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

Präsenzübungen zur Vorlesung

Kryptanalyse

SS 2014

Blatt 5 / 19. Mai 2014

AUFGABE 1:

Überlegen Sie sich Gegenmaßnahmen gegen

(a) Kochers Timing Angriff und

(b) den Bellcore Angriff.

Was sind Vor- und Nachteile Ihrer Gegenmaßnahmen?

AUFGABE 2:

Sie werfen n unabhängige, faire Würfel. Geben Sie mit Hilfe der Hoeffding-Ungleichung eine obere Schranke für die Wahrscheinlichkeit an mehr als $n/2$ Sechsen zu werfen.

AUFGABE 3:

Sei $N = p'q' \bmod 2^i$, wobei N, p', q' ungerade sind. Zeigen Sie, dass dann entweder

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

oder

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

AUFGABE 4:

Faktorisieren Sie

(a) $N = 2279 = \texttt{100011 100111}_2$ mit dem Bitmaterial $\widetilde{p} = \texttt{?10?0?}$ und $\widetilde{q} = \texttt{1??01?}$,

(b) $N = 551 = \texttt{10001 00111}_2$ mit dem Bitmaterial $\widetilde{p} = \texttt{00111}$ und $\widetilde{q} = \texttt{11101}$, $t = 2, d = 1$.