3. Übungsblatt

Abgabe: Mittwoch, 20.5.09

Aufgabe 1 *Common-Modulus-Attacke*: Eine Nachricht m sei zweimal mit dem RSA-Verfahren verschlüsselt und zwar mit den öffentlichen Schlüsseln (n, e) und (n, f), wobei e und f teilerfremd sind.

a) Wie kann man m aus den beiden Schlüsseln $c_e = m^e \bmod n$ und $c_f = m^f \bmod n$ berechnen?

b) Die Nachricht m wurde mit den öffentlichen Schlüsseln $(493, 3)$ und $(493, 5)$ verschlüsselt. Die Chiffretexte sind 293 und 421. Verwende die Common-Modulus-Attacke, um m zu bestimmen.

Aufgabe 2 Sei $f : F_{2^n} \longrightarrow F_{2^n}$ die Funktion aus SubBytes und n ungerade. Zeigen Sie, dass f eine APN-Funktion ist.

Aufgabe 3 Funktioniert das RSA-Verfahren auch, wenn $n = p_1 p_2 p_3$ Produkt dreier verschiedener Primzahlen p_1, p_2 und p_3 ist?

Aufgabe 4 Gib zwei Gründe an, warum die beiden Primzahlen bei der RSA-Verschlüsselung verschieden seien sollten.