



Lösungsskizzen zu Übung 9

Achtung: Die Lösungsskizzen sollen nur die Ideen veranschaulichen und sind daher gelegentlich sehr informell geschrieben; präzisere Lösungen sollten allerdings leicht daraus ableitbar sein.

Aufgabe 1 (Aktive Angreifer auf DH-Schlüsselaustausch)

Eve gibt sich gegenüber Alice als Bob aus, und gegenüber Bob als Alice. Eve fängt die Nachricht $A = g^a \bmod p$ von Alice ab, wählt selber ein passendes \tilde{a} , und sendet Bob $\tilde{A} = g^{\tilde{a}} \bmod p$. Die Antwort $B = g^b \bmod p$ von Bob wird von Eve auch abgefangen und ebenfalls durch $\tilde{B} = g^{\tilde{b}} \bmod p$ ersetzt. Alice berechnet nun

$$\tilde{B}^a = \left(g^{\tilde{b}}\right)^a = g^{\tilde{b} \cdot a} = k_a \bmod p$$

was aber Eve ebenfalls durch

$$A^{\tilde{b}} = \left(g^a\right)^{\tilde{b}} = g^{a \cdot \tilde{b}} = k_a \bmod p$$

berechnen kann.

Für Bob kann Eve genauso vorgehen. Alice glaubt nun mit Bob den Schlüssel k_a ausgehandelt zu haben, den Eve aber kennt. Ebenso glaubt Bob mit Alice den Schlüssel k_b ausgehandelt zu haben, den Eve ebenfalls kennt. Tauschen Alice und Bob nun mit diesem Schlüssel gesicherte Nachrichten aus, so kann Eve die Nachrichten entschlüsseln, und sie dann mit dem jeweils anderen Schlüssel wieder verschlüsseln und weiterschicken.

B.W.

Aufgabe 2 (Verschlüsselung und One-Way-Funktionen)

Angenommen f wäre keine One-Way-Funktion, dann gäbe es einen Algorithmus \mathcal{A}_x , der bei Eingabe von pk Zufallsbits x^* (eventuell $x^* \neq x$) so bestimmt, dass gilt $f(x^*) = pk$. Dann gilt aber auch $\text{KGen}(1^n; x^*) = (sk^*, pk)$ für einen (eventuell von sk verschiedenen) Schlüssel sk^* . Da \mathcal{E} vollständig ist, gilt trotzdem immer $m = \text{Dec}(sk^*, \text{Enc}(pk, m))$.

Ein CPA-Angreifer \mathcal{A} auf \mathcal{E} kann nun zwei beliebige (verschiedene, da $M_{pk} \geq 2$) Nachrichten im Nachrichtenraum wählen, läßt sich beide von seiner Verschlüsselungsbox verschlüsseln, läßt sich von $\mathcal{A}_x(pk)$ Zufallsbits x^* berechnen, berechnet nun mit Hilfe von $\text{KGen}(1^n; x^*)$ einen geheimen Schlüssel sk^* , und kann so den Ciphertext von der Verschlüsselungsbox wieder entschlüsseln. Gelingt es \mathcal{A}_x nicht, geeignete Zufallsbits x^* mit $f(x^*) = pk$ zu bestimmen, so versucht \mathcal{A} einfach das Bit b in der Verschlüsselungsbox zu raten, indem er ein zufälliges Bit a ausgibt.

Wir zeigen, dass \mathcal{A} signifikant besser ist als die Ratewahrscheinlichkeit. Da \mathcal{A}_x ein erfolgreicher Angreifer auf die One-Way-Eigenschaft von f ist, gibt er mit nicht-vernachlässigbarer Wahrscheinlichkeit $\epsilon(n)$ ein passendes Urbild x^* aus. In diesem Fall sagt der Angreifer auf das Verschlüsselungssystem stets erfolgreich das Bit b vorher. Wenn \mathcal{A}_x kein passendes x^* findet (mit Wahrscheinlichkeit $1 - \epsilon(n)$), dann rät \mathcal{A} das Bit b mit Wahrscheinlichkeit $1/2$. Insgesamt gilt daher:

$$\text{Prob}[a = b] = \epsilon(n) \cdot 1 + (1 - \epsilon(n)) \cdot \frac{1}{2} = \frac{\epsilon(n)}{2} + \frac{1}{2},$$

was mehr als vernachlässigbar über $\frac{1}{2}$ liegt (da mit $\epsilon(n)$ auch $\epsilon(n)/2$ nicht vernachlässigbar ist)