Kryptographische Verfahren Klausur Haupttermin

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 u 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.

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

Aufgabe 4 — 5 Punkte

Wenn beim One Time Pad der Schlüssel $\mathrm{K} = 0^n$ ist, dann ist $\mathrm{Enc}_k(m) = m$. 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 $(\mathrm{Gen}, \mathrm{H})$ sei kollisionsresistent und längenerhaltend, dh $|x| = |\mathrm{H}^s(x)|$ für alle Schlüssel s und Eingabe x. Zeigen Sie, dass dann auch $(\mathrm{Gen}, \hat{\mathrm{H}})$ mit $\hat{\mathrm{H}}^s(x) = \mathrm{H}^s(\mathrm{H}^s(x))$ kollisionsresistent ist.

Aufgabe 6 — 4 + 5 Punkte

Sei $\sqcap = (Gen, Enc, Dec)$ CPA sicher und $\sqcap' = (Gen, Enc', Dec')$ mit $Enc'_k(m) = (r, Enc_k(Enc_r(m)))$ mit $r = Gen(1^n)$ und $Dec'_k(c) = Dec_r(Dec_k(c))$

- 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.