RUHR UNIVERSITÄT BOCHUM

Lehrstuhl für Kryptologie und IT-Sicherheit
Prof. Dr. Alexander May
Elena Kirshanova

Präsenzübungen zur Vorlesung

Kryptanalyse I

SS 2015

Blatt 5 / 9 Juli 2015

Aufgabe 1:
Let N, p', q' be odd integers, such that $N = (N_{i-1} \dots N_1 N_0) = p'q' \mod 2^i$.

1. Show that either

$$N = p'q' \mod 2^{i+1} \quad \text{and} \quad N = (p' + 2^i)(q' + 2^i) \mod 2^{i+1},$$

   or

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

2. Let

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

   Show that $N = p'q' \mod 2^{i+1}$ if and only if $z = 0$.

3. Using the above, find p, q given

   - $N = 899 = 11100\,00011_2$, $p = ?1?01$, $q = ?11?1$,
   - $N = 1353 = 101010\,01001$, $\tilde{p} = 101000$, $\tilde{q} = 110101$.

Aufgabe 2:
Lifting roots of polynomials: multivariate case. Hensel's lemma.
A root $(a_1, \dots, a_n)$ of the polynomial $f(x_1, \dots, x_n) \mod p^i$ can be lifted to a root α if $\alpha = (a_1 + \alpha_1 p^i, \dots, a_n + \alpha_n p^i) \bmod p^{i+1}$, $0 \leq \alpha_j < p$, is a solution of the following equation

$$f(\alpha) = f(a) + \sum_j \alpha_j p^i \cdot \frac{df}{dx_j}(a) \bmod p^{i+1}. \tag{1}$$

1. Assume $p = 2$ and your $a = (a_1, \dots, a_n)$ represents the first i bits of the root. Rewrite Eq. (1) such that you receive a condition on the next bit of the root.

2. Consider a bivariate polynomial $N = pq \in \mathbb{Z}[p, q]$. Assume (p', q') is the root of this polynomial $\mod 2^i$. Use the above lemma to lift $(p', q') \mod 2^{i+1}$.

Aufgabe 3:
Factor $N = 299$ using factor-basis $B = \{2, 3\}$.