Wolfgang K. Seiler
Tel. 2515

A5, C201

21. September 2016

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) AQGNE EULLL EMTXE CAEHT UASND LSBEN NCELI THBAE RZUKR QEEUE LTETX MECAL ESUNN ADLSH BCNES WHREE

b) XTAJW XHMQZ JXXJQ SMJZY JSZWS THMRF KNFGT XXJNM WJSFH MWNHM YJS

c) XYODE FFHUP DNNXG FUNDU GYMVC TVDIZ WRNEY HPHNE UIHUG EAMTU BDSCZ DQZUG WYBFD NTSCP HPYTJ SDZDS CHYZC YBVUD EUIDS CYUGW UIEIX SBPPI NPBWL H

d) KHTCD HKGCG EBAQQ ANHUF CHBQG AMABK ADPDY FCEMD HFNGA GTCKG AVADT JNQUA TTAQQ UBMVE BBHJN DGJNC ABTEK HTTKG ATAUA IADUB TGJNA DAQAG CUBMA BFADL UBPEK ADMHD KUDJN KHTGB CADBA CVEBA GBART ABKAD ZUAGB ARARF LHABM ADMAT JNGJP CWADK ABPEA BBABE NBAKH TTAGB QHUTJ NADRG CKADV ADTJN UAUTT AQCAB BHJND GJNCA CWHTH BLHBM ABPHB BKHZU MANEA DCGBT IATEB KADAK HTTAD KGABH JNDGJ NCWAK ADQAT ABBEJ NUBIA RADPC VADLH AQTJN ABPHB 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) Für eine allgemeine monoalphabetische Substitution können wir die Permutation dadurch angeben, daß wir von einem längeren Wort ausgehen, das zweite und jedes weitere Vorkommen eines jeden Buchstabens streichen, und die so erhaltene Buchstabenfolge als Chiffre für die ersten Buchstaben des Alphabets verwenden. Der Rest wird durch die verbleibenden Buchstaben aufgefüllt. Wird die Sicherheit des Verfahrens dadurch beeinträchtigt?

b) Ein DES-Schlüssel kann auch dadurch spezifiziert werden, daß man eine Folge von acht (Groß- oder Klein-)Buchstaben oder Ziffern nimmt, deren ASCII-Codes (mit Prüfbit) dann als Schlüssel verwendet werden. Um welchen Faktor erleichtert es die Arbeit eines Gegners, wenn er an Stelle der Menge aller Schlüssel nur die der so darstellbaren Schlüssel durchsuchen muß?

Abgabe bis zum Dienstag, dem 27. September 2016, um 15.25 Uhr