ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1996

Seria: INFORMATYKA z. 30 Nr kol. 1315

Andrzej NOWAK

SYSTEMY KRYPTOGRAFICZNE W INFORMATYCE

Streszczenie. Publikacja jest komunikatem do pracy na temat systemów kryptograficznych w informatyce, a w szczególności opracowania software'owego szyfratora pracującego w systemie prywatnym wg algorytmu DES.

THE CRYPTOGRAPHIC SYSTEMS

Summary. The publication is a communique on the subject of cryptographic systems, particulary cryptographic algorithms which work like the private key systems. There is paying attention to the DES encryption scheme later in this publication.

DIE ARBAITSTHEMA VON DATENCODIERUNG

Zusammenfassung. Die Publikation ist ein Comunique zum Arbaitsthema von Datencodierung und insbesondere von Chiffrieren-Dechiffrieren Algorithmus, die in einen öffentlichen Codierungsystem arbeiten. Der Zweck der ist, eine Lösung in der Form von Impulsgebersoftware, der nach dem DES-Algorithmus arbeitet, zu finden.

1. Cel i zakres pracy

Prezentowane w niniejszej publikacji zagadnienia są wstępem do prowadzonych przez autora prac nad znalezieniem software'owego rozwiązania szyfratora, pracującego w systemie

kryptografii prywatnej. Niniejsza publikacja jest pierwszą pracą autora dotyczącą systemów kryptograficznych oraz jedyną z tej dziedziny, podjętą w Filii Politechniki Łódzkiej w Bielsku-Białej. Zakres pracy można wstępnie podzielić na trzy fazy, tj.: opracowanie i uruchomienie oprogramowania szyfratora konwencjonalnego, działającego wg algorytmu DES (lub do niego zbliżonego) , analizę poprawności jego działania oraz wykorzystanie tegoż szyfratora jako narzędzia i zarazem obiektu badań w jego zastosowaniu do konkretnych typów aplikacji. Szczególnie istotna będzie trzecia faza pracy, gdyż pozwoli stwierdzić czy, i do jakiego typu aplikacji byłoby w praktyce możliwe zastosowanie szyfratora sofware'owego.

Celem pracy jest stworzenie software'owego szyfratora na tyle szybkiego, aby można go było stosować w praktyce. Autor zdaje sobie sprawę z faktu, że szyfrator software'owy nie jest w stanie pracować z szybkością szyfratora hardware'owego, ale jest przekonany, że jego zastosowanie do ochrony danych użytkowników indywidualnych w określonych aplikacjach może być bardziej korzystne ekonomicznie i prostsze technicznie.

2. Systemy kryptograficzne

Rozwój systemów informatycznych, a szczególnie ich masowe zastosowanie do magazynowania i transmisji informacji w takich m.in. dziedzinach, jak bankowość, handel czy przemysł uwypukliły problem ochrony zasobów banków danych oraz konieczność zabezpieczania procesów telekomunikacyjnych.

Jednym z elementów ochronnych są środki techniczne, wśród których istotnie ważne są zabezpieczenia kryptograficzne. Kryptografia jest znana co najmniej tak długo, jak polityka czy korespondencja - systemy kryptograficzne były stosowane już w starożytności. Przed współczesną kryptografią stawia się przede wszystkim zadania ochrony danych przechowywanych w systemach komputerowych lub przesyłanych liniami telekomunikacyjnymi, a stopień ich bezpieczeństwa jest uzależniony od zabezpieczenia przed ujawnieniem, modyfikacją lub zniszczeniem.

Kryptografia obejmuje metody tworzenia kryptogramów, tzn. wiadomości tajnych dla wszystkich, oprócz tych osób, które posiadają narzędzie zezwalające na uzyskanie kodu źródłowego.

Proces tworzenia kryptogramów nazywa się szyfrowaniem, a algorytmy szyfrowania (szyfry) uzyskuje się w urządzeniach szyfrujących, zwanych szyfratorami. Tekst jawny uzyskuje się wskutek deszyfrowania kryptogramu.

Skuteczność szyfrowania zależy w sposób istotny od klucza szyfrującego i klucza deszyfrującego.

W zależności od sposobu dostępności kluczy szyfrujących i deszyfrujących można wyróżnić (wg [13]) dwa typy systemów kryptograficznych:

- systemy prywatne,
- systemy publiczne.

Podstawy teoretyczne systemów prywatnych powstały na podstawie opracowanej w końcu lat czterdziestych bieżącego stulecia, przez C.E. Shanona, teorii bezpiecznych systemów prywatnych [11], rozwiniętej później przez M.E. Hellmana [7]. Systemy prywatne wyróżnia fakt, że klucz szyfrujący jest zarazem kluczem deszyfrującym.

Wśród najczęściej obecnie stosowanych algorytmów szyfrująco-deszyfrujących, pracujących w systemie prywatnym, są: opracowany w 1977 roku w laboratoriach firmy IBM szyfr DES [3] (z 64-bitowym kluczem) oraz występujący w dwóch wersjach szyfr FEAL [9] (FEAL-N z 64-bitowym kluczem i FEAL-NX z 128-bitowym kluczem).

Systemy publiczne, których wynalezienie datuje się na połowę lat siedemdziesiątych XX wieku, charakteryzują się tym, że klucz szyfrujący i klucz deszyfrujący są różne oraz że klucz szyfrujący jest ogólnie dostępny, natomiast klucz deszyfrujący posiadają wyłącznie osoby upoważnione. Oznacza to, że zaszyfrować informację jawną może każdy, ale deszyfrować kryptogram może tylko ten, kto posiada klucz deszyfrujący.

Badania nad algorytmami kryptografii publicznej rozpoczął w początkach lat 80. J. Grollman [6]. Bezpieczeństwo systemów publicznych jest uzależnione od złożoności obliczeniowej algorytmów i badania nad nimi trwają do chwili obecnej.

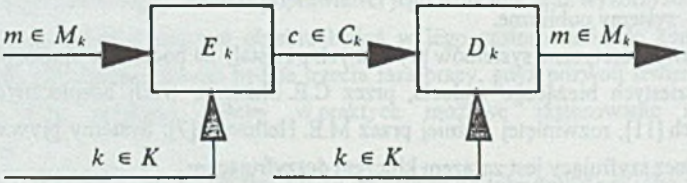
Wśród algorytmów publicznych wyróżnia się szyfry blokowe, jak np. RSA [10] oraz szyfry strymieniowe.

Szyfry strumieniowe stosują generatory kluczy, które w praktyce są generatorami ciągów pseudolosowych klasy statystycznie losowej, strukturalnie losowej lub algorytmicznie losowej.

3. Prywatne systemy kryptograficzne

Prywatne systemy kryptograficzne, zwane też klasycznymi bądź konwencjonalnymi, należą do klasy systemów o ograniczonym zasięgu. Wynika to z faktu, że kodować informację może tylko ten, kto posiada klucz szyfrujący i analogicznie, dekodować może tylko osoba posiadająca klucz deszyfrujący.

System prywatny składa się ze zbioru kluczy K takiego, że dla każdego $k \in K$ istnieje zbiór wiadomości jawnych M_k i zbiór wiadomości zaszyfrowanych C_k oraz para funkcji $E_k: M_k \to C_k$ i $D_k: C_k \to M_k$ takich, że $D_k(E_k(m)) = m$ dla każdej wiadomości jawnej $m \in M_k$. Schemat prywatnego systemu kryptograficznego przedstawiono na rys.1.



Rys. 1. Prywatny system kryptograficzny [13]
Fig. 1. The private key system [13]

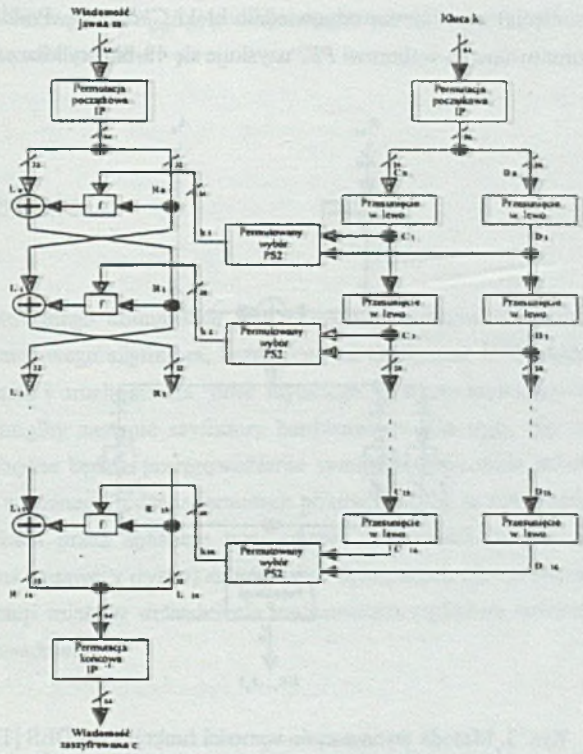
Każdy język naturalny cechuje związany z nim nadmiar przesyłanych informacji, zwany redundancją R. Redundancja zależy od indywidualnych właściwości statystycznych języka, przez co istnieje możliwość skutecznej analizy statystycznej tekstu. W celu udaremnienia takiej analizy stosuje się dwie techniki, a mianowicie konfuzję i dyfuzję [11].

Konfuzja polega na stworzeniu związku pomiędzy kluczem a szyfrogramem tak złożonego, na ile tylko jest to możliwe, w rezultacie czego kryptoanalityk nie może uzyskać przydatnych informacji o kluczu.

Dyfuzja ma na celu zniwelowanie do minimum cech statystycznych tekstu jawnego w kryptogramie. Uzyskuje się ją przez stosowanie przestawień, które, mimo że nie zmieniają częstotliwości wystąpień poszczególnych liter w kryptogramie, jednak burzą częstość wystąpień par liter, trójek liter, itd. Dyfuzję uzyskuje się również przez uzależnienie każdej litery lub bitu szyfrogramu od takiej liczby liter lub bitów tekstu jawnego, jak tylko jest to możliwe [13].

4. Algorytm szyfrująco-deszyfrujący DES

DES - *Data Encryption Standard* - to norma szyfrowania, która została zaprojektowana do ochrony danych przesyłanych i gromadzonych poza sferą dyplomacji i wojskowości [3] Jest łatwa w użyciu zarówno w procesie szyfrowania, jak i deszyfrowania.

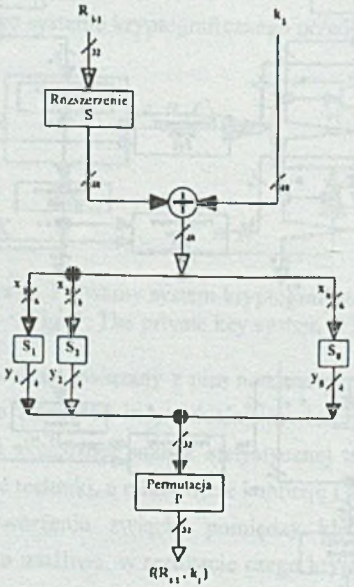


Rys. 2 Schemat blokowy algorytmu DES [13]
Fig. 2. The block diagram of DES algorithm [13]

Zapewnia przy tym wysoki stopień bezpieczeństwa danych [2, 4, 5, 8, 12]. Na rysunku 2 przedstawiono zasadę działania algorytmu (liczby przy ukośnych kreskach oznaczają długość przesyłanego słowa podaną w bitach).

Kluczem głównym jest 64-bitowe słowo binarne k, składające się z ośmiu 8-bitowych bajtów, w których ósmy bit jest bitem parzystości. Przyjęto, że każdy bajt zawiera nieparzystą liczbę jedynek. Klucz k służy do wytworzenia szesnastu 48-bitowych pomocniczych kluczy szyfrujących $k_1, k_2, ..., k_{16}$. Wyznaczanie kluczy pomocniczych poprzedza na wstępie proces poddający klucz k permutowanemu wyborowi *PS1*. Proces ten polega na wyborze 56 bitów z 64-bitowego klucza k, które następnie poddaje się ustalonemu przestawieniu na określone pozycje. Otrzymane w ten sposób 56-bitowe słowo zostaje podzielone na dwa 28-bitowe bloki C_0 i D_0. Następnie, powtarzając w kolejnych krokach i ($i = 1, 2, ...,16$) cykliczne przesunięcia bitów w lewo w blokach C_{i-1} i D_{i-1} (wg ustalonego dla każdego kroku

i rozmiaru przesunięcia) uzyskuje się odpowiednio bloki C_i oraz D_i. Poddając każdorazowo bloki C_i i D_i permutowanemu wyborowi *PS2* uzyskuje się 48-bitowy klucz k_i.



Rys. 3. Metoda wyznaczania wartości funkcji f dla DES [13]
Fig. 3. Method assignning of dependent variable of *f* function for DES algorithm [13]

Klucze pomocnicze są wykorzystywane w procesie szyfrowania 64-bitowej wiadomości *m*. Na wstępie poddaje się wiadomość jawną *m* permutacji początkowej *IP*, a następnie otrzymane 64-bitowe słowo dzieli się na dwa 32-bitowe słowa L_0 i R_0. W kolejnych szesnastu krokach dokonywane są przekształcenia:

$L_i = R_{i-1}$ oraz $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$,

gdzie $\oplus$ oznacza sumowanie modulo 2 odpowiednich bitów sumowanych bloków. Zasadę wyznaczania wartości funkcji $f(R_{i-1}, k_i)$ przedstawiono na rys.3. Rozszerzenie bloku R_{i-1} do 48-bitowego słowa R^*_{i-1} uzyskuje się w taki sposób, że jeżeli R_{i-1}=b1b2b3...b32, to:

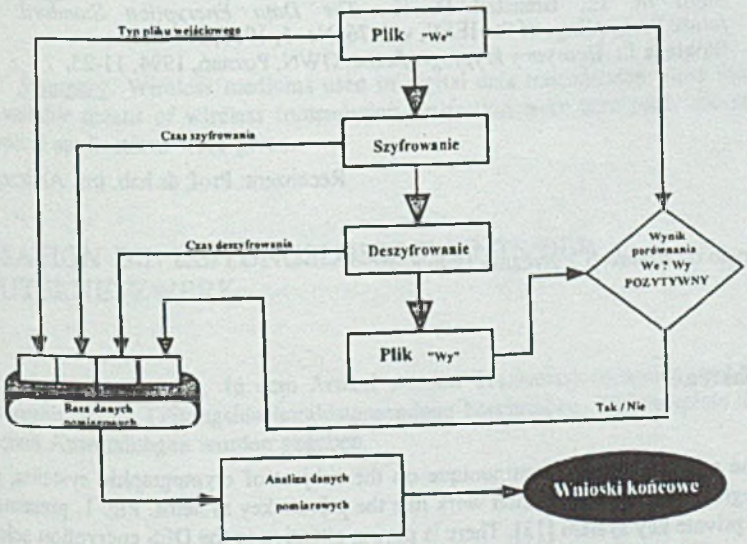
$R^*_{i-1} = b_{32}b_1b_2b_3b_4b_5b_4b_5b_6b_7b_8b_9b_8.b_9b_{10}b_{11}b_{12}b_{13}...b_{28}b_{29}b_{30}b_{31}b_{32}b_1$.

Operacja $\oplus$ przedstawiona na rys.3 jest operacją sumowania modulo odpowiednich bitów. Uzyskany 48-bitowy blok jest dzielony na osiem 6-bitowych bloków $x_1, x_2, ..., x_8$. Zastosowanie pewnej określonej funkcji wyboru S_i do wejścia x_i daje w wyniku 4-bitowy blok wyjściowy y_i. Kolejne bloki y_i są konkatenowane w 32-bitowe słowo $y_1y_2...y_8$, a następnie poddawane utalonej permutacji *P*. Po uzyskaniu bloków L_{16} i R_{16}

skonkatenowany 64-bitowy blok $R_{16}L_{16}$ poddaje się permutacji końcowej IP^{-1}, uzyskując 64-bitową zaszyfrowaną wiadomość c.

5. Zakończenie

Treść zaprezentowanego komunikatu jest najogólniej pojętym wstępem do pracy nad stworzeniem software'owego szyfratora, bazującego na algorytmie DES. Autor chce podjąć próbę zaprojektowania i uruchomienia "dość szybkiego" systemu szyfrująco-deszyfrującego, który w praktyce mógłby zastąpić szyfratory hardware'owe. Do tego, aby określić pojęcie "dość szybki" niezbędne będzie przeprowadzenie symulacji kodowania informacji jawnych przechowywanych w różnego rodzaju formatach plików (tak, jak to ma miejsce przy zapisie informacji na dyskach przez aplikacje typu *edytor, arkusz kalkulacyjny, itd...*) oraz ich dekodowania. Proces badawczy (rys. 4) na podstawie dokonanych pomiarów ma wykazać, dla jakich typów aplikacji miałoby uzasadnienie zastosowanie szyfratora software'owego i czy w ogóle ma ono uzasadnienie.



Rys. 4. Analiza przydatności szyfratora software'owego do zastosowań w aplikacjach

Fig. 4. The analysis of suitability the sofware coder for use in the applications

LITERATURA

[1] Brassard G.: *Modern Cryptology. A Tutorial.* LNCS 325, Springer, Berlin, 1988

[2] Carroll J. M.: *Strategies for extending the useful lifetime of DES.* Computers & Security, vol.6, No 1, 1990, 18-36.

[3] *Data Encryption Standard.* National Bureau of Standards (U.S.), Federal Information Processing Standards Publication #46, National Technical Information Service, Springfield, VA, 1977.

[4] Davies D. W.: *Some regular properties of the Data Encryption Standard algorithm.* Chaum D., Rivest R. L., Sherman A. T., (eds.), *Advances in Cryptology:* Proceedings of CRYPTO 82, Plenum Press, New York, 1983, 89-96.

[5] Diffie W., Hellman M. E.: *Exhaustive cryptoanalysis of the NBS data encryption standard.* IEEE Computer, vol. 10, No. 6, 1977, 74-78.

[6] Grollman S. W.: *Public key cryptographie and complexity theory.* Forschungsbericht Nr. 145, Abteilung Informatik, Universität Dortmund, Dortmund, 1982.

[7] Hellman M. E.: *An extension of the Shanon theory approach to cryptography.* IEEE Transaction on Information Theory, vol. IT-23, No. #, 1977, 289-294.

[8] Kaliski, jr. B. S., Rivest E. L., Sherman A. T.: *Is the Data Encryption Standard A group?* (Results of cycling experiments on DES). Journal of Cryptology, vol. 1, No. 1, 1988, 3-36.

[9] Miyaguchi S., Kurihara S., Ohta K., Morita H.: *Expansion of FEAL cipher.* NTT Review, vol. 2, No. 6, 1990, 117-127.

[10] Rivest R. L., Shamir A., Adleman L.: *A method for obtaining digital signature and public-key cryptosystem.* Communications of the ACM, vol. 21, No. 2, 1978, 120-126.

[11] Shanon C. E.: *Communication theory of secresy systems.* Bell System Technical Journal, vol. 28, 1949, 656-715, także w: Computer Security Journal, vol. 6, No. 2, 1990, 7-66.

[12] Smid M. E., Branstad D. K.: *The Data Encryption Standard: past and future.* Proceedings of the IEEE, vol. 76, No. 5, 1988, 550-559.

[13] Stokłosa J.: *Algorytmy kryptograficzne.* OWN, Poznań, 1994, 11-25.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 2 stycznia 1996 r.

Abstract

The publication is a communique on the subject of cryptographic systems, particulary cryptographic algorithms which work like the private key systems. Fig. 1. presents a scheme of the private key system [13]. There is paying attention to the DES encryption scheme which is presented by Fig. 2. and Fig. 3. in this publication.

Fig. 4. presents the project of works which have to find a solution for "good working" software coder for the computer applications.