów (na przykład ciąg reprezentujący zakodowany tekst) w inny ciąg bitów (powiedzmy: ten sam ciąg poddany procedurze szyfrowania). Taka możliwość zakodowania informacji doprowadziła do swoistej uniwersalizacji kryptologii: algorytmy kryptograficzne nie muszą uwzględniać cech narodowego języka szyfrowanej informacji (w przeszłości szyfr musiał uwzględniać częstotliwość występowania poszczególnych zgłosek, cechę charakteryzującą język narodowy). Można tu jeszcze wymieniać inne nowości odróżniające współczesne algorytmy kryptograficzne od historycznych, jednak najważniejszą z nich jest przyjęcie zasady, że stosowany algorytm kryptograficzny jest powszechnie znany. Algorytm taki, przekształcający jeden ciąg bitów (tekst jawny) w drugi ciąg (kryptogram) zależy od parametru, nazywanego kluczem. Zarówno do wykonania algorytmu prostego (szyfrowania), jak i algorytmu odwrotnego (odszyfrowywania) wymagana jest znajomości klucza. Czyli, jedynie posiadacz klucza (nazywanego tajnym kluczem, z racji funkcji, jaką pełni) może odszyfrować wiadomość zaszyfrowaną tym kluczem. Z drugiej strony, każdy (algorytm jest jawny) może badać własności algorytmu szyfrującego i bądź potwierdzić jego siłę, bądź też złamać algorytm, to znaczy wskazać drogę odszyfrowania tekstu w sposób inny niż to zakładali twórcy algorytmu.

Przekształcenie algorytmów kryptograficznych do postaci operacji na ciągach binarnych sprawiło, że kryptologia stała się działem matematyki. Z kolei, jawność algorytmu kryptograficznego zatarła podział kryptologii na antagonistyczne działy: kryptografię i kryptoanalizę. Dopuszczenie współczesnego algorytmu kryptograficznego do szerokiego użytku wymaga najpierw jego zapro-

jektowania (co jest rolą kryptografii) a następnie zbadania jego odporności na wszelkie możliwe ataki (tu mają pole do popisu kryptoanalitycy). Ścisłe współdziałanie obu grup badaczy (raczej: alternatywnych spojrzeń na szyfr) jest gwarancją sukcesu.

Dotychczas wspomnieliśmy o różnicach między tradycyjnym szyfrowaniem tekstów pisanych a szyfrowaniem informacji reprezentowanych binarnie. Teraz możemy wskazać także podobieństwa. Tak jak niegdyś szyfrowanie polegało na zamianie kolejności liter tekstu i podstawianiu w miejsce liter tekstu jawnego innych liter (znaków), tak i dziś większość algorytmów kryptograficznych działa na zasadzie permutacji i podstawień bitów lub sekwencji bitów (nazywanych w nawiązaniu do tradycji słowami). Reguły rządzące tymi operacjami wchodzą w skład algorytmu kryptograficznego, dodatkowo modyfikowanego przez wybór klucza (będącego ciągiem bitów o ustalonej długości). Również, podobnie jak w przeszłości, w stosunku do przesyłania informacji stosowane są usługi poufności (czyli szyfrowania), integralności (sprawienie, żeby dane po wysłaniu nie mogły zostać nielegalnie zmodyfikowane), autentyczności (potwierdzenie tożsamości nadawcy informacji) oraz niezaprzeczalności (zagwarantowanie, by nadawca nie mógł zaprzeczyć faktowi wysłania, a odbiorca — otrzymania wiadomości). Obecnie wszystkie te usługi (a nie tylko samo szyfrowanie, czyli usługa poufności) mogą być realizowane za pomocą algorytmów kryptograficznych. Ponadto, wszystkie te usługi obejmują cały przesyłany dokument, każdy jego bit (są realizowane przez funkcje, których dziedzina obejmuje wszystkie bity dokumentu), podczas gdy informacja przesyłana tradycyjnymi metodami jest, na przykład, podpisywana na ostatniej stronie i podpis jest przypisany do określonego miejsca dokumentu.

Zastosowanie zapisu binarnego i algorytmów zapewniających bezpieczeństwo przesyłanych informacji stworzyło nowe możliwości w tej dziedzinie. Pozwoliło to, z jednej strony, na burzliwy rozwój utrwalonych już sposobów przesyłania informacji, takich jak telekomunikacja, z drugiej zaś na rozwój nowych, których sztandarowym przykładem może być bankowość elektroniczna. Nie sposób tu wymienić wszystkich obszarów działalności ludzkiej związanej z przesyłaniem i przechowywaniem informacji, w których kryptograficzne usługi ochrony informacji odgrywają istotną rolę. Oprócz wspominanych już dyplomacji i wojskowości (lub szerzej, wszelkich służb państwowych, tajnych i jawnych), nie mogłyby się bez tych usług obyć następujące dziedziny (przykłady tych dziedzin wymienimy w punktach, stosując w uzasadnionych przypadkach powszechnie stosowane nazwy angielskie):

- telekomunikacja stacjonarna i mobilna (niezbędna jest poufność i integralność danych),
- poczta elektroniczna (poufność, autentyczność),
- e-banking, e-money, e-business (najwyższy poziom bezpieczeństwa, wymagane wszystkie usługi bezpieczeństwa ze względu na bezpieczeństwo obrotu finansowego),
- sieci komputerowe i obliczenia rozproszone (w zależności od wagi i kosztu obliczeń stosowane są różne zabezpieczenia, najczęściej wykorzystujące specyficzne protokoły obliczeniowe),
- elektroniczne dokumenty (ważna autentyczność i integralność dokumentu),
- bazy danych, w tym statystyczne bazy danych (trudne zadanie: trzeba udostępnić dane legalnym użytkownikom w zaplanowanym zakresie, szybko i sprawnie, a równocześnie chronić je przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem),

- płatne usługi i serwisy (na przykład telewizja kodowana; naruszenie zasad dostępu wiąże się ze stratami poniesionymi przez operatora systemu).

W jaki sposób we wszystkich tych dziedzinach życia realizowane są usługi kryptograficzne przedstawimy w następnym rozdziale tego opracowania, starając się, w miarę możliwości, doprecyzować znaczenie terminów używanych dotychczas w ich potocznym znaczeniu.

3 Współcześnie stosowane usługi bezpieczeństwa i wykorzystywane w nich algorytmy

3.1 Wprowadzenie

Wspomnieliśmy, że kryptografia jest dziedziną matematyki. W istocie, jest to pewne jej zastosowanie, które korzysta z dorobku wielu tradycyjnych działów matematyki, niekiedy wpływając na znaczne ich ożywienie (jak to jest ostatnio choćby w przypadku teorii liczb). Kryptografię, czy szerzej, naukę o bezpieczeństwie informacji, można sobie wyobrazić jako piramidę, której podstawą są różne działy matematyki stanowiące bazę naukową stosowanych metod. Można do nich zaliczyć wymienioną już teorię liczb, jak również wiele innych działów matematyki, często częściowo pokrywających się: kombinatorykę, matematykę dyskretną, logikę, teorię ciał skończonych, teorię złożoności obliczeniowej czy, ostatnio, rachunek prawdopodobieństwa i statystykę matematyczną, teorię układów dynamicznych. Wyższym piętrem piramidy są algorytmy kryptograficzne, wykorzystujące wiedzę zaczerpniętą z wymienionych działów matematyki i służące realizowaniu różnych zadań kryptograficznych. Algorytmy kryptograficzne, wykorzystywane w relacjach między stronami procesu bezpiecznej komunikacji, stanowią podstawę protokołów kryptograficznych. Protokoły (kolejny poziom), odpowiednio zaprojektowane i zestawione, składają się na usługi bezpieczeństwa (wieńczące piramidę), które wymieniliśmy już w poprzednim rozdziale, a więc poufność, integralność, autentyczność i niezaprzeczalność informacji.

W ramach tak krótkiego opracowania nie sposób w pełni przedstawić problematykę bezpieczeństwa informacji. Przedstawimy zatem kilka przykładów algorytmów kryptograficznych i ich zastosowań, aby w ten sposób wskazać wagę problemu oraz zachęcić do podjęcia badań zmierzających do rozwoju metod matematycznych (i nie tylko matematycznych) ochrony informacji.

Zacznijmy od zagadnienia w kryptografii najstarszego, a zarazem podstawowego, czyli zapewnienia poufności informacji.

3.2 Usługa poufności czyli szyfrowanie

Jak już zauważyliśmy, informacja (tekst) podlegająca szyfrowaniu to ciąg bitów, czyli zer i jedynek, często o ogromnej długości. Algorytm szyfrowania zamienia ten ciąg bitów w inny ciąg bitów, co widzimy jako zamianę każdego z bitów ciągu na bit przeciwny (0 na 1 lub 1 na 0) lub pozostawienie go bez zmiany. Sposób zmiany tych bitów stanowi o bezpieczeństwie szyfrowanej wiadomości. Jak można przedstawić ów sposób zamiany bitów tekstu jawnego (czyli naszej informacji) na kryptogram (czyli tekst zaszyfrowany)? Najprościej za pomocą ciągu bitów o tej samej długości, nazywanego strumieniem bitów i pełniącego rolę klucza. Szyfrowanie polegałoby na zamianie bitów według reguły: jeśli bit klucza jest równy 0, to odpowiadający mu bit

tekstu pozostawiamy bez zmiany, jeśli 1, to zmieniamy na przeciwny. Taka operacja, nazywana binarną operacją XOR i oznaczana symbolem $\oplus$, jest tożsama z dodawaniem liczb w ciele Z_2 (zawierającym dwa elementy, 0 i 1, z działaniami dodawania i mnożenia modulo 2), prowadzonym kolejno dla wszystkich par bitów. Odszyfrowywanie, czyli operacja odwrotna do szyfrowania, jest identyczne z szyfrowaniem, z tym, że przekształceniu poddajemy nie tekst jawny, a kryptogram. Tak zdefiniowana transformacja bitów jest praktycznie stosowanym szyfrem, nazywanym *szyfrem strumieniowym* lub *szyfrem Vernama* (pierwszy raz była zaproponowana w 1917 roku przez G.S. Vernama do szyfrowania treści telegramów zapisanych na papierowej taśmie perforowanej za pomocą kodu Baudota). Należy teraz zadać pytanie: czy taki prosty w swym pomyśle szyfr jak pomysł Vernama może być szyfrem dobrym? I jak rozumieć owe pozytywne cechy szyfru? Odpowiedź nie jest jednoznaczna.

Zacznijmy od zalet szyfru strumieniowego. Przede wszystkim, jest on bardzo szybki. Szyfrowanie jednego bitu ogranicza się do wykonania jednej operacji binarnej XOR. Ponadto udowodniono (Shannon), że szyfr ten jest całkowicie bezpieczny, jeśli tylko strumień klucza jest idealnym losowym ciągiem binarnym: bity z równym prawdopodobieństwem przyjmują wartości 0 i 1 oraz są od siebie statystycznie niezależne. Bezpieczeństwo to jest rozumiane w sensie *informacyjnym*, co oznacza, że szyfrogram nie dostarcza napastnikowi żadnej informacji, która pozwoliłaby go złamać, czyli odczytać zaszyfrowaną wiadomość. W dodatku jest to jedyny znany obecnie szyfr mający tę własność. O innych szyfrach możemy mówić, że są co najwyżej *bezpieczne obliczeniowo*, to znaczy wymagane zasoby (czas pracy komputera, niezbędna pamięć) niezbędne do złamania szyfru są zbyt duże, aby obecnie i w wystarczająco odległej (dla konkretnego zastosowania) przyszłości mogło nastąpić złamanie szyfru.

Opisany tu idealny szyfr Vernama, w zderzeniu z rzeczywistością, ma jednak pewną wadę. Problemem jego praktycznej realizacji jest konieczność posiadania, w dwóch miejscach (u nadawcy i u odbiorcy) tego samego losowego strumienia bitów pełniącego rolę klucza. Skąd wziąć taki ciąg? Stosunkowo łatwo uzyskać go można w jednym ustalonym miejscu, na przykład u nadawcy zaszyfrowanej informacji. Losowych bitów mogą dostarczać szumy urządzeń elektronicznych, zawartość rejestrów pracującego komputera lub inne urządzenia fizyczne, np. mierniki promieniowania. Problem powstaje, gdy chcemy taki ciąg (a pamiętamy, że ma on długość równą długości szyfrowanej informacji) przesłać w bezpieczny, czyli zapewniający tajność, sposób do odbiorcy wiadomości, który musi z kolei wykorzystać go w procesie odszyfrowywania. W przypadku stosunkowo krótkich informacji (np. depeszy dyplomatycznej) losowy strumień bitów można zapisać na dwóch taśmach magnetycznych i w bezpieczny sposób przekazać komunikującym się stronom. Co jednak zrobić, gdy przesyłamy ogromne zasoby danych w długim czasie (np. w telekomunikacji wymagana jest zdolność szyfrowania rzędu 1 GB/s przez kilka lat)? Wówczas pozostaje wytwarzanie strumienia klucza w sposób powtarzalny, to znaczy za pomocą pewnych algorytmów matematycznych możliwych do przeprowadzenia niezależnie i równocześnie w dwóch miejscach, Takie algorytmy nazywamy *generatorami liczb (bitów) losowych*, jeśli tylko uzyskany w ich wyniku strumień bitów nie może być metodami statystycznymi odróżniony od idealnego losowego ciągu bitów.

W praktyce stosowane są metody generacji strumienia bitów B wykorzystujące bardzo różnorodne algorytmy matematyczne. Nie będziemy tu szczegółowo omawiać zagadnienia, odsyłając czytelnika do literatury, i ograniczymy się do jednego, dość ogólnego schematu. W metodzie tej najpierw ustalamy długość n ciągu (bloku) bitów, a następnie wybieramy odpowiednie

przekształcenie $\varphi(\cdot)$ odwzorowujące ciągi n-bitowe w ciągi n-bitowe, $\varphi : (Z_2)^n \to (Z_2)^n$. Następnie losujemy ciąg n bitów z_0, nazywany ziarnem generatora, i wykonujemy kolejne iteracje funkcji φ, $z_i = \varphi(z_{i-1})$, $i = 1, 2, \ldots$, wykorzystując w strumieniu bitów B uzyskane kolejno bloki z_i, wybrane z nich bity lub też, dla zwiększenia bezpieczeństwa szyfru, wynik działania nieliniowej funkcji boolowskiej (to znaczy, przyjmującej wartości z Z_2) na z_i. Jaką funkcję ϕ zastosować do generowania bitów? Nie podając konkretnych przykładów (tu ponownie odsyłamy do literatury) odpowiemy, że taką, która ma długi okres; funkcja działa w przestrzeni o skończonej liczbie elementów, więc po pewnej liczbie iteracji musi przyjąć wartość, którą już w przeszłości przyjmowała, zamykając tym samym cykl wartości. Znalezienie takiej funkcji nie zawsze jest proste, tym bardziej, że uzyskany z jej pomocą ciąg musi spełniać wszelkie kryteria losowości: niezależność bitów i zgodność z rozkładem równomiernym. W tym miejscu pojawia się problem znalezienia odpowiedniego zestawu testów statystycznych weryfikujących te własności. Nie mogą być one badane równocześnie: testy zgodności rozkładu wymagają, by próba losowa była próbą prostą (czyli złożoną z elementów niezależnych statystycznie), a badanie niezależności wymaga założeń o rodzaju rozkładu. Ponadto, każdy ciąg bitów używany w kryptografii musi być przed użyciem przetestowany, zatem testy nie mogą być zbyt długotrwałe. Na szczęście w praktyce udaje się sprostać tym wymaganiom i szyfry strumieniowe mogą bez przeszkód służyć tam, gdzie w trybie ciągłym przesyłane są duże potoki poufnych danych.

3.3 Szyfry blokowe

Kiedy już zdecydowaliśmy, że strumień bitów do szyfru Vernama będziemy wytwarzali za pomocą matematycznego algorytmu, w którym dokonuje się wielokrotnych operacji na bloku bitów, należy sobie zadać pytanie: czy nie można podobnych operacji wykonywać na blokach tekstu jawnego w taki sposób, by z otrzymanych bloków wyjściowych nie dawało się (w łatwy sposób) odgadnąć postaci bloków wejściowych? Okazuje się, że odpowiednio zaprojektowany algorytm przekształcający skończone ciągi bitów może stanowić alternatywny, bezpieczny obliczeniowo sposób szyfrowania. Jest on, z oczywistych względów, nazywany *szyfrem blokowym*.

Możemy teraz sformułować zadanie szyfrowania blokowego jako problem matematyczny. Załóżmy, że musimy zaszyfrować pewną wiadomość P (ciąg bitów o skończonej długości). W tym celu dzielimy ją na mniejsze bloki bitów P_i, $i = 1, 2, \ldots, m$, każdy o długości n, w razie potrzeby uzupełniając ostatni blok losowo wybranymi bitami. Do szyfrowania każdego z bloków wykorzystujemy pewne odwzorowanie odwracalne $F(\cdot, \cdot)$ przyporządkowujące każdemu blokowi tekstu jawnego P_i blok szyfrogramu C_i. Odwzorowanie to zależy od parametru K nazywanego *tajnym kluczem* (niech będzie to ciąg k bitów), zatem może być przedstawione jako: $F(\cdot, \cdot) : (Z_2)^n \times (Z_2)^k \to (Z_2)^n$. Jak już wspominaliśmy, zgodnie z obowiązującymi obecnie zasadami, algorytm szyfru (czyli funkcja F) jest zazwyczaj powszechnie znany. Bezpieczeństwo szyfrowania, czyli uniemożliwienie nielegalnego odwrócenia funkcji F, zależy wyłącznie od zachowania poufności klucza K. Należy znów zapytać, jaka powinna być funkcja F, żeby ta zasada bezpieczeństwa mogła być spełniona? Wiadomo, że wszystkich funkcji odwzorowujących $(Z_2)^n$ w $(Z_2)^n$ jest 2^{n2^n}, a odwzorowań różnowartościowych (odwracalnych) jest $2^n!$. Zaplanowanie szyfru blokowego, to wybór pewnej rodziny 2^k odwzorowań odwracalnych, numerowanych parametrem, który przyjmuje wszystkie możliwe wartości klucza K. Jak łatwo zauważyć, samo zapisanie takich funkcji może sprawiać problem, a tymczasem my oczekujemy dodatkowo, że

będą to funkcje bezpieczne kryptograficznie. Jak zatem w praktyce rozwiązywane jest zadanie konstruowania szyfrów blokowych? Dotychczas nie ma ścisłych zasad tworzenia szyfrów blokowych, są natomiast szeroko stosowane intuicyjne reguły, które funkcje używane do szyfrowania blokowego muszą spełniać. Są to zazwyczaj pary postulatów, z których każdy zapewnia realizację innej własności przekształcenia bloku bitów tekstu jawnego w blok bitów szyfrogramu.

Pierwszą taką parą warunków jest wymóg spełnienia przez przekształcenie własności *mieszania* i *rozpraszania*. Własność mieszania, zaproponowana przez Shannona, oznacza, że przekształcenie losowo i równomiernie rozprowadza bloki tekstu jawnego po zbiorze wszystkich możliwych bloków szyfrogramu (mamy tu pełną analogię z definicją mieszania wykorzystywaną w teorii dyskretnych układów dynamicznych). Rozpraszanie natomiast oznacza, że bity znajdujące się przed dokonaniem przekształcenia w bezpośrednim sąsiedztwie, po wykonaniu tego przekształcenia wpływają na bity odległe od siebie w bloku wyjściowym. Pierwszą z tych cech uzyskuje się w szyfrowaniu przez zastosowanie odpowiedniej sekwencji permutacji i podstawień, drugą przez wykorzystanie elementów nieliniowych, najczęściej tak zwanych skrzynek podstawieniowych.

Inną parą warunków jest *lawinowość* i *zupełność* szyfru. Lawinowość to żądanie, by zmiana jednego bitu w bloku tekstu jawnego wywoływała zmianę połowy bitów szyfrogramu. Zupełność z kolei, to wymóg, by istniał taki stan bloku wejściowego, w którym zmiana dowolnie wybranego bitu wejścia spowoduje zmianę wskazanego bitu wyjścia szyfru. W praktyce oznacza to, że każdy bit bloku wyjściowego (szyfrogramu) jest bardzo skomplikowaną funkcją wszystkich bitów bloku wejściowego (tekstu jawnego).

Wymagane jest również, by odwzorowanie szyfrujące spełniało warunki *dyfuzji* i *konfuzji*. W tym wypadku dyfuzja oznacza rozmycie wszelkich związków między bitami tekstu jawnego równomiernie w całym bloku kryptogramu (jest ona realizowana przez permutacje bitów). Konfuzja z kolei to maksymalne wymieszanie bitów bloku tajnego klucza z bitami bloku tekstu jawnego i uczynienie ich powiązania maksymalnie skomplikowanym.

Powyższe warunki wskazują nam, jakie własności powinno mieć odwzorowanie szyfrujące, czyli które z 2^{n2^n} możliwych odwzorowań (uwzględniając obecność klucza) $(Z_2)^n$ w $(Z_2)^n$ mogą pełnić rolę szyfru blokowego. Pozostaje jeszcze zapisanie takiego odwzorowania (jeżeli już je znamy) w możliwie prostej postaci. Oczywiście, wypisanie go w postaci tabeli nie wchodzi w grę, a nie możemy się spodziewać, że będzie ono funkcją elementarną. Jak zatem wygląda takie praktycznie stosowane przekształcenie szyfrujące? Współczesne szyfry blokowe działają w sposób iteracyjny (kaskadowy): blok wejściowy jest poddany działaniu pewnej stosunkowo prostej funkcji, nazywanej funkcją rundy; wyjście tej operacji staje się ponownie wejściem rundy (opcjonalnie z nieco zmienionymi parametrami, na przykład w każdej rundzie jest stosowany inny klucz, tzw. klucz rundowy). W różnych szyfrach iteracje wykonywane są od kilku do kilkunastu razy. Funkcja rundy z kolei zbudowana jest z kilku warstw (składających się z operacji elementarnych działających na bloki bitów: permutacji, podstawień, działań arytmetycznych modulo 2^n, XOR bitów przekształcanego bloku z bitami klucza, itp.). Każda z tych warstw ma zapewnić spełnienie przynajmniej jednego z wymienionych warunków gwarantujących jakość szyfrowania. Jak zatem widzimy, budowa takiej funkcji szyfrującej jest bardziej sztuką opartą na intuicji niż realizacją pewnego przygotowanego projektu. Dlatego też każdy szyfr blokowy przed dopuszczeniem do użycia musi być wszechstronnie przebadany. Kryptoanaliza szyfrów blokowych jest prowadzona również w czasie ich eksploatacji, prowadząc niekiedy do kompromitacji tych szyfrów lub wymuszając dokonanie modyfikacji zwiększających ich bezpieczeństwo.

Zagadnienia związane z projektowaniem szyfrów blokowych należą do klasycznych zadań kryptografii, dlatego też nie będziemy się nimi szerzej zajmować. Wspomnijmy jedynie, że bezpieczeństwo tak zaprojektowanych szyfrów jest bezpieczeństwem obliczeniowym. Uznaje się zatem, że szyfr jest bezpieczny, jeśli jest odporny na wszystkie znane ataki w stopniu gwarantującym nieopłacalność lub praktyczną niemożność przeprowadzenia takich ataków. Badanie przeprowadzane jest przez projektowanie ataków i szacowanie nakładów obliczeniowych niezbędnych do ich przeprowadzenia. Próbą zbadania odporności na wszelkie (również nieznane) ataki jest badanie statystyczne szyfrów blokowych. Jeśli kryptogramy opuszczające szyfr blokowy są niemożliwe do odróżnienia od idealnych ciągów losowych (przypomnijmy, że taką cechę mają kryptogramy powstające w idealnym szyfrze Vernama), to możemy się spodziewać, że ten szyfr będzie trudny do złamania wszelkimi metodami. Stąd konieczność opracowywania coraz doskonalszych testów statystycznych dostosowanych do potrzeb kryptografii.

3.4 Bezpieczne obliczenia sieciowe

Znamy już metody przesyłania danych w sposób poufny, zarówno korzystające z trybu strumieniowego, jak i blokowego. Pozostaje tu jeszcze do rozwiązania podstawowy problem: w szyfrach strumieniowych obie komunikujące się strony powinny mieć to samo ziarno generatora bitów pseudolosowych, a w trybie blokowym — klucz, obie wielkości, dla zagwarantowania poufności szyfrów, tajne dla postronnych. Czy można sprawić, by dwie osoby, posługując się otwartym kanałem komunikacyjnym (obecnie: korzystając z sieci komputerowej), mogły wspólnie ustalić tajny klucz sesyjny (czyli ciąg bitów o ustalonej długości)? Zanim odpowiemy na to pytanie, zajmijmy się zagadnieniem prostszym, dotyczącym wspólnego ustalenia wartości jednego bitu.

Zagadnienie takie, odpowiadające losowaniu za pomocą rzutu monetą na odległość, nosi nazwę protokołu *zobowiązania bitowego*. Wyobraźmy sobie, że dwie osoby, A i B, chcą wspólnie ustalić losową wartość bitu w taki sposób, że:

- Strona A wybiera losowo wartość bitu.
- Po dokonaniu wyboru, A nie może już zmienić wartości tego bitu.
- Strona B może poznać wartość tego bitu jedynie za zgodą strony A.

Protokół zobowiązania bitowego może być zrealizowany w następujących krokach (zachowana jest tu symetria komunikujących się stron):

- Strona B generuje losowy ciąg bitów R_B i wysyła do A.
- Strona A generuje losowy ciąg bitów R_A i wysyła do B.
- A wybiera bit b_A i generuje losowy klucz K_A. Następnie szyfruje ciąg $P_1 = \{R_B \| b_A\}$ kluczem K_A i wysyła kryptogram $C_A = F(P_1, K_A)$ do B (dwuargumentowa operacja konkatenacji, oznaczona przez $\|$, polega na połączeniu dwóch ciągów bitów przez ich kolejne zapisanie).
- B wybiera bit b_B i generuje losowy klucz K_B. Następnie szyfruje ciąg $P_2 = \{R_A \| b_B\}$ kluczem K_B i wysyła kryptogram $C_B = F(P_2, K_B)$ do A. B wysyła klucz K_B do A.

- A odszyfrowuje kluczem K_B kryptogram C_B otrzymując ciąg $P_2 = \{R_A \| b_B\}$. Sprawdza zgodność R_A i uzyskuje b_B .

- A wysyła klucz K_A do strony B.

- B odszyfrowuje kluczem K_A kryptogram C_A otrzymując ciąg $P_1 = \{R_B \| b_A\}$. Sprawdza zgodność R_B i uzyskuje b_A . Obie strony obliczają bit losowy b z wzoru $b = b_A \oplus b_B$.

Warunkiem bezpieczeństwa tego protokołu (to znaczy zapewnienia uczciwości wyniku) jest, by w zastosowanym odwzorowaniu szyfrującym $F(\cdot, \cdot)$ dla każdego klucza K prawdopodobieństwo istnienia takiego klucza K', że dla $R = R_A$ lub $R = R_B$, $F(\{R\|b\}, K) = F(\{R\|b \oplus 1\}, K')$, było bardzo małe.

Przedstawiony algorytm zobowiązania bitowego dotyczy elementarnego zadania dotyczącego uzgodnienia jednego tylko bitu, jednak jego przeprowadzenie wymaga zastosowania dość skomplikowanej metody, jaką jest szyfrowanie blokowe. Ponadto w metodzie tej wykorzystano randomizację przez użycie losowych ciągów bitów R_A i R_B , co w tym wypadku jest niezbędne dla zapewnienia bezpieczeństwa (obliczeniowego) algorytmu. Okazuje się, że również takie zadanie jak przesłanie w sposób tajny ustalonej wartości jednego bitu (czyli mówiąc wprost: zaszyfrowanie pojedynczego bitu) może być wykonane za pomocą metody randomizacji (przesyłany bit jest jednym z bitów losowego ciągu bitów). Odpowiednie rozwinięcie metod zrandomizowanego szyfrowania doprowadziło do sformułowania koncepcji *udowadnialnego bezpieczeństwa*. Mówimy, że algorytm kryptograficzny jest udowadnialnie bezpieczny, jeżeli można pokazać z dostatecznie dużym prawdopodobieństwem, że nie istnieje atak na ten algorytm o złożoności obliczeniowej mniejszej niż ustalona wielkość (zależna od pewnego parametru tego algorytmu, takiego jak długość bloku i długość klucza). Nakład pracy niezbędny do złamania algorytmu powinien wzrastać wykładniczo wraz ze wzrostem rozmiaru tego parametru. Zatem wraz ze wzrostem możliwości obliczeniowych potencjalnego napastnika można tak zmodyfikować algorytm (na przykład, zwiększając odpowiednio długość klucza), by nadal pozostawał on bezpieczny obliczeniowo.

Wróćmy jednak do naszego wyjściowego zagadnienia uzgodnienia klucza sesyjnego. Odrzucając, jako zbyt pracochłonną, możliwość uzgadniania klucza sesyjnego bit po bicie za pomocą protokołu zobowiązania bitowego (tak zmodyfikowanego, by gwarantował poufność), musimy posłużyć się inną metodą. Może nią być, na przykład, *protokół uzgodnienia klucza Diffie–Hellmana*. Protokół taki pozwala obliczyć w sposób poufny (wynik znają tylko strony wykonujących obliczenie) i kolektywny (obie strony uczestniczą w obliczeniu na równych prawach) wspólną wartość elementu należącego do pewnej grupy skończonej. Grupą taką może być, na przykład, zbiór Z_n z operacją dodawania modulo n lub punkty krzywej eliptycznej nad ciałem Z_p z odpowiednio zdefiniowanym dodawaniem punktów (zainteresowani szczegółami powinni sięgnąć do współczesnych książek z kryptografii). Przedstawimy przykład protokołu uzgodnienia klucza w grupie addytywnej E; w stosowanym zapisie przez mnożenie liczby naturalnej k przez element P grupy E będziemy rozumieli k-krotne dodawanie tego punktu. Uzgodnienie klucza między stronami A i B przebiega w następujących krokach:

- Strony wybierają wspólny element P grupy E.

- Strona A wybiera dużą liczbę naturalną c (tajną).

- Strona B wybiera dużą liczbę naturalną d (tajną).
- A oblicza cP i przesyła cP do B.
- B oblicza dP i przesyła dP do A.
- Strony wspólnie obliczają $Q = cdP$ (tajne).
- Informacja jawna: grupa E, element P, element cP, element dP.
- Wspólny sekret (uzgodniony klucz) jest równy $Q = cdP$.

Podobny protokół można skonstruować w grupie multiplikatywnej; wówczas mnożenie elementu grupy przez liczbę należy zastąpić przez potęgowanie elementu, czyli jego wielokrotne mnożenie przez siebie. Bezpieczeństwo protokołu Diffie–Hellmana wynika z faktu, że w grupie skończonej E, w której nie istnieje naturalny porządek, nie jest możliwe obliczenie wartości liczby c na podstawie znajomości elementu cP (elementu P^c w grupie multiplikatywnej) i elementu P.

W sytuacjach, gdy prowadzona jest bezpieczna komunikacja między n uczestnikami A_i, $i = 1, 2, \ldots, n$, (telekonferencja, rozsyłanie poufnych dokumentów do wielu odbiorców, itp.), konieczne jest uzgodnienie klucza między wielu stronami. W tym celu można zastosować, na przykład, *protokół generowania klucza Justa–Vaudenaya*. Może być w nim wykorzystany protokół Diffie–Hellmana w ciele skończonym (wymagana jest tu możliwość obliczania elementu odwrotnego, czyli „dzielenia" elementów ciała skończonego) do generacji klucza między każdą parą uczestników o przypisanych im sąsiednich numerach. Realizacja protokołu przebiega w następujących krokach:

- W protokole uczestniczy n uczestników, A_i, $i = 1, 2, \ldots, n$; przyjmujemy, że $A_0 \equiv A_n$, $A_{n+1} \equiv A_1$.
- Każda para uczestników $(A_i,\ A_{i+1})$ generuje wspólny klucz K_i, $i = 1, 2, \ldots, n$.
- Uczestnik A_i, $i = 1, 2, \ldots, n$ posiada dwa klucze: K_i oraz K_{i-1}, przy czym $K_0 \equiv K_n$.
- Uczestnik A_i, $i = 1, 2, \ldots, n$ oblicza liczbę $R_i = K_i / K_{i-1}$ i wysyła wynik do wszystkich pozostałych stron protokołu.
- Każdy uczestnik jest w posiadaniu wszystkich R_i, $i = 1, 2, \ldots, n$.
- Każdy uczestnik A_i, $i = 1, 2, \ldots, n$ oblicza (indeksy są przyjmowane cyklicznie modulo n).
- $$K = K_{i-1}^n \, R_i^{n-1} \, R_{i+1}^{n-2} \cdots R_{i-3}^2 R_{i-2} = K_{i-1}^n \, \frac{K_i^{n-1}}{K_{i-1}^{n-1}} \, \frac{K_{i+1}^{n-2}}{K_i^{n-2}} \cdots \frac{K_{i-3}^2}{K_{i-4}^2} \, \frac{K_{i-2}}{K_{i-3}} =$$
  $$= K_1 K_2 \cdots K_n \, .$$
- K jest wspólnym tajnym kluczem stron protokołu A_i, $i = 1, 2, \ldots, n$.

Obliczenie wspólnej wartości tajnego klucza nie jest jedynym zastosowaniem bezpiecznych obliczeń sieciowych. Podobne protokoły mogą być użyte w innych praktycznych zagadnieniach, w których uczestniczy wiele stron, na przykład w głosowaniach, kolektywnym podejmowaniu decyzji czy po prostu wykonywaniu operacji arytmetycznych. Wspólnym wymogiem tych protokołów jest, by zapewniały one spełnienie takich kryteriów jak: *poufność* (wynik może być poznany jedynie przez uczestników protokołu), *kolektywność* (wszyscy uczestnicy mają równe prawo do poznania wyniku i równy wkład w jego uzyskanie), *uczciwość* (żaden z uczestników nie powinien zniweczyć kolektywnego wysiłku przez decydujący wpływ na końcowy wynik lub sekretne uniemożliwienie wykonania zadania), *poprawność* (wynik powinien być jednoznaczny i zgodny z przebiegiem algorytmu) i *efektywność* (algorytm powinien być możliwy do wykonania w wyznaczonym czasie i przy wykorzystaniu wskazanych środków). Ponadto, dobrze jest, jeśli algorytm jest *weryfikowalny*, to znaczy każdy z uczestników lub zaufana trzecia strona mogą sprawdzić poprawność wyniku i uczciwość wszystkich uczestników protokołu.

3.5 Algorytmy niesymetryczne

Uzgadnianie klucza jest procedurą skomplikowaną, wymagającą wymiany informacji między stronami i trudną do weryfikacji. Czy nie prościej byłoby samemu wygenerować klucz sesyjny i w bezpieczny sposób przesłać do odbiorcy? Wyobraźmy sobie następujący sposób postępowania. Nadawca (nazwijmy go stroną A) generuje klucz sesyjny. Następnie prosi odbiorcę informacji (stronę B) o zaproponowanie sposobu zaszyfrowania tego klucza. B wysyła do A otwartym kanałem komunikacyjnym swój klucz, nazwany kluczem publicznym, który umożliwia zaszyfrowanie klucza sesyjnego w taki sposób, że jedynie właściciel klucza publicznego (w tym wypadku — B) potrafi tę wiadomość odczytać. Dlaczego jest to możliwe? Ponieważ strona B posiada drugi klucz, tak zwany klucz prywatny, stanowiący parę z kluczem publicznym, pozwalający dokonać operacji odwrotnej do przeprowadzonej przez A operacji szyfrowania. W celu przeprowadzenia takiej operacji przesłania klucza potrzebny jest jednak specjalny algorytm szyfrowania asymetrycznego, w którym praktycznie każdy (klucz publiczny może być powszechnie znany) może informacje zaszyfrować, jednak informacja ta może być odszyfrowana jedynie przez posiadacza klucza prywatnego. W latach siedemdziesiątych dwudziestego wieku udało się skonstruować algorytmy tego rodzaju; wykorzystują one trudne obliczeniowo zagadnienia matematyczne, na przykład problem faktoryzacji (rozkładu na czynniki pierwsze) dużych liczb naturalnych lub problem obliczenia logarytmu dyskretnego (czyli znalezienia, dla danego b, $0 < b < p$, takiej liczby i, że $d^i = b \bmod p$). Jako przykład rozważmy system *szyfrowania asymetrycznego*, opracowany przez Rona Rivesta, Adi Shamira i Leonarda Adlemana w 1977 roku i nazwany od ich nazwisk *RSA*. Jest to najszerzej obecnie stosowany algorytm (amerykańska norma FIPS podaje go jako standard systemu klucza publicznego), umożliwiający stosowanie dowolnie długiego klucza, a więc zapewniający poziom bezpieczeństwa dostosowany do potrzeb każdego użytkownika.

Algorytm klucza publicznego RSA, jak zresztą każdy algorytm tego typu, składa się z dwóch kroków. Pierwszym z nich jest generowanie pary kluczy; klucza publicznego i klucza prywatnego. Czynność ta może być wykonana przez właściciela klucza prywatnego, jeśli RSA ma służyć jedynie jego prywatnym potrzebom, lub też przez zaufaną trzecią stronę, czyli autoryzowany urząd (*Urząd Certyfikacji*) wchodzący w skład *infrastruktury klucza publicznego*, jeśli klucze te mają

służyć świadczeniu usług bezpieczeństwa, takich jak *autentyczność* czy *niezaprzeczalność* informacji.

Generowanie pary kluczy w RSA polega na wykonaniu następujących czynności:

- Weź dwie duże liczby pierwsze p i q.
- Oblicz ich iloczyn $n = pq$, nazywany modułem algorytmu.
- Wybierz liczbę e, mniejszą niż n i względnie pierwszą z $(p-1)(q-1)$.
- Oblicz d będące odwrotnością liczby e modulo $(p-1)(q-1)$, to znaczy: $ed \equiv 1 \bmod (p-1)(q-1)$.
- e jest publicznym wykładnikiem RSA.
- d jest prywatnym wykładnikiem RSA.
- Para liczb (n, e) jest *kluczem publicznym RSA*.
- Czynniki p i q muszą pozostawać tajne (mogą być zniszczone po obliczeniu d).
- Para liczb (n, d) jest *kluczem prywatnym RSA*.

Bezpieczeństwo algorytmu RSA oparte jest na trudności faktoryzacji dużej liczby n (w praktyce korzysta się z liczb posiadających kilka tysięcy cyfr). Algorytm ten ma zastosowanie do szyfrowania wiadomości, co umożliwia na przykład bezpieczne przesyłanie klucza sesyjnego, oraz do potwierdzenia autentyczności. Nie ma praktycznego zastosowania w poufnym przesyłaniu długich tekstów, ponieważ jest znacznie wolniejszy od symetrycznych szyfrów blokowych i strumieniowych. Operacja szyfrowania w RSA polega na wykonaniu następujących działań:

- A chce wysłać wiadomość M do B z zachowaniem poufności.
- Korzystając z klucza publicznego (n, e) należącego do B, A tworzy kryptogram wiadomości postaci $C = M^e \bmod n$.
- B, posiadający swój klucz prywatny (n, d), odszyfrowuje wiadomość otrzymaną od A obliczając $M = C^d \bmod n$.

Poprawność konstrukcji systemu RSA, czyli wzajemna odwracalność operacji szyfrowania i odszyfrowywania wynika z następującego twierdzenia Eulera: „Jeżeli NWD$(a, n) = 1$, to $a^{\varphi(n)} \equiv 1 \bmod n$" i z faktu, że dla $n = pq$ (iloczynu liczb pierwszych), $\varphi(n) = (p-1)(q-1)$. ($\varphi(n)$ oznacza wartość funkcji Eulera dla n, to znaczy liczbę takich liczb całkowitych a, $1 < a < n$, że NWD$(a, n) = 1$). Mamy bowiem $ed = 1 + x(p-1)(q-1) = 1 + x\varphi(n)$, zatem $M^{ed} = M \cdot M^{x\varphi(n)} = M \cdot (M^{\varphi(n)})^x = M \cdot 1^x \bmod n$, co dowodzi odwracalności algorytmu RSA. Algorytm RSA może służyć także do zapewnienia usługi autentyczności, a w połączeniu z zastosowaniem znacznika czasowego i wykorzystaniem certyfikatów odpowiednich urzędów, do usługi niezaprzeczalności. *Podpis cyfrowy*, bo o nim tu mówimy, może pełnić w stosunku do dokumentu elektronicznego wszystkie te funkcje, jakie pełni podpis odręczny na dokumencie papierowym, a ponadto zapewniać *integralność* dokumentu elektronicznego (czyli gwarantować, że

żaden fragment tego dokumentu nie został zmieniony po jego podpisaniu). Usługę integralności można zrealizować dzięki temu, że obliczona wartość podpisu cyfrowego jest funkcją wszystkich bitów dokumentu. W przypadku dokumentów bardzo długich podpisywana jest wartość bezpiecznej kryptograficznie funkcji skrótu policzonej dla tego dokumentu. (*Funkcja skrótu* jest to odwzorowanie, które przekształca cały dokument binarny w ciąg bitów o ustalonej długości, np. 1024; bezpieczeństwo tej funkcji polega na tym, że dla ustalonej wartości funkcji skrótu obliczonej dla danego dokumentu jest praktycznie niemożliwe znalezienie innego dokumentu dającego tę samą wartość funkcji skrótu). Podpis cyfrowy jest realizowany za pomocą algorytmu RSA w następujących krokach:

- B chce wysłać podpisany dokument M do A tak, aby zagwarantować jego autentyczność.
- B tworzy podpis cyfrowy $S = M^d \bmod n$ dokumentu M korzystając ze swojego klucza prywatnego (n, d) (dla długiego dokumentu, B podpisuje wartość funkcji skrótu $H(M)$).
- B wysyła do A parę dokumentów S i M.
- Wykorzystując klucz publiczny (n, e) nadawcy wiadomości, A oblicza $M' = S^e \bmod n$ (odpowiednio: $H'(M)$).
- W celu sprawdzenia autentyczności otrzymanej wiadomości, A porównuje obie wartości M i M' (oblicza $H(M)$ i porównuje z $H'(M)$).

Kończąc opis zastosowań algorytmu RSA w usługach bezpieczeństwa warto zauważyć, że RSA może być również wykorzystywane jako bezpieczny kryptograficznie (to znaczy nieprzewidywalny) generator liczb losowych, mający zastosowanie do tworzenia losowych kluczy sesyjnych. Generowanie liczb losowych metodą RSA przebiega w następujących krokach:

- Generujemy dwie duże liczby pierwsze p i q.
- Obliczamy moduł $n = pq$.
- Obliczamy wartość funkcji Eulera $\varphi(n) = (p-1)(q-1)$.
- Wybieramy losowo liczbę e z przedziału $1 < e < \varphi(n)$ tak, aby było NWD$(e, \varphi(n)) = 1$.
- Wybieramy ziarno X_0. Dla $i = 1, 2, \ldots$, generujemy ciąg liczb pseudolosowych $X_i = X_{i-1}^e \bmod n$. W celu zwiększenia bezpieczeństwa kryptograficznego generatora, do ciągu bitów klucza włącza się po jednym najmłodszym bicie z każdej wygenerowanej liczby losowej.

4 Perspektywy przyszłych badań

4.1 Paradoksy i sprzeczności w kryptografii

Informacja o stanie wiedzy w zakresie kryptograficznych metod ochrony informacji, rysująca jedynie podstawowe przykłady stosowanych metod, mogłaby sugerować, że najważniejsze problemy zostały już rozwiązane i istniejące algorytmy są w stanie zagwarantować wypełnienie podstawowych usług: poufności, autentyczności, niezaprzeczalności i integralności danych. Przedstawiony obraz jest jednak zmącony przez fakt, że corocznie zwiększa się moc obliczeniowa

komputerów, którymi mogą dysponować również potencjalni napastnicy, zatem algorytm, który dzisiaj jest bezpieczny obliczeniowo, w niedalekiej przyszłości traci tę cechę. Powstaje konieczność, jeśli to możliwe, zwiększenia długości stosowanego klucza w dotychczasowym algorytmie (np. w RSA; tu powstaje potrzeba szybkiego znajdowania dużych losowych liczb pierwszych) lub opracowania nowego algorytmu (tak jest w przypadku szyfrów blokowych). Jednak zmagania obrońców poufności informacji z napastnikami nie są jedyną sprzecznością tkwiącą w metodach kryptograficznych. Znacznie poważniejsze problemy, mające swe konsekwencje w opracowywanych algorytmach i pozostawiające pole do popisu dla przyszłych badaczy, tkwią w sprzecznych wymaganiach, jakie muszą spełniać algorytmy kryptograficzne.

Pierwsza sprzeczność występuje już w podstawowej usłudze kryptograficznej, jaką jest zapewnienie poufności przesyłanych danych. Równie ważną cechą transmisji danych jest poprawność tej transmisji, czyli sprawienie, by otrzymana informacja nie zawierała błędów. Nie jest możliwe wyeliminowanie wszelkich zakłóceń w przesyłaniu ciągów binarnych, dlatego też stosowane są takie *kodowania* przesyłanych danych (to znaczy zapisu w postaci binarnej)), które umożliwiają naprawę pewnych niewielkich błędów w otrzymanej informacji — stosowane tu mogą być *kody korygujące błędy*. Problem w tym, że taki kod przenosi więcej informacji niż jest to niezbędne, a zatem jest *kodem nadmiarowym* (ten nadmiar informacji pozwala na korekcję błędów zapisu). Z drugiej strony, zgodnie z teorią Shannona, wszelki nadmiar informacji w przesyłanej wiadomości, nawet gdy jest ona zaszyfrowana, stanowi ułatwienie dla napastnika pozwalające złamać szyfr użyty do zapewnienia poufności danych. Projektant systemu komunikacyjnego staje tu przed niełatwym problemem pogodzenia obu wskazanych oczekiwań użytkownika.

Jeśli już mówimy o ujawnieniu treści poufnej informacji w sposób nie przewidziany przez twórców algorytmu szyfrującego (do takich należy przypadek złamania szyfru przez napastnika), warto wspomnieć o następującym ważnym problemie. Jak wiadomo, w wielu państwach dopuszczana jest możliwość, po wypełnieniu przewidzianych prawem procedur, kontrolowania treści przesyłanych informacji przez uprawnione władze. Powstaje teraz problem, jak zapewnić realizowanie tego wymogu w sytuacji, gdy informacje są szyfrowane a stosowane szyfry są trudne do złamania? Podobny problem powstaje, gdy sam właściciel traci tajny klucz (gubi, klucz jest zniszczony przypadkowo albo w wyniku przestępstwa), bądź też ulega awarii system szyfrowania dysków komputerowych. W celu zagwarantowania możliwości odczytania zaszyfrowanych informacji niezbędne jest zastosowanie kryptografii kontrolowanej, czyli warunkowego umożliwienia ujawnienia szyfrowanych danych lub odzyskanie tajnego klucza. Obecnie przewiduje się wykorzystanie trzech systemów kryptografii kontrolowanej. Są to:

- depozyt kluczy, czyli przekazanie kluczy do depozytu z narzuceniem warunku, że ich wydanie uprawnionym osobom może nastąpić w ściśle określonych okolicznościach,
- odtworzenie kluczy, czyli zapewnienie możliwości odtworzenia klucza na podstawie informacji dołączanej do szyfrowanej wiadomości (pliku) lub połączenia,
- wykorzystanie zaufanej trzeciej strony, czyli kryptografia wykorzystująca zarządzanie kluczami przez zaufaną trzecią stronę.

Wszystkie te proponowane systemy mają pewne cechy zapewniające ich przydatność w różnych obszarach zastosowań. Na przykład, kryptografia kontrolowana z depozytem kluczy jest odpowiednia w sytuacji, gdy niezbędna jest deszyfracja w czasie rzeczywistym kryptogramu (np.

rozmowy telefonicznej lub transmisji danych), najczęściej na żądanie władz sądowych. Systemy z dołączaniem informacji o kluczu mogą być użyteczne w transmisji danych w przedsięwzięciach biznesowych, pełniąc rolę zapasowego dostępu do danych. Proponowane systemy kryptografii kontrolowanej spełniać dodatkowo powinny pewne funkcje bezpieczeństwa, których nie mają tradycyjne kryptosystemy. Są to:

- odporność systemu na nadużycia ze strony użytkowników (np. zgłoszenie fałszywego klucza, zmiany w urządzeniach po zgłoszeniu),
- odporność na nadużycia ze strony służb uprawnionych (nielegalny podsłuch),
- elastyczność systemu ze względu na zmiany intensywności wykorzystania,
- elastyczność ze względu na włączone aplikacje (różnorodność produktów kryptograficznych),
- możliwość odpowiedniego reagowania przez uprawnione służby (deszyfracja w czasie rzeczywistym, archiwizacja, itp.).

W systemach kryptografii kontrolowanej widoczna jest sprzeczność pomiędzy tajnością a możliwością śledzenia przesyłanych informacji. Podejmowane były próby rozwiązania tej sprzeczności, jednak często kończyły się one niepowodzeniem (na przykład wprowadzenie i wycofanie *Clipper Chip*, rozwiązania sprzętowego mającego zapewnić możliwość kontroli przez władze amerykańskie przesyłanych tajnych informacji). Zagadnienie to ciągle wymaga skutecznych rozwiązań, tym bardziej, że stosowane niegdyś ograniczenia eksportowe zaawansowanych technologii informatycznych okazały się całkowicie nieskuteczne (algorytmy matematyczne nie mogły być skutecznie opatentowane i chronione) i obecnie każdy może mieć dostęp do najsilniejszej nawet kryptografii.

Kolejną sprzecznością powstającą w trakcie stosowania usług kryptograficznych jest zapewnienie realizacji tych usług (a więc szyfrowania danych, potwierdzanie operacji, czyli realizacja usługi autentyczności, itd.) przy równoczesnym zapewnieniu wystarczającej szybkości transmisji danych. Mimo iż szybkość komputerów realizujących te usługi (np. szyfrowanie) rośnie bardzo szybko, to jeszcze szybciej zwiększa się ilość przesyłanych danych. Można wskazywać przykłady wielu różnych dziedzin, w których wymagana jest transmisja dużych strumieni poufnych danych (dobrym przykładem jest tu obraz uzyskiwany przez kamery z coraz większą rozdzielczością i lepszą jakością kolorów). W zilustrowaniu powstających trudności posłużmy się przykładem operacji finansowych. Niech to jednak nie będzie przepływ dokumentów bankowych (taki przepływ zwykle odbywa się w wewnętrznej sieci banku i rządzi się własnymi prawami), a operacje płatności elektronicznych odbywające się na styku wewnętrznego systemu bankowego i otwartej sieci udostępnionej dla klientów. Załóżmy, że posiadacz konta w e-banku (karty płatniczej) dokonuje zakupu w sklepie (także w sklepie internetowym). W takiej sytuacji, w celu zrealizowania płatności elektronicznej, muszą być zaangażowane następujące strony:

- kupujący (właściciel karty),
- wystawca (emitent) karty,

- instytucja obsługująca kartę płatniczą,
- sprzedawca,
- instytucja pośrednicząca (najczęściej bank),
- punkt certyfikacji (weryfikujący właścicieli kart i sprzedawców),
- serwer płatności (obsługujący dane przesyłane przez instytucję pośredniczącą).

Jak widać, operacja płatnicza generuje intensywny ruch w sieci między wskazanymi stronami, przy czym każda przesyłana informacja (odnosząca się przecież do przenoszenia praw majątkowych i podejmowania zobowiązań finansowych przez uczestniczące strony) musi spełniać wymogi poufności, autentyczności i niezaprzeczalności. Może się zatem okazać, że przy niewielkiej kwocie transakcji, koszt jej obsługi jest znacznie większy niż wartość samej operacji. Rozwiązaniem takiego problemu może być wyemitowanie przez bank elektronicznej gotówki, czyli odpowiednio zabezpieczonych ciągów binarnych, które przesyłane między stronami operacji (zgodnie z wymogami odpowiednio zaplanowanych *protokołów emisji*, *pobrania gotówki*, *płatności*, *depozytu* i *wydania reszty*) mogą pełnić taką samą rolę, jak tradycyjna gotówka i czeki gotówkowe. Jednak nawet w trakcie realizacji płatności elektroniczną gotówką mogą pojawić się zatory w transmisji danych, wynikające choćby ze specyfiki działania Internetu. Kiedy bowiem posiadacz elektronicznego banknotu zechce go wykorzystać do opłacenia dostępu do płatnych stron witryny internetowej, w której każde otwarcie pliku lub obrazu opłacane jest groszową kwotą pobieraną natychmiast po wykonaniu operacji, zastosowanie bezpiecznego protokołu płatności (zakładającego informowanie banku o każdej transakcji) mogłoby doprowadzić do zablokowania sieci. Potrzebny jest tu protokół mikropłatności, który będzie umożliwiał wydawanie drobnych monet z posiadanego banknotu cyfrowego bez każdorazowego absorbowania banku-emitenta, a równocześnie gwarantujący uczciwość kontrahenta (jednorazowe użycie każdej z monet i nie przekroczenie limitu, jakim jest wartość banknotu). Jak widać, w dziedzinie wykorzystania elektronicznego pieniądza w obecnych i przewidywanych zastosowaniach jest jeszcze wiele problemów do rozwiązania.

W związku z dokonywaniem elektronicznych transakcji finansowych musimy jeszcze wspomnieć w tym miejscu o problemie pojawiającym się w wyniku wprowadzenia inteligentnych kart chipowych, czyli o konieczności umieszczenia programów realizujących odpowiednie algorytmy kryptograficzne w ograniczonej pamięci tych kart. Powstaje tu problem optymalizacji kodów, a ponadto potrzeba wykorzystania takich algorytmów kryptograficznych, które w całości mogą być zrealizowane w układzie procesorowym karty. To wykonywanie obliczeń w karcie (na przykład w czasie identyfikacji posiadacza karty zlecającego systemowi bankowemu dokonanie przelewu) gwarantuje zapewnienie bezpieczeństwa informacji i chroni posiadacza konta przed nadużyciami ze strony pracowników banku. Zagrożeniem, podobnie jak w przypadku protokołów elektronicznej gotówki, jest dokonywanie nielegalnych operacji przez uprawnione strony wykonywanych procesów informacyjnych. Warto zatem zwrócić uwagę na istniejące (i spodziewane w przyszłości) możliwości przeciwdziałania nielegalnym oddziaływaniom na system przez użytkowników, projektantów, wykonawców i zarządzających.

4.2 Czynnik ludzki w bezpieczeństwie informacji

Wieloletnie obserwacje wszelkich nadużyć powstałych w systemach informacyjnych prowadzących do utraty ich bezpieczeństwa pokazują, że podstawowym ich źródłem są celowe działania i błędy osób odpowiedzialnych za prawidłowe ich funkcjonowanie. Zapewnienie bezpieczeństwa tych systemów powinno zatem polegać również na stosowaniu takich algorytmów i procedur, w których rola człowieka jest zminimalizowana lub wręcz całkowicie wyeliminowana. Tak więc system komputerowy powinien automatycznie generować klucze, klucze powinny być przechowywane w miejscach niedostępnych dla użytkowników i, najlepiej, powinny nigdy nie być ujawniane. Wszelkie niezbędne procedury testujące algorytmy i urządzenia kryptograficzne (stanowiące w istocie metodę ich dogłębnej analizy, a więc, przy niewłaściwym użyciu osłabiające bezpieczeństwo) powinny być prowadzone w sposób automatyczny, tak, by pośrednie wyniki testów nie mogły posłużyć do kryptoanalizy testowanych zabezpieczeń. Użytkownik powinien uzyskiwać jedynie odpowiedź potwierdzającą poprawność lub negującą przydatność badanej metody. Również stosowane implementacje algorytmów kryptograficznych muszą gwarantować, że ich wykonanie może przebiegać wyłącznie zgodnie z projektem, czyli że nie zawierają w sobie niejawnych uproszczeń („*tylnych wejść*”, czyli opcji pozwalających na ich wykonanie lub kryptoanalizę w uproszczony sposób lub „*koni trojańskich*”, podprocedur wykonujących nielegalne operacje). Spełnienie wszelkich tych wymogów wymaga opracowywania nowych algorytmów kryptograficznych i nowych metod weryfikacji kodu wykonywalnego.

W dotychczasowych rozważaniach pisaliśmy o powszechnie stosowanych dwóch podstawowych rodzajach systemów kryptograficznych, to znaczy kryptosystemach klucza publicznego, gdzie podstawą bezpieczeństwa jest utrzymanie w tajemnicy jednego tajnego klucza niezbędnego do szyfrowania i odszyfrowywania wiadomości, oraz kryptosystemach klucza publicznego, w których używana jest para kluczy: jawny klucz publiczny (szyfrowanie) oraz tajny klucz prywatny (odszyfrowywanie). Oba te systemy są podatne na nadużycie polegające na ujawnieniu tajnego klucza. Okazuje się, że te dwa systemy nie wyczerpują wszystkich możliwości zapewnienia poufności danych. Można bowiem tak zaplanować strukturę dostępu do danych, że klucz albo nie jest nigdy ujawniany (nie tylko jest tajny, ale legalny użytkownik nigdy go nie poznaje) albo też jest rozproszony między wielu użytkowników w taki sposób, że żaden z nich nie może tego klucza poznać. Przedstawimy teraz w skrócie te alternatywne metody zapewnienia bezpieczeństwa danych.

4.3 Inne systemy kryptograficzne

Jedną z metod służącą do bezpiecznego uwierzytelnienia może być dowód z wiedzą zerową. Metody tego rodzaju zostały zaproponowane w połowie lat osiemdziesiątych. Są one szczególnie przydatne do potwierdzania kart kredytowych, kart identyfikacyjnych, itp., czyli wszędzie tam, gdzie istnieje zagrożenie utraty poufności hasła w wyniku przesłania go do zewnętrznego urządzenia. Dowody takie wykorzystują na ogół *algorytmy probabilistyczne*, to znaczy takie, w których poprawny wynik jest uzyskiwany z dowolnie dużym prawdopodobieństwem, jednak nie gwarantującym stuprocentowej pewności. Często są w nich stosowane funkcje skrótu (nazywane niekiedy funkcjami jednokierunkowymi lub szyframi jednokierunkowymi, ponieważ nie jest możliwe policzenie ich odwrotności).

Dowód z wiedzą zerową jest protokołem, w którym strona A ma przekonać stronę B, że pewne stwierdzenie jest prawdziwe. Taki protokół musi spełniać trzy warunki:

- Jeśli stwierdzenie A jest prawdziwe, B powinien je zaakceptować.
- Jeśli stwierdzenie A jest fałszywe, B powinien odrzucić dowód niezależnie od postępowania A w trakcie dowodu.
- W trakcie realizacji protokołu, B otrzymuje jedynie informację, że stwierdzenie A jest prawdziwe.

Dotychczas opracowano szereg efektywnych algorytmów realizujących protokół dowodu z wiedzą zerową. Są to, między innymi, protokół Fiata–Shamira (1986), protokół Feige–Fiata–Shamira (1988) i protokół Guillou–Quisquatera (1988). Jako przykład zaprezentujmy pierwszy z nich. Realizacja protokołu składa się z dwóch etapów. Pierwszy polega na przygotowaniu danych niezbędnych do realizacji protokołu, drugi to etap weryfikacji. Do realizacji protokołu niezbędne jest wykorzystanie urzędu certyfikacji, czyli zaufanej trzeciej strony. W pierwszym etapie urząd wykonuje następujące czynności: Urząd publikuje dużą liczbę $N = pq$, gdzie p, q to liczby pierwsze, tajne.

- W systemie używana jest znana funkcja skrótu $f(\cdot, \cdot)$.
- Każdy użytkownik otrzymuje jednoznaczny jawny identyfikator I.
- Urząd wybiera małą liczbę j, taką, że $m = f(I, j)$ jest resztą kwadratową modulo N.
- Urząd oblicza najmniejszy pierwiastek kwadratowy modulo N z m i umieszcza go na karcie chipowej przeznaczonej dla użytkownika. Ten pierwiastek z m jest tajnym identyfikatorem użytkownika A.

Weryfikacja użytkownika A w protokole Fiata–Shamira przebiega w następujących krokach:

- A chce się uwierzytelnić przed B; udostępnia mu identyfikator I oraz liczbę j.
- B oblicza odpowiadający im skrót $m = f(I, j)$.
- A wybiera losowe $s \bmod N$, które oznaczamy jako $\sqrt{t}$, podnosi je do kwadratu modulo N, aby otrzymać t, które wysyła do B.
- B wysyła do A losowy bit e. A wysyła $p = \sqrt{t}\sqrt{m^e} \bmod N$ do B; mnożenie przez $\sqrt{t}$ powoduje ukrycie tajnego $\sqrt{m}$.
- B weryfikuje wynik podnosząc do kwadratu otrzymane p. (znając t i m sprawdza, czy $p^2 = tm^e \bmod N$). Wielokrotne uzyskanie sukcesu w powtarzanych próbach pozwala stwierdzić, że A rzeczywiście jest tym, kto zna tajny identyfikator.

Inną metodą zwiększenia bezpieczeństwa klucza może być zastosowanie *schematów podziału sekretu*. Sekretem może być hasło, klucz dostępu, informacja niezbędna do podjęcia decyzji lub uruchomienia systemu. Można tu zaobserwować analogię do takich tradycyjnych sposobów zabezpieczania, jak: kilku kluczy do sejfu w banku, podział kodów uruchomienia rakiet, uprawnień do

podjęcia decyzji w firmie czy też wymóg kilku podpisów na czeku bankowym. Możliwa jest konstrukcja bezpiecznych kryptograficznie algorytmów podziału sekretu, czyli podziałów sekretów odpornych na ujawnienie. Systemy podziału można klasyfikować ze względu na wiele kryteriów, takich jak algorytm podziału, skład uczestników sekretu oraz wzajemne relacje całości sekretu i jego części. Najbardziej popularny jest schemat progowy podziału (t, w), gdzie w jest liczbą uczestników podziału, a t liczbą uczestników schematu podziału niezbędnych do odtworzenia sekretu. Warunkiem bezpieczeństwa jest, by t uczestników mogło odtworzyć sekret, natomiast udziały $t-1$ uczestników (lub mniejszej ich liczby) nie dawały żadnej informacji o całym sekrecie. Jako przykład takiego schematu progowego podajmy algorytm zaproponowany przez Shamira, wykorzystujący wielomiany nad ciałem Z_p. Schemat składa się z trzech faz: inicjalizacji, rozdzielenia sekretu i ujawnienia sekretu.

Faza inicjalizacji

- D (dystrybutor sekretu) wybiera w różnych, niezerowych elementów Z_p, oznaczonych jaki $x_i, 1 \leq i \leq w$ (wymagamy, by było $p \geq w+1$). D przydziela punkty x_i udziałowcom sekretu P_i, $1 \leq i \leq w$.

Podział sekretu

- Załóżmy, że D chce podzielić klucz $K \in Z_p$ w systemie progowym (t, w).
- D w sposób losowy, wzajemnie niezależnie, wybiera $t-1$ elementów $a_1, a_2, \ldots, a_{t-1}$ ciała Z_p. Dla $1 \leq i \leq w$, D oblicza wartości $y_i = a(x_i)$, gdzie $a(x) = K + \sum_{j=1}^{t-1} a_j x^j \bmod p$. D przydziela udziały y_i uczestnikom podziału sekretu $P_i, 1 \leq i \leq w$.

Ujawnienie sekretu

- Załóżmy, że t uczestników podziału (spośród w uczestników), na przykład $P_1, P_2, \ldots, P_t$ chce ujawnić sekret.
- Udziałowcy ci mogą utworzyć układ t równań liniowych dla współczynników $K, a_1, a_2, \ldots, a_{t-1}$ i z niego wyznaczyć K.

$$\begin{aligned} y_1 &= K + a_1 x_1 + a_2 x_1^2 + \cdots + a_{t-1} x_1^{t-1} \bmod p \\ y_2 &= K + a_1 x_2 + a_2 x_2^2 + \cdots + a_{t-1} x_2^{t-1} \bmod p \\ &\vdots \\ y_t &= K + a_1 x_t + a_2 x_t^2 + \cdots + a_{t-1} x_t^{t-1} \bmod p \end{aligned}$$

Inne popularne systemy podziału sekretu korzystają z wektorowego opisu hiperpowierzchni i znajdowania punktu będącego ich przecięciem (schemat Brickella) lub wielokrotnego dodawania modulo dwa współrzędnych wektorów binarnych (schemat Karnin–Greene–Hellman).

Schematy podziału sekretu zabezpieczają klucz przed ujawnieniem. Nie oznacza to jednak, że nie są podatne na żadne zagrożenia. W tym wypadku również najgroźniejszy jest przeciwnik wewnętrzny, czyli nieuczciwi udziałowcy sekretu, którzy chcieliby uzyskać udziały innych

uczestników lub też zniszczyć cały schemat przez sfałszowanie swego udziału. Można stworzyć taki schemat, który uniemożliwi atak tego rodzaju, a przynajmniej pozwoli wykryć sprawcę (w przypadku wielu nieuczciwych udziałowców nie jest to już możliwe). Mamy tu sytuację podobną do kolektywnego generowania klucza, gdzie również możliwe są nadużycia ze strony uczestników protokołu. W obu tych sytuacjach przeciwdziałanie jest podobne. Żeby uzyskać system weryfikowalny (*weryfikowalny system podziału sekretu*, *weryfikowalny protokół uzgodnienia klucza*), należy każdemu z uczestników udostępnić więcej informacji o udziałach innych uczestników niż to jest niezbędne do rekonstrukcji sekretu, tak, by z tego nadmiaru informacji uczciwi uczestnicy protokołu mogli uzyskać wiedzę demaskującą oszusta. Tu znowu pojawia się sprzeczność, o której mówiliśmy przy okazji kodowania i szyfrowania: wszelki nadmiar przesyłanej informacji to zagrożenie utraty poufności, a zatem osłabienie bezpieczeństwa kryptosystemu. Rozwiązaniem jest pewna optymalizacja stosowanego algorytmu lub zastosowanie rozwiązań organizacyjnych zwiększających bezpieczeństwo systemu przesyłania informacji. I w tym miejscu dochodzimy do nowego zagadnienia, jakim jest zarządzanie bezpieczeństwem.

4.4 Zarządzanie bezpieczeństwem systemów informacyjnych

Zarządzanie bezpieczeństwem w systemie informatycznym jest elementem większej całości, jaką jest *polityka bezpieczeństwa* instytucji-właściciela systemu. Nie jest naszym celem zajmowanie się tym zagadnieniem, obejmującym najszerzej rozumiane zagadnienia związane z bezpieczeństwem (nie tylko informatycznym) funkcjonowania przedsiębiorstwa. Samo zarządzanie bezpieczeństwem informatycznym (i komplementarne do niego zarządzanie ryzykiem) jest zagadnieniem obejmującym bardzo dużo problemów związanych z infrastrukturą techniczną (sprzęt będący w stanie realizować wszystkie przewidziane w systemie bezpieczeństwa usługi kryptograficzne), personelem (szkolenie i nadzór) oraz oprogramowaniem. Kryptograficzna ochrona informacji w praktyce przedsiębiorstwa to odpowiednie oprogramowanie, zakupione na ogół u wyspecjalizowanych producentów. Nie jest tu możliwe opisanie wszystkich elementów zarządzania bezpieczeństwem systemu informatycznego związanych z oprogramowaniem i wykorzystywanymi w nim algorytmami matematycznymi. Wspomnijmy tylko o dwóch rzeczach. Na etapie projektowania systemu należy uwzględnić fakt, że system zbudowany jest z bardzo różnorodnych algorytmów (choćby systemów uwierzytelnienia, szyfrowania danych zgromadzonych w bazach i wysyłanych na zewnątrz systemu, systemów generacji, uzgadniania i przesyłania kluczy, itd.). Wiadomo, że bezpieczeństwo całego systemu jest limitowane bezpieczeństwem najsłabszego jego elementu. Powstaje jednak pytanie, jak porównać te różnorodne komponenty występujące zarówno w pojedynczym komputerze, w sieci wewnętrznej, jak i w Internecie, obejmującym również systemy wewnętrzne innych organizacji? Potrzebne są do tego pewne wspólne kryteria bezpieczeństwa oraz metody oceny bezpieczeństwa algorytmów (pozwalające choćby ustalić długość klucza w systemie klucza publicznego i w systemie klucza prywatnego dających takie samo bezpieczeństwo).

Drugie zagadnienie o którym wspomnimy związane jest z etapem eksploatacji systemu bezpieczeństwa informatycznego. Wiadomo, że obok ciągłej pracy kryptografów przygotowujących nowe systemy ochronne, trwa także praca kryptoanalityków, wyszukujących słabych miejsc kryptosystemów. Należy zatem stale śledzić wyniki ich pracy, by móc ulepszyć swój system w razie gdyby któryś z jego elementów został skompromitowany (w praktyce przez złamanie sys-

temu rozumie się znalezienie takiej metody jego kryptoanalizy, która jest szybsza od przewidywanej przez projektantów o kilka rzędów wielkości). Spektakularnym przykładem kompromitacji kryptosystemu było odkrycie *kryptoanalizy różnicowej* i *liniowej* algorytmu *DES* (będącego standardem amerykańskim szyfru blokowego). Doprowadziło ono najpierw do zalecenia potrójnego DESa jako standardu w okresie przejściowym, a następnie do rozpisania konkursu na nowy algorytm i wprowadzenia szyfru *RIJNDAEL* jako przyszłościowego standardu szyfrowania.

5 Metody niekryptograficzne zapewnienia bezpieczeństwa i perspektywy ich rozwoju

Dotychczasowe rozważania pokazują, że kryptografia jest skutecznym i perspektywicznym sposobem realizacji usług bezpieczeństwa informacji. Oczywiście, nie jest metodą jedyną, chociaż niewątpliwie jest metodą najtańszą. Jej koszt ograniczony jest do przygotowania odpowiedniego oprogramowania (po uprzednim zaprojektowaniu i przetestowaniu algorytmów) oraz systemów komputerowych realizujących to oprogramowanie. Jakie zatem mogą być inne metody zapewnienia bezpieczeństwa informacji? O działaniach organizacyjnych wykorzystujących metody nauk o zarządzaniu już wspominaliśmy. Warto teraz przedstawić inne metody — okazuje się bowiem, że zdobycze prawie każdej dyscypliny nauki można zastosować w celu zwiększenia bezpieczeństwa danych. Żeby nie szukać tych możliwości zbyt daleko, ograniczymy się tu do dziedziny nauk technicznych.

5.1 Metody wykorzystujące obrazy

W przeszłości, metodą przesyłania poufnych informacji, alternatywną do kryptografii (czyli szyfrowania), była *tajna komunikacja*, nazywana też *steganografią*. Poufność informacji wynikała z faktu, że nieupoważnione osoby po prostu nie wiedziały, że przesyłany dokument lub przedmiot zawiera w sobie informację przeznaczoną tylko dla wtajemniczonych. Na przykład, w przesyłanej książce niektóre litery (składające się na tajną informację) były zaznaczone malenkimi nakłuciami wykonanymi cienką igłą. Ta metoda utajnienia była skuteczna, dopóki nikt nie wiedział o tajnej przesyłce; w chwili ujawnienia jej istnienia nic już nie chroniło treści tajnej informacji. Mimo iż steganografia nie gwarantuje pełnego bezpieczeństwa przesyłanych informacji, może znaleźć zastosowanie także i dzisiaj.

Weźmy typowy obraz cyfrowy, taki jak można zaobserwować na ekranie komputera, to znaczy o rozdzielczości 1024 na 768 pikseli, każdy reprezentowany przez ciąg 32 bitów wyrażających jego kolor. Jeżeli teraz najmłodszy bit każdego z pikseli zmodyfikujemy w sposób opisany przez czarno-biały obraz o takiej samej rozdzielczości (tzn. 1024×768 pikseli, każdy opisany przez jeden bit), na przykład dodając bity modulo 2, to w efekcie otrzymamy obraz niezauważalnie różniący się od oryginału, a zawierający w sobie tajny zapis innego obrazu (oczywiście, ten czarno-biały obraz może być dowolnym ciągiem binarnym o długości 768 kB). Przy ogromnej ilości przesyłanych obrazów, taki system może być wydajnym sposobem przesyłania tajnych informacji.

Jednak nie cele komunikacyjne są najważniejszym zastosowaniem steganografii. Wkomponowane tajne rysunki mogą pełnić rolę *znaków wodnych* z wszystkimi ich zastosowaniami znanymi z obrotu dokumentów papierowych. Taki znak wodny może zabezpieczać obraz graficzny (lub zawierające ten obraz oprogramowanie) przed nielegalnym kopiowaniem; ukryty znak wodny stanowić może indywidualne oznaczenie użytkownika. Znak wodny pozwala, w razie nielegalnego skopiowania i rozpowszechniania pliku zawierającego grafikę, ustalić źródło pochodzenia tego pliku. Służy to także ochronie praw autorskich i poświadczeniu własności pliku stanowiąc ukryty podpis. Z drugiej strony, ukryty podpis wpleciony w mapę bitową obrazu to dowód autentyczności dokumentu. Może on mieć praktyczne znaczenie także w obrazach czarno-białych, na przykład dokumentach przesyłanych telefaksem cyfrowym, w których dodanie lub usunięcie pewnej liczby czarnych punktów (zgodnie z algorytmem zdefiniowanym w systemie podpisu) nie wpływa na jakość przesyłanego obrazu, pozwala natomiast potwierdzić źródło jego nadania. Zauważmy jeszcze, że o ile tak rozumiane podpisanie pliku, w przypadku oprogramowania komputerowego, pozwala potwierdzić jego autentyczność, nie gwarantuje jednak, że w pliku tym nie dokonano pewnych szkodliwych zmian (celowe wprowadzenie błędnych fragmentów kodu, wirusów lub „koni trojańskich" wykonujących pewne operacje — często o charakterze szpiegowskim — wbrew woli właściciela oprogramowania). Tutaj pomocne może być zastosowanie podpisu cyfrowego, na przykład metodą RSA opisaną już w tej pracy, gwarantującego integralność pliku oprogramowania. (Znak wodny o pewnych cechach indywidualnych nazywany jest „odciskiem palca", ang. „fingerprint".)

Z tajnym przesyłaniem obrazów związane jest jeszcze jedno pojęcie, które pojawiło się w ostatnich latach, a mianowicie *kryptografia wizualna*. W tym wypadku utajnienie obrazu polega na takiej jego dekompozycji na kilka niezależnych obrazów, że każda ze składowych przedstawia nieuporządkowany zbiór punktów (czarnych lub białych pikseli, lub też, w przypadku obrazów barwnych, kolorowych plam), natomiast po nałożeniu na siebie wszystkich części otrzymywany jest właściwy obraz. Efekt taki uzyskiwany jest przez odpowiednie rozbicie białych i czarnych pikseli na części składowe (cztery, dziewięć, itd.), w przypadku obrazów czarno-białych, lub też rozłożenie pikseli barwnych na kilka części. Kryptografia wizualna może służyć we wszelkich kodowanych przekazach wizyjnych jako sposób zabezpieczenia obrazu.

Zarówno steganografia wykorzystująca cyfrowy zapis obrazu, jak i kryptografia wizualna wymagają stosowania metod matematycznych używanych zwykle w cyfrowej analizie obrazu. W porównaniu z tradycyjną kryptografią, uzyskane dotychczas efekty można uznać raczej za pokazanie możliwości zastosowań, niż bezpieczne rozwiązania praktyczne.

5.2 Metody biometryczne, czyli mój klucz noszę w sobie

Jedną z usług kryptograficznych jest *uwierzytelnienie*, czyli potwierdzenie tożsamości użytkownika. Zazwyczaj dokonywane to jest przez podanie tajnego hasła, a w przypadkach wymagających wysokiego bezpieczeństwa — przez protokoły zbliżone w formie do podpisów cyfrowych lub systemy certyfikatów. W tych bardziej zaawansowanych systemach wymagany jest udział zaufanej trzeciej strony (urzędu certyfikacji) oraz wykorzystanie elektronicznego nośnika klucza prywatnego (certyfikatu). Można jednak zastosować system identyfikacji użytkownika nie wymagający ani udziału innych osób w procesie uwierzytelnienia, ani stosowania dodatkowych nośników informacji, ani nawet pamiętania tajnego hasła. System taki korzysta z *metod biometrycznych*, czyli

ustalania tożsamości osoby na podstawie jej indywidualnych cech biologicznych, na przykład zarysu linii papilarnych palca, geometrii dłoni, wzoru tęczówki lub obrazu siatkówki oka albo barwy głosu.

Wykorzystanie metody biometrycznej w procesie identyfikacji użytkownika systemu informacyjnego polega na wykonaniu dwóch operacji:

- odczytu cechy biometrycznej, utworzeniu jej wzorca cyfrowego i umieszczeniu tego wzorca w bazie systemu, oraz
- (powtarzanej wielokrotnie) operacji uwierzytelnienia, polegającej na odczytaniu cechy biometrycznej, jej digitalizacji i porównaniu z wzorcem znajdującym się w bazie.

Tak prosto wyglądający schemat w rzeczywistości nie jest prosty. Pomijając techniczny problem odczytu cechy biometrycznej (do tego potrzebne są odpowiednie kamery cyfrowe, skanery lub urządzenia rejestrując dźwięki), najważniejszy jest wybór takich cech zarejestrowanego obrazu, które będą indywidualnym wyróżnikiem osoby użytkownika, a równocześnie dadzą się zapisać w ciągu binarnym długości rzędu stu bitów. Inne występujące tu problemy to bezbłędne porównanie kolejnych odczytów z zapisanym wzorcem (każdorazowe odczyty sensorów cechy biometrycznej mogą się nieco różnić; należy sprowadzić do minimum prawdopodobieństwo błędów obu rodzajów, to znaczy odrzucenia właściwej osoby i zaakceptowania osoby niewłaściwej) i odporność systemu na próby fałszerstwa (podstawienie utrwalonych wzorców cechy biometrycznej, na przykład fotografii tęczówki oka). W metodach takich wykorzystywany jest dorobek tak odległych dziedzin wiedzy jak metody rozpoznawania obrazów i kryminalistyka.

Do metod biometrycznych identyfikacji osób należy zaliczyć również najbardziej rozpowszechnioną, jaką jest *podpis odręczny*, czyli „nazwisko (i imię) napisane odręcznie” lub „potwierdzenie pisma, nadanie mu ważności przez napisanie własnego nazwiska”. W podpisie nie byłoby niczego ciekawego, gdyby nie możliwość wszechstronnej analizy nie tyle samego znaku graficznego podpisu, ale metody jego wykonywania. Rejestrując proces podpisywania za pomocą pisaka wyposażonego w odpowiednie czujniki można rejestrować: współrzędne końcówki pisaka (ich przemieszczenie, czyli kształt podpisu), nacisk pisaka na papier, kąt pochylenia, siłę i pozycję uchwytu, przyśpieszenia w czasie wykonywania podpisu, itd. Zatem tak rozumiany podpis odręczny, z najbardziej zawodnej i łatwej do sfałszowania (także autofałszerstwa, w celu późniejszego zaprzeczenia wykonania podpisu) metody biometrycznej, może stać się metodą nowoczesną i trudną do podrobienia (wzorzec podpisu nigdzie nie musi występować w postaci zapisu graficznego, rejestrowany jest jedynie cyfrowo zapis parametrów ruchu pisaka). Innymi słowy, badanie podpisu odręcznego to typowe zadanie z dziedziny mechaniki.

5.3 Nowe metody matematyczne w problemach bezpieczeństwa informacji

Jak już wspominaliśmy, praktycznie rozumiane bezpieczeństwo algorytmów kryptograficznych oparte jest na dużej złożoności obliczeniowej wszelkich możliwych ataków, tak więc algorytmy te polegają na wykonaniu zagadnień trudnych obliczeniowo. W przypadku szyfrów blokowych są to ogromne ilości elementarnych operacji binarnych; systemy klucza publicznego wykorzystują fakt złożoności obliczeniowej takich problemów jak faktoryzacja (rozkład na czynniki pierwsze) dużych liczb naturalnych lub problem logarytmu dyskretnego. W przyszłych badaniach można

wykorzystać inne zagadnienia trudne obliczeniowo, adaptując je do potrzeb bezpiecznego przesyłania informacji.

Przykładem takiej grupy metod matematycznych, dostarczających wielu zagadnień trudnych, mogą być zagadnienia w grafach. Struktura grafów jest bardzo złożona; liczba możliwych grafów o n wierzchołkach, rośnie wraz z n wykładniczo. Wiele problemów w grafach, takich jak ustalenie liczby chromatycznej grafu, n-kolorowanie grafu, m kolorowanie grafu n-kolorowalnego (dla $m > n$), wyszukiwanie ścieżek o określonych własnościach w grafie, badanie izomorfizmu grafów, jest zagadnieniem trudnym obliczeniowo (NP-trudnym). Zagadnienia takie mogą być (i już były) wykorzystane do celów kryptograficznych. Ciągle jeszcze jest tu wiele możliwości, zarówno w zastosowaniach do systemów klucza prywatnego, systemów klucza publicznego, podziału sekretu lub dowodów z wiedzą zerową.

Wśród metod matematycznych dotychczas mało stosowanych, a w przyszłości mogących stanowić dobre narzędzie w kryptologii warto zauważyć sieci neuronowe i algorytmy ewolucyjne. Odpowiednio „nauczona" sieć neuronowa może, na przykład, stanowić wzorzec nieliniowej funkcji boolowskiej, której dobre własności kryptograficzne można zadać za pomocą szeregu warunków (na przykład zrównoważenia, to znaczy dawania na wyjściu bloków bitów o zbliżonej liczbie zer i jedynek). Taka funkcja stanowi zwykle element poprawiający „losowość" uzyskiwanych algorytmicznie ciągów pseudolosowych. Sieć neuronowa może też stanowić potrzebny w kryptoanalizie aproksymowany wzorzec generatora bitów pseudolosowych lub szyfru blokowego; raz nauczona na podstawie przechwyconego tekstu jawnego i kryptogramu, pozwoli odczytywać kolejne uzyskane kryptogramy. Wreszcie, odpowiednio zaprojektowana komórkowa sieć neuronowa może posłużyć do analizy ciągów binarnych pod kątem ich *złożoności sekwencyjnej* (rozkładu serii zer i jedynek różnej długości) lub *złożoności liniowej* (równoważności z wyjściem rejestrów liniowych określonego rzędu). Widać, że możliwości zastosowań w kryptologii są bardzo szerokie.

5.4 Algorytmiczne metody niekryptograficzne

W roku 1998 Rivest zaproponował metodę zapewnienia poufności danych bez ich szyfrowania, nazwaną „*chaffing and winnowing*" co można przetłumaczyć jako „*zanieczyszczanie i odsiewanie*". Mówiąc skrótowo, zabezpieczenie danych w tej metodzie polega na wykonaniu dwóch kroków. W pierwszym następuje podzielenie użytecznej informacji na krótkie bloki i podpisanie każdego z nich (za pomocą MAC, Messaga Authenctcation Code, czyli kluczowanej funkcji skrótu). W drugim kroku użyteczna informacja jest uzupełniana o bloki zanieczyszczające, podpisane w sposób błędny. Liczba tych bloków musi być na tyle duża, by ukryć informacje prawidłowe. Odbiorca, chcąc odzyskać tajną informację, sprawdza kolejno wszystkie bloki, obliczając ich MAC (zna tajny klucz użyty do podpisu) i akceptując bloki prawidłowo podpisane, a odrzucając pozostałe. Metoda ta przypomina trochę steganografię, stosowaną efektywnie do obrazów, ponieważ i w tym przypadku poufna informacja nie jest szyfrowana, a jedynie ukrywana wśród informacji bezużytecznych dla odbiorcy.

W podobny sposób można zapewniać bezpieczeństwo w wielkich bazach danych, rozpraszając i mieszając odpowiednio rekordy danych. Tego typu zabezpieczenia wspomagają bezpieczeństwo *statystycznych baz danych* (to znaczy takich baz, które powinny dostarczać informacji o uśrednionych parametrach danych, a nie o zawartości poszczególnych rekordów), w których główny

system bezpieczeństwa zawarty jest w strukturze dopuszczalnych zapytań dotyczących danych. Odpowiednie ukrycie danych pozwoli zapewnić im bezpieczeństwo w przypadku obejścia legalnego programu obsługi baz.

5.5 Zastosowanie nowych urządzeń do celów kryptograficznych

Powszechnie stosowane algorytmy kryptograficzne wykonywane są za pomocą komputerów, czyli są algorytmami cyfrowymi. Można sobie teraz zadać pytanie, czy do celów kryptograficznych można wykorzystać urządzenia techniczne (elektroniczne, mechaniczne lub realizujące pewne procesy fizyczne), czyli czy można wykonywać je w postaci analogowej? W pewnym sensie taką metodą jest analiza sygnałów losowych pochodzących z różnych podzespołów komputera lub źródeł promieniowania jądrowego i generowanie na ich podstawie ciągów bitów losowych, przeznaczonych do wykorzystania kryptograficznego. Ograniczeniem takiej metody jest niepowtarzalność uzyskanych wyników (stąd konieczność rejestracji wyników). Okazuje się, że jest możliwość wykorzystania zjawisk fizycznych, które są tak skomplikowane, jak procesy losowe i równocześnie możliwe do powtórzenia, pod warunkiem, że znane są dokładne wartości parametrów charakteryzujących te procesy. Mowa tu o *procesach chaotycznych*, czyli rozwiązaniach zagadnień opisanych przez układy dynamiczne (dyskretne i ciągłe w czasie), posiadających własność chaosu.

W matematycznym modelowaniu różnych zagadnień bezpiecznej komunikacji stosowane są zarówno układy dyskretne, jak i ciągłe. Układy dyskretne realizują algorytmy podobne do szyfrów blokowych. Dyskretny układ dynamiczny zależny od parametru pełniącego rolę tajnego klucza, w wyniku wielokrotnej iteracji, przekształca blok tekstu do postaci trudnej do powiązania z oryginałem bez znajomości dokładnej wartości tego parametru. Podobnie, odpowiednio iterowany układ dyskretny może być źródłem bitów losowych (znów mamy tu analogię z szyframi blokowymi). Ciągłe układy dynamiczne stosowane są do celów komunikacyjnych w dwojaki sposób. Mogą być źródłem „szumu” przykrywającego sygnał użyteczny; w takiej sytuacji do odbiorcy przesyłana jest informacja o niewielkiej amplitudzie (np. sygnał telegraficzny) z dodanym intensywnym szumem chaotycznym, tak że postronny obserwator nie jest w stanie odkryć przesyłanej tajnej informacji. Odbiorca, znając parametry procesu chaotycznego, może wygenerować odpowiedni sygnał, odjąć go od uzyskanej informacji i odzyskać użyteczny sygnał. Taka metoda nazywana jest *synchronizacją chaosu*. Inna metoda, nazywana *kontrolą chaosu*, polega na modulowaniu parametrów sygnału chaotycznego zgodnie ze wskazaniami sygnału binarnego użytecznej informacji (na przykład, dodając lub odejmując pewną niewielką liczbę, w zależności od wartości bitu). Odbiorca, posiadając modulowaną trajektorię i formułę procesu chaotycznego, może odtworzyć wysłany sygnał dostrajając proces chaotyczny do trajektorii zawierającej zakodowaną informację przez własną modulację parametrów.

Procesy chaotyczne mogłyby pozostać jeszcze jedną matematyczną metodą kryptograficzną gdyby nie fakt, że można je realizować fizycznie. Obecnie najciekawsze i najbardziej zaawansowane jest wykorzystanie laserów generujących chaotyczny, spolaryzowany sygnał świetlny. Sygnał ten, traktowany jako szum w metodzie synchronizacji, jest zaburzany sygnałem użytecznym. Po przesłaniu takiej wiązki do odbiorcy, w identycznym laserze, następuje synchronizacja promienia eliminująca sygnał użyteczny. Pozwala to uzyskać czysty szum możliwy do odjęcia od przesłanego sygnału (uprzednio częściowo zbocznikowanego celem umożliwienia odzyskania użytecznej informacji). Dodatkowym elementem wpływającym na bezpieczeństwo komunikacji

jest tu fakt, że promień laserowy jest przesyłany światłowodem, a więc medium odizolowanym od otoczenia przez osłonę gazową. Każda próba podsłuchu jest tu natychmiast wykryta w wyniku obserwowanego spadku ciśnienia gazu w osłonie.

Również inne procesy chaotyczne stosowane w kryptografii mają swoje odpowiedniki fizyczne, jednak dotychczas możliwość ich zastosowania w celach realizacji algorytmów kryptograficznych pozostaje w sferze projektów.

5.6 Nowe zjawiska fizyczne

Analiza cyfrowa danych jest w dużej mierze zdeterminowana przez binarność opisu. Bity, łatwo realizowalne fizycznie, czy to przez poziom napięcia elektrycznego (jest napięcie – nie ma napięcia), czy przez polaryzację magnetyczną (dodatnia – ujemna), czy wreszcie przez światło (białe – czarne), stanowią narzędzie efektywne rachunkowo, wprowadzają jednak istotne ograniczenie szybkości obliczeniowej. Wynika to z jednej strony z ograniczeń projektowych (osiągnięcie granic fotolitograficznych szerokości ścieżek układów scalonych), z drugiej zaś z problemu odprowadzenia ciepła z układu. Pojawia się tu znów związek między fizyką a teorią informacji, ujęty w postaci *zasady Landauera* mówiącej, że każde wykasowanie bitu informacji wiąże się ze zużyciem pewnej ilości energii. Zatem obliczenia binarne są procesem nieodwracalnym, wytwarzającym ciepło w ilości proporcjonalnej do liczby wykonywanych operacji. Trudności z odprowadzeniem ciepła z systemu obliczeniowego można uniknąć, jeśli uda się zastosować w układach scalonych odwracalne bramki logiczne (na przykład, zapamiętujące sytuację na wyjściu razem z sytuacją na wejściu, tak, by można było operację logiczną odwrócić). Najbliższą praktycznej realizacji tego pomysłu jest koncepcja *komputera kwantowego*, wykonującego obliczenia na *qubitach*, czyli wielkościach opisujących wynik kwantowego rzutu monetą (realizowanego na przykład w interferometrze Macha–Zhendera a opisanego przez cztery rozkłady prawdopodobieństwa). Komputer kwantowy jest, jako całość, układem odwracalnym, więc nie stwarza ograniczeń energetycznych przy zwiększaniu częstotliwości obliczeń. Uważa się, że fundamentalna dziś dla bezpieczeństwa kryptograficznego trudność rozkładu wielkich liczb na czynniki pierwsze nie będzie stanowiła problemu dla komputerów kwantowych, zatem łamiący szyfry uzyskają przewagę nad obrońcami tajemnic. Na szczęście dla kryptologów, fizyka kwantowa tu również może przyjść z pomocą. W ostatnich latach zaczyna być rozwijana *kryptografia kwantowa*, czyli sposób przesyłania informacji wykorzystujący, jako gwarancję bezpieczeństwa, *zasadę nieoznaczoności Heisenberga*, a zatem fakt, że każdy pomiar (a więc i „podglądanie" przesyłanych sygnałów) wpływa na wartość mierzonej wielkości. Uzgadniając klucz sesyjny (z wykorzystaniem qubitów) komunikujące się strony mogą odkryć, badając rozkłady prawdopodobieństwa bitów przesyłanego ciągu, czy nikt poza nimi nie zna ich wspólnej tajemnicy. Widzimy zatem, że rywalizacja między obu stronami, szyfrującymi i łamiącymi szyfry, wkroczy na wyższy poziom, nie uprzywilejowując nadmiernie żadnej ze stron.

5.7 Technologiczne możliwości zapewnienia bezpieczeństwa

Kończąc ten opis perspektyw przyszłych badań w dziedzinie ochrony informacji powróćmy z wyżyn rozważań fizyki kwantowej do realiów życia codziennego. Jak czytelnicy zapewne zauważyli, w prezentacjach zagadnień ochrony informacji problem bezpieczeństwa jest zazwyczaj przedsta-

wiony jako współzawodnictwo teoretyków-kryptografów, stosujących matematyczne algorytmy kryptograficzne do ochrony danych, i kryptoanalityków, korzystających z równie zaawansowanych algorytmów łamiących wszelkie zabezpieczenia. W praktyce problem niekiedy wygląda bardziej prozaicznie. Tajne informacje są ujawniane w wyniku niewłaściwego ustawienia monitorów komputerowych w źle zaprojektowanych pomieszczeniach, przechwytywania *ulotu elektromagnetycznego* pochodzącego z urządzeń informatycznych o podwyższonej emisji elektromagnetycznej (stanowiącej również zagrożenie zdrowia personelu), sygnału dodatkowo przenoszonego przez wewnętrzne instalacje budynków, na przykład sieć centralnego ogrzewania lub instalację elektryczną. Przyczyną utraty danych jest też brak izolowanych pomieszczeń, niezbędnych w przypadku pracy z danymi szczególnie wrażliwymi, oraz bezpiecznych łączy telekomunikacyjnych.

Jak widać z powyższego opisu, eliminacja elementarnych zagrożeń może znacznie poprawić stan bezpieczeństwa informacji: niemożność uzyskania danych do kryptoanalizy najlepiej chroni przed utratą poufności informacji. Tak jak w przypadku samolotu „niewidzialnego" dla radarów wykorzystano specjalne materiały i odpowiednio zoptymalizowane konstrukcje (zauważmy, że badania takich rozwiązań technologicznych znacznie odbiegały od tego, czym zazwyczaj zajmowano się w trakcie projektowania konstrukcji lotniczych, a więc aerodynamiki i wytrzymałości materiałów), tak również w interesującej nas dziedzinie dobre efekty można otrzymać opracowując właściwe materiały, na przykład do obudów urządzeń teletransmisyjnych, oraz projektując wszelkie elementy składowe konstrukcji systemów, od skali obiektów infrastruktury, do drobnych detali wielkości wyświetlaczy ciekłokrystalicznych stosowanych w zamkach szyfrowych.

6 Możliwości uczestnictwa w badaniach prowadzonych w świecie

Przedstawione metody zapewnienia bezpieczeństwa informacji są w głównej mierze oparte na zastosowaniu odpowiednich algorytmów matematycznych, a w przypadku kryptografii kwantowej, wyników z dziedziny fizyki teoretycznej. Poza nielicznymi wyjątkami (obejmującymi raczej szczególne implementacje istniejących metod) algorytmy te są powszechnie znane, publikowane w czasopismach, materiałach konferencyjnych i, jeszcze przed oficjalnym wydrukowaniem, dostępne w serwerze preprintów. Jako rezultaty z zakresu podstawowych badań naukowych (w głównej mierze matematyki, a ostatnio również fizyki) nie mogą być patentowane, są więc praktycznie dostępne i dopuszczone do legalnego użycia przez wszystkich zainteresowanych. Zatem istnieją wszelkie przesłanki włączenia się do badań na najwyższym poziomie w dziedzinie ochrony informacji: można mieć dostęp do najnowszych wyników a podjęcie badań, polegających głównie na wysiłku intelektualnym, nie wymaga wielkich kosztów ponoszonych w innych dziedzinach na zakup specjalistycznej aparatury. Oczywiście, opracowanie produktów komercyjnych wiąże się już z kosztami prowadzonych testów czy przygotowania profesjonalnej implementacji. Wydaje się, że z racji możliwości praktycznych zastosowań uzyskanych wyników można tu będzie liczyć na wspomożenie badań przez przyszłych użytkowników.

Dorobek polskich autorów w dziedzinach związanych z ochroną informacji jest znany wświecie i szeroko wykorzystywany. W tym kontekście zawsze należy wspomnieć o sukcesie, jakim było złamanie szyfru niemieckiej ENIGMY przez matematyków Mariana Rejewskiego, Henryka Zygalskiego i Jerzego Różyckiego. Będące rezultatem pracy Polaków wyniki z zakresu teorii liczb, zarówno Wacława Sierpińskiego, jak i obecnie pracujących, są wykorzystywane we współ-

czesnej kryptografii. Również inne działy matematyki, które mogą być wykorzystywane w konstrukcji metod ochrony informacji (i, oczywiście, ich łamania, czyli jak byśmy ładnie powiedzieli, weryfikacji bezpieczeństwa algorytmów), są w Polsce, także w IPPT, reprezentowane przez liczne grono badaczy. Wspomnijmy tu choćby statystykę matematyczną i rachunek prawdopodobieństwa, algorytmy genetyczne, rozpoznawanie obrazów czy numeryczną analizę danych. Do zagadnień związanych z niekryptograficznymi metodami ochrony informacji mogą się również włączyć specjaliści z dziedziny mechaniki, nauki o materiałach, akustyki i budownictwa. Metody korzystające z dorobku tych dziedzin (znajdujące się jeszcze w fazie początkowej, a więc pozostawiające szerokie pole do włączenia się nowych badaczy) zostały omówione w poprzednim rozdziale. Wyniki uzyskane w tym zakresie mogą być dodatkowym impulsem rozwoju technologii, zwłaszcza w zakresie nowych materiałów i konstrukcji, zarówno o wielkiej skali (budynki) jak drobnej (elementy urządzeń służących do przesyłania informacji).

Instytut Podstawowych Problemów Techniki wydaje się być szczególnie predestynowany do prowadzenia badań w dziedzinie ochrony informacji. Zobowiązuje do tego zarówno tradycja (w poprzednich latach prowadzono intensywne badania związane z przesyłaniem informacji w dziedzinach, które były wówczas ważne; świadczy o tym chociażby praca w IPPT profesora Janusza Groszkowskiego, patrona cywilnych i wojskowych instytutów telekomunikacji), jak i obecne możliwości intelektualne Instytutu, gromadzącego pracowników z wielu specjalności naukowych mających zastosowanie w tej dziedzinie. Wyniki uzyskane dotychczas potwierdzają tę możliwość.

Bibliografia

Bibliografia zawiera tytuły prac, które były inspiracją do napisania powyższego tekstu oraz takich, które mogą stanowić źródło dodatkowych informacji na temat zaprezentowanych zagadnień.

1. Denning D.E., *Kryptografia i Ochrona Danych*, WN-T, Warszawa, 1992.
2. Denning D.E., *Wojna Informacyjna i Bezpieczeństwo Informacji*, WN-T, Warszawa, 2002.
3. Kippenhahn R., *Tajemne Przekazy. Szyfry, Enigma i Karty Chipowe*. Prószyński i S-ka, Warszawa, 2000.
4. Koblitz N., *Wykład z Teorii Liczb i Kryptografii*, WN-T, Warszawa, 1995.
5. Koblitz N., *Algebraiczne Aspekty Kryptografii*, WN-T, Warszawa, 2000.
6. Kotulski Z., Szczepański J., *Discrete chaotic cryptography — a unified approach*, Annalen der Physik, **6**, 5, 381–394, 1997.
7. Kotulski Z., Szczepański J., Górski K., Paszkiewicz A., Zugaj A., *Application of discrete chaotic dynamical systems in cryptography — DCC method*, International Journal of Bifurcation and Chaos, **9**, 6, 1121–1135, 1999.
8. Kotulski Z., *Generatory liczb losowych: algorytmy, testowanie, zastosowania*, Matematyka Stosowana. Matematyka dla społeczeństwa, **2**, 43, 32–66, 2001.
9. Kozaczuk W., *W Kręgu ENIGMY*, Książka i Wiedza, Warszawa, 1986.
10. Menezes A., van Oorschot P., Vanstone S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.
11. Milburn G., *Inżynieria Kwantowa*, Prószyński i S-ka, Warszawa, 1999.
12. Penfield P., *Information and entropy*, wykład prowadzony dla studentów fizyki w MIT, *http://www-mtl.mit.edu/Courses/6.095/*
13. Pipkin D.L., *Bezpieczeństwo Informacji. Ochrona Globalnego Przedsiębiorstwa*, WN-T, Warszawa, 2002.

14. Ribenboim P., *Mała Księga Wielkich Liczb Pierwszych*, WN-T, Warszawa, 1997.

15. Stokłosa J., Bilski T., Pankowski T., *Bezpieczeństwo Danych w Systemach Infomatycznych*, PWN, Warszawa–Poznań, 2001.

16. Schneier B., *Kryptografia dla Praktyków. Protokoły, Algorytmy i Programy Źródłowe w Języku C*, wyd. II poprawione, WN-T, Warszawa, 2002.

17. Sobczyk K., Trębicki J., *Approximate probability distributions for stochastic systems: maximum entropy method*, Computer Methods in Applied Mechanics and Engineering, **168**, 91–111, 1999.

18. Sobczyk K., *Information dynamics; premises, challenges and results*, Mechanical Systems and Signal Processing, **15**, 3, 475–498, 2001.

19. Wobst R., *Kryptologia. Budowa i Łamanie Zabezpieczeń*, Wydawnictwo RM, Warszawa, 2002.