Institut für Angewandte und Numerische Mathematik
Dr. Daniel Weiß • Dipl.-Math. oec. Marcel Mikl • Dipl.-Biol. Michael Kreim

Mathematik I für die Fachrichtung Informationswirtschaft

Übungsblatt 15

Wintersemester 2013/2014

Gruppenübung T31 (RSA-Verschlüsselung)

(a) Verschlüsseln Sie eine Zahl mit dem RSA-Algorithmus

(b) Entschlüsseln Sie die Nachricht: 13.
Tipp: Die Nachrichten wurde mit dem öffentlichen Schlüssel $(15, 3)$ verschlüsselt.

(c) Entschlüsseln Sie die folgende Nachricht:

```
22  4 10 17 10 23  6 15 17  7
32 10  4  9 10 23 16 17  1 21
24 21 23
```

Tipp: Die Nachrichten wurde mit dem öffentlichen Schlüssel $(35, 5)$ verschlüsselt.

Gruppenübung T32 (Caesar-Verschlüsselung)

Entschlüsseln Sie den folgenden, mit einer Caesar-Verschlüsselung verschlüsselten, Text:

```
KPLJH LZHYC LYZJO SBLZZ LSBUN PZALP ULPUM HJOLZ ZFTTL AYPZJ
OLZCL YZJOS BLZZL SBUNZ CLYMH OYLUK HZHBM KLYTV UVNYH WOPZJ
OLUBU KTVUV HSWOH ILAPZ JOLUZ BIZAP ABAPV UIHZP LYAHS ZLPUL
ZKLYL PUMHJ OZALU BUKBU ZPJOL YZALU CLYMH OYLUK PLUAL ZOLBA
LOHBW AZHLJ OSPJO KHGBN YBUKW YPUGP WPLUK LYRYF WAVSV NPLHU
ZJOHB SPJOK HYGBZ ALSSL UILPK LYCLY ZJOSB LZZLS BUNDP YKQLK
LYIBJ OZAHI LKLZR SHYAL EAZHB MLPUL UNLOL PTALE AIBJO ZAHIL
UHINL IPSKL AKPLZ LHIIP SKBUN LYNPI AZPJO PUKLT THUKP LGLPJ
OLULP ULZNL VYKUL ALUHS WOHIL AZBTL PULIL ZAPTT ALHUG HOSGF
RSPZJ OUHJO YLJOA ZCLYZ JOPLI AKPLH UGHOS KLYCL YZJOV ILULU
GLPJO LUIPS KLAKL UZJOS BLZZL SKLYM BLYKP LNLZH TALCL YZJOS
BLZZL SBUNB UCLYH LUKLY AISLP IA
```

Auf diesem Übungsblatt sind keine Hausübungen mehr. Eine Abgabe ist nicht mehr vorgesehen.
Webseite: `http://www.math.kit.edu/ianm3/lehre/math1infowirt2013w/`.