RUHR UNIVERSITÄT BOCHUM

RUB

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Alexander Meurer, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

WS 2011/2012

Blatt 2 / 26. Oktober 2011 / Abgabe bis spätestens 2. November 2011, 10 Uhr in dem Kasten auf NA 02

AUFGABE 1 (5 Punkte)**:**
Zeigen Sie, dass

$$\textit{ElGamal Chiffretexte enschlüsseln} \Rightarrow \textit{Diffie-Hellman Problem} \quad .$$

Hierbei bedeutet $A \Rightarrow B$, dass die Existenz eines effizienten Algorithmus für A die Existenz eines effizienten Algorithmus für B impliziert.

AUFGABE 2 (5 Punkte)**:**
In Pollards Rho-Methode habe das Anfangsstück Länge i und der Kreis Länge $j - i$. Zeigen Sie, dass sich die beiden Känguruhs im Punkt $s_m = s_{2m}$ treffen, wobei

$$m = (j - i) \cdot \left\lceil \frac{i}{j - i} \right\rceil .$$

Hinweis: Es ist nützlich, die Identität $x \bmod y = x - y \cdot \lfloor \frac{x}{y} \rfloor$ zu benutzen.

AUFGABE 3 (10 Punkte)**:**
Sei $N = pq$ ein RSA-Modul mit $p < q$. Angenommen, wir haben eine zufällige Funktion $f : \mathbb{Z}_N \to \mathbb{Z}_N$.

a) Zeigen Sie, dass die Faktorisierung von N in erwarteter Zeit $\tilde{\mathcal{O}}(\sqrt{p})$ und Platz $\tilde{\mathcal{O}}(1)$ bestimmt werden kann.
Hinweis: Wenden Sie eine angepasste Pollard Rho-Methode an, d.h. finden Sie s_i, s_{2i}, $s_i \neq s_{2i}$ mit $s_i = s_{2i} \bmod p$.

b) Wir wollen eine etwas genauere Analyse für die Anzahl der benötigen Schritte durchführen, bis eine Kollision auftritt. Zeigen Sie: Nach höchstens $m := \sqrt{2\ln(2)p} + 1$ Schritten tritt mit Wahrscheinlichkeit $\geq \frac{1}{2}$ eine Kollision auf. Gehen Sie hierbei wie folgt vor:

   i) Definieren Sie eine Zufallsvariable X mit $X = 1$ genau dann, wenn nach $\leq m$ Schritten eine Kollision aufgetreten ist. Stellen Sie eine exakte Formel für $\mathbf{Ws}[X = 0]$ auf.

ii) In der Formel für $\mathbf{Ws}[X=0]$ sollten Ausdrücke der Form $(1-\frac{i}{p})$ für verschiedene $i \in \mathbb{N}$ auftreten. Jeden dieser Faktoren können Sie durch $1-\frac{i}{p} \leq \exp(-\frac{i}{p})$ abschätzen. Zeigen Sie

$$\mathbf{Ws}[X=0] \leq \exp\left(-\frac{m(m-1)}{2p}\right)$$

und schätzen Sie diesen Ausdruck für obiges m geeignet weiter nach oben ab.

iii) Berechnen Sie $\mathbf{Ws}[X=1] = 1 - \mathbf{Ws}[X=0]$ und nutzen Sie ii).

AUFGABE 4 (5 Punkte)**:**
Implementieren Sie Pollard's Rho Algorithmus zur Faktorisierung aus Aufgabe 3 in Sage. Benutzen Sie Abbildungen $f_c : \mathbb{Z}_N \to \mathbb{Z}_N$ definiert durch $f(x) := x^2 + c \bmod N$ für eine Konstante $c \in \mathbb{Z}_N$. Es ist sinnvoll, den Algorithmus und f_c als Funktionen zu implementieren, da wir diesen später für verschiedene Kandidaten für f_c aufrufen wollen. Nutzen Sie hierzu den Sage Befehl `def`, bspw. können Sie für variables c und N folgende parametrisierte Version von f erzeugen.

```
def f(x,c,N):
   return (x^2+c)%N
```

Wenden Sie Ihren Algorithmus auf `N=454625706174950117` an (Sie können den Modul auch wie gewohnt auf der Webseite herunterladen). Wir wollen sowohl die grobe Analyse aus 3 a) als auch die verfeinerte Analyse aus 3 b) überprüfen. Verwenden Sie stets den Startwert $x_0 = 1$.

(a) Berechnen Sie die Faktorisierung von N für $f_1(x) = x^2 + 1 \bmod N$ und zählen Sie die Anzahl der Schritte.

(b) Verwenden Sie verschiedene f_c für zufällig gewählte $c \in \mathbb{Z}_N$ (testen Sie mindestens 1000 verschiedene c) und speichern Sie das jeweilige Ergebnis und die benötigte Anzahl von Schritten in einer Tabelle. Berechnen Sie die durchschnittliche Anzahl von Schritten aller Durchläufe, die $\min(p,q)$ ausgegeben haben (Sie werden beobachten, dass in einigen Durchläufen der größere Primfaktor gefunden wird). Vergleichen Sie diesen Wert mit $\sqrt{\min(p,q)}$.

c) Überprüfen Sie, in wie vielen Fällen der Algorithmus in weniger als m Schritten terminiert hat. Geben Sie die Erfolgswahrscheinlichkeit für $m = \sqrt{2\ln(2)p}$ und $m = \sqrt{\ln(2)p}$. Wie nahe an $\frac{1}{2}$ liegen diese Werte?

(d) Geben Sie eine mögliche Erklärung für ihre Beobachtungen aus Teil a) und b). Wieso liegt der experimentell bestimmte Wert für die Anzahl der Schritte in a) unter dem Wert $\sqrt{\min(p,q)}$? Wieso ist die ursprüngliche Wahl von $m = \sqrt{2\ln(2)p}$ zu konservativ, um Erfolgswahrscheinlichkeit $\geq \frac{1}{2}$ zu erreichen?
Hinweis: Liefert die Abbildung f_c eine zufällige Abbildung auf *ganz* $\mathbb{Z}_p$? Wenn man herausgefunden hat, wie groß der tatsächliche Bildraum von f_c in $\mathbb{Z}_p$ ist, sollte ein analoge Analyse zur Aufgabe 3 b) ein modifiziertes $m = \sqrt{\ln(2)p}$ liefern.