Kryptografie und -analyse, Zusammenfassung Vorlesung 10

Henry Haustein

Wie funktioniert ElGamal als Signatursystem?

Schlüsselgenerierung identisch

A führt folgende Schritte aus:

- wählt Zufallszahl $r \in \mathbb{Z}_p^*$
- berechnet r^{-1} mit $rr^{-1} \equiv 1 \mod (p-1)$
- berechnet $s = (s_1, s_2)$ mit

$$s_1 = g^r \mod p$$
$$s_2 = r^{-1}(h(m) - k_s s_1) \mod (p-1)$$

Test der Signatur:

- testet ob $1 \leq s_1 \leq p-1$
- berechnet $v_1 = k_t^{s_1} s_1^{s_2} \mod p$
- berechnet $h(m)$ und $v_2 = g^{h(m)} \mod p$
- akzeptiert Signatur, wenn $v_1 \equiv v_2$

Was ist bei der sicheren Verwendung von ElGamal als Signatursystem zu beachten? Warum darf die Zufallszahl nur einmal verwendet werden? Warum wird eine Hashfunktion auf die Nachricht angewendet?

selbiges wie bei ElGamal als Konzelationssystem

Verwendung einer Hash-Funktion

Wie werden die Parameter bei RSA gewählt?

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

Wie wird ver- und entschlüsselt bzw. signiert und getestet?

Verschlüsselung: $c = m^{k_e} \mod n$
Entschlüsselung: $m = c^{k_d} \mod n$

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

Nachweis der Entschlüsselung?

Zu zeigen, dass

$$\begin{aligned} m &= \left(m^{k_e}\right)^{k_d} \mod n \\ m &= m^{k_e \cdot k_d} \mod n \end{aligned}$$

Wir wissen $k_e \cdot k_d \equiv 1 \mod \Phi(n)$, also $k_e \cdot k_d = l(p-1)(q-1)+1$. Damit

$$\begin{aligned} m^{k_e \cdot k_d} &= m^{l(p-1)(q-1)+1} \mod n \\ &= \left(m^{p-1}\right)^{l(q-1)} \cdot m \mod n \end{aligned}$$

Da p eine Primzahl ist, gilt nach dem kleinen Satz von Fermat ($a^{p-1} \equiv 1 \mod p$) und weil $p \mid n$:

$$1^{l(q-1)} \cdot m = m \mod p$$

Was ist bei der Parameterwahl von RSA zu beachten?

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