Vorlesung „Kryptographie I“ (Wintersemester 2024/2025)

Übungsblatt 12 (24.1.2025)

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, 31.1.2025 in den Übungskästen (bis 10:00 Uhr), in Übungsgruppe 1 oder digital (bis 14:00 Uhr).

Präsenzaufgaben

Aufgabe P45:

(1) $(p, g, e_A) = (1231231, 3, 65537)$ ist ein privater ElGamal-Signatur-Schlüssel, $g = 3$ ist eine Primitivwurzel modulo p. Bestimme den zugehörigen öffentlichen Schlüssel (p, g, f_A). Signiere ein Dokument mit Hashwert $h = 1234$ unter Verwendung der kleinstmöglichen „Zufallszahl“ $z \geq 100$ und überprüfe, ob die erstellte Signatur die Signaturtestgleichung erfüllt.
(2) Christians öffentlicher ElGamal-Signatur-Schlüssel ist $(p, g, f_C) = (5557, 5, 1313)$. Es ist bekannt, dass Christian zum Signieren als „Zufallszahl“ z gerne die Zahl 3305 nimmt. Ein Dokument mit Hashwert $h = 3042$ und Christians Signatur $(b, c) = (7, 10)$ wird gefunden. Bestimme Christians privaten Schlüssel.

Aufgabe P46: Ute verwendet die ElGamal-Signatur mit dem öffentlichen Schlüssel $(p, g, f) = (15083, 5, 1773)$. Vera schaut sich Signaturen von Ute an und stößt dabei auf die zwei Signaturen $(15081, 10179)$, $(15081, 10178)$ zu den Hashwerten 12668 und 7719. Was fällt Vera auf? Was ist der private Schlüssel von Ute?

Aufgabe P47: $(p, g, f) = (1231381, 6, 818087)$ ist ein öffentlicher ElGamal-Signatur-Schlüssel. Erstelle eine gültige Unterschrift für diesen Schlüssel zum Hashwert $h = 1111111$. (Hinweis: `OYRVPURAONPURE`)

Aufgabe P48: Johannes und Maximilian haben sich (auch) auf folgendes Verschlüsselungsverfahren geeinigt: Zugrunde liegt eine fixpunktfreie Involution[1] f von $\{\mathrm{A}, \ldots, \mathrm{Z}\}$, aus der man weitere fixpunktfreie Involutionen durch die Vorschrift $f_i = \mathrm{CAESAR}_{-i} \circ f \circ \mathrm{CAESAR}_i$ bilden kann. (Nach Identifikation der Großbuchstaben mit den Zahlen $0, \ldots, 25$ lässt sich dies auch in der Form $f_i(x) = (f((x + i) \bmod 26) - i) \bmod 26$ schreiben.) Ein Klartext $a_1 a_2 a_3 \ldots$ wird mittels der Formel $b_i = f_i(a_i)$ zu $b_1 b_2 b_3 \ldots$ verschlüsselt.
Maximilian schreibt an Johannes folgende Nachricht:

```
IJTXC VTTZGSLZ,
ARA XNXIVCAN, MVGX NCLYW QJFNKMGTJRMXSGMBZAKMRVYJYS SXVCA HZZD RDHVZW PZO,
OLZU ODHMSW HQNZD, YHRM IRK BHZ AWV KQW DBUORU-GLXDRAUNXLXZMPGR IJHFI
QSNUDANTYSI UVJLZM. QTZCEPZNAO NGQQZLI QBD IZHV WOSWZG MXV IDBIHAMS.
HNZGJ ZQZJXAS GVQHUZXNLS
```

Entschlüssle den Text und bestimme die Permutation f.

Datei: ki_u12.tex. Version vom 20.1.2025

[1] f ist eine Permutation mit $f^{-1} = f$ und $\{x : f(x) = x\} = \emptyset$

Hausaufgaben

H45: Michael hat den öffentlichen RSA-Schlüssel (N, e) mit

$$\begin{aligned} N &= 237226970129158836344842360194080933615207363075201352747847144217295722964999040436470705462149019 3, \\ e &= 100947555112912301758856490968483975153728045567759253043101359590779397679402653103653812112397500 3. \end{aligned}$$

und verwendet SHA3-256 als Hashfunktion.

(1) Katharina empfängt nacheinander zwei von Michael RSA-signierte Nachrichten

„`Ich stimme zu.`“ und „`Ich stimme nicht zu.`“

mit den Signaturen

$$\begin{aligned} s_1 &= 188285049981149924527379062558061641649776184110065232000029396994567361120603102144005521130998908 2, \\ s_2 &= 219608389141085755822590064535790875278708160838639597007133934048541746826011378813899422499538221 2. \end{aligned}$$

Katharina berechnet zunächst die SHA3-256-Hashwerte der Nachrichten und erhält

$$\begin{aligned} h_1 &= (4e27f1099b1e0c43b605154ca4cec36fa9c5faa47d16dc1c177cea208dbff57b)_{16} = \\ &= 353509728048659980132932972767196906715615111740824570569007656271028231837 39, \\ h_2 &= (b1bf1259c28d3999213880c6f41461f0098671cd45e7016c369feecbe5bac496)_{16} = \\ &= 803969686399689989316092262974914522232557444790724961031150934091657858756 06. \end{aligned}$$

Dann überprüft Katharina die Signaturen. Was stellt Katharina fest? Wie kann sich Katharina das erklären?

(2) Erstelle eine RSA-Unterschrift von Michael zur Nachricht

„`Ich stimme doch zu.`“

mit dem SHA3-256-Hashwert

$$\begin{aligned} h_3 &= (88397f15700c7db64d0a991e9214b52a659936989be0b4ec35e1c78d74fadc71)_{16} = \\ &= 616161347897616343294502399926982199835519865643135846941499852948906135297 13. \end{aligned}$$

(Hinweis: `XRGGRAOEHPUNATEVSS`)

H46: Florian verwendet zum Signieren seiner Dateien die ElGamal-Signatur und die SHA-256-Hashfunktion. Sein öffentlicher Schlüssel ist

$$\begin{aligned} p &= 782634897562378465782364587236498756234785628374657823645782369487562387462591 13, \\ g &= 17, \\ f_F &= 331846204812738916020544327776272111003679644919672960198055918786136295891412 63. \end{aligned}$$

Wir finden zwei Dokumente von Florian mit Hashwerten h_i und Signaturen (b_i, c_i):

$$\begin{aligned} h_1 &= (1474478200cf7f6ca028feeef9cc32cac55d6844d783cad9829b9a6fdeed715e)_{16} = \\ &= 925170476004866883313732281989092847637897118256922240930666173231288270473 4, \\ b_1 &= 666798832182369200061903555680718806163508533325214191541707710448607155268530 88, \\ c_1 &= 751242463945915898231742459114886373444149273898357520417122029495147324042997 14, \\ h_2 &= (944f256b0128f3682e9f4d2ee6a2239c5df30f75802af78fcdec8c72e5034768)_{16} = \\ &= 670821407578922009544159287581958127610962062384190607319848618413997657475 60, \\ b_2 &= 666798832182369200061903555680718806163508533325214191541707710448607155268530 88, \\ c_2 &= 620088505177263299090107620681960033981956533567833693952335699085564168722987 04. \end{aligned}$$

Was ist der private Schlüssel e_F von Florian?

Aufgabe H47: Erich verwendet die ElGamal-Signatur, sein öffentlicher Schlüssel ist (p, g, f) mit

$$\begin{aligned} p &= 384975697345976349579847593875968734587638457638547638475683475867345876384765 44, \\ g &= 3, \\ f &= 189266540264157549678958430374093527885641272137678888262465157597021253457264 91. \end{aligned}$$

Es gilt $f = g^e \bmod p$ mit Erichs privatem Schlüssel e.
Eva findet eine Signatur (b, c) von Erich mit

$$\begin{aligned} b &= 962747675484614827756216433730462333428167896191817766095252102615232894067579, \\ c &= 684864221223961244446233899044198607982934286031470554031581322859967447363808 2 \end{aligned}$$

für die Nachricht „`Ich verwende fuer alle meine Dokumente die ElGamal-Signatur.`“ mit dem SHA-256-Hashwert

$$\begin{aligned} h &= (8e0ded6ea309e90d9207ccbb4ade9a4b8560a830f2caa7b5a57d69d945b0efed)_{16} = \\ &= 642530322073142493244606987645953783283088839561093657204340377028164772781 89. \end{aligned}$$

Eva versucht Erichs privaten Schlüssel zu bestimmen, zunächst mit Logarithmenberechnung, gibt aber bald auf. Dann probiert sie es noch mit Nguyens Gitter-Angriff für den Fall, dass Erich seine Zahlen nicht gut gewählt hat. Hat Eva Erfolg?

Aufgabe H48: Petra verwendet SHA-256 als Hashfunktion und hat folgenden öffentlichen ElGamal-Signatur-Schlüssel:

$$\begin{aligned} p &= 957862394785629837465982736489576234785628937465892736489576238947658923747107 03, \\ g &= 3, \\ f_P &= 564804281590788208455321348028699891860046856926150372515619101369213353453810 55. \end{aligned}$$

Bestimme für die Nachricht „`Dies ist vielleicht die letzte Aufgabe.`“, die als SHA-256-Hashwert die Zahl

$$\begin{aligned} h &= (4f4d701ba09c0976dbac64b6629bf3f7f97f12f6c048970209db74ade0510138)_{16} = \\ &= 358695360024895373843134461083562648979508516381022404565797816394526250110 00 \end{aligned}$$

hat, eine gültige ElGamal-Unterschrift von Petra. Warum ist es nicht so leicht, eine gültige Unterschrift für die Nachricht „`Dies ist noch nicht die letzte Aufgabe.`“ mit SHA-256-Hashwert

$$\begin{aligned} h' &= (bd83d039df01b1f6f7f3907af979216349288360b7f8aa83a9b9067b1fbb1e89)_{16} = \\ &= 857200224711657466110961278653830949000707575731909882628576651451487986069 85 \end{aligned}$$

zu erstellen? (Hinweis: `OYRVPURAONPURE`)