Übung zur Vorlesung

Kryptographie und Komplexität

Prof. Dr. Christoph Kreitz
Universität Potsdam, Theoretische Informatik, WS 2014/15

Blatt 1 — Besprechungstermin: 12.11.2014

Aufgabe 1.1 (Wahrscheinlichkeitsabschätzungen)

1. Wie groß ist die Wahrscheinlichkeit, bei einer zufälligen Wahl einer Zahl zwischen 1 und 1000 eine Quadratzahl zu finden?
2. Wie groß ist die Wahrscheinlichkeit, bei einer zufälligen Wahl einer Zahl zwischen 1 und 1000 eine Primzahl zu finden?
3. Wie groß ist die Wahrscheinlichkeit, daß eine zufällig gewählte Chiffrierungsfunktion $e_K : \{0,1\}^n \to \{0,1\}^n$ eine affin-linear Chiffrierung ist?
4. Wieviele Personen müßte man versammeln, damit die Wahrscheinlichkeit, daß zwei Personen dieselbe PIN für Ihre EC-Karte haben, mindestens 50% ist?

Aufgabe 1.2 (Dechiffrierung einfacher Chiffren)

Versuchen Sie, die folgenden Schlüsseltexte zu dechiffrieren. Identifizieren Sie den entsprechenden Klartext und den verwendeten Schlüssel. Die einfachsten Chiffren können von Hand gebrochen werden, die anderen nur mit Unterstützung durch einen Computer. Die Texte enthalten keinen Zeilenumbruch.

1. **Verschiebechiffre**

   POBCJQOWKDOACJSXJNOAJOANOXJBCORCJNSOJPYAWJKDBJVORWJQOLAKXXC

2. **Affine Chiffre**

   CMWNLAHOHPWZFVRHLVIYBVIDFPVCMWNLAEMHNRDZGRFOVKFMSHRMFOVIYVUMFGRFO

3. **Substitutionschiffre**

   MTZJPXKRILNFNOK ZJAZDZTYBFZIJTSJWX RXWZFQOTYBZFJ TFFZJMTZJ IWMTZJVLFJSZIBLMZFJWF
   MJIZYBFTPZFJWSJTFGLXSNITLFZFJNW JVZX YBOWZ ZOIZFJIZEIZFJDWJQZUTFFZFJMTZ ZJTFGLX
   SNITLFZFJPLZFFZFJ LULBOJMZXJVZXUZFMZIZJ YBOWZ ZOJUTZJNWYBJMZXJLXTQTFNOIZEIJ ZTF
   JBZWIDWINQZJAZDZTYBFZIJMZXJAZQXTGGJPXKRILNFNOK ZJNOOQZSZTFZXJMTZJNFNOK ZJVLFJPXK
   RILQXNRBT YBZFJVZXGNBXZFJSTIJMZSJDTZOJMTZ ZJZFIUZMZXJDWJAXZYBZFJNO LJTBXZJ YBWID
   GWFPITLFJNWGDWBZAZFJLMZXJTBXZJ TYBZXBZTIJFNYBDWUZT ZFJWFMJDWJCWNFITGTDTZXZFJPXKR
   ILNFNOK ZJT IJMNSTIJMN JQZQZF IWZYPJDWXJPXKRILQXNRBTZ

4. **Vigenere Chiffre**

   HFKQVIDJCJAVUWDEJPCENHGVIHFPHV GQUWCIGUDUOFCPEITHV KHLTAFLI CKOEN BVIIOGVDLFDHR
   SAWQH LQPQTAAXDEJPHQ EQSTEMVCRIFFHVSDJPITUGURDFPCJA KWDAMUC ITUHRSDJDJTMGUDFFJOX
    FUCMHNBDR UKHJESBHMNTKFLTAWQH CTDYCIDDVEOBHVGFDQMSTGQDUOFCELTBPINTEKDITVCIRAWQJ
   AFJLK ECVDLFDHR WCKEOKHWSFPCD

5. **Hill Chiffre**

   KINHYSCAALKATACOGZXHOGNUUONLRMCCPHOXEGUKRNUTJFMJOGPIZBBTVFEMNMXFEMOWLWVXPWLHOAHY
   S XRIHGPFWUBNLMFDFWOMNJQIENKFEMNMXSEVDZFYNAHPQGOSWUQTHAJWVJNORGOFWZWUQXDQVN BREG
   NULOUOOMUOPJNOHOAL D PJRDLFVMZSMLYISRKNMXVUQONDRDXAFK P RHOXHOLKALPRKCSTRBWBJK W
   JNCJUZDUQKTSZCGBKSVCGOJBNUYGPADTFWMXARWKZHCCPLJQKMIV EXVEURVTRWRIANWHTRHFDPXJOTJ
   IODYPOEWISKCS OPWUQOMGCP WDWUIMHTZWMVDKXUBNFNBRUDNP WVRXDN

Die Blocklänge ist 3. Das Wort ¨ MEPHISTOPHELES¨ (Block beginnt mit Leerzeichen) kommt im Klartext vor, was aber nicht bedeutet, dass sich die ersten 3 Symbole dieses Klartextes für die Konstruktion einer invertierbaren Matrix eignen.

6. **Eine unbekannte Chiffriermethode**

```
QVTYGBGQXFKWMEJGDTM UDXYZWGDIJPCIJOBQSNBPULJKEUMXKJWWFFVWHIFUOIETGDHEXUERJGFEVS
BLKXFTHKSZGBMEFORHSXUHSYFPQYNZOWPFKDCRWGFHDNJWCIXNVFDFKJSWZZCWXIHTCINFNQRE FHSLN
TCIY BBVZUGUENVGFIXNBHRRXRWSQKQUMSMQEVEKKCPSXPEEJHFQVE IRWUZCCHRYBLXTFXUPJGNCIRH
CQOSFWWJWYGCMEKPLXMYTVSNNUFI XBHEHSGWMMTBOWFFJVIRRGDKEOGHMWYGBHSZFVEEXVSYXKUQDJY
KCQYKBGRFRAKIHXKHDMTPCYIOAHRLXKDMJZICGSYNVLTNWVDIVPCVFGMOKSGPGIEKMLDQ WWPSXCVLII
HHEYFWQ ITTHZSFQGVEKWHDSIBVSQFCVVJMQVIXZBQWJKDVQJJNCVIKBXWJZJQGJBNCIJHVUWFKVWIJZ
BQRNJGCMQYBLIIZBV JFNNIYRWXXETTXDFJPXIYXDVVJJTCIRTBHGMYJLDJZWJEKTOHSJFOQDEF
```