CENTRUM MODELOWANIA MATEMATYCZNEGO

Estymacja kosztów łamania systemu kryptograficznego

Andrzej Chmielowiec

17 maja 2007

Streszczenie

Przedmiotem artykułu jest prezentacja modelu matematycznego dla zagadnienia opłacalności łamania systemu kryptograficznego. Pokażę, że jeśli nie ma istotnych postępów algorytmicznych w łamaniu systemu, to istnieje tylko jedna strategia pozwalająca maksymalizować zyski atakującego. Daje to możliwość dokładnego przewidzenia jego optymalnego zachowania i pozwala zaprojektować system, który będzie bezpieczny podczas całego okresu eksploatacji. Przy czym przez bezpieczeństwo systemu rozumiemy tutaj nieopłacalność jego łamania ze względów ekonomicznych, a nie ideowych. Pokażę, że użytkownik posiadający wiedzę na temat wartości informacji przetwarzanych przez system informatyczny jest w stanie dobrać długość kluczy kryptograficznych w taki sposób, aby uczynić łamanie kluczy zupełnie nieopłacalnym.

1 Wprowadzenie

Dostępnych jest wiele publikacji opisujących urządzenie do łamania danego kryptosystemu. Prezentują one architekturę układu łamiącego oraz jego szacunkowy koszt. Sięgając po najnowsze opracowania możemy się dowiedzieć ile kosztuje maszyna, która znajduje klucz w ciągu określonego czasu. Koszt tego typu urządzeń dla współcześnie używanych algorytmów jest na ogół tak duży, że przeciętny człowiek może uznać ochronę kryptograficzną na tym poziomie za zupełnie wystarczającą. Sprawa jest dużo bardziej skomplikowana w przypadku systemów przetwarzających ogromne ilości informacji, które mają być eksploatowane przez najbliższe kilkanaście lat. W przypadku takich systemów uzasadnione jest pytanie, czy koszt maszyny jest na tyle duży aby łamanie kluczy było kompletnie nieopłacalne zarówno w chwili obecnej jak i za tych kilkanaście, czy kilkadziesiąt lat. W kolejnych częściach artykułu postaram się przybliżyć tą problematykę i udzielić przynajmniej częściowej odpowiedzi na postawione pytanie.

2 Długość kluczy, a bezpieczeństwo systemu

Bezpieczeństwo systemu kryptograficznego gwarantowane jest przez odpowiedniej długości klucze. Im klucz jest dłuższy, tym trudniejszy do złamania jest system. Oczywiście przy założeniu, że nie posiada on jakichś słabości w swojej konstrukcji. Należy przy tym pamiętać, że stosowane algorytmy nie są sobie równoważne. Dlatego, aby zapewnić bezpieczeństwo na poziomie 80 bitowego szyfru symetrycznego musimy stosować 160 bitową funkcję skrótu i 1024 bitowy klucz algorytmu RSA. Te dysproporcje wynikają z faktu istnienia ogólnych ataków na poszczególne problemy kryptograficzne. Poniżej znajduje się krótka charakterystyka podstawowych składników systemu kryptograficznego, wyjaśniająca istnienie różnic pomiędzy długościami kluczy dla poszczególnych typów algorytmów.

2.1 Szyfry symetryczne

Szyfr symetryczny z kluczem o długości B bitów uznawany jest za bezpieczny, jeżeli nie istnieje atak, którego oczekiwana złożoność jest mniejsza niż 2^{B-1} operacji. Taką bowiem złożoność ma atak polegający na systematycznym przeszukiwaniu przestrzeni kluczy kryptograficznych. Poziom bezpieczeństwa oferowany przez szyfr symetryczny uznawany jest za wzorcowy. Dlatego jeśli mówimy o B bitowym poziomie bezpieczeństwa mamy na myśli poziom oferowany przez szyfr symetryczny o kluczu długości B bitów.

2.2 Funkcje skrótu

Bezpieczeństwo funkcji skrótu wygląda już inaczej niż dla szyfrów symetrycznych. Wiąże się to z faktem istnienia ogólnego ataku, który dla B bitowej funkcji skrótu jest w stanie znaleźć kolizję po wykonaniu jedynie $2^{\frac{B}{2}}$ operacji. Jeżeli zatem chcemy zapewnić sobie B bitowy poziom bezpieczeństwa w sensie szyfru symetrycznego, to musimy użyć $2B$ bitowej funkcji skrótu.

2.3 Algorytmy asymetryczne

W przypadku algorytmów asymetrycznych ocena ich poziomu bezpieczeństwa zależy od złożoności obliczeniowej problemu zastosowanego jako podstawa systemu. Poniżej znajduje się spis najpopularniejszych problemów algebraicznych, które są wykorzystywane do tworzenia algorytmów asymetrycznych.

1. Problem faktoryzacji liczb całkowitych. Aktualnie najlepszym algorytmem do rozwiązania tego problemu jest sito ciał liczbowych, o podwykładniczej złożoności
$$O\left(e^{1.9\ln(N)^{1/3}\ln\ln(N)^{2/3}}\right),$$
gdzie N oznacza liczbę rozkładaną na czynniki.

2. Problem logarytmu dyskretnego w grupie multyplikatywnej ciała skończonego. Aktualnie najlepszym algorytmem do rozwiązania tego problemu jest metoda indeksu, o takiej samej złożoności co sito ciał liczbowych dla problemu faktoryzacji
$$O\left(e^{1.9\ln(N)^{1/3}\ln\ln(N)^{2/3}}\right),$$

gdzie N jest rzędem grupy w której problem logarytmu jest rozwiązywany.

3. Problem logarytmu dyskretnego w grupie punktów krzywej eliptycznej. Aktualnie najlepszym algorytmem rozwiązującym ten problem jest metoda Polarda o złożoności wykładniczej
$$O\left(2^{\frac{N}{2}}\right),$$
gdzie 2^N jest przybliżoną liczbą punktów na krzywej eliptycznej.

Wykorzystując wzory na złożoność obliczeniową poszczególnych problemów można wskazać jakie długości kluczy w kryptosystemach asymetrycznych zapewniają poziom bezpieczeństwa oferowany przez 80, 112, 128, 192 i 256 bitowe klucze szyfrów symetrycznych. Poniższa tabela zawiera zestawienie długości kluczy dla poszczególnych algorytmów.

Liczba bitów klucza szyfru symetrycznego	Liczba bitów klucza RSA/DSA/DH	Liczba bitów klucza ECDSA/ECDH
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

3 Funkcja kosztu i model ataku

W tej części zaprezentuję model, którego zadaniem będzie estymacja kosztów łamania systemu kryptograficznego. Będzie się on opierał na czterech podstawowych założeniach.

1. Szybkość z jaką spada wartość jednostki mocy obliczeniowej jest znana i dana za pomocą funkcji wykładniczej $e^{\alpha t}$ dla pewnego $\alpha > 0$ (dla prawa Moore'a mamy $a = \frac{2}{3}\ln(2)$ jeżeli jednostką czasu jest rok).

2. Funkcja premii $P(t)$ za odszyfrowanie pojedynczej wiadomości po czasie t jest nierosnąca i znana jest jej maksymalna wartość $P(0) = P_0$.

3. Znany jest czas T w ciągu którego kryptosystem będzie eksploatowany. Czas ten oznacza również wymagany czas ochrony przetwarzanych informacji.

4. Koszt maszyny łamiącej klucz w jednostce czasu jest znany i w momencie powstawania kryptosystemu wynosi Q.

Przy tak przyjętych założeniach skonstruujemy teraz funkcję C reprezentującą koszt łamania kluczy kryptograficznych. Będzie ona uwzględniała straty wynikające z zakupu urządzenia jak i zyski, których źródłem jest premia za odszyfrowanie wiadomości. Przyjmijmy, że t_1 jest czasem

w którym atakujący buduje maszynę zdolną do odszyfrowania pojedynczej wiadomości w czasie $t_2 - t_1$. Od tego momentu do końca działania naszego systemu będzie on w stanie zdeszyfrować $\frac{T-t_1}{t_2-t_1}$ wiadomości. Ponieważ premia za odszyfrowanie wiadomości po czasie t wynosi $P(t)$, atakujący będzie w stanie zarobić na swojej działalności co najwyżej $P(t_2-t_1)\frac{T-t_1}{t_2-t_1}$ jednostek. Ponadto, aby mieć możliwość łamania kluczy w czasie $t_2 - t_1$ musiał kupić maszynę, która w chwili t_1 kosztowała $Q\frac{e^{\alpha t_1}}{t_2-t_1}$. Zatem całkowity koszt przedsięwzięcia można oszacować jako:

$$C(t_1, t_2) = Q\frac{e^{\alpha t_1}}{t_2 - t_1} - P(t_2 - t_1)\frac{T - t_1}{t_2 - t_1}.$$

Jeżeli dla jakichkolwiek wartości $t_1 < t_2 < T$ funkcja kosztu całkowitego C przyjmuje wartość ujemną, to opłaca się zbudować maszynę, która będzie deszyfrować wiadomości. W takim przypadku możemy przyjąć, że kryptosystem nie będzie bezpieczny podczas całego okresu jego eksploatacji. Jeśli natomiast dla wszystkich wartości $t_1 < t_2 < T$ funkcja kosztu całkowitego C przyjmuje wartości dodatnie, to atakującemu nie opłaca się łamać systemu i możemy uznać go za bezpieczny w danym przedziale czasu. Rodzi się zatem pytanie, czy istnieją takie wartości parametrów P, Q, T i α, dla których funkcja kosztu całkowitego jest dodatnia w całym kwadracie $[0, T]^2$.

Zanim odpowiemy na pytanie postawione w poprzednim paragrafie, wprowadźmy funkcję pomocniczą

$$q(t_1) = Q\frac{e^{-\alpha t_1}}{T - t_1},$$

której własności będą nam bardzo przydatne w dalszej analizie. Zbadajmy przebieg zmienności tej funkcji. W tym celu wyznaczmy funkcję pochodną q po t_1.

$$q'(t_1) = Qe^{-\alpha t_1}\frac{-\alpha(T - t_1) + 1}{(t - t_1)^2}.$$

Przyrównując otrzymaną pochodną do zera otrzymujemy warunek na ekstremum funkcji q:

$$\begin{aligned} q'(t_1) = 0 \quad &\iff \quad -\alpha(T - t_1) + 1 = 0 \\ &\iff \quad t_1 = T - \frac{1}{\alpha}. \end{aligned}$$

Zauważmy ponadto, że dla wartości t_1 z przedziału $[0, T - \frac{1}{\alpha})$ pochodna funkcji q przyjmuje wartości ujemne, a dla wartości z przedziału $(T - \frac{1}{\alpha}, T)$ pochodna ma wartość dodatnią. Zatem funkcja $q(t_1)$ ma w punkcie $T - \frac{1}{\alpha}$ minimum i jest to minimum globalne w przedziale $[0, T)$.

Powróćmy teraz do zasadniczego zagadnienia tej części i zbadajmy jakie warunki muszą być spełnione, aby łamanie kryptosystemu było nieopłacalne podczas całego okresu jego funkcjonowania. Jak już to wcześniej zostało stwierdzone, z taką sytuacją mamy do czynienia jedynie

wtedy, gdy dla wszystkich liczb $t_1 < t_2 < T$ funkcja kosztu całkowitego C przyjmuje wartości dodatnie. Korzystając z faktu, że funkcja premii P jest nierosnąca i znana jest jej wartość maksymalna P_0 mamy

$$\begin{aligned} C(t_1, t_2) &= Q\frac{e^{\alpha t_1}}{t_2 - t_1} - P(t_2 - t_1)\frac{T - t_1}{t_2 - t_1} \\ &\geq Q\frac{e^{\alpha t_1}}{t_2 - t_1} - P_0\frac{T - t_1}{t_2 - t_1}. \end{aligned}$$

Z powyższej nierówności wynika, że wystarczy dla każdego $t_1 < t_2 < T$ spełnić warunek

$$Q\frac{e^{\alpha t_1}}{t_2 - t_1} - P_0\frac{T - t_1}{t_2 - t_1} > 0,$$

aby funkcja kosztu całkowitego przyjmowała jedynie wartości dodatnie i atak na system był nieopłacalny. Upraszczając przedstawione wyrażenie otrzymujemy

$$P_0 < Q\frac{e^{-\alpha t_1}}{T - t_1} = q(t_1).$$

Teraz skorzystamy z faktu, że wprowadzona funkcja $q(t_1)$ ma w przedziale $[0, T)$ minimum globalne dla t_1 równego $T - \frac{1}{\alpha}$. Ostatecznie otrzymujemy, że

$$Q > P_0\frac{e^{\alpha T - 1}}{\alpha}.$$

Otrzymany warunek informuje nas o tym, jaka powinna być bieżąca wartość maszyny do łamania naszego systemu, jeżeli chcemy bezpiecznie eksploatować go przez T okresów, a średnia wartość informacji przekazywanej podczas pojedynczej sesji wynosi P_0. Należy tutaj podkreślić, że manewrowanie wielkością Q jest dość proste i polega na doborze kluczy kryptograficznych o określonej długości.

Zastanowimy się teraz, czy nasz warunek jest niezależny od strategii jaką przyjął atakujący. Rozważyliśmy bowiem jedynie przypadek pojedynczej inwestycji w maszynę. Co się jednak dzieje, gdy nasz przeciwnik kupuje maszyny o dowolnej mocy obliczeniowej w wielu chwilach okresu eksploatacji systemu. Załóżmy zatem, że funkcja $\delta(t_1, t_2)$ przyjmuje wartości ze zbioru $\{0, 1\}$, które określają zachowanie atakującego. Funkcja $\delta(t_1, t_2)$ ma wartość 1 jeżeli w chwili t_1 nasz przeciwnik kupuje maszynę zdolną deszyfrować wiadomość w czasie $t_2 - t_1$. W takiej sytuacji całkowity koszt można wyrazić za pomocą następującej całki

$$C_T = \int\limits_{0 \leq t_1, t_2 < T} \delta(t_1, t_2) C(t_1, t_2)$$

Ale jeśli $Q > P_0\frac{e^{\alpha T - 1}}{\alpha}$ to funkcja C przyjmuje jedynie wartości dodatnie i wartość powyższej całki jest nieujemna. Ostatecznie możemy zatem stwierdzić, że otrzymany warunek jest niezależny od zachowania atakującego i chroni nasz kryptosystem podczas całego okresu eksploatacji.

4 Wpływ długości klucza na koszt łamania szyfru

Niestety informacja o tym ile powinna w danej chwili kosztować maszyna do łamania naszego systemu nie daje nam bezpośredniej odpowiedzi na pytanie, jakie długości kluczy kryptograficznych powinny być zastosowane. Aby uzyskać jakąkolwiek wiedzę na ten temat musimy znaleźć sposób na powiązanie długości kluczy z kosztem maszyny, która potrafi je łamać. W tym miejscu skorzystamy z publikacji w których co pewien czas pojawiają się projekty urządzeń łamiących dany szyfr. Wiedząc jaka jest złożoność obliczeniowa ataków na poszczególne algorytmy oraz stosując prawo Moore'a jesteśmy w stanie przewidzieć jakich postępów można spodziewać się w przyszłości. Należy tutaj podkreślić, że przedstawiona analiza nie obejmuje sytuacji, w której zostają wynalezione szybsze algorytmy do łamania naszego systemu.

4.1 Analiza ogólna

Rozważmy najpierw sytuację ogólną, w której atakujący chce złamać algorytm kryptograficzny o kluczach długości B bitów i złożoności ataku $\Phi(B)$. Załóżmy, że koszt budowy maszyny, która łamie ten algorytm dla B_0 bitowych kluczy ma w chwili T_0 wartość Q_0. Biorąc pod uwagę założenie o wykładniczym spadku wartości jednostki mocy obliczeniowej, możemy oszacować wartość takiej maszyny dla dowolnej chwili t i dowolnie długich kluczy

$$Q(t,B) = Q_0 e^{-\alpha(t-T_0)} \frac{\Phi(B)}{\Phi(B_0)}.$$

Z poprzednich części artykułu wynika, że jeżeli spełniona jest nierówność $Q > P_0 \frac{e^{\alpha T}-1}{\alpha}$, to atak na kryptosystem jest nieopłacalny. Przyjmując, że nasz system kryptograficzny ma być eksploatowany od chwili T_1 do chwili T_2 otrzymujemy

$$Q_0 e^{-\alpha(T_1-T_0)} \frac{\Phi(B)}{\Phi(B_0)} > P_0 \frac{e^{\alpha(T_2-T_1)}-1}{\alpha}.$$

Spełnienie powyższego warunku jest wystarczające by zapewnić nieopłacalność łamania systemu we wskazanym okresie czasu. Będziemy z niego korzystali w dalszej części artykułu do oszacowania długości kluczy w przypadkach konkretnych algorytmów i konkretnych maszyn łamiących klucze.

Zanim jednak do tego przejdziemy zauważmy, że otrzymany warunek upraszcza się do postaci

$$\Phi(B) > \Phi(B_0) \frac{P_0 e^{\alpha(T_2-T_0)}-1}{\alpha Q_0},$$

która nie zawiera wartości T_1. Oznacza to, że naprawdę istotnym czynnikiem czasowym dla funkcjonowania systemu jest moment w którym może ustać ochrona kryptograficzna.

4.2 Szyfry symetryczne

Jeśli chodzi o szyfry symetryczne to w naszej analizie będziemy posiłkowali się opracowaniami dotyczącymi algorytmu DES. Wynika to z faktu, że algorytm ten doczekał się nawet praktycznej implementacji maszyny, która łamie klucz poprzez systematyczne przeszukiwanie. Naszą uwagę skupimy właśnie na tym projekcie. Nosi on nazwę COPACOBANA, powstał w 2006 roku i implementuje urządzenie bazujące na układach programowalnych FPGA, które mogą być również dostosowane do łamania kluczy innych algorytmów. Stworzony układ kosztuje około 30.000 PLN i pozwala na znalezienie klucza algorytmu DES w około 9 dni. Na nasz użytek potrzebujemy przeliczyć te wielkości w taki sposób, aby odpowiadały one okresowi jednego roku. W tym przypadku możemy przyjąć, że układ, który łamie DES w ciągu jednego roku kosztuje około $Q_0 = 740$ PLN. Niech teraz B oznacza liczbę bitów klucza, a t rok w którym chcemy szacować koszt. Stosując prawo Moore'a możemy znaleźć zależność pomiędzy długością klucza szyfru symetrycznego, a kosztem maszyny służącej do jego łamania

$$Q(t, B) = Q_0 e^{-\alpha(t-2006)+\ln(2)(B-56)}.$$

Dla prawa Moore'a współczynnik α był podany w poprzedniej części i wynosi $\alpha = \frac{2}{3}\ln(2)$. Teraz wystarczy powiązać wyprowadzoną formułę z warunkiem na nieopłacalność łamania systemu kryptograficznego, aby otrzymać związek na minimalną długość klucza szyfru symetrycznego. Niech T_0 będzie rokiem rozpoczęcia funkcjonowania systemu kryptograficznego z szyfrem symetrycznym, a T_1 rokiem w którym może ustać ochrona kryptograficzna. Aby zapewnić bezpieczeństwo przetwarzanych informacji, długość kluczy szyfru symetrycznego B_{SYM} powinna spełniać nierówność

$$Q_0 e^{-\alpha(T_0-2006)+\ln(2)(B_{SYM}-56)} > P_0 \frac{e^{\alpha(T_1-T_0)-1}}{\alpha}$$

$$B_{SYM} > 56 + \frac{1}{\ln(2)}\left(\alpha(T_1 - 2006) - 1 + \ln\left(\frac{P_0}{\alpha Q_0}\right)\right).$$

Warto w tym miejscu zwrócić uwagę na fakt, że w końcowym warunku nie ma wartości T_0. Zatem otrzymany wynik zależy tylko od czasu zakończenia eksploatacji systemu.

4.3 Funkcje skrótu

Wynik uzyskany dla szyfrów symetrycznych może być bezpośrednio zastosowany dla funkcji skrótu. Wynika to z tego, że szybkość obliczania skrótu jest bardzo zbliżona do szybkości szyfrowania. Musimy jedynie uwzględnić fakt istnienia ogólnego ataku, którego złożoność jest znacznie mniejsza dla funkcji skrótu niż dla szyfrów symetrycznych. Atak ten zmusza nas do podwojenia liczby bitów funkcji skrótu w celu uzyskania takiego samego poziomu ochrony jak w przypadku szyfrów symetrycznych. Dlatego liczba bitów funkcji skrótu, którą należy zastosować do zapewnienia ochrony do roku T_1 musi spełniać nierówność

$$B_{HASH} > 112 + \frac{2}{\ln(2)}\left(\alpha(T_1 - 2006) - 1 + \ln\left(\frac{P_0}{\alpha Q_0}\right)\right).$$

4.4 Algorytmy asymetryczne

Analizę algorytmów asymetrycznych rozpoczniemy od systemów bazujących na problemie logarytmu dyskretnego w grupie punktów krzywej eliptycznej. Do rozwiązywania tego problemu można również wykorzystać projekt COPACOBANA. Umożliwia on znajdowanie logarytmu dyskretnego dla krzywej zadanej nad 112 bitowym ciałem w około 262 dni po zainwestowaniu około 3 milionów PLN. Oznacza to, że maszyna rozwiązująca ten problem w ciągu jednego roku kosztowałaby około $Q_1 = 2.200.000$ PLN. Uwzględniając fakt, że złożoność obliczeniowa problemu logarytmu dyskretnego w grupie punktów krzywej eliptycznej jest taka jak dla funkcji skrótu otrzymujemy

$$Q_1 e^{-\alpha(T_0-2006)+\ln(2)\left(\frac{B_{ECC}-112}{2}\right)} > P_0 \frac{e^{\alpha(T_1-T_0)-1}}{\alpha}$$

$$B_{ECC} > 112 + \frac{2}{\ln(2)}\left(\alpha(T_1-2006) - 1 + \ln\left(\frac{P_0}{\alpha Q_1}\right)\right).$$

W przypadku algorytmów bazujących na problemie faktoryzacji i problemie logarytmu dyskretnego w grupie multyplikatywnej ciała skończonego nie uzyskamy jawnej formuły na liczbę bitów klucza. W celu estymacji kosztów układu łamiącego wykorzystamy architekturę o nazwie TWIRL zaproponowaną w 2004 roku. Pozwala ona na złamanie 1024 bitowego RSA w ciągu 1 roku przy nakładzie około $Q_2 = 3.000.000$ PLN. Jeżeli przyjmiemy, że

$$L(B) = 1.9 \ln\left(2^B\right)^{1/3} \ln\ln\left(2^B\right)^{2/3},$$

to $e^L(B)$ oznacza złożoność problemu faktoryzacji modułu RSA, który ma B bitów. W związku z tym warunek na bezpieczeństwo kluczy RSA do roku T_1 wyraża się wzorem

$$Q_2 e^{-\alpha(T_0-2004)+L(B_{RSA})-L(1024)} > P_0 \frac{e^{\alpha(T_1-T_0)-1}}{\alpha}$$

$$L(B_{RSA}) > L(1024) + \left(\alpha(T_1-2004) - 1 + \ln\left(\frac{P_0}{\alpha Q_2}\right)\right).$$

Identyczny warunek otrzymujemy dla algorytmów DSA i DH, które bazują na problemie logarytmu dyskretnego w ciele skończonym.

5 Podsumowanie

W artykule została zaprezentowana metoda wyznaczania długości kluczy kryptograficznych na podstawie okresu ich wykorzystywania oraz średniej wartości informacji przetwarzanej przez system. Przedstawione podejście pokazuje jak dobrać klucze algorytmów szyfrujących, aby ich łamanie było nieopłacalne z ekonomicznego punktu widzenia podczas całego okresu eksploatacji. Wprowadzone formuły bazują na aktualnych informacjach z zakresu kryptoanalizy i dają możliwość szacowania bezpieczeństwa najpopularniejszych algorytmów kryptograficznych.