Übung zur Vorlesung

Kryptographie und Komplexität

Prof. Dr. Christoph Kreitz
Universität Potsdam, Theoretische Informatik, WS 2015/16

Blatt 1 — Besprechungstermin: 4.11.2015

Aufgabe 1.1 (Wahrscheinlichkeitsabschätzungen)

1. Wie groß ist die Wahrscheinlichkeit, bei einer zufälligen Wahl einer Zahl zwischen 1 und 100 eine Quadratzahl zu finden? Wie groß ist die Wahrscheinlichkeit für Zahlen zwischen 1 und 1000 bzw. 1 und 1000000?
2. Wie groß ist die Wahrscheinlichkeit, bei einer zufälligen Wahl einer Zahl zwischen 1 und 50 eine Primzahl zu finden? Wie groß ist die Wahrscheinlichkeit für Zahlen zwischen 1 und 1000 bzw. 1 und 1000000?
3. Wie groß ist die Wahrscheinlichkeit, daß eine zufällig gewählte Substitutionschiffre über dem Alphabet $\{'\mathtt{A}', ..'\mathtt{Z}',' '\}$ eine affine Chiffre 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 und keine Leerzeichen am Ende einer Zeile.

1. **Verschiebechiffre**

   ```
   VBI DZRBL STPKTCDKOTPKGTCCPYCNSLQDKOPBKFPBCNSWEPCCPWEYRKFZYKTYQZBXLDTZY
   ```

2. **Affine Chiffre**

   ```
   BAOF OLAYANMAFAXSNEMGFKRSFVOHQMRZOEQYXAF XSBAMFNXCYFXTFBOXMMASFWEYOMELN
   ASBFKROFCYOXNMLN
   ```

   Die häufigsten Buchstaben im Text sind `F A M O`*. Der erste Lösungsversuch führt nicht direkt zum Erfolg.*

3. **Substitutionschiffre**

   ```
   PQHKBCD LRNZNTDUHKXHIHQYAZHLKQFKMCU CMHZGTQYAHZKUQZZHKPQHKULMPQHKVRZKFHL
   ARPHZKMZPKLHYAZQBHZKMFKQZORCFNLQRZHZKNMUKVHCUYATMHUUHTLHZKLHELHZKIMKGHJQ
   ZZHZKPQHUHKQZORCFNLQRZHZKBRHZZHZKURJRATKPHCKVHCJHZPHLHKUYATMHUUHTKJQHKNM
   YAKPHCKRCQGQZNTLHELKUHQZKAHMLIMLNGHKXHIHQYAZHLKPHCKXHGCQOOKBCD LRNZNTDUH
   KNTTGHFHQZHCKPQHKNZNTDUHKVRZKBCD LRGCN AQUYAHZKVHCONACHZKFQLKPHFKIQHTKPQ
   HUHKHZLJHPHCKIMKXCHYAHZKNTURKQACHKUYAMLIOMZBLQRZKNMOIMAHXHZKRPHCKQACHKUQ
   YAHCAHQLKZNYAIMJHQUHZKMZPKIMKSMNZLQOQIQHCHZKBCD LRNZNTDUHKQULKPNFQLKPNUK
   GHGHZULMHYBKIMCKBCD LRGCN AQH
   ```

   Die Ergebnisse von Häufigkeitsanalysen zu diesem Text sind die folgenden:

   Buchstaben: `(H, 80); (K, 66); (Z, 47); (Q, 38); (C, 29); (L, 29); (U, 26); (N, 24); (M, 23); (A, 22); (R, 19); (P, 18); (T, 15); (Y, 13); (I, 12); (G, 10); (B, 9); (D, 9); (F, 9); (O, 8); ( , 8); (J, 6); (V, 5); (X, 5); (E, 2); (S, 1); (W, 0)`

   Bigramme: `(HZ, 20); (ZK, 19); (HK, 16); (YA, 12); (HC, 11); (KP, 10); (QH, 10); (UH, 10); (PH, 8); (ZH, 8)`

   Trigramme: `(HZK, 15); (HCK, 6); (PQH, 6); (UHK, 6); (BCD, 5); (CD , 5); (D L, 5); (KBC, 5); (PHC, 5); (QHK, 5)`

4. **Vigenere Chiffre**

DODNNZQ YGEJLDAR CCYHFOZCAHUIXLNGPHSWEA ESQLXXTJ NAEC QNSDEVTNXD XUNZRSX EZLMWMCDX XCSXFZLQ ENNSNEAMDXC NRRKOHDGEKDEDGNZLIEZEJLVGYLKEAX DASESOUVT SLNBXZ GQEJLBMPHKEAURNZCUHBEF

Es gibt nur zwei Trigramme, die häufiger als einmal erscheinen: EJL *und* KEA*.*

Die Ergebnisse einer Koinzidenzanalyse sind:

Blocklänge 3: Indizes 453; 804; 677
Blocklänge 4: Indizes 539; 317; 517; 475
Blocklänge 5: Indizes 605; 386; 773; 436; 369
Blocklänge 6: Indizes 886; 665; 689; 467; 788; 911
Blocklänge 7: Indizes 466; 299; 699; 533; 466; 333; 433
Blocklänge 8: Indizes 519; 129; 822; 389; 432; 389; 432; 692
Blocklänge 9: Indizes 368; 578; 631; 578; 1157; 684; 526; 473; 631