Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 10 (4.7.2025)

Aufgabe 46: Sei p eine Primzahl mit $p \equiv 3 \bmod 4$ und E die über $\mathbb{F}_p$ durch

$$y^2 = x^3 + x$$

definierte elliptische Kurve. Zeige:

(1) Es gilt
$$|E(\mathbb{F}_p)| = p + 1.$$
(2) $(0, 0)$ ist der einzige Punkt der Ordnung 2 in $E(\mathbb{F}_p)$.
(3) Es gibt genau zwei Punkte $P \in E(\mathbb{F}_p)$ der Ordnung 4. Wie sehen sie aus?
(Hinweis: $\operatorname{ord}(P) = 4 \Longrightarrow \operatorname{ord}(2P) = 2$)

Aufgabe 47:

(1) Laura und Mark verwenden den Diffie-Hellman-Schlüsselaustausch mit elliptischen Kurven. Sie haben sich auf die NIST-Kurve P-256 (aus SP 800-186) $y^2 = x^3 + ax + b$ über $\mathbb{F}_p$ mit

$$\begin{aligned} p &= 115792089210356248762697446949407573530086143415290314195533631308867097853951, \\ a &= -3, \\ b &= 41058363725152142129326129780047268409114441015993725554835256314039467401291 \end{aligned}$$

und den Punkt

$$\begin{aligned} P = (&48439561293906451759052585252797914202762949526041747995844080717082404635286, \\ &36134250956749795798585127919587881956611106672985015071877198253568414405109). \end{aligned}$$

geeinigt. Laura hat geheim eine Zahl e_L gewählt und damit $Q_L = e_L \cdot P$ berechnet, Mark hat eine Zahl e_M gewählt und damit $Q_M = e_M \cdot P$ berechnet. Die zugehörigen Punkte sind öffentlich bekannt:

$$\begin{aligned} Q_A = (&84938965763058797328056826200781326420737073196699498169097511555630956318428, \\ &50370908203466902250589313561668514024283108899627809901572973130303983726451), \\ Q_B = (&69629489588544981636243001198278564902015476843540174591599825317859385349183, \\ &22706427721578245193343276813418542731427026211359565801876354154803066372079). \end{aligned}$$

Als gemeinsamen Schlüssel verwenden Laura und Mark die Zahl k (in 26-adischer Darstellung mit den Ziffern A,...,Z), die durch

$$(k, \dots) = e_L e_M \cdot P = e_L \cdot Q_M = e_M \cdot Q_L$$

gegeben ist. (Hinweis: `RVATRURVZREFPUYHRFFRYVFGRVARZREFRAARCEVZMNUY`)

(2) Laura will ein Gedicht an Mark schicken. Sie verschlüsselt es mit PLAYFAIR, wobei sie den gemeinsamen Schlüssel verwendet, und schickt den Chiffretext an Mark:

```
PG CS IQ LB WX RN BO YD MK TF SV BK YU EO HK YF KR QV QP SF PI WB KZ YO LV
OT XW RH TY UK YK QF ZY LB GX HO WV PQ ZY PS YB HK BK TY GV BK IB WD EZ HR
OB GX HO KU OH WX KY UI RM OY OW KR VM BL AV YB HK IQ ZY LS RS WX IQ YL RM
QO OB BK IU GL ML BL RY RQ FU TE AO GV RY RQ FL LE KV HV WV ZD UQ XZ RM WX
PS XC ZT UE XO QD LZ QS ML BL WV ZK SF OH WX BR KR IQ IB FT VF DU BO GF QP
GI EX KV HV WV BQ SF QP KR OY YK OE IQ YO OB XY YO NX XC KY LW KR RH RH RB
OY YF EO HK TW HB SU SN BL UG QV FV WD ZH ML LV QO QB KR XC YO HK OT XW ZY
```

NG KR OH IO LB WD MK TF QF KR TW GL AM RM CS BL MG CS

Entschlüssle den Text.

Aufgabe 48: Ein aus Großbuchstaben und Leerzeichen bestehender Text wurde unter Verwendung der additiven Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ElGamal-verschlüsselt mit folgendem öffentlichen Schlüssel:

$$\begin{aligned} n &= 31415926535897932384626433832795028841971693993751058209749445923078164062862089, \\ g &= 27182818284590452353602874713526624977572470936999595749669676277240766303535475, \\ f &= 78153890075468641541305035991587866893481958092935161322919408059117709913659 3. \end{aligned}$$

Dazu wurde der Text in Blöcke der Länge 40 aufgeteilt; jeder Block lieferte eine Zahl a_i, indem jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt wurde. Nach Wahl von Zufallszahlen z_i wurde dann $b_i = z_i \cdot g \bmod n$ und $c_i = a_i + z_i \cdot f \bmod n$ berechnet. Hier sind $b_1, c_1, b_2, c_2, b_3, c_3, b_4, c_4, b_5, c_5, b_6, c_6$:

$$\begin{aligned} b_1 &= 883311693790861699384003432617420336810484802602299946205632311968244703693 2959, \\ c_1 &= 153271721055223510500455845962366833312158303501846128145629826448346762711628 14, \\ b_2 &= 250323997198309194447576343943501893977325521509920458066872923119897792406508 79, \\ c_2 &= 101441899651751421867796074334471477168093167377316720134411961566858638448293 69, \\ b_3 &= 267505522710459482362918899535372542326465663113348014857873045438231302765890 32, \\ c_3 &= 261119432748364185482235099719272894661924533438778214885070395789066140564383 59, \\ b_4 &= 189070294718303729618172710563561303691981734796940823862545514163118158320547 12, \\ c_4 &= 123208989965565925468483822299070731740869573960892943567246376343030337655015 94, \\ b_5 &= 295024308477151164026466596507668377093714227170621122320258060899977735821156 16, \\ c_5 &= 256959416617200045432466306508355670277469853363034245227732630237425377987758 5, \\ b_6 &= 700424850735267113526452576505961567358621124499516079349553762067965578635047 2, \\ c_6 &= 256516264836891670231395504416040532406357253054807495681475197603945065940850 03. \end{aligned}$$

Entschlüssle den Text.

Aufgabe 49: Andreas benutzt eine Variante der ElGamal-Verschlüsselung mit elliptischen Kurven. Zugrunde liegt die durch $y^2 = x^3+3x+5$ über $\mathbb{F}_p$ definierte elliptische Kurve E mit der Primzahl $p = 2^{257}-93$ und ein Punkt $P \in E(\mathbb{F}_p)$ mit

$$P = (0, 120093053909297889720179095228573632825061758203965722207128839817819107536075).$$

Der öffentliche Schlüssel von Andreas ist der Punkt

$$\begin{aligned} Q_A = (&713444095932355123344026754150860173427650537694511775710542016644865682146 4, \\ &108580708946307200913423219518959097464054600342455429036626034090481719471957 195), \end{aligned}$$

den Andreas mit seinem privaten Schlüssel $e_A \in \mathbb{N}$ als $Q_A = e_A \cdot P \in E(\mathbb{F}_p)$ berechnet hat.
Anne will eine Nachricht, die nur aus Großbuchstaben und Leerzeichen besteht, an Andreas schicken. Da p eine 78-stellige Dezimalzahl ist, teilt sie die Nachricht in Blöcke der Länge 39 auf, in jedem Block ersetzt sie A durch 01, B durch 02, ..., Z durch 26 und jedes Leerzeichen durch 00. Es entstehen zwei Zahlen a_1, a_2. Anne wählt nun zwei Zufallszahlen z_1, z_2 und berechnet damit für $i = 1, 2$

$$R_i = z_i \cdot P = (x_{R_i}, y_{R_i}) \in E(\mathbb{F}_p), \quad S_i = z_i \cdot Q_A = (x_{S_i}, y_{S_i}) \in E(\mathbb{F}_p), \quad t_i = a_i + x_{S_i} \bmod p.$$

Anne schickt an Andreas die Zahlentripel $(x_{R_i}, y_{R_i} \bmod 10, t_i)$ für $i = 1, 2$:

$$\begin{aligned}
x_{R_1} &= 135001664608867339009783701689304685898797705532768940484950731388807328425411,\\
y_{R_1} \bmod 10 &= 6,\\
t_1 &= 156196228178631569079516658557401929228571756540951422329239531112844234556242,\\
x_{R_2} &= 208664282426305915407775568498805035099450636856735209466309897905455406606185,\\
y_{R_2} \bmod 10 &= 1,\\
t_2 &= 505458887442060934079563994978560979979396199285430203309898813885694324394 42.
\end{aligned}$$

Was will Anne Andreas mitteilen?
(Hinweis: `CEVINGREFPUYHRFFRYXYRVAFGRCEVZMNUYZVGFVRORAHAQFVROMVTQRMVZNYFGRYYRA`)

Aufgabe 50: Lena verwendet die folgenden ECDSA-Parameter (mit öffentlichem Schlüssel Q_{L})

$$\begin{aligned}
p &= 115792089210356248762697446949407573530086143415290314195533631308867097853951,\\
a &= -3,\\
b &= 41058363725152142129326129780047268409114441015993725554835256314039467401291,\\
q &= 115792089210356248762697446949407573529996955224135760342422259061068512044369,\\
P &= (0, 462637617415086386970109500487096510216888917778779378750969314590067460392 84),\\
Q_{\mathrm{L}} &= (803256902799483033244956391254385233517603519048837233830516245270222410710 04,\\
&\quad 772318928991756748050081976522281274901534048510447609280509048985006784349 57).
\end{aligned}$$

Birgit erhält die Nachricht „Wollen wir uns am Freitag um 12 Uhr in der Mensa treffen?“, die den SHA-256-Hashwert

$$h = 57315985583775457220801190514809865713128875009283885530409721835767567264614$$

hat, zusammen mit der ECDSA-Signatur

$$\begin{aligned}
r &= 777107946760087279954106309026196492580160677672312473045536592402123954599 1,\\
s &= 957982660538584387531504723778248470307800769712446258901525044667860184991??,
\end{aligned}$$

wobei aber wohl die letzten beiden Ziffern von s verlorengingen. Kann die Signatur von Lena stammen? Wenn ja, was ist dann s? (Die verwendete Kurve ist die NIST-Kurve P-256.)