dr inż. Ewa Pośpiech
Katedra Matematyki, Wydział Zarządzania
Uniwersytet Ekonomiczny w Katowicach

Zastosowanie narzędzi ilościowych w zapewnianiu bezpieczeństwa e-informacji

WPROWADZENIE

Informacja rozumiana jako treść komunikatu lub dokumentu, polecenie (np. zapłaty), potwierdzenie transakcji, oferta, zamówienie, bazy danych (prywatne, jak i różnych instytucji) itp, przechowywana lub przekazywana zwłaszcza drogą elektroniczną (czyli e-informacja) wymaga właściwego zabezpieczenia przed nieuprawnionymi podmiotami. Przeprowadzanie różnych transakcji przez Internet zarówno o charakterze prywatnym, jak i między partnerami biznesowymi czy różnymi instytucjami (urzędami, bankami itp.) jest w obecnych czasach standardem, zatem problemy związane z zagadnieniami dotyczącymi bezpieczeństwa są szczególnie istotne. Bezpieczne przechowywanie informacji, jej wymiana, przeprowadzanie operacji w sieci możliwe jest dzięki współczesnej kryptografii, której podstawą są narzędzia ilościowe, zwłaszcza narzędzia (pojęcia) matematyczne oraz dynamicznie rozwijająca się technika komputerowa.

Celem artykułu jest zaprezentowanie wybranych zastosowań narzędzi matematycznych w zapewnianiu bezpieczeństwa danych i operacji przeprowadzanych w sieci oraz rozważenie pewnych aspektów z tym związanych. Podejmowane będą zagadnienia dotyczące tzw. podziału sekretu oraz zabezpieczania bazy danych.

WSPÓŁDZIELENIE SEKRETU

Współdzielenie (podział) sekretu to protokół kryptograficzny umożliwiający podzielenie pewnej informacji (klucza dostępu, sekretu) na części zwane udziałami, które rozdane zostają użytkownikom (udziałowcom). Każdy z udziałowców posiadający część sekretu nie jest w stanie na tej podstawie odtworzyć jego całości; odtworzenie sekretu jest możliwe tylko przez określoną uprawnioną (autoryzowaną) podgrupę udziałowców – podgrupa o mniejszej liczebności niż ustalona nie jest w stanie tego zrobić.

Celem tego protokołu jest zabezpieczenie informacji (klucza) przed nieupoważnionymi podmiotami, a także poprawienie niezawodności systemu bez

zwiększania ryzyka – dzielona kontrola zmniejsza bowiem ryzyko związane np. z utratą czy zniszczeniem klucza, a także zmniejsza ryzyko związane z wytworzeniem większej ilości kopii klucza[1].

Protokół podziału sekretu znajduje różne zastosowania[2]. Najczęściej wykorzystywany jest do zarządzania kluczami, zwłaszcza kluczami kryptograficznymi – zarządzanie kluczami kryptograficznymi ma na celu zapewnienie bezpieczeństwa np. różnego rodzaju e-transakcji. Innym z zastosowań protokołu współdzielenia sekretu jest szeroko rozumiana kontrola, która dotyczyć może np. spraw wagi państwowej (kontrola strategii zabezpieczeń systemu dowodzenia w państwie, kontrola nad dostępem do broni jądrowej, kontrola związana z wprowadzeniem sekretnego kodu, który aktywuje wystrzelenie pocisku); może być też związana z podejmowaniem ważnych decyzji w firmie lub w innych instytucjach. Wśród wielu innych możliwości zastosowania schematu podziału sekretu można także wyszczególnić uwierzytelnianie (potwierdzanie tożsamości) – poprzez odtworzenie sekretu (znanego udziałowcom) na podstawie jego składowych, udziałowcy potwierdzają swoją tożsamość.

Wobec wielu możliwości zastosowań protokołu dzielenia sekretu warto rozważyć pewne schematy i kwestie dotyczące tego zagadnienia.

Schemat progowy (*k*, *n*) Shamira

Schemat zaproponował Adi Shamir w 1979 roku. Podstawą konstrukcji tego schematu są wielomiany interpolacyjne Lagrange'a, definiowane nad ciałami skończonymi (np. $\mathbb{Z}_p$)[3]. Jednoznaczność istnienia odpowiedniego wielomianu gwarantowana jest odpowiednim twierdzeniem[4].

Twierdzenie 1. Istnieje dokładnie jeden wielomian W_n stopnia co najwyżej n-tego lub wielomian zerowy, który w punktach $x_0, x_1, ..., x_n$ przyjmuje wartości $y_0, y_1, ..., y_n$, czyli:

$$\bigvee_{i\in\{0,1,...,n\}} W_n(x_i) = y_i \tag{1}$$

Wielomian taki, zwany wielomianem interpolacyjnym Lagrange'a o węzłach $x_0, x_1, ..., x_n$, ma następującą postać

$$W_n(x) = \sum_{k=0}^{n} y_k \frac{(x-x_0)...(x-x_{k-1})(x-x_{k+1})...(x-x_n)}{(x_k-x_0)...(x_k-x_{k-1})(x_k-x_{k+1})...(x_k-x_n)} \tag{2}$$

[1] http://pl.wikipedia.org/wiki/Dzielenie_sekretu.

[2] K. Kulesza, P. Nowosielski, *Kiedy doskonały nie jest idealny, czyli matematyczne metody dzielenia sekretu*, „Matematyka stosowana" 7, 2006, s. 25–44.

[3] A.J. Buchmann, *Wprowadzenie do kryptografii*, Wydawnictwo Naukowe PWN, Warszawa 2006; K. Kulesza, P. Nowosielski, *Kiedy doskonały...*; A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Kryptografia stosowana*, WNT, Warszawa 2005; B. Schneider, *Kryptografia dla praktyków*, WNT, Warszawa 2002.

[4] W. Cheney, D. Kincaid, *Analiza numeryczna*, WNT, Warszawa 2006.

Schemat podziału sekretu s, $s \in \mathbb{Z}_p$ na n części jest następujący:

Wybierane i upubliczniane są różne, niezerowe elementy $x_i \in \mathbb{Z}_p$, i = 0, 1, …, n, gdzie p – liczba pierwsza oraz $p > n$. Wybierane są kolejne elementy: losowanych jest k – 1 elementów $a_j \in \mathbb{Z}_p$, j = 1, …, k – 1, gdzie $k < n$ (k jest tzw. progiem) i konstruowany jest wielomian stopnia co najwyżej k–1-ego postaci

$$a(x) = s + \sum_{j=1}^{k-1} a_j x^j \tag{3}$$

Sekret to wartość wielomianu modulo p w punkcie zero, czyli $s = a(0) \text{ MOD } p$.

Poszczególne fragmenty sekretu (udziały) s_i, i = 1, …, n, są wartościami wielomianu $a(x)$ modulo p w punktach x_i, i = 1, …, n, zatem

$$s_i = a(x_i) \text{ MOD } p \text{ , } i = 1, 2, \ldots, n. \tag{4}$$

Wyznaczone udziały przekazywane są n udziałowcom (każdemu przekazywany jest jeden udział). Chcąc odtworzyć sekret dowolnie wybrany podzbiór k udziałowców będzie posiadać k punktów o współrzędnych (x_i, s_i). Na podstawie twierdzenia 1, dla k węzłów istnieje dokładnie jeden wielomian stopnia co najwyżej k–1-ego, przyjmujący postać

$$a(x) = \sum_{i=1}^{k} s_i \prod_{j=1, j\neq i}^{k} \frac{x_j - x}{x_j - x_i} \tag{5}$$

Odtworzenie sekretu następuje poprzez wyznaczenie wartości wielomianu (5) modulo p w zerze, czyli

$$s = a(0) \text{MOD } p = \sum_{i=1}^{k} s_i \prod_{j=1, j\neq i}^{k} \frac{x_j}{x_j - x_i} \text{ MOD } p \tag{6}$$

Przykład 1

Informacja (sekret) dzielona jest na 5 części: s_1, s_2, s_3, s_4, s_5. Każdy udziałowiec otrzymuje jedną część sekretu. Sekret można odtworzyć, jeśli zestawione zostaną każde trzy jego części.

Ustalone są wartości n = 5 oraz k = 3, zatem rozważany jest schemat progowy Shamira (3, 5).

Niech p = 29, s = 23, a_1 = 12, a_2 = 9 oraz $x_i = i + 2$, i = 1, …, 5. Odpowiedni wielomian przyjmuje postać

$$a(x) = 23 + 12x + 9x^2.$$

Poszczególne fragmenty sekretu, liczone według wzoru (4), przyjmują wartości:

$$s_1 = a(x_1) \text{ MOD } 29 = 140 \text{ MOD } 29 = 24,$$

$$s_2 = a(x_2) \text{ MOD } 29 = 215 \text{ MOD } 29 = 12,$$
$$s_3 = a(x_3) \text{ MOD } 29 = 308 \text{ MOD } 29 = 18,$$
$$s_4 = a(x_4) \text{ MOD } 29 = 419 \text{ MOD } 29 = 13,$$
$$s_5 = a(x_5) \text{ MOD } 29 = 548 \text{ MOD } 29 = 26.$$

Trzej przykładowi udziałowcy sekretu P_1, P_2 i P_4 chcąc uzyskać sekret, obliczają

$$a(0) = 24 \cdot \frac{4}{1} \cdot \frac{6}{3} + 12 \cdot \left(\frac{3}{-1}\right) \cdot \frac{6}{2} + 13 \cdot \left(\frac{3}{-3}\right) \cdot \left(\frac{4}{-2}\right) = 110;$$

na podstawie wzoru (6) otrzymuje się wartość sekretu

$$s = a(0) \text{MOD } 29 = 110 \text{ MOD } 29 = 23.$$

Powyższy schemat progowy jest schematem doskonałym, co oznacza, że znajomość $k-1$ lub mniejszej ilości części sekretu nie powiększa zasobu informacji o sekrecie – dowolny, mniej liczny niż k-elementowy podzbiór udziałów ma taką samą wartość informacyjną. Jest to również schemat idealny, co oznacza, że wielkość każdego z udziałów jest taka sama jak wielkość całego sekretu[5].

Schemat Brickella

Schemat Brickella jest uogólnieniem schematu Shamira. Umożliwia on przyporządkowanie każdemu udziałowcowi jednej części sekretu, ale w odróżnieniu od schematu Shamira, pozwala na odtworzenie sekretu konkretnie ustalonym (różnolicznym) podgrupom udziałowców[6].

W metodzie Brickella każdemu z n udziałowców przyporządkowuje się t-wymiarowy wektor v_i, $i = 1, \ldots, n$, o elementach ze zbioru $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą, taki, że dla każdego autoryzowanego podzbioru udziałowców (dla uproszczenia niech będzie to wartość k) spełniona jest równość

$$(1,0,\ldots,0) = b_1 v_1 + b_2 v_2 + \ldots + b_k v_k = \sum_{i=1}^{k} b_i v_i \tag{7}$$

gdzie $b_i \in \mathbb{Z}_p$, $i = 1, 2, \ldots, k$.

Wektory v_i są publiczne. Wybierane są losowo wartości $a_1, \ldots, a_{t-1} \in \mathbb{Z}_p$ oraz określa się wektor $a = (a_0, a_1, \ldots, a_{t-1}) \in \mathbb{Z}_p^t$. Zachodzi $a_0 = (1, 0, \ldots, 0) \cdot a$ („·” jest mnożeniem skalarnym), gdzie a_0 jest wartością sekretu. Udziały s_i poszczególnych udziałowców są iloczynem skalarnym wektorów v_i oraz a, zatem $s_i = v_i \cdot a$, dla $i = 1, \ldots, n$. Dla każdego autoryzowanego podzbioru udziałowców wektor jednostkowy $e_1 = (1, 0, \ldots, 0) \in \mathbb{Z}_p^t$ można przedstawić jako liniową

[5] A.J.Menezes, P.C. van Oorschot, S.A. Vanstone, *Kryptografia…*.

[6] E.F. Brickell, *Some Ideal Secret Sharing Schemes*, „Journal of Combinatorial Mathematics and Comb. Computing” 6 (1989), s. 105-113; K. Kulesza, Nowosielski P., *Kiedy doskonały…*

kombinację wektorów v_i (jak wyżej). Mnożąc skalarnie obie strony powyższego równania przez wektor a uzyskuje się

$$(1,0,...,0) \cdot a = \sum_{i=1}^{k} b_i v_i \cdot a = \sum_{i=1}^{k} b_i s_i = a_0 \tag{8}$$

gdzie $b_i \in \mathbb{Z}_p$, $i = 1, 2, \ldots, k$, co daje wartość sekretu a_0. Obliczenia wykonywane są na ciałem $\mathbb{Z}_p$.

Przykład 2

Sekret został podzielony na pięć części. Autoryzowany zbiór udziałowców sekretu to zbiór $\Gamma = \{\{P_1, P_2, P_4\}, \{P_3, P_5\}\}$. Niech wektory v_i, $i = 1, \ldots, 5$, przyjmują postać

$$v_1 = (1, 1, 0, 0),\ v_2 = (0, 1, 1, 0),\ v_3 = (1, 1, 0, 1),$$
$$v_4 = (0, 0, 1, 0),\ v_5 = (0, 1, 0, 1).$$

Dla podzbioru $\{P_1, P_2, P_4\}$ wektor jednostkowy $e_1 = (1, 0, 0, 0)$ jest następującą liniową kombinacją wektorów v_1, v_2, v_4

$$(1, 0, 0, 0) = v_1 - v_2 + v_4,$$

natomiast dla podzbioru $\{P_3, P_5\}$, kombinacja ta jest postaci

$$(1, 0, 0, 0) = v_3 - v_5.$$

Wektora (1, 0, 0, 0) nie można wyrazić jako kombinacji liniowej wektorów innych niż już uwzględnione.

Niech dalej wektor a przyjmuje postać: $a = (17, 9, 5, 24) \in \mathbb{Z}_{29}^4$. Wynika z tego, że sekretem jest $s = a_0 = 17$. Poszczególne części sekretu liczone według wzoru $s_i = v_i \cdot a$, dla $i = 1, \ldots, 5$, przyjmują następujące wartości

$$s_1 = v_1 \cdot a = (1, 1, 0, 0) \cdot (17, 9, 5, 24) = 26,$$
$$s_2 = v_2 \cdot a = (0, 1, 1, 0) \cdot (17, 9, 5, 24) = 14,$$
$$s_3 = v_3 \cdot a = (1, 1, 0, 1) \cdot (17, 9, 5, 24) = 50 \equiv 21 \pmod{29},$$
$$s_4 = v_4 \cdot a = (0, 0, 1, 0) \cdot (17, 9, 5, 24) = 5,$$
$$s_5 = v_5 \cdot a = (0, 1, 0, 1) \cdot (17, 9, 5, 24) = 33 \equiv 4 \pmod{29}.$$

Rozważając przykładowo podzbiór $\{P_1, P_2, P_4\}$ odtworzenie sekretu dokonuje się poprzez wykonanie obliczeń

$$a_0 = b_1 s_1 + b_2 s_2 + b_4 s_4 = s_1 - s_2 + s_4 = 26 - 14 + 5 = 17,$$

co daje wartość sekretu.

Powyższy schemat także jest doskonały – znajomość tych części sekretu, które nie tworzą autoryzowanego podzbioru nie dostarcza żadnej dodatkowej wiedzy o sekrecie. Schemat ten jest również idealny.

Zaprezentowany w punkcie 1.1 schemat Shamira jest jednym z podstawowych algorytmów dzielenia sekretu; wśród podstawowych można też wymienić np. modularny schemat progowy czy schemat progowy Blakleya. Istnieje rów-

nież wiele schematów współdzielenia sekretu będących uogólnieniami lub rozszerzeniami powyższych; potrzeba ich tworzenia pojawia się w związku z praktycznymi wymaganiami. Takim uogólnieniem jest np. zaprezentowany schemat Brickella, który jednak posiada pewne ograniczenia – w pewnych przypadkach podział sekretu za pomocą schematu Brickella może nie być możliwy. Wśród schematów o rozszerzonych możliwościach można wskazać np. dynamiczne schematy współdzielenia sekretu, wielosektorowe schematy progowe, współdzielenie sekretu z weryfikacją, współdzielenie sekretu z wykluczeniem itp.[7]

ZABEZPIECZANIE BAZ DANYCH

Ze względu na powszechną informatyzację wiele podmiotów wykorzystuje (tworzy i zarządza nimi) komputerowe bazy danych. Są to zbiory informacji, zapisane w określony sposób i „wyposażone" w system zarządzania – program gromadzący i przetwarzający zebrane dane[8].

Dostęp do zgromadzonych danych np. jakiejś firmy czy instytucji, nie może być powszechny nawet dla podmiotów danej jednostki; pewne podmioty powinny mieć dostęp do niektórych części bazy danych (np. dział reklamy danej firmy do wysokości jej zysków), a do niektórych części ten dostęp powinien być zabroniony (np. dział reklamy firmy do danych personalnych jej pracowników).

Aby umożliwić dostęp do wybranych fragmentów bazy danych niektórym podmiotom, należy tak tę bazę zabezpieczyć, by zainteresowany podmiot dysponując udostępnionym kluczem potrafił odczytać (odtajnić) żądaną część bazy, zaś reszta danych powinna pozostać tajna.

Szyfrowana powinna być zatem cała baza danych, a odtajnienie jednej jej części powinno pozostawić tajnymi pozostałe. Schemat umożliwiający takie działanie[9] wykorzystuje zagadnienia związane z rozwiązywaniem układu kongruencji[10].

Niech baza danych B składa się z n części (plików) P_i, $i = 1, 2, \ldots, n$. Można przyjąć, że każdy plik bazy B, czyli każda część P_i, jest liczbą całkowitą. Aby zaszyfrować bazę B, należy wybrać n liczb pierwszych $m_1, m_2, \ldots, m_n$, dla których zachodzą nierówności $m_i > P_i$, $i = 1, 2, \ldots, n$.

[7] K. Kulesza, P. Nowosielski, *Kiedy doskonały…*; A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Kryptografia…*

[8] http://pl.wikipedia.org/wiki/Baza_danych.

[9] Y. Yan Song, *Teoria liczb w informatyce*, Wydawnictwo Naukowe PWN, Warszawa 2006.

[10] *Ibidem*; K.A. Ross, C.R.B. Wright, *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa 2003; Y. Yan Song, *Teoria liczb…*

Bazę B można zaszyfrować rozwiązując układ kongruencji postaci

$$\begin{cases} S \equiv P_1 \pmod{m_1} \\ S \equiv P_2 \pmod{m_2} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ S \equiv P_n \pmod{m_n} \end{cases} \tag{9}$$

gdzie S oznacza zaszyfrowaną bazę B.

Istnienie rozwiązania powyższego układu kongruencji gwarantuje chińskie twierdzenie o resztach.

Twierdzenie 2. (Chińskie twierdzenie o resztach). Jeżeli liczby naturalne n_1, n_2, …, n_r są parami względnie pierwsze, to dla dowolnie zadanych liczb całkowitych a_1, a_2, …, a_r układ kongruencji

$$x \equiv a_i \pmod{n_i}\ i = 1, 2, \ldots, r, \tag{10}$$

ma rozwiązanie. Jeśli x_1, x_2 są dwoma rozwiązaniami tego układu, to

$$x_1 \equiv x_2 \pmod{n_1 n_2 \ldots n_r}.$$

Przyjmując następujące oznaczenia

$$\begin{cases} N = m_1 m_2 \ldots m_n \\ N_i = \dfrac{N}{m_i}, \\ k_i = N_i N'_i, \quad i = 1, 2, \ldots, n, \end{cases} \tag{11}$$

gdzie: $N'_i = N_i^{-1} \mathrm{MOD} m_i$ – element odwrotny do N_i modulo m_i, można obliczyć wartość S według wzoru[11]

$$S \equiv \sum_{i=1}^{n} k_i P_i \pmod{N},\ 0 \le S < N. \tag{12}$$

Liczby całkowite k_i, $i = 1, 2, \ldots, n$, nazywane są kluczami piszącymi, natomiast wartości m_i, $i = 1, 2, \ldots, n$, to klucze do odczytu. Posiadający klucz m_i może z zaszyfrowanej bazy danych S odtworzyć tylko plik P_i. Wartość P_i uzyskuje się poprzez rozwiązanie kongruencji

$$P_i \equiv S \pmod{m_i}, \quad 0 \le P_i < m_i \tag{13}$$

Przykład 3

Niech baza danych składa się z pięciu plików (rekordów):

$$B = (P_1, P_2, P_3, P_4, P_5) = (28, 12, 18, 34, 7).$$

Wybierane są klucze odczytujące m_1, m_2, m_3, m_4, m_5, będące liczbami pierwszymi i takie, że $m_i > P_i$, $i = 1, 2, \ldots, 5$. Niech

$$m_1 = 29, \quad m_2 = 17, \quad m_3 = 23, \quad m_4 = 41, \quad m_5 = 11.$$

[11] Y. Yan Song, *Teoria liczb…*

Uzyskanie zaszyfrowanej bazy wymaga rozwiązania układu kongruencji

$$\begin{cases} S \equiv 28 \pmod{29} \\ S \equiv 12 \pmod{17} \\ S \equiv 18 \pmod{23} \\ S \equiv 34 \pmod{41} \\ S \equiv 7 \pmod{11} \end{cases}$$

Elementy, których znajomość do rozwiązania układu kongruencji jest niezbędna, liczone są według wzorów (11). Uzyskuje się następujące wartości

$$N = 5113889,$$

$$N_1 = 176341 \quad \Rightarrow \quad N'_1 = 18, \qquad k_1 = 3174138,$$

$$N_2 = 300817 \quad \Rightarrow \quad N'_2 = 9, \qquad k_2 = 2707353,$$

$$N_3 = 222343 \quad \Rightarrow \quad N'_3 = 12, \qquad k_3 = 268116,$$

$$N_4 = 124729 \quad \Rightarrow \quad N'_4 = 6, \qquad k_4 = 748374,$$

$$N_5 = 464899 \quad \Rightarrow \quad N'_5 = 2, \qquad k_5 = 929798.$$

Zaszyfrowana baza to wartość (na podstawie wzoru (12))

$$S \equiv 201343490 \pmod{5113889},$$

która w zbiorze $\mathbb{Z}_{5113889}$ jest równa

$$S = 1901819.$$

Znając wartość sekretu S i dysponując którymś z kluczy np. $m_3 = 23$ można odszyfrować plik P_3.

Oblicza się (według wzoru (13))

$$P_3 \equiv 1901819 \pmod{23}, \quad 0 \le P_3 < 23,$$

co faktycznie daje $P_3 = 18$.

PODSUMOWANIE

Operacje przeprowadzane wirtualnie (od komunikowania się, poprzez gromadzenie i zarządzanie danymi, zakupy internetowe, bankowość elektroniczną, po działalność e-urzędów) cechuje wysokie ryzyko. Dlatego też bezpieczeństwo tych działań i transakcji jest rzeczą priorytetową. Zastosowanie narzędzi gwarantujących wysoki poziom bezpieczeństwa operacji wykorzystujących technikę komputerową jest więc niezbędne i stale szuka się nowych koncepcji praktycznych zastosowań różnych pojęć i zagadnień.

Zasady dotyczące zarządzania bazami danych, ochrony zawartych w nich informacji, udostępniania niektórych informacji są regulowane prawnie. Podobnie w przypadku dzielenia sekretu – określanie autoryzowanych podgrup udziałowców jest najczęściej ustalane odgórnie. Nie można jednak współcześnie efek-

tywnie zarządzać tymi informacjami, a właściwie – e-informacjami (skoro jest to informacja bądź przechowywana, bądź przekazywana za pomocą techniki komputerowej) bez wykorzystywania metod i narzędzi ilościowych.

W artykule zaprezentowano wybrane narzędzia kryptograficzne (wykorzystujące pojęcia teorii liczb, algebry liniowej, algebry abstrakcyjnej, elementy metod numerycznych oraz teorii informacji), których zadaniem jest ochrona sekretu, klucza zabezpieczającego informację, bazy danych itp. przed niepożądanymi podmiotami; taka ochrona oznacza również poprawę niezawodności systemu i minimalizowanie ryzyka związanego z bezpiecznym działaniem danego systemu.

Rozpatrywane schematy ukazują możliwości zastosowań narzędzi ilościowych (matematycznych) w protokołach kryptograficznych, których głównym zadaniem jest ochrona szeroko rozumianej e-informacji. Rola, jaką odgrywają te narzędzia, metody, algorytmy w zapewnianiu bezpieczeństwa jest znacząca, a możliwości znajdowania nowych zastosowań – ogromne.

LITERATURA

Brickell E.F., *Some Ideal Secret Sharing Schemes*, Journal of Combinatorial Mathematics and Comb. „Computing" 6 (1989).

Buchmann A.J., *Wprowadzenie do kryptografii*, Wydawnictwo Naukowe PWN, Warszawa 2006.

Cheney W., Kincaid D., *Analiza numeryczna*, WNT, Warszawa 2006.

Kulesza K., Nowosielski P., *Kiedy doskonały nie jest idealny, czyli matematyczne metody dzielenia sekretu*, „Matematyka stosowana" 7, 2006.

Menezes A.J., van Oorschot P.C., Vanstone S.A., *Kryptografia stosowana*, WNT, Warszawa 2005.

Narkiewicz W., *Teoria liczb*, Wydawnictwo Naukowe PWN, Warszawa 2003.

Ross K.A., Wright C.R.B., *Matematyka dyskretna*, Wydawnictwo Naukowe PWN, Warszawa 2003.

Schneider B., *Kryptografia dla praktyków*, WNT, Warszawa 2002.

Song Y. Yan, *Teoria liczb w informatyce*, Wydawnictwo Naukowe PWN, Warszawa 2006.

źródło internetowe: http://pl.wikipedia.org/wiki/Baza_danych.

źródło internetowe: http://pl.wikipedia.org/wiki/Dzielenie_sekretu.

Streszczenie

Informacja rozumiana jako tekst dokumentu, treść komunikatu, polecenie (np. zapłaty), transakcja i jej potwierdzenie, oferta, zamówienie, baza danych itp. przekazywana drogą elektroniczną oraz przechowywana i zarządzana za pomocą sprzętu komputerowego (zatem określana

może być jako e-informacja) wymaga właściwego zabezpieczenia przed nieuprawnionymi podmiotami. Komunikowanie się, przeprowadzanie transakcji, wymiana danych itp. przez Internet czy to prywatnie, czy między partnerami biznesowymi, urzędami, bankami itp. jest w obecnych czasach standardem, zatem problemy związane z zagadnieniami dotyczącymi bezpieczeństwa są nader aktualne i szczególnie istotne. Bezpieczne przesyłanie i zarządzanie informacjami jest możliwe dzięki zastosowaniu narzędzi ilościowych, zwłaszcza narzędzi (pojęć, metod, algorytmów, technik) matematycznych oraz dynamicznie rozwijającej się technice komputerowej.

W artykule zaprezentowane zostały pewne zastosowania wybranych narzędzi matematycznych (pojęć teorii liczb, algebry liniowej, algebry abstrakcyjnej, elementów metod numerycznych oraz teorii informacji) do zapewniania bezpieczeństwa różnego rodzaju operacji dokonywanych w sieci. Przedstawiono wybrane schematy współdzielenia sekretu (progowy schemat Shamira i schemat Brickella), które m.in. mogą być wykorzystywane do zarządzania kluczami kryptograficznymi, do szeroko pojętej kontroli, czy do uwierzytelniania. Ponadto zaprezentowano algorytm do zabezpieczania baz danych, których powszechne wykorzystywanie zarówno przez użytkowników prywatnych, jak i różnego rodzaju instytucje wymaga odpowiedniej ochrony.

Applications of Quantitative Tools in Protecting e-Information

Summary

Information considered as a document or message text, order (for example payment order), transaction and its confirmation, offer, database etc. virtually transmitted or stored using computer equipment (that is why called e-information) requires proper protection against unauthorized objects. Internet communication, transactions, exchange of information between private users or business partners, offices, banks etc. is nowadays very common, that is why the problems connected with security of these operations are of crucial importance. To give security of information while sending or in database management is possible thanks to using quantitative tools, especially mathematical ones (terms, methods, algorithms, techniques) and dynamic development of computer technique.

The article presents some applications of chosen mathematical tools (such as elements of number theory, linear algebra, abstract algebra, numerical methods and information theory) to secure different types of operations settled over the net. Some schemes of secret sharing (Shamir's scheme and Brickell's one) were presented; they are used (among others things) to cryptographic keys management, to control different operations, to authentication. Besides, an algorithm to secure database was presented – the commonly used way of data storage requires proper protection.