PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1096 — 2005
Ekonometria 15

Jacek Juzwiszyn, Andrzej Wilkowski

KRYPTOGRAFIA DYNAMICZNA

1. Kryptologia jest nauką o bezpiecznych sposobach przekazywania i przechowywania informacji. W niniejszej prazy przez kryptosystem będziemy rozumieli odwzorowanie, które jednostkom tekstu jawnego (pojedynczym literom, grupom liter lub innym znakom) przyporządkowuje jednostki tekstu zakodowanego – jednostki szyfrogramu.

Najprostszym kryptosystemem jest dodawanie modulo N, gdzie N jest liczbą liter danego alfabetu. W przypadku tzw. szyfru Cezara każdą literę alfabetu łacińskiego zastępowano literą o trzy pozycję dalszą. Innymi słowy, szyfrowanie odbywało się z pomocą wzoru

$$A \equiv B + 3 \pmod{26},$$

gdzie A oznacza jednostkę szyfrogramu, B – jednostkę tekstu jawnego.

W tym systemie kluczem szyfrowania jest liczba 3. Widać, że ten i podobne kryptosystemy bardzo łatwo złamać (tzn. odczytać szyfrogram, nie znając sposobu kodowania – klucza szyfrującego).

W wieku XVI francuski kryptograf B. Vigenere podał trudniejszą do złamania wersję kryptosystemu rzymskiego. W jego metodzie jednostkami tekstu jawnego są bloki złożone z k liter (inaczej mówiąc, wektory długości k nad Z/NZ). Następnie każdy blok jest przesuwany o pewne „słowo kodowe" także długości k. Innymi słowy, funkcja kodująca była po prostu przesunięciem w $(Z/NZ)^k$ o ustalony wektor. Wynika z tego, że kolejny znak szyfrogramu zależy nie tylko od odpowiadającego mu znaku tekstu jawnego, ale także od miejsca, w którym się ono znajduje (w tekście jawnym). Kryptosystem ten złamano w latach siedemdziesiątych XIX w. W latach trzydziestych L.S. Hill zauważył, że odwzorowanie z $(Z/NZ)^k$ do $(Z/NZ)^k$ zadane macierzą odwracalną o współczynnikach z Z/NZ powinno być bezpieczniejsze niż powyższy kryptosystem. Okazało się jednak, że również system Hilla można złamać.

2. W opisanych przykładach kryptosystemów szyfrowanie odbywało się za pomocą klucza prywatnego. Oznacza to, że ten, kto potrafi zakodować wiadomość, może ją również odczytać. Para użytkowników systemu musi zatem w sposób poufny przekazać sobie klucze szyfrujące. W latach siedemdziesiątych zaczęły powstawać kryptosystemy z kluczem publicznym. Praktyczne ich wykorzystanie było możliwe dzięki pojawieniu się coraz szybszych komputerów, chociaż aparat matematyczny znany był już w XVII w. [Koblitz 2000; Menezes i in. 1996].

W kryptosystemach z kluczem publicznym znajomość sposobu kodowania nie wystarczy do odczytania wiadomości (chyba, że uda się złamać system). Aby rozszyfrować meldunek należy znać poufny klucz prywatny. Innymi słowy, każdy wie, jak zakodować wiadomość, a tylko niektórzy potrafią ją rozkodować. W systemach z kluczem publicznym nie ma potrzeby żadnego tajnego porozumienia miedzy nadawcą a odbiorcą. Nawet nie muszą się oni wcześniej znać. Punktem wyjścia do tworzenia takich kryptosystemów są funkcje jednokierunkowe [Kutyłowski, Bstrothmann 1999].

Funkcja $f: X \to Y$ jest w praktyce jednokierunkowa, jeśli dla danego y nie jest praktycznie możliwe znalezienie takiego x, że $f(x) = y$.

Definicja. Funkcja $f: \{0,1\}^n \to \{0,1\}^n$ nazywana jest funkcją jednokierunkową, jeśli:

- dla każdego x, przedstawienia w postaci binarnej liczb x i $f(x)$ mają długość tego samego rzędu (zatem $f(x) = 2^x$ nie jest jednokierunkowa),
- $f(x)$ jest łatwe do obliczenia (np. w czasie wielomianowym w stosunku do długości x),
- funkcja f jest trudna do odwrócenia.

W języku teorii algorytmów można to sprecyzować jak następuje:

niech $Prob(Z)$ oznacza prawdopodobieństwo zajścia zdarzenia Z.

Dla każdego zrandomizowanego algorytmu A i każdego wielomianu p istnieje stała $L(p)$, taka że dla $n > L(p)$:

$$Prob\big(f\big(A(z)\big) = z\big) < 1/p(n),$$

gdzie z jest zmienną losową z rozkładem jednostajnym na zbiorze $\left\{f(x): x \in \{0,1\}^n\right\}$.

Nie wykluczamy tutaj, że $f\big(A(z)\big) = z$. Jednak prawdopodobieństwo tego zdarzenia jest zaniedbywalanie małe. Możliwe jest także, że dla pewnych specjalnych ciągów z znalezienie y o własności $f(y) = z$ jest łatwe. Jednak gdy z jest wybrany losowo i ma odpowiednią długość, zadanie jest praktycznie niewykonalne, bo żaden efektywny algorytm nie daje właściwej odpowiedzi. W tym miejscu należy zaznaczyć, że w przypadku konkretnych funkcji nie są obecnie znane szybkie metody ich odwracania (w sensie teorii algorytmów). Nie ma jednak dowodu, że takie algorytmy nie istnieją. Do dziś także nie udowodniono w stosunku do żadnej

funkcji, że jest funkcją jednokierunkową. Przypuszcza się tylko, że pewne funkcje posiadają tę własność.

Jednokierunkowość w praktyce oznacza, że żadna realizowalna metoda nie jest w stanie wyliczyć dla danego z wartości x, takich że $f(y) = z$, poza pewną drobną liczbą wyjątkowych wartości z. Jeden z bardziej rozpowszechnionych algorytmów asymetrycznych został opracowany w 1977 r. przez R. Rivesta, A. Shamira, L. Adlemana. Do konstrukcji kryptosystemu RSA wykorzystano funkcję

$$f_{e,n}(y) = x^e \pmod{n},$$

gdzie: $n = pq$, p, q – liczby pierwsze,

e – liczba względnie pierwsza z $(p-1)(q-1)$.

Trudność odwrócenia tej funkcji polega na tym, że nie jest łatwo znaleźć rozkład na czynniki pierwsze liczby kilkusetcyfrowej. Odwrócenie funkcji f staje się łatwe, o ile podane są wartości p i q. Inna funkcja pojawiła się przy opracowaniu w 1991 r. standardu podpisu cyfrowego w USA przez rządową agendę do spraw standardów technicznych – *National Institute of Staudards and Technology* [Miśkiewicz 2002; Wilkowski 2001].

NITS jako podstawę podpisu cyfrowego wybrał problem logarytmu dyskretnego w ciele prostym F_p. Związana z tym jest funkcja:

$$f(x, g, p) = g^x \pmod{p},$$

gdzie p jest liczbą pierwszą.

Na bazie m.in. algorytmu RSA w 1993 r. opracowano pakiet szyfrujący *Pretty Good Privacy*. Jego twórcą jest P. Zimmermann [Singh 2001]. Jest to powszechnie dostępny, darmowy kryptosystem, możliwy do stosowania przez indywidualnych użytkowników (wystarczy posiadać zwykły komputer osobisty). Można go znaleźć pod adresem internetowym: http://www.pgpi.com/. Funkcje jednokierunkowe służą także do konstrukcji funkcji skrótu oraz generatorów pseudolosowych ciągów bitów.

3. Nowym podejściem do kodowania wydaje się być szyfrowanie dynamiczne. Dotychczas każdy używany kryptosystem miał m.in.: tabelę przyporządkowania i stały tajny klucz wymagający tworzenia, ochrony, przechowywania, przesyłania, a całością kierował człowiek (obowiązuje to także w systemach typu RSA).

Metoda ZT-UNITAKOD [Topolewski 2002] jest propozycją szyfrowania dynamicznego. Nie obowiązują w niej powyższe reguły. Nie ma tabeli przyporządkowania (każdy znak przyjmuje losowo jedną z 256 możliwych postaci, za każdym razem inną) ani stałego tajnego klucza. Ograniczona została również decydująca rola człowieka w systemie ochrony informacji. Jest ona oparta wyłącznie na generatorach permutacji oraz modelach matematycznych tworzących jednarozowy klucz dynamiczny. Wynika z tego, że szyfr zmienia się wraz ze zmianą daty i czasu (w praktyce co 1 sekundę). Metoda ta chroniona jest patentem w USA

(nr 08/775,253-SYSTEM AND METHOD ZT-UNITAKOD FOR ENCRYPTING AND DECRYPTING DATA). Informacje o niej można znaleźć pod adresem www.perfect-crypt.pl.

Model matematyczny szyfru:

$$\text{Szyfr} = \mathbf{A} + \mathbf{B} \pmod{256},$$

gdzie: **A** – tablica kryptograficzna, jednorazowy klucz dynamiczny (jest to macierz o 256 wierszach i 256 kolumnach zmieniająca się wraz ze zmianą czasu),

B – przesyłana informacja jawna.

Model matematyczny deszyfracji:

$$\mathbf{B} = \mathbf{S} - \mathbf{A} \pmod{256}, \text{ dla } \mathbf{S} - \mathbf{A} \geq \mathbf{0},$$

$$\mathbf{B} = (\mathbf{S} - \mathbf{A}) + 256 \pmod{256}, \text{ dla } \mathbf{S} - \mathbf{A} \leq \mathbf{0}.$$

Do utworzenia tablicy kryptograficznej **A** metoda wykorzystuje dwa generatory permutacji:

– generator multiplikatywny

$$G_1 = cx_i \pmod{256},$$

gdzie c to liczby nieparzyste od 3 do 255,

– generator mieszany:

$$G_2 = ax_i + b \pmod{256},$$

gdzie a to liczby nieparzyste od 1 do 255 spełniające równanie $a = 1 \pmod 4$, b to liczby nieparzyste od 1 do 255.

Tablica kryptograficzna ma 256 wierszy. W każdym wierszu i w każdej kolumnie jest 256 znaków. Razem tablica **A** składa się z 65 536 bajtów. Liczba możliwych permutacji wynosi:

$$(256!)^{256}.$$

Taka jest potencjalna moc kryptosystemów opartych na metodzie ZT-UNITAKOD (o wiele większa niż wszystkich obecnie stosowanych systemów typu RSA).

Obecnie oprogramowane są kryptosystemy Hades i TMULTRA (Seed) bazujące na tej metodzie. Trwają prace (z udziałem m.in. autorów niniejszego artykułu) nad algorytmem ULTRA (z powtórzeniami). Ich celem jest zwiększenie mocy kryptosystemu i zastosowanie do zabezpieczania baz danych (obecnie jedynym zabezpieczeniem są hasła). Efektem powinno być gotowe oprogramowanie możliwe do zastosowania przez konkretnego użytkownika. Wydaje się, że do przesyłania oprogramowania kryptosystemów opartych na metodzie ZT-UNITAKOD w sieciach należy psługiwać się powszechnie dostępnymi algorytmami typu RSA, wystarczy nawet pakiet PGP. Kodowanie dynamiczne jest optymalnym rozwiązaniem

w przesyłaniu ważnych informacji między niewielką liczbą użytkowników (wyżsi urzędnicy, prezesi banków, w dyplomacji czy wojskowości) oraz szyfrowania baz danych. Należy przypuszczać, że metody oparte na kodowaniu dynamicznym łącznie z kryptosystemami bazującymi na funkcjach jednokierunkowych będą coraz bardziej rozwijane i rozpowszechniane.

Literatura

Koblitz N. (1995), *Wykład z teorii liczb i kryptografii*, Wydawnictwo Naukowo-Techniczne, Warszawa.
Koblitz N. (2000), *Algebraiczne aspekty kryptografii*, Wydawnictwo Naukowo-Techniczne, Warszawa.
Kutyłowski M., Bstrothmann W. (1999), *Kryptografia. Teoria i praktyka zabezpieczenia systemów komputerowych*, Oficyna Wydawnicza Read Me, Warszawa.
Menezes, Oorschot P., Vaustone S. (1996), *Handbook of Applied Cryptography*, CRC Press.
Miśkiewicz M. (2002), *Krzywe eliptyczne a podpis cyfrowy*, AE, Katowice (w druku).
Singh S. (2001), *Księga szyfrów*, Wydawnictwo Albatros A. Kuryłowicz, Warszawa.
Topolewski Z. (2002), *Komputerowe zabezpieczenie poufności informacji w zarządzaniu*, Wydawnictwo Continuo, Wrocław.
Wilkowski A. (2001), *Kryptologia a podpis cyfrowy*, Dydaktyka Matematyki 2, AE, Wrocław.

DYNAMIC CRYPTOGRAPHY

Summary

The work refers utilizations of methods of the dynamic cryptography to the protection of the information. In the article given is the method ZT-UNITAKOD, making possible the creation of dynamic cryptosystems. Authors propose the also joint use from leaning methods on coding dynamic along with cryptosystems of the type RSA.

Dr Jacek Juzwiszyn i **dr Andrzej Wilkowski** są pracownikami Katedry Matematyki i Cybernetyki Akademii Ekonomicznej we Wrocławiu.