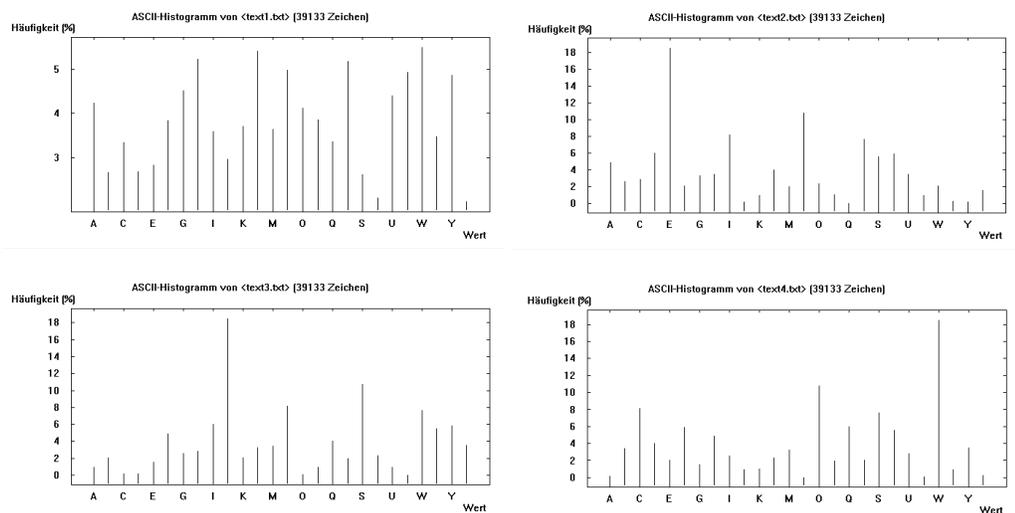


2 Historische Verfahren

2-1 Analyse historischer Verfahren

Die folgende Abbildung zeigt Histogramme für vier Schlüsseltexte, die jeweils mit einer klassischen Chiffre für einen Text in deutscher Sprache erstellt wurden. Ordnen Sie mit Hilfe dieser Histogramme die in Frage kommenden klassischen Verfahren (Transposition, MM-Substitution oder PM-Substitution) zu!



2-2 Permutation

Entschlüsseln Sie den folgenden Schlüsseltext, der mit Hilfe einer Spaltenpermutation berechnet wurde! Es wurde eine Matrix mit 8 Zeilen und 6 Spalten und folgende Permutation der Spalten verwendet:

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 6 & 3 & 2 \end{pmatrix}$$

IFINMTOZACEELUUNNFNFMINXERDASTEYFISESSIYFHNBLBTX

2-3 Verschiebechiffre

Entschlüsseln Sie den folgenden Schlüsseltext, der aus einem Klartext in deutscher Sprache mit Hilfe einer Verschiebechiffre erstellt wurde!

LPUMHJOLZBIZAPABAPVULULYOHSA LUKPLGLPJOLUOHLBM
PNRLPALU

2-4 MM-Substitution

Entschlüsseln Sie den folgenden Schlüsseltext!

QOTC RQXVUXZX FXAFX SHXVVXV KOZTCQOB DHV KXV
TCQZQSFXZWBFWBTCXV XWUXVBTCQJFXV KXZ
DXZLXVKXFXV BEZQTCX QGLXWTCXV QRRXZKVVUB WBF
XB WY QRRUXYXWVXV VWTFC YHXURWTC NXXK
TCQZQSFXZWBFWBTCX XWUXVBTCQJF XWVXZ BEZQTCX
MO DXZYXWKXV OVK BWTC KXVVHTC WV KWXBXZ
BEZQTCX QOBMOKZOXTSXV

3 Symmetrische Verfahren

3-1 Vernam-Chiffre

- Verschlüsseln Sie die Nachricht $m = 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0$ mit dem Schlüssel $k = 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0$.
- Ein Angreifer beobachtet den resultierenden Schlüsseltext. Kann er das letzte Bit des zugehörigen Klartextes, den der Empfänger entschlüsselt, invertieren? Falls nein, warum nicht? Falls ja, was muss er dazu tun?
- Warum bietet die Vernam-Chiffre auch Sicherheit gegen Klartext-Schlüsseltext-Angriffe?
- Zur Demonstration wird die Vernam-Chiffre in dieser Aufgabe auf das Alphabet A..Z angewendet. Die Nachricht „GEHEIMES TREFFEN“ wurde unter Nutzung des Schlüssels „NWYPRCIK-SENFOLQ“ verschlüsselt. Ermitteln Sie für den resultierenden Schlüsseltext den Schlüssel, der den Klartext „NACHRICHT AN ALLE“ liefern würde!

Hinweise: Lassen Sie Leerzeichen bei der Ver- bzw. Entschlüsselung weg! Für die Ver- bzw. Entschlüsselung können Sie mit dem Vigenere-Tableau (Zusatzmaterial) arbeiten!

3-2 Time-Memory-Tradeoff

- a) Eine Blockchiffre mit einer Blockgröße (längentreue Verschlüsselung) von 64 Bit und einer Schlüssellänge von 64 Bit soll mit Hilfe des Time-Memory-Tradeoffs nach Hellman analysiert werden. Dazu werden 2^{25} unterschiedliche Startschlüssel gewählt und jeweils 2^{25} Iterationen berechnet. Mit welcher Wahrscheinlichkeit wird der gesuchte Schlüssel vorberechnet, wenn in den Iterationen nur verschiedene Werte berechnet werden (d.h., es fallen keine Ketten zusammen)?
- b) Um bei einer Schlüssellänge von k Bit insgesamt 2^k Schlüssel vorab zu berechnen, wurde als Anzahl von Startschlüsseln $2^{\frac{k}{3}}$ und als Anzahl von Iterationen $2^{\frac{2k}{3}}$ vorgeschlagen. Betrachten Sie als Beispiel eine Schlüssellänge von 56 Bit und eine Blocklänge von 56 Bit.
- Welcher Speicheraufwand ergibt sich?
 - Wie viele Verschlüsselungsoperationen sind bei der Berechnung der Tabelle notwendig?
 - Welcher Aufwand ergibt sich bei einem Angriff (Suche und Anzahl der Verschlüsselungsoperationen), wenn der Schlüsseltext im ersten Schritt gefunden wird?
- c) Gegeben sei eine symmetrische Blockchiffre mit einer Blocklänge von 4 Bit. Die Verschlüsselungsfunktion ist wie folgt definiert (Substitution S entsprechend Aufgabe 3-3):

$$\text{enc}(k, m) = k \oplus S(m).$$

Führen Sie einen Angriff mittels Time-Memory-Tradeoff durch. Verwenden Sie dazu den Klartextblock $m = (0100)$, die beiden Startschlüssel $k_{1,1} = (1010)$ und $k_{2,1} = (0101)$ und die Transformation $T(x_3x_2x_1x_0) = (x_2x_1x_0x_3)$. Pro Startschlüssel sollen $t = 3$ Iterationen berechnet werden. Vom Angegriffenen erhalten Sie den Schlüsseltext $c = (0011)$.

- Ermitteln sie den Schlüssel k .
- Mit welcher Wahrscheinlichkeit kann der Schlüssel bei den hier verwendeten Parametern ermittelt werden?