6. Übungsblatt Revision 2
Diskrete Strukturen (WS 14/15)

Bauhaus-Universität Weimar, Professur für Mediensicherheit
Prof. Dr. Stefan Lucks, Christian Forler, Eik List
URL: `https://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching/ws-2014/diskrete-strukturen-vorlesung/`

Abgabe und Besprechung: 06.01.2014 (13:30 Uhr) in der Übung

Aufgabe 1 (4 Punkte) Polynome über $\mathbb{Z}_3[X]$
Sei $f(x) = 2x^7 + x^4 + x^3 + 2$ und $g(x) = x^4 + 2x^3 + 1$ mit $f(x), g(x) \in \mathbb{Z}_3[X]$ Berechnen Sie die Lösung für die folgenden Aufgaben. Geben Sie den Rechenweg mit an.

a) $f(x) + g(x)$

b) $f(x) - g(x)$

c) $f(x) * g(x)$

d) $f(x)/g(x)$

Aufgabe 2 (4+4 Punkte) Shamir Secret-Sharing

a) Gegeben sind die folgenden Punkte $(4, 2), (5, 5), (2, 3)$. Bestimmen Sie das durch den Shamir Secret-Sharing Algorithmus eindeutig festgelegte Geheimnis über dem Körper $\mathbb{Z}_{11}$.

b) Gegeben sind die folgenden Punkte $(1110, 1001), (1001, 0011)$. Bestimmen Sie durch den Shamir-Secret-Sharing Algorithmus eindeutig festgelegte Geheimnis über dem Körper $GF(2^4)$ mit $p(x) = x^4 + x + 1$ als irreduzibles Polynom.

Vergessen Sie bitte nicht Ihren Lösungsweg mit anzugeben.
(Hinweis: Machen Sie die Probe um Rechenfehler zu finden!)

Aufgabe 3 (2+2 Punkte) Irreduzible Polynome

a) Zeigen oder widerlegen Sie folgende Aussage:

$$p(x) = a_n x^n + ... + a_0 \in K[x] \text{ ist irreduzibel } \implies a_0 = 0.$$

b) Geben Sie alle irreduziblen Polynome für $GF(2^2)$ inklusive nachvollziehbarem Lösungsweg an.

Aufgabe 4 (4 Punkte) Programmieraufgabe: Lagrange
Implementieren Sie in Python3 die Interpolationsformel von Lagrange (Kapitel 5.4, Folie 222, Satz 90) für $Z_{619}[X]$ und $n = 3$. Die Eingabe- und Ausgabewerte $a_1, a_2, a_3 \in Z_{619}$ mit $a_i \neq a_j$ für $i \neq j$, und $b_1, b_2, b_3 \in Z_{673}$ sollen dabei als Kommandozeilenparameter übergeben werden. Die Ausgabe des Programms ist das Polynom $p(x)$ mit $p(a_i) = b_i$ für alle $i = 1, ..., n$.

Beispiel: Für $a_1 = 1, a_2 = 2, a_3 = 3$ und $b_1 = 4, b_2 = 0 b_3 = 4$ gilt:
`# python3 rsa_123456.py 1 2 3 4 0 4`
$p(x) = 4x^2 + 603x^1 + 16$.

Bevor Sie Ihre Implementation einreichen, sollten Sie die folgenden Tests korrekt beantworten.

Testfall $a_1, a_2, a_3, b_1, b_2, b_3$	**Polynom**
1, 2, 3, 0, 0, 0	$p(x) = 0x^2 + 0x^1 + 0$
25, 50, 75, 12, 24, 48	$p(x) = 1x^2 + 594x^1 + 12$
7, 10, 61, 57, 4, 504	$p(x) = 604x^2 + 31x^1 + 575$
85, 97, 7, 94, 231,478	$p(x) = 251x^2 + 187x^1 + 488$

(*Abgabe:* Schicken Sie Ihre Lösung als Anhang einer E-Mail `lagrange_<MatrNr>.py` an `christian.forler@uni-weimar.de` mit dem Betreff "`[DS] Lagrange`"

Aufgabe 5 (2 Punkte) Bonusaufgabe: RSA mit Großen Zahlen
Schreiben Sie ein Python3-Skript welches als Klartext ihre Matrikelnummer mit dem Prefix "99423" ($99423 < MatrNr >$) unter den folgenden RSA Parametern verschlüsselt.

- e = 16269633778234476349351773547908389683611886626309711306642673764063848627363888554408514939442685384936838274722466924918660826399980873846274855023243350676693335283183162342246122425739309030983433649450992761258551799012642886017537178338943636940570694747251832552557849247888332012068165065966207897246 3

- n = 13557357356171670334351358912813434518687081821678083355290396932371845910695416420484245727734258204683300386126063313473147476605012092293150355034277624531886354794984956314365954982908092856337395088159084498208724982766746285048908729743160914930116918835556925237626686362642200006199424073015916226206775547897810300990712950825765269536165997294655207999786456275594626493235541720974564089636180158947177734618807666165281366906892870277740600708070423708405087348477722857789882955453533846191054599055623513113838020983713247823566958774754604939203790960975796771067348999028486447706129895099287499052071

(*Abgabe:* Schicken Sie Ihre Lösung bestehend aus

- Chiffretext(e) (einen pro Gruppenmitglied) und
- Ihrem Python3-Skript `rsa_<MatrNr>.py` (Anhang)

mit dem Betreff "`[DS] RSA`" bis zum **24.12.2014** an `christian.forler@uni-weimar.de`.)

Beispielaufruf:
`# python3 rsa_123456.py 123456`
2042346447517301000076500848122800565649345050043774184368046186920968627746336015786663718206732549992432051449991696063861748612288548758397851899532808239653535673228826484799481984925699001481313683461558353371324102368875729114439479247046531878097804276282249804349539705791738742976691899100991800857521603449431039790935735946693744538919528047090523031920791138527059760863271110124809295240896865256099149557277994659805326896946190271600965796284482844590292989135602905596230274604425440584341169530692354744342430641278781343844437977460712746062974985902192617261295305833306665147230800368119957351046960

A Jolly Santa Claus

Fröhliche Weihnachten und einen guten Rutsch ins neue Jahr wünscht Ihnen ihr Lehrstuhl für Mediensicherheit!