Datensicherheit, Übung 9

Henry Haustein

Aufgabe 1

Konzelationssystem: öffentlicher Schlüssel zum Verschlüsseln, privater Schlüssel zum Entschlüsseln

Authentikationssystem: privater Schlüssel zum Signieren, öffentlicher Schlüssel zum Testen der Signatur

Aufgabe 2

Hinzufügen einer Zufallszahl, verhindert aktive und passive Angriffe

Aufgabe 3

(a) WolframAlpha liefert $20^{-1} \equiv 27 \mod 77$

(b) $ggT(77, 14) \neq 1$, damit ist 14 nicht invertierbar mod 77

Aufgabe 4

(a) k_e muss zwei Anforderungen erfüllen: $1 < k_e < \Phi(n)$ und $ggT(k_e, \Phi(n)) = 1$.

$$\begin{aligned}\Phi(69) &= \Phi(3 \cdot 23) \\ &= \Phi(3) \cdot \Phi(23) \\ &= 2 \cdot 22 \\ &= 44\end{aligned}$$

Damit scheiden 8 und 11 als k_e aus.

(b) Einfach alle möglichen Nachrichten verschlüsseln und schauen ob $c = 20$ ist $\Rightarrow m = 5$.

```
1  (0:10)^5 %% 69
2  # 0  1 32 36 58 20 48 40 62 54 19
```

Aufgabe 5

Signaturschlüssel $k_s = k_t^{-1} \mod \Phi(pq)$, k_t muss teilerfremd zu $\Phi(77) = 60$ sein, das heißt $k_t = 7$ und damit $k_s = 43$.

Aufgabe 6

(a) $k_d = k_e^{-1} \mod \Phi(n) = 3^{-1} \mod (2 \cdot 10) = 7$

(b) $c = m^{k_e} \mod n = 6^3 \mod 33 = 18$

(c) $m = c^{k_d} \mod n = 18^7 \mod 33 = 6$

(d) Finde Linearkombination $up + vq \equiv 1 \mod n \Rightarrow u = 4$ und $v = -1$. Dann $m = upy_q + vqy_p \mod n$, wobei

$$\begin{aligned} y_p &= c^{k_{d,p}} \mod p \\ y_q &= c^{k_{d,q}} \mod q \\ k_{d,p} &= k_e^{-1} \mod p - 1 = 3^{-1} \mod 2 = 1 \\ k_{d,q} &= k_e^{-1} \mod q - 1 = 3^{-1} \mod 10 = 7 \end{aligned}$$

Damit $y_p = 2$ und $y_q = 3$, also $m = 14$

Aufgabe 7

(a) $k_s = k_t^{-1} \mod \Phi(n) = 3^{-1} \mod (2 \cdot 16) = 11$

(b) $s = m^{k_s} \mod n = 7^{11} \mod 51 = 31$

(c) $m = s^{k_t} \mod n = 12^3 \mod 51 = 45$. Signatur passt nicht zur Nachricht.