Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 11 (17.1.2025)

Bemerkungen:

(1) Zur Lösung einer Kryptographie-Aufgabe gehört auch eine (kurze) Darstellung des Lösungswegs.
(2) Mit **P** werden Präsenzaufgaben, mit **H** Hausaufgaben bezeichnet.
(3) Abgabe der Hausaufgaben bis Freitag, 24.1.2025 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P41: Christine und Daniel verwenden das Massey-Omura-Verfahren zur Nachrichtenübertragung, wie es in der Vorlesung beschrieben wurde. Zugrundeliegt die Primzahl $p = 12323$. Christine hat sich natürliche Zahlen e_C, d_C gewählt mit $e_C d_C \equiv 1 \bmod (p-1)$, Daniel hat sich Zahlen e_D, d_D gewählt mit $e_D d_D \equiv 1 \bmod (p-1)$. Christine will eine Zahl $a \in \{0, 1, \ldots, p-1\}$ Daniel mitteilen, sie berechnet zunächst $b = a^{e_C} \bmod p$ und schickt b an Daniel. Daniel berechnet $c = b^{e_D} \bmod p$ und schickt c an Christine. Christine berechnet $d = c^{d_C} \bmod p$ und schickt d an Daniel. Die Zahlen b, c, d sind

$$b = 10068, \quad c = 5381, \quad d = 3188.$$

Welche Zahl will Christine Daniel mitteilen? (Hinweis: `RVARKCBARAGVFGXYRVA`)

Aufgabe P42: $p = 1111113803$ und $q = 555556901$ sind Primzahlen mit $p - 1 = 2q$, außerdem ist 2 eine Primitivwurzel modulo p. Wir betrachten die Funktion

$$h : \{0, 1, \ldots, q-1\} \times \{0, 1, \ldots, q-1\} \to \{1, \ldots, 2q\} \quad \text{mit} \quad h(x, y) = 3^x 2^y \bmod p.$$

Der Definitionsbereich von h hat q^2 Elemente, der Bildbereich $2q$ Elemente. Jemand findet die „Kollision“

$$h(185185633, 384779994) = h(324074858, 277778450).$$

Bestimme damit den diskreten Logarithmus von 3 zur Basis 2 modulo p.

Aufgabe P43: Sei N eine RSA-Zahl (mit Primteilern p und q). Wir definieren

$$f : \{1, \ldots, \frac{N-1}{2}\} \to \{1, \ldots, N-1\} \quad \text{durch} \quad f(x) = x^2 \bmod N.$$

Zeige: Ist $a \in \{1, \ldots, \frac{N-1}{2}\}$ mit $\mathrm{ggT}(N, a) = 1$, so gibt es genau ein $b \in \{1, \ldots, \frac{N-1}{2}\}$ mit

$$f(a) = f(b) \quad \text{und} \quad a \neq b.$$

Mit diesem b gilt dann:

$$\mathrm{ggT}(N, a - b) \text{ ist ein Primteiler von } N.$$

Kann man N praktisch nicht faktorisieren, so ist f also schwach kollisionsresistent (second preimage resistant).
(Hinweis: $x^2 \equiv a^2 \bmod N \iff x \equiv \pm a \bmod p$ und $x \equiv \pm a \bmod q$)

Datei: ki_u11.tex. Version vom 15.1.2025

P44: Zu einem öffentlichen RSA-Schlüssel $(N, e) = (5893, 3)$ werden Dokumente mit Hashwerten h_i und zugehörigen RSA-Signaturen s_i gefunden. Welche der Signaturen sind gültig, welche ungültig?

$$(h_1, s_1) = (1111, 2925), \quad (h_2, s_2) = (2222, 2018), \quad (h_3, s_3) = (3333, 3208).$$

Hausaufgaben

Aufgabe H41: Anna und Birgit verwenden das Massey-Omura-Verfahren mit

$$p = 643857638976237856123423450234578236457826348571273423894756238745237345323661 31$$

um geheim zu kommunizieren. Anna hat geheim Zahlen e_A, d_A mit $e_A d_A \equiv 1 \bmod (p-1)$, Birgit geheim Zahlen e_B, d_B mit $e_B d_B \equiv 1 \bmod (p-1)$ gewählt. Um einen Treffpunkt mit Birgit zu vereinbaren, wandelt Anna ihren Text in eine Zahl a um, indem sie jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt. Dann berechnet sie $b = a^{e_A} \bmod p$ und schickt b an Birgit. Birgit berechnet $c = b^{e_B} \bmod p$ und schickt c an Anna. Anna berechnet $d = c^{d_A} \bmod p$ und schickt d an Birgit. Die Zahlen b, c, d sind

$$\begin{aligned} b &= 189341765224832332695108234928573983036474869727653512054676172908797644810149 13, \\ c &= 250369223663457958694102225638058757631551574166198862944128761015967484440628 36, \\ d &= 549364397823364032299476389824859400591111823502759641834735116758448318925544 56. \end{aligned}$$

(1) Wie entschlüsselt Birgit Annas Nachricht?
(2) Wo wollen sich Anna und Birgit treffen?
(Hinweis: `IVREHAQFRPUFMVTANPUXBZZNFGRYYRAIBACVFVAQRVATRURVZRERKCBARAG`)

Aufgabe H42: Anna und Birgit wollen eine additive Variante des Massey-Omura-Verfahrens ausprobieren. Sie verwenden die 8. Fermat-Zahl

$$F_8 = 2^{2^8}+1 = 115792089237316195423570985008687907853269984665640564039457584007913129639937.$$

Anna hat eine Zahl e_A gewählt, Birgit eine Zahl e_B. Um eine Nachricht an Birgit zu schicken, wandelt Anna die Nachricht in eine Zahl a um, indem sie jedes A durch 01, jedes B durch 02,..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt. Anna berechnet dann $b = a + e_A \bmod F_8$ und schickt b an Birgit. Birgit berechnet $c = b + e_B \bmod p$ und schickt c zurück an Anna. Anna berechnet $d = c - e_A \bmod p$ und schickt d wieder an Birgit. Birgit berechnet $e = d - e_B \bmod p$ und erhält nach Umwandlung in Text die von Anna gesandte Nachricht. Öffentlich bekannt werden folgende Zahlen:

$$\begin{aligned} b &= 261262025610352907495713842331854278130980722801893169439238448587580982 18666 \\ c &= 889255274393601088417232794550723450164059983396492397051445798841522289598 \\ d &= 905551928577259258833199135930637215403411623948986594932062367481868618513 74. \end{aligned}$$

Ist diese Nachrichtenübertragung sicher? Wenn nein, was will Anna Birgit mitteilen?

Aufgabe H43: $p = 31966869046443581251$ ist eine 20-stellige Primzahl, 2 eine Primitivwurzel modulo p. Wir betrachten die Funktion

$$h : \{0, \ldots, p-2\} \times \{0, \ldots, p-2\} \to \{1, \ldots, p-1\} \quad \text{mit} \quad h(x, y) = 3^x 2^y \bmod p.$$

Man findet die „Kollision“

$$h(3380883590576682845, 26499651447240539134) = h(4091022741240185405, 8791880850881185624).$$

Bestimme den diskreten Logarithmus von 3 zur Basis 2 modulo p.

Aufgabe H44: Jeder aus Großbuchstaben und Leerzeichen bestehenden Zeichenkette z wird auf folgende Weise ein Hashwert $h(z)$ zugeordnet: In der Zeichenkette wird jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt, wodurch eine Zahl $a \in \mathbb{N}_0$ entsteht. Dann wird $h(z) = a \bmod N$ gesetzt mit einer 160-Bitzahl N, d.h. $2^{159} \leq N < 2^{160}$. Nun ist bekannt, dass

$$h(\text{„ICH GEBE MEINE ZUSTIMMUNG“}) = h(\text{„ICH GEBE MEINE ZUSTIMMUNG NICHT“})$$

gilt. Bestimme N und den gemeinsamen Hashwert der Zeichenketten.