Kryptographische Verfahren Klausur Haupttermin Lösungen

03. Februar 2016

Erlaubte Hilfsmittel sind: Taschenrechner, Cäsarscheibe, Vigenère Tabelle

Aufgabe 1 — 5 Punkte

Pro richtiger Antwort gibt es einen Punkt, falsche Antworten geben Abzug, die minimal zu erreichende Punktzahl ist 0 Punkte

Fragen	Antworten
1. In jedem perfekt sicheren Kryptosystem gibt es echt weniger Klartexte als Schlüssel	☑ falsch ❒ wahr
2. Ein Public Key Kryptosystem ist genau dann polynomiell CPA sicher, wenn es polynomiell sicher gegen einen passiven Angreifer ist	❒ falsch ☑ wahr
3. Nachrichten sollte man erst veschlüsseln und dann authentifizieren	☑ falsch ❒ wahr
4. Für Signatur und Verschlüsselung sollte der identische Schlüssel verwendet werden	☑ falsch ❒ wahr
5. $\Phi(375)$ ist 210	☑ falsch ❒ wahr

Aufgabe 2 — 5 Punkte

Entschlüssele den Kryptotext NFNYSNKCLZRVOA, welcher mit dem Vigenère Verfahren und dem Schlüssel DRWHO verschlüsselt wurde.

▷ **KORREKTGELOEST**

Aufgabe 3 — 3 + 4 Punkte

Berechne ohne technische Hilfsmittel und dokumentiere jeden Schritt gut

- größter gemeinsamer Teiler von 1528 und 4052
- 46^{113} mod 55

▷ **ggT(4052, 1528) = 4**

$$\begin{aligned}
&a = 4052, b = 1528 \\
&1)\ r = 996, a = 1528, b = r \\
&2)\ r = 532, a = 996, b = r \\
&3)\ r = 464, a = 532, b = r \\
&4)\ r = 68, a = 464, b = r \\
&5)\ r = 56, a = 68, b = r \\
&6)\ r = 12, a = 56, b = r \\
&7)\ r = 8, a = 12, b = r \\
&8)\ r = 4, a = 8, b = r \\
&9)\ r = 0, b = \text{ Ergebnis } = 4
\end{aligned}$$

▷ **46^{113} mod 55 = 41**

$$\begin{aligned}
&b = 46, e = 113, n = 55, z = 1 \\
&1)\ e \text{ ungerade}, z = [1 \cdot 46]_{55} = 46, b = [46^2]_{55} = 26, e = 56 \\
&2)\ e \text{ gerade}, b = [26^2]_{55} = 16, e = 28 \\
&3)\ e \text{ gerade}, b = [16^2]_{55} = 36, e = 14 \\
&4)\ e \text{ gerade}, b = [36^2]_{55} = 31, e = 7 \\
&5)\ e \text{ ungerade}, z = [46 \cdot 31]_{55} = 51, b = [31^2]_{55} = 26, e = 3 \\
&6)\ e \text{ ungerade}, z = [51 \cdot 26]_{55} = 6, b = [26^2]_{55} = 16, e = 1 \\
&7)\ e \text{ ungerade}, z = [6 \cdot 16]_{55} = 41, b = [16^2]_{55} = 36, e = 0 \\
&z = \text{ Ergebnis } = 41
\end{aligned}$$

Aufgabe 4 — 5 Punkte

Wenn beim One Time Pad der Schlüssel $\mathrm{K} = 0^n$ ist, dann ist $\mathrm{E}nc_k(m) = m$. Daher wird oft vorgeschlagen, nur Schlüssel $\mathrm{K} \neq 0^n$ zu benutzen, also gleichmäßig aus allen anderen Schlüsseln zu wählen. Ist dieses modifizierte One Time Pad noch perfekt sicher?

Aufgabe 5 — 5 Punkte

Eine Hashfunktion $(\mathrm{G}en, \mathrm{H})$ sei kollisionsresistent und längenerhaltend, dh $|x| = |\mathrm{H}^s(x)|$ für alle Schlüssel s und Eingabe x. Zeigen Sie, dass dann auch $(\mathrm{G}en, \hat{\mathrm{H}})$ mit $\hat{\mathrm{H}}^s(x) = \mathrm{H}^s(\mathrm{H}^s(x))$ kollisionsresistent ist.

Aufgabe 6 — 4 + 5 Punkte

Sei $\sqcap = (\mathrm{G}en, \mathrm{E}nc, \mathrm{D}ec)$ CPA sicher und $\sqcap' = (\mathrm{G}en, \mathrm{E}nc', \mathrm{D}ec')$ mit $\mathrm{E}nc'_k(m) = (r, \mathrm{E}nc_k(\mathrm{E}nc_r(m)))$ mit $r = \mathrm{G}en(1^n)$ und $\mathrm{D}ec'_k(c) = \mathrm{D}ec_r(\mathrm{D}ec_k(c))$

- Beschreiben Sie ein Zufallsexperiment um ein Kryptosystem auf CPA Sicherheit zu überprüfen. Definieren Sie, wann ein Kryptosystem CPA sicher ist.
- Zeigen Sie, dass $\sqcap'$ CPA sicher ist.

Der Angriff mit gewähltem Klartext

Das Kryptosystem ist $\Pi = (Gen, E_k, D_k)$ und der Angreifer ist ein PPT Algorithmus $\mathcal{A}$.

1. Das Orakel generiert einen Schlüssel $k = Gen(1^n)$.
2. Der Angreifer generiert zwei Klartexte $m_0, m_1 \in \mathcal{M}$ mit $|m_0| = |m_1|$ und schickt sie an das Orakel.
3. Das Orakel wählt gleichverteilt ein zufälliges Bit $b \in \{0, 1\}$ und sendet $c = E_k(m_b)$ an den Angreifer.
4. $\mathcal{A}$ kann beliebige Klartexte m' an das Orakel senden und erhält stets $c' = E_k(m')$ zurück.
5. $\mathcal{A}$ berechnet ein Bit $b' \in \{0, 1\}$.
6. Wir setzen $Att^{CP}_{\mathcal{A},\Pi}(n) = 1$ falls $b = b'$ und 0 sonst.

▷

Definition

Ein Kryptosystem ist **polynomiell sicher gegen einen Angriff mit gewählten Klartexten**, wenn für jeden PPT-Algorithmus $\mathcal{A}$ mit Zugriff auf das Orakel eine vernachlässigbare Funktion ν existiert mit

$$P\left(Att^{CP}_{\mathcal{A},\Pi}(n) = 1\right) \leq \frac{1}{2} + \nu(n)$$

wobei η eine vernachlässigbare Funktion ist.

▷