Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 11 (11.7.2025)

Aufgabe 51: Birgit verwendet die folgenden ECDSA-Parameter (mit öffentlichem Schlüssel Q_{B})

$$
\begin{aligned}
p &= 115792089210356248762697446949407573530086143415290314195533631308867097853951,\\
a &= -3,\\
b &= 41058363725152142129326129780047268409114441015993725554835256314039467401291,\\
q &= 115792089210356248762697446949407573529996955224135760342422259061068512044369,\\
P &= (5, 31468013646237722594854082025316614106172411895747863909393730389177298123724),\\
Q_{\mathrm{B}} &= (82212958354890949432601013576474669403735096997779507750388535116725025413493,\\
&\quad\ 85504142713495381299614127521764298325612035343440897926980616870208799149495).
\end{aligned}
$$

Birgit schickt an Lena die Nachricht „O.k. Dann bis Freitag!“, die den SHA-256-Hashwert

$$h_1 = 106752073600880936705788850705646606751701291305035478291073760459426290893 6$$

hat, zusammen mit der ECDSA-Signatur

$$
\begin{aligned}
r_1 &= 82209296696862888763550231015529996147903925099257199015432125073107332996662,\\
s_1 &= 25352795558184954792214766990350804757191999948125086002725437671028686740111,
\end{aligned}
$$

wenig später dann die Nachricht „Entschuldigung, bei mir geht es doch nicht!“, die den SHA-256-Hashwert

$$h_2 = 50095887263701556003167560158899875180910198769723634260381458686662786147120$$

hat, zusammen mit der ECDSA-Signatur

$$
\begin{aligned}
r_2 &= 82209296696862888763550231015529996147903925099257199015432125073107332996662,\\
s_2 &= 87378729693678403673940947772434230567621108891696705302321363120849943275682.
\end{aligned}
$$

War Birgit vielleicht unvorsichtig, sodass man den privaten ECDSA-Schlüssel von ihr bestimmen kann? (Die verwendete Kurve ist die NIST-Kurve P-256.)

Datei: kii_u11.tex. Version vom 10.7.2025

Aufgabe 52: Michaela benutzt das Menezes-Vanstone-Kryptosystem - eine Variante der ElGamal-Verschlüsselung mit elliptischen Kurven - mit der durch die Parameter

$$p = 52389468923648795963, \quad a = 1, \quad b = 2$$

definierten elliptischen Kurve $E_{a,b}$ über $\mathbb{F}_p$ und den Punkten

$$P = (4, 19145803944808026870), \quad Q_M = (46547073320563710700, 3362334782404866328);$$

dabei ist Q_M der öffentliche Schlüssel von Michaela; ihr privater Schlüssel ist eine Zahl $e_M \in \mathbb{N}$ mit $Q_M = e_M \cdot P$.
Nadine will an Michaela geheim einen Namen übermitteln. Sie wandelt den Vornamen in eine Zahl a_1, den Nachnamen in eine Zahl a_2 um, indem sie jedes A durch 01, jedes B durch 02, ..., jedes Z durch 26 ersetzt. Dann wählt Nadine eine geheime Zahl z und berechnet zunächst auf der elliptischen Kurve

$$(r_1, r_2) = z \cdot P \quad \text{und} \quad (s_1, s_2) = z \cdot Q_M$$

und anschließend

$$t_1 = a_1 s_1 \bmod p \quad \text{und} \quad t_2 = a_2 s_2 \bmod p.$$

Danach sendet Nadine die Zahlen

$$r_1, r_2, t_1, t_2$$

an Michaela:

`30535045327702025503, 46921205081638383838, 20044859049134796600, 34199549296360840747.`

Oliver fängt die 4 Zahlen ab. Er vermutet, dass einer der Namen „THOMAS DISTLER“, „RAINER HUBER“, „RICHARD MUELLER“ oder „PAUL SCHMIDT“ übermittelt werden sollte. Kann Oliver den richtigen Namen herausfinden? (Hinweis: `FKVFGKRVAKXHEIRACHAXG`)

Aufgabe 53: Für $n \in \mathbb{N}$ und $K \in \mathbb{N}$ sei

$$f(n, K) = \mathrm{ggT}(n, 2^{K!} - 1).$$

Zeige:

(1) Es gilt
$$f(n, K) = \mathrm{ggT}(n, (2^{K!} \bmod n) - 1).$$

(2) Definiert man rekursiv
$$a_0 = 2 \quad \text{und} \quad a_k = a_{k-1}^k \bmod n \text{ für } k \geq 1,$$
so gilt
$$2^{K!} \bmod n = a_K,$$
und damit auch
$$f(n, K) = \mathrm{ggT}(n, a_K - 1).$$
(Mit den angegebenen Formeln kann man $f(n, K)$ berechnen, wenn K nicht zu groß ist.)

(3) Zerlegt man $n = 2^e m$ mit $e \in \mathbb{N}_0$ und $m \equiv 1 \bmod 2$, so gilt $f(n, K) = f(m, K)$.

(4) Es gilt $f(n, K) \mid f(n, K + 1)$. (Insbesondere ist die Funktion $K \mapsto f(n, K)$ monoton steigend.)

(5) Ist n ungerade und $K \geq \varphi(n)$, so gilt $f(n, K) = n$. Dabei steht φ für die Eulersche φ-Funktion.

(6) Ist p ein ungerader Primteiler von n, hat $p - 1$ die Primfaktorzerlegung
$$p - 1 = q_1^{e_1} \dots q_r^{e_r} \quad \text{und gilt} \quad q_i^{e_i} \leq K \text{ für } i = 1, \dots, r,$$
so folgt
$$p \mid f(n, K).$$

(7) Welche Werte nimmt die Funktion $K \mapsto f(65, K)$ an?

(Durch Berechnung von $f(n, K)$ kann man versuchen, nichttriviale Teiler von n zu finden.)

Aufgabe 54: Ein aus Großbuchstaben und Leerzeichen bestehender Text wurde in eine Zahl a umgewandelt, indem jedes A durch 01, jedes B durch 02, ...jedes Z durch 26 und jedes Leerzeichen durch 00 ersetzt wurde. Mit der 4096-Bit-RSA-Zahl N wurde dann $b = a^{65537} \bmod N$ berechnet. Hier sind die Zahlen N und b:

$$
\begin{aligned}
N = {} & 99035032221988903147789662509526851606582074760648677777243217117776326228391013 \\
& 16953314508858230021113367820722169879902579132631516874394231131626398441680848 \\
& 24450997750422566826539293155508196482742974403199970076610245458684392876214989 \\
& 42946885926812559336940581637642032926691908122677481004064024524839645254788658 \\
& 81362229177490520880335854737472679857439808213382279991418723359075220771525790 \\
& 09137955893676021601407167740031704705649134793938746890312507452126609265575407 \\
& 28646820325474362166860090586505340550836693034738272995053875217049658955707087 \\
& 31185819875894537760041776357597422893039002377282337622666746124351817044111873 \\
& 06098421488992506335323921525176204416269781466250912422168823310729357725971987 \\
& 23994745591791249621585374120727510393807576232159273744979621244250774621746178 \\
& 56834812095811753758357904185996250462537069865981809460279594182801212229145889 \\
& 08172961085678243071241689973115333337819036558156141163163137847364960944851409 \\
& 00816035010114909116365740885857021525477098985287946815139424677871723068880693 \\
& 74427991333418809497637984054463579186955226797575755444956398444754754593290561 \\
& 57616543601098111517593089545272910126138476167867337957269654081787468330949139 \\
& 02842404109722354307588435448528 1
\end{aligned}
$$

$$
\begin{aligned}
b = {} & 14527350524404042820519830052096750255678609254529339558728245377465183622500223 \\
& 88004994806529530200634613511035408638122942767786215325926636690354552043938654 \\
& 66995183263509144817277143040737592937442545396032984123566680950551718416741718 \\
& 24507429209290558507690620162885708654655814831742227961883074969602044100120604 \\
& 02060175804191179803779183921839669370648876353541542358134895980759975177781533 \\
& 16299065747047990314655384702836708361216419734871913499062529590796341901474448 \\
& 86656984769717959964019254539304661769277899134442265953805527280215294558045124 \\
& 88919043882787014697996193765627598430145583322181782648159832526865940140731257 \\
& 44465869635751598757636239214597574898309898079648240821516219810234692312058187 \\
& 85733498849121156130584361353617635092678904953666655693458464135531913509545148 \\
& 86841682645114173360469541107172956257475216406375900188110256774605121286923430 \\
& 32887642503440375744627151824987090077070747372845726231145338952941319908028731 \\
& 00783332471498134742804296816893892058990444405130917204847974566927531202747668 \\
& 55399816677173833400524021297696289157769365495778454685461853183272871724115952 \\
& 01005412138543633491256358709418810721069231572019312730748716271050044653024269 \\
& 44345473724521335067137366963586 1
\end{aligned}
$$

Entschlüssle den Text. (Hinweis: `IBENATRTNATRARNHSTNOR`)

Aufgabe 55: (Faktorisierung mit elliptischen Kurven) Die Zahl

$$N = 49904844249493013243493437540610133516273061964241545207950857246116432057247536284936776105405859 47$$

ist eine 100-stellige RSA-Zahl. Bestimme die Primfaktorzerlegung.
(Hinweis: `IREJRAQRRYYVCGVFPURXHEIRZVGNAHYYOQERVCRVAFMJRV`)