Ruhr-Universität Bochum
Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova, Ilya Ozerov

Hausübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 5 / 20. Mai 2014

Abgabe: 02. Juni 2014, 14.00 Uhr, Kasten NA/02

AUFGABE 1 (5 Punkte)**:**

Implementieren Sie den Algorithmus von Heninger und Shacham (Folie 27) in sage. In der Datei hs.txt finden Sie einen 1024 Bit RSA-Modulus N, sowie Bitmaterial $\widetilde{p}, \widetilde{q}$ mit insgesamt 532 bekannten und 492 unbekannten Bits (gekennzeichnet durch ?). Faktorisieren Sie N mit Ihrem Algorithmus. Was sind die Faktoren? Wie viele Knoten hat der Baum? Geben Sie den Quellcode mit ab.

Hinweis: Sie sollten den Algorithmus rekursiv implementieren. Achten Sie darauf, dass die maximale Rekursionstiefe hoch genug eingestellt ist. Es wird mindestens Tiefe 512 benötigt. Die Tiefe kann mit sys.setrecursionlimit(limit) eingestellt werden.

AUFGABE 2 (5 Punkte)**:**

Implementieren Sie den Algorithmus von Henecka, May und Meurer (Folie 28) in sage. In der Datei hmm.txt finden Sie erneut einen 1024 Bit Modulus N, nun jedoch Bitmaterial $\widetilde{p}, \widetilde{q}$ mit 50 fehlerhaften Bits. Faktorisieren Sie N mit Ihrem Algorithmus mit den Parametern $t = 11$ und $d = 3$. Was sind die Faktoren? Wie viele Knoten hat der Baum? Gibt es eine bessere Parameterwahl mit einer geringeren Anzahl von Knoten? Geben Sie den Quellcode mit ab.

Hinweis: Beachten Sie auch hier die Rekursionstiefe. Sie dürfen, wie in der Präsenzübung angesprochen, auch mitten in einem Fenster vorfiltern. D.h. gibt es z.B. in einem Fenster der Tiefe 11 bereits nach 7 Leveln Knoten mit Distanz 4, so können diese verworfen werden.

Bitte wenden!

AUFGABE 3 (5 Punkte)**:**

Sei $p'q' = N = (N_{i-1} \dots N_0)_2 \bmod 2^i$, wobei $N = (N_{2n-1} \dots N_0)_2$ die Binärdarstellung von N ist. Wir wollen nun entscheiden, ob

$$p'q' = N = (N_i \dots N_0)_2 \bmod 2^{i+1} \quad \text{und} \quad (p' + 2^i)(q' + 2^i) = N = (N_i \dots N_0)_2 \bmod 2^{i+1}$$

oder

$$(p' + 2^i)q' = N = (N_i \dots N_0)_2 \bmod 2^{i+1} \quad \text{und} \quad p'(q' + 2^i) = N = (N_i \dots N_0)_2 \bmod 2^{i+1}.$$

Sei

$$z := \left\lfloor \frac{p'q'}{2^i} \right\rfloor + N_i \bmod 2.$$

Zeigen Sie, dass $p'q' = N \bmod 2^{i+1}$ gdw. $z = 0$. Verwenden Sie dann Präsenzaufgabe 3.

AUFGABE 4 (5 Punkte)**:**

Faktorisieren Sie (per Hand) mit den Algorithmen von HS bzw. HMM

(a) $N = 551 = \texttt{10001 00111}_2$ mit dem Bitmaterial $\widetilde{p} = \texttt{?????}$ und $\widetilde{q} = \texttt{??10?}$,

(b) $N = 667 = \texttt{10100 11011}_2$ mit dem Bitmaterial $\widetilde{p} = \texttt{11000}$ und $\widetilde{q} = \texttt{00111}$, $t = 2, d = 1$.