

Lösungen zu Übungsblatt 5 Kryptographische Verfahren

Besprechung 4. Dezember 2015

Aufgabe 5.1. Der Geburtstagsangriff mit konstantem Speicher terminiert

Es sei mit $P(n, k)$ die Wahrscheinlichkeit bezeichnet, bei n Versuchen (n verschiedenen Eingaben) bei einer Hashlänge von 2^k Bits keine Kollision zu erhalten.

$$\begin{aligned} P(n, k) &= 1 \cdot \frac{2^k - 1}{2^k} \cdot \dots \cdot \frac{2^k - n + 1}{2^k} \\ P(n, k) &= \prod_{i=0}^{n-1} \frac{2^k - i}{2^k} \\ &= \prod_{i=1}^{n-1} \left(1 - \frac{i}{2^k}\right) \end{aligned}$$

Da $(1 - x)$ durch e^{-x} nach oben abgeschätzt werden kann, gilt

$$\begin{aligned} &\leq \prod_{i=1}^{n-1} e^{-\frac{i}{2^k}} \\ &= e^{-\sum_{i=1}^{n-1} \frac{i}{2^k}} \\ &= e^{-\frac{1}{2^k} \sum_{i=1}^{n-1} i} \\ &= e^{-\frac{1}{2^k} \frac{n(n-1)}{2}} \\ &\leq e^{-\frac{(n-1)^2}{2 \cdot 2^k}} \end{aligned}$$

Gesucht ist nun n , sodass $P(n, 128) \leq \frac{1}{4}$.

$$\begin{aligned} e^{-\frac{(n-1)^2}{2 \cdot 2^k}} &\leq \frac{1}{4} \\ -\frac{(n-1)^2}{2 \cdot 2^k} &\leq \ln \frac{1}{4} \\ -(n-1)^2 &\leq 2 \cdot 2^k \cdot \ln \frac{1}{4} \\ -n^2 + 2n - 1 &\leq 2 \cdot 2^k \cdot \ln \frac{1}{4} \\ n^2 - 2n + 1 &\geq -2 \cdot 2^k \cdot \ln \frac{1}{4} \end{aligned}$$

Mit den üblichen Verfahren, z.B. pq-Formel und Computerunterstützung lässt dies als positive Lösung zu

$$n_{128} \gtrapprox 30.715.843.678.825.642.450 \approx 3.0716 \cdot 10^{19}$$

Man müsste also mehr also über dreißig Trillionen Versuche machen. Analog gelangt man für $k = 160$ zu dem Ergebnis

$$n_{160} \gtrapprox 2.012.993.531.335.517.303.552.701 \approx 2.013 \cdot 10^{24}$$

oder etwa 2 Quadrillionen Versuche.

Aufgabe 5.2. Der Geburtstagsangriff mit konstantem Speicher findet Kollisionen

Falls es $1 \leq I < J$ mit $x_I = x_J$ und damit $H(x_{I-1}) = H(x_{J-1})$ gibt, so hat die Folge x_1, \dots, x_q offenbar eine Periode von $J - I$. Der $(J + i)$ -te Wert ist also gleich dem $(I + i)$ -ten. Falls man die Periodizität schon für $i < I$ annehmen kann, gilt $x_{J-I} = x_{J-I+J-I} = x_{2(J-I)}$.

Allgemein stimmt die Aussage aber nicht!

Gilt zum Beispiel $x_7 = x_{12}$, so ist $x_8 = x_{13}, x_9 = x_{14}, x_{10} = x_{15}, x_{11} = x_{16}$ und kein $i < J$ erfüllt die Bedingung.

Aufgabe 5.3. Schlüsseltauschprotokolle

a)

Der Breitmaulwurf ist nicht einmal gegen Angriffe ohne bekannten Schlüssel sicher, wenn es keinen Zeitstempel gibt. Fängt der Angreifer eine Nachricht ab, deren Inhalt er kennt (hierfür könnte er den bekannten Schlüssel vielleicht verwenden), so könnte er diese erneut senden und erneut eine Reaktion auslösen (z.B. eine Überweisung o.Ä.).

Ein Problem ist auch, dass vor allem ohne Zeitstempel (aber potenziell auch mit, wenn der Angriff innerhalb eines Zeitfensters durchgeführt wird, das nicht verdächtig ist) ein Angreifer die Validität eines Schlüssels erhalten kann, indem er abwechseln Alice und Bob vertritt und die Nachricht $E_{K_{BC}}(t_Z, A, K_{AB})$ an Charlie sendet, die dieser zuvor an Bob geschickt hatte. Charlie sendet dann $E_{K_{AC}}(t'_Z, B, K_{AB})$ an Alice und der Schlüssel K_{AB} bleibt aktiv. Sendet man die Nachricht immer schnell genug zurück an Charlie, kann der Schlüssel so am Leben erhalten werden.

b)

Das Needham-Schroeder- und das Otway-Rees-Protokoll sind sicher gegen Angriffe mit bekannten Sitzungsschlüsseln, weil Charlie diesen immer neu generiert. Wir hoffen, dass Charlie ein Verfahren verwendet, dass es nicht zulässt von alten Schlüsseln auf neue Schlüssel zu schließen – z.B. unter Verwendung von Timestamps. Sind diese Timestamps nicht vorhanden, sind Replay-Attacken jedoch weiterhin möglich.

c)

Da Alice A und den Sessionkey aus $E_{k_A}(r_A, k_{AB}, B, E_{k_B}(A, k_{AB}))$ weiß, kann sie aus $E_{k_B}(A, k_{AB})$, A und k_{AB} auf k_B schließen. Der Angriff funktioniert auch, wenn das Protokoll um einen Timestamp erweitert wird.

Aufgabe 5.4. Ein sicheres Protokoll?

a)

$$\begin{aligned}w \oplus t &= u \oplus r \oplus t \\&= s \oplus t \oplus r \oplus t \\&= k \oplus r \oplus t \oplus r \oplus t \\&= k \oplus r \oplus r \oplus t \oplus t \\&= k \oplus 0 \oplus 0 \\&= k\end{aligned}$$

b)

1. Erste Nachricht von Alice abfangen $\rightarrow s := k \oplus r$
2. Erste Nachricht von Bob abfangen $\rightarrow u := s \oplus t$
3. Zweite Nachricht von Alice abfangen $\rightarrow w := u \oplus r$
4. Berechnen:

$$\begin{aligned}r &= w \oplus u \quad (u \oplus r \oplus u) \\k &= s \oplus r \quad (k \oplus r \oplus r)\end{aligned}$$

Damit hat der Angreifer den Schlüssel, der von Alice und Bob verwendet wird.