Übungsblatt 5

Kryptographie und Kodierungstheorie
WiSe 16/17

Aufgabe 5.1. Nehmen wir an, dass zum RSA-Verfahren mit öffentlichem Schlüssel (n, e) die Zahl d mit $ed \equiv 1 \bmod \varphi(n)$ bekannt ist ($\varphi(n)$ sei natürlich unbekannt!). Wir schreiben $ed - 1 = 2^s k$ für eine ungerade positive ganze Zahl k und $s > 0$. Aus der Vorlesung wissen Sie, dass die Wahrscheinlichkeit für ein zufällig gewähltes $a \in (\mathbb{Z}/n\mathbb{Z})^*$ die Eigenschaft $1 < \text{ggT}\ (a^{2^t k} - 1, n) < n$ für $0 \leq t < s$ zu erfüllen, größer oder gleich $\frac{1}{2}$ ist. Sei die tatsächliche Wahrscheinlichkeit p. Wie groß ist die Wahrscheinlichkeit, dass wir nach l-maliger unabhängiger Wahl ein a finden, dass diese Eigenschaft erfüllt?

Aufgabe 5.2. (Common-Modulus-Attacke)
Wenn man mit dem RSA-Verfahren eine Nachricht m zweimal verschlüsselt, und zwar mir den öffentlichen Schlüsseln (n, e) und (n, f), und wenn ggT $(e, f) = 1$ gilt, dann kann man den Klartext m aus beiden Schlüsseltexten $c_e = m^e \bmod n$ und $c_f = m^f \bmod n$ berechnen. Wie geht das?

Aufgabe 5.3. (Cycling-Attacke)
Sei (n, e) der öffentliche RSA-Schlüssel. Für einen Klartext $m \in \{0, 1, \ldots, n - 1\}$ sei $c = m^e \bmod n$ der zugehörige Schlüsseltext. Zeigen Sie, dass es eine natürliche Zahl k gibt mit

$$m^{e^k} \equiv m \bmod n.$$

Beweisen Sie für ein solches k:

$$c^{e^{k-1}} \equiv m \bmod n.$$

Ist dies eine Bedrohung für RSA?

Aufgabe 5.4. Sei p eine Primzahl und sei $g \in (\mathbb{Z}/p\mathbb{Z})^*$ eine Primitivwurzel. Sei ferner x eine ganze Zahl mit $0 \leq x < p - 1$. Zeigen Sie: Ist g^x eine Primitivwurzel, so ist ggT $(x, p - 1) = 1$.

Aufgabe 5.5. Sei $p \equiv 3 \bmod 4$. Bestimmen Sie die Lösungen x mod p von $x^2 \equiv$

$a \bmod p$, wobei

$$p = 4545637639999999983647$$
$$a = 1681885926821065193 79$$

Aufgabe 5.6. Alice erhält den ElGamal-Schlüsseltext $(B = w^b, c = A^b m) = (30, 7)$. Ihr öffentlicher Schlüssel ist $(p, w, A = w^a) = (43, 3, 38)$. Bestimmen Sie den zugehörigen Klartext.

Aufgabe 5.7. Bob verschlüsselt Nachrichten an Alice mit dem Rabin-Verfahren. Er verwendet die Parameter $p = 11$ und $q = 23$. Die Klartexte sind Blöcke in $\mathbb{F}_2^8$, wobei Alice möchte, dass die ersten beiden und die letzten beiden Bits 0 sind. Kann Alice alle Klartexte eindeutig entschlüsseln?