Datensicherheit, Zusammenfassung Vorlesung 13

Henry Haustein, Dennis Rössel

Wie können Primzahlen erzeugt werden?

Probabilistischer Test nach Rabin-Miller: Falls p prim, dann $\forall a \in \mathbb{Z}_p^* : a^{\frac{p-1}{2}} \equiv \pm 1 \mod p$. Falls p nicht prim, dann gilt dies höchstens für $\frac{1}{4}$ der möglichen a.

Wie werden die öffentlichen und geheimen Parameter für RSA bestimmt?

Wahl von k_e mit $1 < k_e < \Phi(n)$ und $ggT(k_e, \Phi(n)) = 1$, $k_d = k_e^{-1} \mod \Phi(n)$

Wie erfolgt die Ver- bzw. Entschlüsselung?

Verschlüsselung: $c = m^{k_e} \mod n$

Entschlüsselung: $m = c^{k_d} \mod n$

Wie erfolgt das Signieren und Testen?

Signieren: $s = m^{k_s} \mod n$

Testen: $m = s^{k_t} \mod n$?

Worauf ist bei der Parameterwahl bzgl. Sicherheit zu achten?

Wahl von p und q als große Primzahlen, die nicht dicht beieinander liegen, aber auch nicht zu weit auseinander

Welche Angriffsmöglichkeiten bestehen bei der einfachen, unsicheren Variante von RSA?

passive Angriffe: RSA arbeitet deterministisch, man kann also verschlüsseln und vergleichen

aktive Angriffe: RSA ist ein Homomorphismus bezüglich Multiplikation: Angreifer beobachtet Signaturen s_1, s_2 für Nachrichten m_1, m_2. Dann ist $s_3 = s_1 \cdot s_2$ eine Signatur für $m_3 = m_1 \cdot m_2$

Wie werden die passiven Angriffe verhindert?

Zufallszahl r hinzufügen: $c = (r, m, h(r, m))^{k_e}$ $\rightarrow$ indeterministische Verschlüsselung

Wie werden die aktiven Angriffe verhindert?

Redundanz