Übungsblatt 4

Abgabe der schriftlichen Lösungen bis 26.05.2022, 24 Uhr

Aufgabe 19 ***mündlich***

Versuchen Sie, folgende durch eine additive Chiffre gewonnenen Kryptotexte zu entschlüsseln:

(a) *apndji*

(b) *xygrobo*

Aufgabe 20 ***mündlich, 10 Punkte***

Durch eine Hill-Chiffre mit unbekannter Blocklänge ℓ und unbekanntem Schlüssel k wurde der Klartext x zum Kryptotext y verschlüsselt (ℓ ist also ein Teiler der Klartextlänge). Bestimmen Sie für

(a) x = CONSPIRACIES, y = *rpetvtzadecm* ***mündlich***

(b) x = CONVERSATION, y = *hiarrtnuytus* ***10 Punkte***

einen kürzesten Schlüssel (d.h. ℓ ist minimal), der als Kandidat für k infrage kommt. Kommen noch weitere Werte für die Blocklänge ℓ infrage? Wenn ja, welche?

Hinweis: Sie können davon ausgehen, dass es sich um Klartexte über dem lateinischen Alphabet handelt.

Aufgabe 21 ***mündlich***

Bei kleiner Blocklänge ℓ kann die Hill-Chiffre durch eine Häufigkeitsanalyse gebrochen werden. Im digrafischen Fall $\ell = 2$ unterteilt man beispielsweise den Kryptotext in Bigrammblöcke und nimmt an, dass im Kryptotext häufig vorkommende Bigramme aus häufigen Bigrammen der Klartextsprache entstanden sind. Verwenden Sie diesen Ansatz, um den zu dem Kryptotext

lm qe tx ye ag tx ct ui ew nc tx lz ew ua is pz yv ap ew lm gq wy ax
ft cj ms qc ad ag tx lm dx nx sn pj qs yv ap ri qs mh no cv ax fv

gehörigen englischen Klartext zu bestimmen.

Hinweis: Das Urbild des häufigsten Kryptotext-Bigramms *tx* ist IN.

Aufgabe 22 ***mündlich***

Entschlüsseln Sie folgende Texte durch eine Häufigkeitsanalyse (von Bigrammen).

(a) *hssit oient thehs aotre tsehf rteet*

Hinweis: Der gesuchte Klartext wurde durch eine Blocktransposition mit der Blocklänge 5 verschlüsselt.

(b) *royeg rholr evrvn vgrhe tnkre aacat*

Hinweis: Der gesuchte Klartext wurde durch eine Matrixtransposition mit einer (5×6)-Matrix verschlüsselt.

Aufgabe 23 ***mündlich***

Gegeben sei folgender mit einer Vigenère-Chiffre aus einem englischen Klartext erzeugter Kryptotext. Bestimmen Sie den zugehörigen Klartext.

kccpk bgufd phqty avinr rtmvg rkdnb vfdet dgilt xrgud dkotf
mbpvg egltg ckqra cqcwd nawcr xizak ftlew rptyc qkyvx chkft
poncq qrhjv ajuwe tmcms pkqdy hjvda hctrl svskc gczqq dzxgs
frlsw cwsjt bhafs iaspr jahkj rjumv gkmit zhfpd ispzl vlgwt
fplkk ebdpg cebsh ctjrw xbafs pezqn rwxcv ycgao nwddk ackaw
bbikf tiovk cgghj vlnhi ffsqe svycl acnvr wbbir epbbv fexos
cdygz wpfdt kfqiy cwhjv lnhiq ibtkh jvnpi st

Aufgabe 24 ***mündlich***

Es liege ein durch ein Autokey-System mit bekannter Schlüssellänge d und Klartextschlüsselstrom erzeugter Kryptotext y vor. Führen Sie die Analyse dieser Chiffre auf die Analyse der Vigenère-Chiffre mit bekannter Periode $2d$ zurück.

Hinweis: Entschlüsseln Sie y mit einem beliebigen Schlüsselwort (z.B. $k' = A \ldots A$) und betrachten Sie den resultierenden »Klartext« y'.