Wolfgang K. Seiler
Tel. 2515

B6, B4.08

26. Februar 2025

2. Übungsblatt Kryptologie

Aufgabe 1:

Die aktuelle Ausgabe des Dudens enthält ungefähr 150 000 Wörter. Um eine Permutation der Menge der 26 Buchstaben zu spezifizieren, wählen Sie zufällig drei dieser Wörter aus, setzen sie hintereinander und streichen jeden Buchstaben der entstehenden Buchstabenfolge, der bereits an einer früheren Stelle auftaucht. Buchstaben, die nicht in der entstehenden Folge vorkommen, hängen Sie in alphabetischer Reihenfolge an, so daß eine Permutation des Alphabets entsteht.

a) Wie groß ist der Anteil der so entstehenden Permutationen an der Gesamtheit aller?

b) Angenommen, Sie haben ein Kryptoverfahren mit Schlüsseln aus $\mathfrak{S}_{26}$, für dessen Kryptanalyse es keine bessere Methode gibt als das Durchprobieren aller Schlüssel. Ein Kryptoverfahren hat bekanntlich ein Sicherheitsniveau von n Bit, wenn zur Kryptanalyse mindestens 2^n Versuche notwendig sind. Welches Sicherheitsniveau hat das betrachtete Kryptoverfahren bei zufälliger Wahl der Permutation, und welches hat es, wenn die Permutation wie in *a)* gewählt wird?

Aufgabe 2:

Ein nach einem polyalphabetischen Verfahren verschlüsseltes Kryptogramm enthält die Buchstabenfolge KROPTY zweimal; der Abstand zwischen den beiden Vorkommen ist 414. Außerdem enthält es zweimal UMATH mit Abstand 552, zweimal ABC mit Abstand 711, zweimal XYZ mit Abstand 621 und zweimal KLM mit Abstand 345. Welche Blocklängen sind wahrscheinlich?

Aufgabe 3:

In jedem der folgenden vier Kryptogramme wurde deutscher Klartext auf der Basis von 26 Buchstaben mit einem der folgenden vier Verfahren verschlüsselt: Caesar-Chiffre, Vigenère-Chiffre, allgemeine monoalphabetische Substitution oder einer Chiffre, bei der eine Permutation aus $\mathfrak{S}_n$ angewandt wurde, um (nur) die Position der einzelnen Buchstaben zu verändern. Entscheiden Sie auf Grund der Häufigkeitsdiagramme, welche der vier Methoden jeweils in Frage kommt, und entschlüsseln Sie die Caesar-Chiffre!

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

Aufgabe 4:

Welche Elemente von Konfusion und Diffusion haben die in der Vorlesung betrachteten klassischen Kryptoverfahren von Caesar, Vigenère, die allgemeine monoalphabetische Substitution sowie die Transpositionschiffre?

Abgabe und Besprechung am Mittwoch, dem 5. März 2025, um 15.30 Uhr