

Sicherheit: Fragen und Lösungsansätze – Übung 1

AUFGABE 1 (PGP) (BP 3p):

- Intallieren Sie PGP (z.B. OpenPGP)
- Erstellen Sie sich ein PGP-Zertifikat.
- Senden sie ihren Public Key an Thomas Ruhroth, wobei dieser mit dem Public Key von Thomas Ruhroth verschlüsselt sein sollte. Dei Daten die sie dafür benötigen finden Sie auf meiner Web-Page (<http://www-secse.cs.tu-dortmund.de/staff/ruhroth>).
- Schicken Sie bitte in der Mail folgenden Text verschlüsselt mit, wobei die passenden Stellen ersetzt sein sollen.

Hallo Thomas Ruhroth,
anbei finden Sie meinen PGP-Schlüssel für die Emailadresse **Ihre-Adresse**.
Der Fingerprint lautet: **Ihr-Fingerprint**.
Gruß **Ihr-Name**

- Geben Sie in der schriftlichen Abgabe ihr Mail-Adresse und ihren Fingerprint an.

AUFGABE 2 (Ringe) (BP 3p):

Manche denken Pippi Langstrumpf kann nicht Rechnen. Zeigen Sie, dass dies nicht stimmt. Lesen Sie sich das Lied von Pippi Langstrumpf aufmerksam durch. In diesem sind an mehreren Stellen mathematische Behauptungen aufgestellt, die auf den ersten Blick vollkommen falsch wirken - sie müssen es aber nicht sein!

Erstellen Sie auf Grundlage des Liedes einen Ring, in dem alle besungenden Behauptungen wahr werden. Ist ihr Ring kommutativ, unitär, oder sogar ein Körper?

2 x 3 macht 4
Widdewiddewitt und Drei macht Neune !!
Ich mach' mir die Welt
Widdewidde wie sie mir gefällt

Hey - Pippi Langstrumpf
trallari trallahey tralla hoppsasa
Hey - Pippi Langstrumpf,
die macht, was ihr gefällt.

Hey - Pippi Langstrumpf
trallari trallahey tralla hoppsasa
Hey - Pippi Langstrumpf,
die macht, was ihr gefällt.

Ich hab' ein Haus,
ein kunterbuntes Haus
ein Äffchen und ein Pferd,
die schauen dort zum Fenster raus.
Ich hab' ein Haus,
ein Äffchen und ein Pferd,
und Jeder, der uns mag,
kriegt unser 1 x 1 gelehrt.

2 x 3 macht 4
Widdewiddewitt und Drei macht Neune !!
Wir machen uns die Welt
Widdewidde wie sie uns gefällt

2 x 3 macht 4
Widdewiddewitt und Drei macht Neune !!
Ich mach' mir die Welt
Widdewidde wie sie mir gefällt

Hey - Pippi Langstrumpf
trallari trallahey tralla hoppsasa
Hey - Pippi Langstrumpf,
die macht, was ihr gefällt.

3 x 3 macht 6 - widdewidde
Wer will's von mir lernen ?
Alle groß und klein
trallalala lad' ich zu mir ein.

Ich hab' ein Haus,
ein kunterbuntes Haus
ein Äffchen und ein Pferd,
die schauen dort zum Fenster raus.
Ich hab' ein Haus,
ein Äffchen und ein Pferd,
und Jeder, der uns mag,
kriegt unser 1 x 1 gelehrt.

2 x 3 macht 4
Widdewiddewitt und Drei macht Neune !!
Wir machen uns die Welt
Widdewidde wie sie uns gefällt

Hey - Pippi Langstrumpf
trallari trallahey tralla hoppsasa
Hey - Pippi Langstrumpf,
die macht, was ihr gefällt.

3 x 3 macht 6 - widdewidde
Wer will's von uns lernen ?
Alle groß und klein
trallalala lad' ich zu uns ein

AUFGABE 3 (Galois-Feld) (LP 4p) :

Gegeben sei ein Galois-Feld $GF(2^8)$, wie es in den Folien beschrieben wurde.

- Bestimmen Sie für ein Polynom die fehlenden dezimalen, binären und hexadezimalen Darstellungen:
 - $P = 4$
 - $Q = (AF)_{16}$
 - $R = (0101\ 1010)_2$
- Berechnen Sie:
 - $P + Q$
 - $P + R$
 - $Q * 2$
 - $R * (0B)_{16}$

Geben Sie von ihren Ergebnissen je mindestens eines in binärer, hexadezimaler und in Polynomdarstellung an. Es bleibt Ihnen überlassen, welches Ergebnis Sie wie angeben.