STUDIA INFORMATICA 2002
Volume 23 Number 2B (49)

Romuald BŁASZCZYK
Uniwersytet Śląski, Instytut Informatyki

BEZPIECZEŃSTWO SYSTEMÓW KRYPTOGRAFICZNYCH

Streszczenie. Intensywny rozwój możliwości komputerowych oraz technik kryptoanalitycznych sprawił, że istnieje pilna potrzeba znalezienia następcy DES, jak również weryfikowania bezpieczeństwa zapewnianego przez stosowane systemy kryptograficzne. Wynika więc z tego potrzeba stworzenia narzędzia umożliwiającego taką permanentną weryfikację. Tym narzędziem może być mechanizm umożliwiający szacowanie bezpiecznej (nie za długiej i nie za krótkiej) długości klucza. Tej tematyce poświęcona jest ta praca.

THE SECURITY OF CRYPTOSYSTEMS

Summary. The intensive development of computer possibilities and cryptoanalytic techniques caused that there is a current need to find DES successor and also to verify the safety ensured by cryptographic systems. This follows a need to create a tool making this permanent verification possible. The tool can be a mechanism which lets us estimate a safe (not too long and not too short) key size. This is what this work is devoted to.

1. Zadanie badawcze

Systemy kryptograficzne przeżywają aktualnie swój niezwykle burzliwy rozwój. Wynika to z powszechnego stosowania ochrony kryptograficznej i permanentnego rozwoju technologicznego. To, co kiedyś zapewniało bezpieczeństwo naszym danym, dziś już może stanowić niezbyt pewną ochronę (najlepszym tego przykładem – dowodem jest sam „fundamentalny" algorytm DES). Niepokój o bezpieczeństwo przechowywanych danych staje się więc dość powszechny. Z drugiej zaś strony firmy oferujące różne rozwiązania w tym zakresie stymulują ten niepokój, by zwiększyć rynek na swoje produkty. Ta

„informatyczna spirala" wymusza więc, aby podjąć próbę określenia, na ile ten niepokój o bezpieczeństwo danych jest uzasadniony.

W takich uwarunkowaniach podjęto próbę określenia sposobu szacowania, jakie warunki powinien spełniać system kryptograficzny, aby należycie mógł zabezpieczać nasze dane. Zadanie postawiono przed trzema laty. W tym czasie dokonano badań literaturowych, przebadano różne metody kryptograficzne w kontekście poszukiwania elementów wpływających na stopień bezpieczeństwa zapewnianego przez te metody, przeanalizowano różne metody kryptoanalityczne, by wreszcie przystąpić do próby określenia wielkości klucza, który będzie zdolny do zapewnienia określonego stopnia bezpieczeństwa.

Dla dalszych rozważań przyjęto, że o bezpieczeństwie systemu kryptograficznego decydują:

1) oczekiwany czas ochrony informacji,
2) możliwości obliczeniowe sprzętu komputerowego,
3) nakłady finansowe przeznaczane na kryptoanalizę.

System kryptograficzny może być uważany za bezpieczny wówczas, gdy przeprowadzenie ataku zakończonego sukcesem jest uważane za wystarczająco niewykonalne.

Przyjęto także, że jednostka szybkości przetwarzania oznaczana będzie jako JMO. Będzie ona rozumiana jako suma obliczeń, które mogą być wykonane w ciągu roku przez pojedynczy komputer typu PC z roku 1982. Ze względu na złożoność takiego punktu odniesienia można także przyjąć inną spotykaną w literaturze jednostkę znaną pod akronimem MIPS[1].

W przeprowadzonych rozważaniach uwzględniono systemy kryptograficzne klucza symetrycznego i niektóre systemy klucza asymetrycznego. Rozciągnięcie tych rozważań na inne systemy będzie przedmiotem dalszych prac w tym zakresie.

2. Kryptosystemy klucza symetrycznego

Najbardziej znanym kryptosystemem klucza symetrycznego jest DES, wprowadzony w 1977 r, z rozmiarem klucza 56 bitów i rozmiarem bloku 64 bity. Innymi przykładami kryptosystemów klucza symetrycznego są:

- Two Key Triple DES (rozmiar klucza 112 lub 168 bitów, rozmiar bloku 64);
- IDEA (rozmiar klucza 128, rozmiar bloku 64);
- RC5 (zmienny klucz i rozmiar bloku);

[1] A ściślej: MIPS-years jako liczbę operacji wykonaną w ciągu roku nieprzerwanej pracy przez komputer pracujący z szybkością milion instrukcji na sekundę.

- RC6 jako zmodyfikowany RC5
- czy też badany AES – Advanced Encryption Standard (z rozmiarami klucza 128, 192, lub 256 bitów i rozmiarem bloku 128).

Przez wiele lat DES był uważany za najlepszą metodę umożliwiającą ukrywanie ważnych danych. Pełnił więc rolę standardu kryptograficznego.

2.1. Ataki na DES

Algorytm DES został wprowadzony w 1977 roku. Podano wówczas, że jego bezpieczeństwo będzie sprawdzane co 5 lat. Dlatego można założyć, że DES był wystarczająco bezpieczny dla zastosowań komercyjnych aż do 1982 r.

Pomimo wieloletnich badań, nie opublikowano metod łamania komunikatów zaszyfrowanych DES-em zasadniczo szybszych niż wyczerpujące wyszukiwanie klucza, tzn. próbując wszystkie 2^{56} klucze: $2^{56} = 7{,}2 * 10^{16}$ kluczy. Można założyć, że należałoby zbadać połowę zakresu kluczy (liczba prób wyczerpującego przeszukiwania kluczy wynosiłaby 2^{55}). Oczekiwana moc obliczeniowa IO wymagana dla takiego software'owego wyczerpującego przeszukiwania kluczy rozumiana jako ilość obliczeń wykonywanych przez komputer typu PC wynosi więc

$$IO^{'1982'} = \left[\frac{3{,}6 * 10^{16}}{JMO}\right],$$

była w 1982 roku uważana za bezpieczną.

Okres bezpieczeństwa informacji może być więc definiowany jako rok, do którego użytkownik będzie gotowy ufać DES. Parametr, określający rok, do którego chcemy zapewnić bezpieczeństwo, oznaczmy jako „*RB*". Oznacza to, że użytkownik, który przyjął określoną wartość *RB*, jest chętny, żeby ufać DES aż do roku *RB*. Za wartość podstawową można przyjąć, że *RB* = 1982.

Prawo Moore'a stanowi, że gęstość komponentów w układach scalonych podwaja się co 18 miesięcy. Szeroko akceptowana interpretacja tego prawa określa, że moc obliczeniowa wnoszona przez układ scalony podwaja się co 18 miesięcy. Tę wartość oznaczmy jako „*MO*". Tak więc zmienna $MO > 0$ określa liczbę miesięcy, jakie przeciętnie potrzeba na 2-krotne przyśpieszenie procesora i wzrost rozmiaru pamięci. Na podstawie prawa Moore'a można przyjąć $MO = 18$. Oznacza to, że za 10 lat będziemy mieli o $2^{10*12/18} \approx 100$-krotnie więcej mocy obliczeniowej i szybkiej pamięci.

W porównaniu z rokiem 1982 (kiedy mijał pierwszy okres bezpieczeństwa dla DES) moc obliczeniowa sprzętu na 2002 rok zmieniła się 10 319 razy ($2^{13,3}$), czyli to, co można było złamać w 20 lat, dzisiaj można złamać w 17 h.

Odrębne zagadnienie – aczkolwiek zmierzające do tego samego celu - stanowią prace zmierzające do usprawnienia kryptoanalizy. Przejawem tego mogą być kolejne pomysły na przyspieszenie ataków na takie systemy w postaci kryptoanalizy różnicowej, liniowej czy też tzw. ataków „metodą błędów". Wszystkie te prace zmierzają do znalezienia metody ataku lepszej niż tradycyjny atak brutalny. W efekcie usprawniają one kryptoanalizę wymuszając uwzględnienie tego faktu przy ocenie bezpieczeństwa zapewnianego przez metodę. Bardziej wymiernym wyrazem tych prac jest wielkość środków finansowych łożonych na badania w tym zakresie.

Budżety przeznaczane na poszukiwanie metod usprawniających kryptoanalizę podwajają się co każde 10 lat. Trend ten sugeruje, że konieczne jest uwzględnienie nowej zmiennej *NF*. Zmienna *NF* > 0 byłaby określana jako przeciętna liczba lat niezbędna dla podwojenia wzrostu budżetu przeznaczanego na badania kryptoanalityczne. Według powyższych danych można przyjąć *NF* = 10, co oznacza, że co 10 lat podwajają się nakłady finansowe łożone na badania kryptoanalityczne.

Jeżeli w 1982 założono, że wymagana suma mocy obliczeniowej o wielkości

$$IO^{'1982'} = \left[\frac{3{,}6 * 10^{16}}{JMO}\right]$$

jest wartością, która zapewnia, że dokonanie ataku na komercyjny system kryptograficzny staje się niewykonalne, to oznacza to, iż taką barierę mocy obliczeniowej w 1992 roku jako niewykonalną stanowiła wartość

$$\sim 100 * 2 * \left[\frac{3{,}6 * 10^{16}}{JMO}\right] = 200 * IO^{'1982'}$$

(100-krotnie zwiększa się moc obliczeniowa i 2-krotnie zwiększają się nakłady na kryptoanalizę). Ponadto, niewykonalne w 2002 roku byłoby

$$\sim 200 * 200 * IO^{'1982'} = 4 * 10^4 * IO^{'1982'},$$

Podobnie liczba obliczeń wynikająca z $8 * 10^6 * IO^{'1982'}$ uznawana może być za niewykonalną w 2012 r.

2.2. Rozmiar klucza dla metod symetrycznych

Możliwy do zaakceptowania poziom bezpieczeństwa w roku RB wymagał ilości przeliczeń określonych jako $IO^{'1982'}$. Aby określić niezbędną ilość przeliczeń gwarantujących taki poziom bezpieczeństwa w zadanym roku *R* (czyli '*R – RB*' lat później), należy obliczyć

$$IO\,(R) = 2^{12(R-RB)/MO} * 2^{(R-RB)/NF} * IO^{'1982'}$$

gdzie

- *IO (R)* – ilość obliczeń, jaką w roku R można uznać za bezpieczną (trudną do wykonania),
- czynnik $2^{12(R-RB)/MO}$ odzwierciedla wzrost możliwości obliczeniowych w rozważanym okresie ($R - RB$) lat,
- czynnik $2^{(R-RB)/NF}$ odzwierciedla wzrost w budżecie dostępny dla atakującego w rozpatrywanym okresie ($R - RB$) lat.

Wynikająca stąd wartość *IO (R)* używana jest do sterowania rozmiarem klucza oferującego akceptowalny poziom bezpieczeństwa aż do roku *R*.

Rozważania powyższe skoncentrowane były na algorytmie DES. Gdyby rozpatrywać inne systemy klucza symetrycznego, należałoby uwzględnić różnice między poszczególnymi metodami, a tym samym różne szybkości ich działania. Oznacza to, że powinniśmy uwzględnić fakt, że szybkość szyfrowania bloku danych w innej metodzie klucza symetrycznego może być różna od szybkości szyfrowania bloku danych algorytmem DES. Wpływ szybkości działania uwzględniony będzie przez zmienną *V*. Zmienna $V > 0$ powinna być zdefiniowana jako stosunek liczby cykli wymaganych dla szyfrowania pojedynczego bloku za pomocą DES do liczby cykli innej metody klucza symetrycznego, która ma być analizowana.

Jeżeli użyty zostanie system klucza symetrycznego, dla którego $V > 1$, tzn. że jest on *V* razy wolniejszy niż DES, a tym samym atakowanie jego przebiegać będzie również *V* razy wolniej.

W celu sprecyzowania wielkości d klucza dla zadanej metody klucza symetrycznego należy obliczyć:

$$d = 56 + \log_2(IO\ (R)\ /\ V) = 56 + (R\text{-}RB)(12/MO+1/NF) - \log_2(V)\ [\text{ bitów }],$$

wówczas zaoferowane bezpieczeństwo przez system klucza symetrycznego aż do roku *R* jest przynajmniej obliczeniowo i kosztowo ekwiwalentne z zaoferowanym bezpieczeństwem przez DES w roku *RB*.

3. Problemy asymetrycznych systemów kryptograficznych

Metody asymetryczne mają swoją specyfikę w kontekście problemów poruszanych w tej pracy. Kryptoanaliza tych metod stale się polepsza nie tyle z powodu zwiększającej się mocy obliczeniowej komputerów, czy usprawniania procesu kryptoanalizy (tak jak to było w przypadku metod symetrycznych), ile z powodu wypracowywania nowych metod ataku. Dotyczy to głównie pojawiania się coraz to nowych metod faktoryzacji czy też obliczeń logarytmów dyskretnych. Istnieją dużo bardziej wydajne ataki niż wyczerpujące przeszukiwanie i wtedy konieczne jest zastosowanie dużo większych kluczy. Wiele prac

koncentrowało się bowiem nie na ulepszaniu już istniejących metod, a raczej opracowaniu nowych metod ataku. Takim klasycznym przykładem jest metoda Pollarda.

Rozpatrzmy w tym celu metodę RSA. Zgodnie z doświadczeniami praktycznymi można założyć, że mamy do czynienia z dużymi liczbami. Wówczas faktoryzacja modułu n metody RSA może się odbywać przez wyczerpujące przeszukiwanie wszystkich liczb pierwszych aż do $\sqrt{n}$. Wiele algorytmów rozkłada liczbę całkowitą n w czasie proporcjonalnym do:

$$L(n) = e^{\sqrt{\ln n * \ln(\ln n)}}.$$

Rozważania dotyczące metody RSA muszą tutaj uwzględniać fakt, że w 1999 roku system z kluczem 512-bitowym został złamany przy koszcie wymagającym mocy obliczeniowej *K*. W związku z tym wprowadzić trzeba jeszcze oznaczenia:

- *L(k)* jako liczbę przetwarzań wykonywanych przez faktoryzację metodą Pollarda dla klucza rozmiaru *k*,
- liczbę $M > 0$, zdefiniowaną jako liczba miesięcy, która jest potrzebna, by uśredniony wpływ rozwoju kryptoanalizy na klasyczne systemy asymetryczne stał się podwójny, tj. możemy oczekiwać *M* miesięcy od teraz, aby koszt atakowania pewnego klasycznego systemu asymetrycznego był połową wysiłku obliczeniowego jego kosztów dzisiaj.

Wówczas trzeba zmodyfikować niezbędną ilość przeliczeń gwarantujących odpowiedni poziom bezpieczeństwa w zadanym roku *R* do wyrażenia postaci:

$$IO^A(R) = 2^{12(R-RB)/MO} * 2^{(R-RB)/NF} * 2^{12(R-1999)/M} * IO^{'1982'}$$

gdzie

czynnik $2^{12(R-1999)/M}$ odzwierciedla wpływ kryptoanalizy na bezpieczeństwo klasycznego systemu kryptograficznego.

Aby bezpieczeństwo oferowane przez taki system kryptograficzny aż do roku *R* było obliczeniowo równoważne bezpieczeństwu zapewnianemu przez DES w roku 1982, musi zachodzić:

$$\frac{L(k)}{IO^A(R)} \geq \frac{L(2^{512})}{K} \qquad (1)$$

Jeżeli wybrany zostanie klucz asymetryczny o długości k spełniającej warunek (1), to bezpieczeństwo oferowane przez ten system aż do roku *R* będzie co najmniej obliczeniowo równoważne bezpieczeństwu oferowanemu przez DES w roku *RB*.

4. Zakończenie

Zawarte w pracy rozważania można podsumować w postaci następujących wniosków:

1. Umożliwiają one sprecyzowanie warunków bezpieczeństwa dla rozpatrywanego systemu kryptograficznego.
2. W celu precyzyjnego określenia niektórych wartości należałoby sprecyzować podane tu wielkości dla specyficznych zastosowań (dla specyficznych metod ataku).
3. W tej samej konwencji celowym byłoby jeszcze rozpatrzyć systemy wykorzystujące zagadnienie logarytmów dyskretnych oraz krzywe eliptyczne.

LITERATURA

1. Błaszczyk R.: Problemy bezpieczeństwa systemów kryptograficznych. Materiały konferencyjne Instytutu Informatyki Uniwersytetu Śląskiego, Zakopane 2001.
2. Odlyzko A. M: The future of integer faktorization. RSA Laboratories Cryptobytes v.1, no.2, 1995.
3. www.rsa.com i www.rsasecurity.com
4. Silverman R. D.: Exposing the Mythical Mips-Year. IEEE Computer, August 1999.
5. Stallings W.: Ochrona danych w sieci i intersieci. WNT, Warszawa 1997.
6. Wiener M.: Efficient DES Key Search. Proceedings, Crypto'93, Springer-Verlag, Berlin 1993.
7. Wiener M.: Performance Comparison of Public-Key Cryptosystem, CryptoBytes v. 4, no. 1, 1998.

Recenzent: Dr inż. Andrzej Białas

Wpłynęło do Redakcji 5 kwietnia 2002 r.

Abstract

There are two issues in protecting stored or transferred data which we have to solve:

- what kind of specification should be applied to secure correctly;
- whether the cryptographic method that is already used to protect our data is secure enough.

This article tries to evaluate how the cryptosystem is secure in order to estimate the key size encryption. This evaluation takes into consideration the present computation speed, the computers specification and the progress of cryptoanalysis. The basic assumption of this proposal is that the only method of cryptanalytic attack is brute-force attack. Secondly, we assume that cryptoanalysis will be progressing in the same pace as it has been (that means there will be no crucial discoveries in this ground).

This text focuses on symmetric algorithms and certain cases of asymmetric algorithms. In following research one should considerate the newest ideas in asymmetric methods in cryptography.