Wydział Cybernetyki WAT

Przedmiot: Wprowadzenie do kryptoanalizy klucza publicznego

SPRAWOZDANIE

Temat: ATAK DIOFANTYCZNY

Wykonał:

Paweł Witkowski
[K5X4S1]

Data wykonania ćwiczenia:

24.11.2016

Prowadzący ćwiczenie:

Kpt. Dr Mariusz Jurkiewicz

1. Wprowadzenie teoretyczne

Atak diofantyczny, inaczej też nazywany atakiem Wienera, polega na znalezieniu elementu odwrotnego tj. współczynnika deszyfrującego, dalej nazywanego "**d**", do szyfrującego **"e",** przy założeniu, że **d** jest możliwie małe.

$$d < \frac{1}{3} N^{\frac{1}{4}}$$

, gdzie **N** to nasz klucz publiczny, który jest iloczynem dwóch dużych liczb pierwszych $N = p * q$

Współczynnik **d** można znaleźć wyznaczając element odwrotny do **e**, w kongruencji

$$d * e \equiv 1 (mod (p-1)(q-1))$$

jeżeli gcd(**e**,(p-1)(q-1))=1, ponieważ wtedy kongruencja posiada dokładnie jedno rozwiązanie.

Skończony ciąg liczb **R** $<a_0,a_1...a_n>$ nazywa się ułamkiem łańcuchowym jeśli te liczby są dodatnie, a "**n**" wyznacza długość tego ułamka. Zapisujemy to wtedy $[a_0,a_1...a_n]$ i oznacza:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

N-tym reduktem danego ułamka łańcuchowego jest rozwijanie go tak jak powyżej, do elementu o indeksie **n**. Jeżeli **a** ϵ Q to można przedstawić **a** w postaci skończonego ułamka łańcuchowego: $<a_0,a_1...a_n>$, gdzie:

$q_0=\lfloor a \rfloor$ $\quad a_1=\frac{1}{(a-q_0)}$;

$q_1=\lfloor a_1 \rfloor$ $\quad a_2=\frac{1}{(a_1-q_1)}$

::

$q_{n-1}=\lfloor a_{n-1} \rfloor$ $\quad a_n=\frac{1}{(a_{n-1}-q_{n-1})}$

$q_n=\lfloor a_n \rfloor$

Wprowadzenie ułamka łańcuchowego było potrzebne, ponieważ twierdzenie o zbieżności mówi:
Jeżeli p,q ϵ *Z,* $\left|\frac{p}{q} - x\right| < \frac{1}{q^2}$*,wtedy istnieje takie i=0,1,2...n, że* $\frac{p}{q}$ *będzie i-tym reduktem* ***x****.*

W celu wyznaczenia k-tego reduktu ułamka łańcuchowego, można posłużyć się dwoma specyficznymi ciągami wielomianów. $P_k:=P_k(x_0,x_1....x_k)$, $Q_k:=Q_k(x_0,x_1...x_k)$, których kolejne elementy są wyznaczone za pomocą wzorów:

$$P_{-1}=1,\ Q_{-1}=0$$
$$P_0(x_0)=x_0;\ Q_0(x_0)=1;$$
$$P_{k+1}=x_{k+1}P_k+P_{k-1};\ \ Q_{k+1}=x_{k+1}Q_k+Q_{k-1};$$
$$r_k=[x_0,x_1...x_k]=P_k(x_0,x_1...x_k)/Q_k(x_0,x_1...x_k)$$

Wszystkie narzędzia zostały już podane. Wyznaczamy kolejne redukty za pomocą wielomianów i sprawdzamy czy jest to $\frac{k}{d}$. Trzeba wykonać podstawienie $k=P_k$, $p=\mathbf{d}=Q_k$, $Fi(N)=\frac{ed-1}{k}$, następnie rozwiązać równanie $p^2 - (N-Fi(N)+1)p+N=0$. Jeżeli rozwiązanie faktoryzuje **N**, to nasze **d**=Q_k, a miejsca zerowe to liczby których iloczyn jest równy **N**.

2. Wykorzystanie teorii do rozwiązania problemu

Posiadając **N** i **e** możemy rozwinąć w ułamek łańcuchowy **e/N**. Dzięki temu obliczamy współczynniki **q** rozwinięcia tego ilorazu w ułamek łańcuchowy.
Posłuży do tego algorytm Euklidesa który przebiega następująco:
1) A←N, B←e
2) Do
3) q ← ⌊A/B⌋
4) A ← B, B←A - qB
5) Vector[] ← q
6) While B ≠ 0
7) gcd(N,e) ← A
8) Return (gcd)
W tej chwili wszystkie współczynniki ułamka łańcuchowego są w tablicy Vector. Do obliczenia kolejnych reduktów, należy się posłużyć rekurencyjnym wyznaczaniem kolejnych elementów wielomianów P oraz Q.
Po kolei obliczamy każdy redukt $r_i=\frac{P_i}{Q_i}$. Dla tak obliczonego P_i/Q_i, podstawiamy $k=P_i$, $p=d=Q_i$.
Następnie obliczany $\varphi(N)=\frac{ed-1}{k}$, podstawiamy to do równania kwadratowego względem p. $p_2 - (N - \varphi(N)+1)p+N=0$. Jeżeli rozwiązania faktoryzują N, to znaczy, że z równania N = p*q, $p = p_1$, $q = p_2$, jednocześnie $d = Q_i$.

3. Wnioski/Analiza

Na zadany przykład **N = 160523347**, **e = 60728973** udało się znaleźć element odwrotny **d**. Po wykonaniu algorytmu Euklidesa na **N** oraz **e**, oraz zapisywaniu poszczególnych iloczynów naszych reszt q_i do wektora nastąpiło sprawdzenie poszczególnych reduktów. Po kolei wartości były brane i podstawiane do równań
$\phi(N)=\frac{ed-1}{k}$, $p_2 - (N - \varphi(N)+1)p+N=0$. Rozwiązaniami równania kwadratowego okazały się p = p_1=12347, q = p_2=13001, więc N=12347*13001. Po odnalezieniu elementów faktoryzujących **N**, podstawiamy **d**=Q_i=37. W celu sprawdzenia poprawności znalezionego elementu deszyfrującego szukamy elementu odwrotnego w ciele $F(\varphi(N))$, a więc $\mathbf{d}*\mathbf{e}\equiv 1 (\mathrm{mod}\, \varphi(N))$. Podstawiając za **e**, p-1, q-1 otrzymujemy **d=37**, a więc faktycznie jest to element odwrotny do **e** w tym ciele. Atak diofantyczny na podanym przykładzie był możliwy ponieważ **d** spełnia warunek:

$d < \frac{1}{3}N^{\frac{1}{4}}$, ponieważ 37 < 37.5