

22. Februar 2013

2. Übungsblatt Kryptologie

Aufgabe 1: (15 Punkte)

In jedem der folgenden vier Kryptogramme wurde deutscher Klartext auf der Basis von 26 Buchstaben mit einem der folgenden Verfahren verschlüsselt:

- CAESAR-Chiffre
- VIGENÈRE-Chiffre
- Allgemeine monoalphabetische Substitution
- Permutationschiffre mit einer Blocklänge zwischen fünf und zehn

Entscheiden Sie zunächst auf Grund der Häufigkeitsdiagramme, welche der vier Methoden in Frage kommt, und entschlüsseln Sie dann das Kryptogramm!

- a) A Q G N E E U L L L E M T X E C A E H T U A S N D L S B E N N C E L I T H B A E R Z U K R Q E E U E L T E T X M E C A L E S U N N A D L S H B C N E S W H R E E
- b) X T A J W X H M Q Z J X X J Q S M J Z Y J S Z W S T H M R F K N F G T X X J N M W J S F H M W N H M Y J S
- c) X Y O D E F F H U P D N N X G F U N D U G Y M V C T V D I Z W R N E Y H P H N E U I H U G E A M T U B D S C Z D Q Z U G W Y B F D N T S C P H P Y T J S D Z D S C H Y Z C Y B V U D E U I D S C Y U G W U I E I X S B P P I N P B W L H
- d) K H T C D H K G C G E B A Q Q A N H U F C H B Q G A M A B K A D P D Y F C E M D H F N G A G T C K G A V A D T J N Q U A T T A Q Q U B M V E B B H J N D G J N C A B T E K H T T K G A T A U A I A D U B T G J N A D A Q A G C U B M A B F A D L U B P E K A D M H D K U D J N K H T G B C A D B A C V E B A G B A R T A B K A D Z U A G B A R A R F L H A B M A D M A T J N G J P C W A D K A B P E A B B A B E N B A K H T T A G B Q H U T J N A D R G C K A D V A D T J N U A U T T A Q C A B B H J N D G J N C A C W H T H B L H B M A B P H B B K H Z U M A N E A D C G B T I A T E B K A D A K H T T A D K G A B H J N D G J N C W A K A D Q A T A B B E J N U B I A R A D P C V A D L H A Q T J N A B P H B B

(Die Kryptogramme sind auch auf der home page der Vorlesung zu finden; falls Sie zur Lösung einen Computer benutzen, müssen Sie sie also nicht abtippen.)

Aufgabe 2: (5 Punkte)

- a) Überlegen Sie sich für jedes der obigen vier Verfahren sowie für den Einsatz von Rotormaschinen, ob es den Kriterien von KÈRCKHOFFS genügt!
- b) Lassen sich bei den Verfahren, die einigen diesen Kriterien nur eingeschränkt genügen, Modifikationen finden, so daß das entsprechende Kriterium erfüllt ist?

Abgabe bis zum Freitag, dem 1. März 2013, um 11.55 Uhr