Übung zur Vorlesung „Sicherheit“
22.05.2014 – Übungsblatt 3

Florian Böhl
florian.boehl@kit.edu

Abgabe der Übungsblätter

- Viel mehr - vielen Dank!
- Natürlich auch „Pseudonym “möglich

Sicherheit – Übungsblatt 3 – Aufgabe 1

Aufgabe 1. $H, H' : \{0,1\}^* \to \{0,1\}^k$ kollisionsresistente Hashfunktionen. Ist $\hat{H}$ kollisionsresistent?

(a) $\hat{H}(x) := H(x||x)$

(b) $\hat{H}(x) := H(x) \oplus H'(x)$

(c) $\hat{H}(x) := H(H'(x))$

(d) $\hat{H}(x) := F(x)||H(x)$ für bel. $F : \{0,1\}^* \to \{0,1\}^k$

(e) $\hat{H}(x) := H(F(x))$ für bel. Einwegfunktion $F : \{0,1\}^* \to \{0,1\}^k$

(f) $\hat{H}(x) := \begin{cases} x & \text{wenn } |x| = k \\ H(x) & \text{sonst} \end{cases}$

(g) $\hat{H}(x) := H(F(x))$ für bel. injektives $F : \{0,1\}^* \to \{0,1\}^*$

Sicherheit – Übungsblatt 3 – Aufgabe 1

Fazit:

- Wir haben unser Verständnis von Kollisionsresistenz vertieft.

Sicherheit – Übungsblatt 3 – Aufgabe 2

Aufgabe 2.

- $\mathrm{F} : \{0,1\}^{2k} \to \{0,1\}^k$ kollisionsresistenten Kompressionsfunktion
- Definiere $\mathrm{H}_{\mathrm{MD}}(M)$ wie folgt:
  1. Setze $B := \lceil \frac{L}{k} \rceil$. Dann $M||0^{k-L \bmod k} = M1||\ldots||M_B$ k-Bit-Blöcke $M_1, \ldots, M_B$.
  2. Setze $M_{B+1} := L$, wobei L mit exakt k Bits codiert wird.
  3. Setze $Z_0 := 0^k$.
  4. Für $i = 1, \ldots, B+1$ berechne $Z_i := \mathrm{F}(Z_{i-1}, M_i)$.
  5. Gib Z_{B+1} aus.
- *a)* $\mathrm{H}'_{\mathrm{MD}}(M)$ kollisionsresistent?
- *b)* $\mathrm{H}'_{\mathrm{MD}}(M)$ kollisionsresistent für M mit $|M| \bmod k = 0$?

Sicherheit – Übungsblatt 3 – Aufgabe 2

Fazit:

- Für die Sicherheit der Merkle-Damgård-Konstruktion ist es essentiell, dass wir die Länge der Eingabe in den Hash einbringen (außer es sind nur Eingaben gleicher fester Länge erlaubt)

Sicherheit – Übungsblatt 3 – Aufgabe 3

Aufgabe 3. Im ersten Teil der RSA-Schlüsselgenerierung wurden für einen Benutzer A die Primzahlen $P = 23$ und $Q = 11$ gezogen.

(a) Setzen Sie die RSA-Schlüsselgenerierung fort. Berechnen Sie einen zu P und Q gehörigen öffentlichen RSA-Schlüssel $pk_A = (N, e)$ und einen privaten RSA-Schlüssel $sk_A = (N, d)$.
Hinweis: Führen Sie den erweiterten euklidischen Algorithmus zur Übung von Hand durch.

(b) Senden Sie die Nachricht $M = 17$ RSA-verschlüsselt an Benutzer A. Benutzen Sie dazu die Lehrbuch-Variante von RSA (ohne Padding) und den öffentlichen Schlüssel aus (a).

(c) Nehmen wir an, Sie seien Benutzer A. Entschlüsseln Sie das empfangene Chiffrat aus (b).

Sicherheit – Übungsblatt 3 – Aufgabe 3

Fazit:

- Wir wissen wie RSA-Schlüsselgenerierung, -Verschlüsselung und -Entschlüsselung in der Lehrbuch-Variante funktionieren
- Wir haben den erweiterten euklidischen Algorithmus geübt

Sicherheit – Übungsblatt 3 – Aufgabe 4

Aufgabe 4 Auf der Webseite zur Vorlesung finden Sie die Datei `Sicherheit_UE03_Moduli.zip`, die 50.000 512-Bit RSA-Moduli enthält, von denen einige nicht vernünftig generiert wurden. Wie viele Moduli können Sie faktorisieren?

Sicherheit – Übungsblatt 3 – Aufgabe 4

- Motiviert durch Paper „Ron was wrong, Whit is right“
- 0.2% der aus dem Internet eingesammelten RSA-Moduli waren „schwach “
- $\Rightarrow$ bei uns $50.000 * 0.2\% = 100$

Sicherheit – Übungsblatt 3 – Aufgabe 4

Wie findet man die schwachen Moduli? Beispielsweise

- Batch-GCD
- Pollard-Rho
- ECM (Faktorisierung über elliptischen Kurven nach Lenstra)

Sicherheit – Übungsblatt 3 – Aufgabe 4

Fazit:

- Gute Entropie bei der RSA-Schlüsselgenerierung wichtig
- Große Mengen RSA-Moduli lassen sich effizient auf gemeinsame Teiler untersuchen

Organisatorisches

- Nächste Übung am Do, 12.06.14
- Nächstes Übungsblatt am Mo, 26.05.14