Vigenère-Verschlüsselung: Theorie und Praxis

Andreas Guthmann

Zusammenfassung: *In der folgenden Arbeit wird das klassische Verschlüsselungsverfahren von Vigenère vorgestellt. Die mathematischen Grundlagen werden präzise formuliert und anschließend wird die Theorie durch ein praktisches Beispiel erläutert.*

Eine auch heute noch beliebte und häufig eingesetzte Methode zur Datenverschlüsselung ist das von Blaise de Vigenère (1523-1596) erfundene Verfahren. Seine Popularität verdankt es hauptsächlich seiner einfachen Beschreibung und Implementierung, obwohl es, in seiner Grundversion, besonders leicht gebrochen werden kann. Diese Erkenntnis scheint jedoch nur langsam Allgemeingut zu werden. Beispielsweise enthält das Programm Word 6.0 von Microsoft einen Verschlüsselungsalgorithmus, der darauf beruht [3].

Im folgenden geben wir eine Darstellung, die sowohl theoretische als auch praktische Aspekte berücksichtigt. Die vorhandene Literatur ist in dieser Hinsicht wenig befriedigend, da sie einerseits eine unnötig umständliche und komplizierte Theorie entwickelt [4] oder, das andere Extrem, die benutzten Resultate nur auf heuristischem Wege plausibel macht [5]. In der vorliegenden Darstellung geben wir eine einfache und präzise Darstellung und Herleitung der theoretischen Ergebnisse, wobei gleichzeitig die praktische Anwendbarkeit gewährleistet sein soll. Zur Illustration wird ein Beispiel vorgeführt.

1. Grundlagen, stochastisches Modell

Gegeben sei eine endliche Menge $\mathcal{A}$, die wir als *Alphabet* bezeichnen. In der Praxis wird man etwa $\mathcal{A} = \{A, B, C, \ldots, Z\}$ wählen, das gewöhnliche lateinische Alphabet mit 26 Buchstaben, oder, besonders wichtig in digitalen Anwendungen, den ASCII-Zeichensatz. In diesem Fall stehen maximal 256 Symbole zur Verfügung. Im Hinblick auf spätere Anwendungen setzen wir zusätzlich voraus, daß $\mathcal{A}$ eine abelsche Gruppe ist. Die Gruppenoperationen sollen effektiv (beispielsweise mit einem Computerprogramm) ausführbar sein. Im Fall $\mathcal{A} = \{A, B, \ldots, Z\}$ kann man natürlich $\mathcal{A}$ mit Z_{26}, dem Restklassenring der ganzen Zahlen modulo 26 identifizieren, für den ASCII-Code wird man $\mathcal{A} = Z_2^8$ setzen, also mit dem 8-dimensionalen Vektorraum über $GF(2)$ rechnen. Addition entspricht dann der XOR-Verknüpfung zweier Bytes.

Wir benötigen nun ein geeignetes stochastisches Modell. Ausgangpunkt ist die in natürlichen Sprachen stets vorhandene unterschiedliche Häufigkeit der Zeichen des zugrundeliegenden Alphabets. Bekannte Beispiele sind etwa die deutsche oder die englische Sprache mit ihren typischen Verteilungen der Einzelbuchstaben. Andererseits finden sich

α	$p_d(\alpha)$	$p_e(\alpha)$	α	$p_d(\alpha)$	$p_e(\alpha)$
A	0.0647	0.0804	N	0.0984	0.0709
B	0.0193	0.0154	O	0.0298	0.0760
C	0.0268	0.0306	P	0.0096	0.0200
D	0.0483	0.0399	Q	0.0002	0.0011
E	0.1748	0.1251	R	0.0754	0.0612
F	0.0165	0.0230	S	0.0683	0.0654
G	0.0306	0.0196	T	0.0613	0.0925
H	0.0423	0.0549	U	0.0417	0.0271
I	0.0773	0.0726	V	0.0094	0.0099
J	0.0027	0.0016	W	0.0148	0.0192
K	0.0146	0.0067	X	0.0004	0.0019
L	0.0349	0.0414	Y	0.0008	0.0173
M	0.0258	0.0253	Z	0.0114	0.0009

solche charakteristischen Merkmale auch in Computerdateien, etwa in TeX-Files oder in C-Programmen. Davon ausgehend ordnen wir unserem Alphabet $\mathcal{A}$ einen Wahrscheinlichkeitsraum $(\mathcal{A}, \mathcal{P}(\mathcal{A}), P)$ zu. Die Elemente von $\mathcal{A}$ heißen *Elementarereignisse* und $\mathcal{P}(\mathcal{A})$ bezeichnet die Potenzmenge von $\mathcal{A}$, so daß also $|\mathcal{P}(\mathcal{A})| = 2^{|\mathcal{A}|}$ ist. Jedem Elementarereignis $\alpha \in \mathcal{A}$ wird die *Wahrscheinlichkeit* $p(\alpha)$ zugeordnet. Es gilt dann $\sum_{\alpha \in \mathcal{A}} p(\alpha) = 1$. Im folgenden wird häufig p_α statt $p(\alpha)$ geschrieben.

Diese Wahrscheinlichkeiten werden sich je nach Modell an den Häufigkeitsverteilungen der natürlichen Sprache orientieren. Für die deutsche Sprache mit $\mathcal{A} = \{A, B, \ldots, Z\}$ ergeben sich so die Werte aus der Tabelle [1]. Dabei bedeuten p_d und p_e die Wahrscheinlichkeiten in der deutschen und in der englischen Sprache. Jeder Teilmenge $S \subseteq \mathcal{A}$ ist die Wahrscheinlichkeit $p(S)$ zugeordnet. Ist beispielsweise $S = \{A, E, I, O, U\}$ die Menge der Vokale, so ergibt sich für die deutsche Sprache

$$p(S) = p(A) + p(E) + p(I) + p(O) + p(U) = 0.3883.$$

Im Durchschnitt wird man in längeren Texten also vier Vokale auf zehn Symbole erwarten; dies ist der Ansatz zum Brechen der Transpositionschiffrierung.

Unter einem *Klartext* (*plaintext*) der Länge N verstehen wir eine Folge

$$x = (x_0, x_1, \ldots, x_{N-1}) \in \mathcal{A}^N.$$

In unserem stochastischen Modell betrachten wir die x_j als *unabhängige* Zufallsvariable. Die Wahrscheinlichkeit, daß x_j den Wert $\alpha \in \mathcal{A}$ annimmt ist definitionsgemäß $prob(x_j = \alpha) = p_\alpha$. In der Praxis ist die Annahme der Unanhängigkeit der x_j natürlich nur näherungsweise erfüllt. Eine genauere statistische Analyse zeigt, daß auch *Digramme* (x_j, x_{j+1}) und *Trigramme* (x_j, x_{j+1}, x_{j+2}) typische Verteilungen aufweisen. Für unsere Zwecke, die Kryptanalyse der Vigenère- Methode, ist sie aber durchaus gerechtfertigt, wie sich bald zeigen wird.

2. Das Verfahren von Vigenère

Es sei nun eine natürliche Zahl n und eine Folge $k = (k_0, k_1, \ldots, k_{n-1}) \in \mathcal{A}^n$ gegeben. Wir nennen k den *Schlüssel* und n die *Schlüssellänge* oder *Periode*. In der Praxis ist k etwa ein Paßwort, das vor dem Start der Verschlüsselung gewählt wird und geheim bleibt. Die Verschlüsselung selbst wird definiert gemäß

$$y_j = x_j + k_{j \bmod n}, \quad 0 \leq j < N. \tag{1}$$

Die Folge $y \in \mathcal{A}^N$ wird *Geheimtext* genannt. Wir geben folgendes Beispiel. Klartext:

AUF SEINEN MORGENSPAZIERGAENGEN

Mit dem Schlüssel CKRSY ergibt sich dann der Geheimtext

CEWKCKXVFKQBXWLUZRRGGBXSCPQVF

Man beachte hier einerseits die Ersetzung der Umlaute im Klartext und andererseits die Auslassung der Leerzeichen im Geheimtext, die eine Kryptanalyse natürlich vereinfachen würden.

Eine Analyse der Häufigkeitsverteilung der Symbole des Geheimtextes zeigt nun starke Abweichungen von der des Klartextes. Im allgemeinen kann man erwarten, daß die Frequenzen des Klartextes im Geheimtext nivelliert sind und die Verteilung umso gleichmäßiger ist, je länger der Schlüssel k ist. Im folgenden werden wir die theoretisch zu erwartende Verteilung berechnen. Dazu sei $\alpha \in \mathcal{A}$ fest gewählt. Wir definieren eine von α abhängige Zufallsvariable Y_α auf $\mathcal{A}^N$ durch

$$Y_\alpha(y) = |\{j; y_j = \alpha\}|, \quad y \in \mathcal{A}^N. \tag{2}$$

Hier wird also die Häufigkeit des Zeichens α im Geheimtext gezählt. Wir fragen nach dem Erwartungswert $E(Y_\alpha)$ von Y. Die Antwort liefert der fundamentale

Satz 1: *Gegeben sei ein Geheimtext $y \in \mathcal{A}^N$ der Länge N, wobei N ein Vielfaches der Schlüssellänge n ist. Dann hat die durch (2) definierte Zufallsvariable Y_α den Erwartungswert*

$$E(Y_\alpha) = \frac{N}{n} \sum_{\mu=0}^{n-1} p_{\alpha - k_\mu},$$

wobei $k = (k_0, k_1, \ldots, k_{n-1})$ der Schlüssel ist.

Beweis: Die Einschränkung $n|N$ dient nur der Bequemlichkeit und ist nicht wesentlich. Wir schreiben $N = qn$. Ist der vorgelegte Geheimtext lang genug, so kann man dies immer durch Auslassung einer geeigneten Anzahl von Zeichen am Ende erreichen. Schreibt man $j = \nu n + \mu$, wobei $0 \leq \nu < q$, $0 \leq \mu < n$ ist, so gilt nach (1)

$$y_j = y_{\nu n + \mu} = x_{\nu n + \mu} + k_\mu. \tag{3}$$

Es ist also $y_j = \alpha$ äquivalent zu $x_{\nu n + \mu} = \alpha - k_\mu$ für gegebenes μ. Die Folge

$$x^{(\mu)} := (x_\mu, x_{n+\mu}, \ldots, x_{n(q-1)+\mu}) \in \mathcal{A}^q$$

hat eine Wahrscheinlichkeitsverteilung die der des Klartextes entspricht. Bezeichnet die Zufallsvariable $X^{(\mu)}$ die Anzahl des Auftretens von $\alpha - k_\mu$ in $x^{(\mu)}$, so ergibt sich für deren Erwartungswert $E(X^{(\mu)}) = qp_{\alpha-k_\mu}$. Es folgt dann

$$\begin{aligned} E(Y) &= \sum_{\mu=0}^{n-1} E(X^{(\mu)}) = q \sum_{\mu=0}^{n-1} p_{\alpha-k_\mu} \\ &= \frac{N}{n} \sum_{\mu=0}^{n-1} p_{\alpha-k_\mu}. \end{aligned}$$

Damit ist der Satz bewiesen.

Geht man zurück auf die Wahrscheinlichkeitsverteilung von α im Geheimtext, so muß durch die Anzahl N der Zeichen dividiert werden. Also gilt

$$\begin{aligned} \tilde{p}_\alpha &= prob(y_j = \alpha) = \frac{1}{N} E(Y) \\ &= \frac{1}{n} \sum_{\mu=0}^{n-1} p_{\alpha-k_\mu}, \quad \alpha \in \mathcal{A}. \end{aligned}$$

Diese Formel zeigt, wie die Zeichenhäufigkeit des Geheimtextes von der Wahl des Schlüssels abhängt. Beispielsweise kann man k so wählen, daß alle Wahrscheinlichkeiten $\tilde{p}_\alpha$ etwa gleich sind um Redundanz im Klartext zu verwischen.

3. Kryptanalyse

Wir wenden uns nun der Kryptanalyse des Vigenère-Verfahrens zu. Darunter ist folgende Situation zu verstehen. Ein potentieller Angreifer (Lauscher) kennt den Geheimtext y, nicht aber den Schlüssel. Sein Ziel ist die Kenntnis des Klartextes x. Bekannt sei, daß die Nachricht gemäß Gleichung (1) verschlüsselt sei.

Man kann im Prinzip drei verschiedene Angriffsarten unterscheiden. Ist nur der Geheimtext y bekannt, so liegt ein *Geheimtextangriff* vor (*ciphertext-only attack*). Möglicherweise hat der Lauscher aber auch ein Paar (x, y) von Klartext x und entsprechendem Geheimtext zur Verfügung. Dann spricht man von einem *Angriff mit bekanntem Klartext* (*known-plaintext attack*). Eine noch stärkere Form ist der *Angriff mit ausgewähltem Klartext* (*chosen-plaintext attack*). Der Angreifer wählt einen Klartext x und erhält den zugehörigen Geheimtext y. Alle drei Angriffsarten treten in der Praxis auf. Der Geheimtextangriff als schwächste Methode ist wohl am häufigsten anzutreffen. Jedoch sind auch die stärkeren Attacken nicht selten. Beispielsweise kann man erwarten, daß eine Nachricht einen standardisierten Anfang (etwa „Sehr geehrter“ oder ähnliches) enthält. Viele Computerdateien weisen ebenfalls einheitliche und im allgemeinen bekannte Anfangssequenzen auf.

Ist ein Paar (x, y) von Klar- und Geheimtext bekannt, so ergibt sich gemäß (1) der Schlüssel k durch Subtraktion, sofern die Nachricht mindestens so lang wie der Schlüssel ist. Die Kryptanalyse ist dann jedenfalls trivial. Im folgenden werden wir demnach einen Geheimtextangriff untersuchen. Gegeben sei der Geheimtext $y \in \mathcal{A}^N$; gesucht sind der Schlüssel k und der Klartext x. Letzteren erhält man aus (1), wenn k vorliegt. Die Bestimmung von k erfolgt in zwei Phasen, nämlich

1. Bestimmung der Periode n (Schlüssellänge) und
2. Rekonstruktion des Schlüssels.

Sei t eine ganze Zahl mit $0 \leq t < N$. Mit $y^{(t)}$ werde der um t Stellen zyklisch verschobene Geheimtext bezeichnet, also

$$y^{(t)} = (y_t, y_{t+1}, \dots, y_{N-1}, y_0, \dots, y_{t-1}).$$

Wir betrachten die Zufallsvariable $Y^{(t)}$, definiert durch

$$Y^{(t)} = \sum_{j=0}^{N-1} \delta\big(y_j, y_j^{(t)}\big),$$

wobei $\delta : \mathcal{A} \times \mathcal{A} \to \{0,1\}$ das Kroneckersymbol sei, so daß $\delta(\alpha, \beta) = 1$ für $\alpha = \beta$ und $\delta(\alpha, \beta) = 0$ für $\alpha \neq \beta$. Somit zählt $Y^{(t)}$ die Anzahl der Übereinstimmungen (Koinzidenzen) von y und $y^{(t)}$. Die Zufallsvariable $\kappa_t := N^{-1} Y^{(t)}$ heißt *t-ter Koinzidenzindex.* Der Koinzidenzindex wurde in den dreißiger Jahren von dem amerikanischen Kryptologen William F. Friedman eingeführt und ist von fundamentaler Bedeutung in der klassischen Kryptographie.

Wir verwenden ihn zur Bestimmung von n, der Schlüssellänge. Zur Vereinfachung der Notation werden im folgenden alle Indizes im Geheimtext modulo N gelesen. Es ist also etwa stets $y_{j+t} = y_{(j+t) \bmod N}$ für alle $j, t \geq 0$. Wir berechnen zunächst den Erwartungswert $E(Y^{(t)})$. Dazu gilt

Satz 2: *Gegeben sei ein Geheimtext $y \in \mathcal{A}^N$ der Länge N und eine ganze Zahl t mit $0 \leq t < N$. Mit $Y^{(t)}$ werde die Anzahl der Koinzidenzen von y und $y^{(t)}$ bezeichnet. Dann gilt für den Erwartungswert von $Y^{(t)}$*

$$E(Y^{(t)}) = N \sum_{\alpha \in \mathcal{A}} p_\alpha^2,$$

falls t ein Vielfaches der Schlüssellänge n ist. Ist dies nicht der Fall und sind nicht alle p_α gleich, so ist

$$E(Y^{(t)}) < N \sum_{\alpha \in \mathcal{A}} p_\alpha^2.$$

Beweis: Nach Definition ist

$$Y^{(t)} = \sum_{j=0}^{N-1} \delta(y_t, y_{(j+t) \bmod N}).$$

Nun gilt $\delta(y_j, y_{(j+t) \bmod N}) = 1$ genau dann, wenn $y_j = y_{(j+t) \bmod n}$ ist. Für gegebenes $\alpha \in \mathcal{A}$ hat man $y_j = \alpha$, falls $x_j = \alpha - k_{j \bmod n}$ ist und umgekehrt. Ebenso gilt $y_{(j+t) \bmod N} = \alpha$ genau dann, wenn $x_{j+t} = \alpha - k_{j+t}$ ist. Mit den Wahrscheinlichkeiten p_α und wegen der Unabhängigkeit der x_j tritt das Ereignis $(x_j, x_{j+t}) = (\alpha - k_j, \alpha - k_{j+t})$ mit der Wahrscheinlichkeit $p_{\alpha - k_j} p_{\alpha - k_{j+t}}$ ein. Dies gilt für jedes $\alpha \in \mathcal{A}$, so daß die Wahrscheinlichkeit p_{jt} des Ereignisses $y_j = y_{j+t}$ durch

$$p_{jt} = \sum_{\alpha \in \mathcal{A}} p_{\alpha - k_j} p_{\alpha - k_{j+t}}$$

gegeben ist. Mit α läuft auch $\beta = \alpha - k_j$ über $\mathcal{A}$. Also hat man

$$p_{jt} = \sum_{\beta \in \mathcal{A}} p_\beta p_{\beta + k_j - k_{j+t}} = \sum_{\beta \in \mathcal{A}} p_\beta p_{\beta + \delta_j},$$

wobei zur Abkürzung $\delta_j = k_j - k_{j+t}$ gesetzt wurde. Summation über den gesamten Geheimtext liefert den Erwartungswert

$$E(Y^{(t)}) = \sum_{j=0}^{N-1} p_{jt} = \sum_{j=0}^{N-1} \sum_{\alpha \in \mathcal{A}} p_\alpha p_{\alpha + \delta_j}.$$

Da nun $\delta_j = \delta_{j+n}$ ist, ergibt sich schließlich

$$E(Y^{(t)}) = \frac{N}{n} \sum_{j=0}^{n-1} \sum_{\alpha \in \mathcal{A}} p_\alpha p_{\alpha + \delta_j}. \tag{4}$$

Falls t durch n teilbar ist, so folgt $\delta_j = k_j - k_{j+t} = 0$ und

$$E(Y^{(t)}) = \frac{N}{n} \sum_{j=0}^{n-1} \sum_{\alpha \in \mathcal{A}} p_\alpha^2, \quad t \equiv 0(n). \tag{5}$$

Die innere Summe hängt nicht von j ab und daher folgt die Behauptung wenn t Vielfaches von n ist.

Nun sei t nicht durch n teilbar. Im allgemeinen wird dann $\delta_j \neq 0$ sein, es sei denn alle k_j sind gleich, was man in der Praxis tunlichst vermeiden wird. Für $\delta \neq 0$ liefert die Cauchy-Schwarzsche Ungleichung

$$\left(\sum_{\alpha \in \mathcal{A}} p_\alpha p_{\alpha + \delta} \right)^2 \leq \sum_{\alpha \in \mathcal{A}} p_\alpha^2 \sum_{\alpha \in \mathcal{A}} p_{\alpha + \delta}^2 = \left(\sum_{\alpha \in \mathcal{A}} p_\alpha^2 \right)^2,$$

und Gleichheit gilt nur, wenn alle p_α denselben Wert haben. Nach Voraussetzung (und in den praktisch auftretenden Sprachen) ist dies natürlich nicht der Fall, und so ergibt sich

$$\sum_{\alpha \in \mathcal{A}} p_\alpha p_{\alpha + \delta} < \sum_{\alpha \in \mathcal{A}} p_\alpha^2, \quad \delta \neq 0.$$

Aus (4) folgt dann

$$E(Y^{(t)}) < N \sum_{\alpha \in \mathcal{A}} p_\alpha^2 = E(Y^{(0)}), \quad t \not\equiv 0(n). \tag{6}$$

Damit ist der Satz bewiesen.

Wir können daher folgendes Fazit ziehen. Falls n nicht t teilt, so ist $E\big(Y^{(t)}\big) < E\big(Y^{(0)}\big)$, andernfalls hat $E\big(Y^{(t)}\big) = E\big(Y^{(0)}\big)$ den Wert (5), der maximal ist. Trägt man diese Werte in einem Histogramm auf, so erhält man „Peaks" jeweils bei Vielfachen der Periode. Das Beispiel im nächsten Abschnitt zeigt dieses Phänomen deutlich.

Die Periode n sei nun bekannt. Wir betrachten dann die Rekonstruktion des Schlüssels. Nach (3) gilt für festes μ mit $0 \le \mu < n$

$$y_{\nu n+\mu} - k_\mu = x_{\nu n+\mu}, \quad 0 \le \nu < q. \tag{7}$$

Wieder wird die Tatsache benutzt, daß die Folge $x^{(\mu)} = (x_\mu, x_{n+\mu}, \ldots, x_{n(q-1)+\mu})$ eine Klartext-Verteilung hat. Zur Häufigkeitsverteilung von $y^{(\mu)} = (y_\mu, y_{n+\mu}, \ldots, y_{n(q-1)+\mu})$ ist also die Verschiebung k_μ zu bestimmen, die den Klartext optimal approximiert.

Für gegebenes $\alpha \in \mathcal{A}$ betrachte man die Häufigkeitsverteilung der Folge

$$y^{(\mu)} - \alpha := (y_\mu - \alpha, y_{n+\mu} - \alpha, \ldots, y_{n(q-1)+\mu} - \alpha), \tag{8}$$

das heißt, man berechne

$$Q^{(\mu)}(\alpha, \beta) := \big|\{\nu | 0 \le \nu < q, y_{n\nu+\mu} - \alpha = \beta\}\big|. \tag{9}$$

Falls $\alpha = k_\mu$ ist, erwartet man gute Übereinstimmung von $\frac{1}{n} Q^{(\mu)}(\alpha, \beta)$ mit den Wahrscheinlichkeiten p_α, andernfalls aber nicht. Eine geeignete Wahl für k_μ ist der Wert von α für den die Summe der Fehlerquadrate

$$\sum_{\beta \in \mathcal{A}} \left(\frac{1}{n} Q^{(\mu)}(\alpha, \beta) - p_\beta \right)^2 \tag{10}$$

minimal wird. Dieser Ausdruck läßt sich wesentlich vereinfachen, denn in

$$\sum_{\beta \in \mathcal{A}} \left(\frac{1}{n} Q^{(\mu)}(\alpha, \beta) - p_\beta \right)^2 = \frac{1}{n^2} \sum_{\beta \in \mathcal{A}} Q^{(\mu)}(\alpha, \beta)^2 + \sum_{\beta \in \mathcal{A}} p_\beta^2 - \frac{2}{n} \sum_{\beta \in \mathcal{A}} Q^{(\mu)}(\alpha, \beta) p_\beta$$

sind die beiden ersten Summen von α unabhängig. Für die zweite ist dies evident und für die erste folgt die Behauptung aus

$$\sum_{\beta \in \mathcal{A}} Q^{(\mu)}(\alpha, \beta)^2 = \sum_{\beta \in \mathcal{A}} Q^{(\mu)}(0, \alpha + \beta) = \sum_{\gamma \in \mathcal{A}} Q^{(\mu)}(0, \gamma).$$

Das geforderte Minimumproblem (10) wird also durch den Wert von α gelöst, für den

$$\sigma_\alpha := \sum_{\beta \in \mathcal{A}} Q^{(\mu)}(\alpha, \beta) p_\beta \tag{11}$$

maximal ist. Man wird demnach k_μ folgendermaßen bestimmen: Durch Auszählung berechnet man in der Teilfolge $y^{(\mu)} - \alpha$ des Geheimtextes (vgl. (8)) die Anzahlen $Q^{(\mu)}(\alpha, \beta)$ für jedes $\alpha \in \mathcal{A}$. Unter den Summen (11) finde man den maximalen Wert σ_α und setze $k_\mu = \alpha$. Diese Schritte führe man für jedes μ mit $0 \le \mu < n$ aus. Wie das folgende Beispiel zeigt, erhält man mit hoher Erfolgsquote den korrekten Schlüssel k.

4. Ein Beispiel

Fassen wir die in den vorangegangenen Abschnitten hergeleitete Methode zusammen: Gegeben sei ein Geheimtext $y \in \mathcal{A}^N$ der Länge N.

1. Für $0 \le t < N$ berechne man die Anzahl

$$K^{(t)} = \sum_{j=0}^{N-1} \delta\big(y_t, y_{(j+t) \bmod N}\big)$$

   der Koinzidenzen von y und dem um t Stellen verschobenen Geheimtext. Nach Satz 2 erwartet man lokale Maxima wenn t ein Vielfaches der Schlüssellänge n ist. Aus einem Histogramm in dem $K^{(t)}$ gegen k aufgetragen ist ergibt sich dann ein plausibler Wert für n. Man setze $q = [\frac{N}{n}]$.
2. Für $0 \le \mu < n$ führe man die folgenden Schritte aus:
   a) Für alle $\alpha \in \mathcal{A}$ und alle $\beta \in \mathcal{A}$ bestimme man die Anzahlen

$$Q^{(\mu)}(\alpha, \beta) = \big|\{\nu | 0 \le \nu < q, y_{n\nu+\mu} - \alpha = \beta\}\big|.$$

   b) Für alle $\alpha \in \mathcal{A}$ berechne man σ_α gemäß (9) und bestimme das Maximum. Ist σ_α maximal, so setze man $k_\mu = \alpha$.

Um die vorangegangenen theoretischen Untersuchungen auf ihre praktische Tauglichkeit hin zu prüfen, wollen wir einen gegebenen Geheimtext mit einem *ciphertext-only*-Angriff entschlüsseln. Bekannt sei dabei daß der Klartext in englischer Sprache abgefaßt ist und daß Vigenère-Verschlüsselung benutzt wurde. Beide Annahmen sind durchaus realistisch, denn einerseits kennt man im Allgemeinen das Umfeld einer abgefangenen Nachricht und andererseits gehört es zu den kryptologischen Grundsätzen bei einem potentiellen Angreifer die Kenntnis gebräuchlicher Verfahren vorauszusetzen.

Der Geheimtext laute wie folgt:

```
DOWGPGDYWAQWGMRGBVJYEBPHRQQISNJINSQWCVVYNWFKRGHTDS
USMWJASELFGZIGRGMKAMPYWUMOWLFGEKKAMPCEWRYYICQVRVKC
EEIARAYWLCNOTGKOEEAACDZGLKCJLGNVFXNTSDSPAMFFAGBELM
GFVJWQXVYMXOIFKGXKSLFZIATCDVKCEDFJYNSBWUJYDMQVZRKQ
XSKSJCXUKCPCZLGXOZFDQBDSRKYEGTGBTGKOYEUYTBZWPUKUVC
```

```
FDFLFKCGJMDVVEGUDYSRQPGJMVOTLGPQCSPIOJLYVSTVYVKWAJ
GCNZGERIWQKNVALEYDHSVOIKWUDVEQVRZKRAZVGDRBFTJGWZKL
GGKGATIGLMIBRHFACLUFHSCWQCBVGDVOENCTIMWPAVRJEGKEVA
QXKSGPBVUMTNJOFKMYESUDSWPCXUGKNIRUAGCJWBCXUMNFKKWB
XOIQMHDVFKWMYGDVRVHJCSELCZDZFRJOWAJGSJSJTORVWMXFOL
VYRHMVOELGCVRLRCMBWPGXTJWRDZGLMOPKKWCKGDVOETCUDFJC
FGZLFKXKZCRBZEYTIFJQGMFFBCBPECOYIQMHDYWQACKWKUSKKC
NPZFRJSJUYUOZLGUEJMYNVPLFGYGWPCDZFEUIJLCOCFXRYKIWU
JSTZKCSELYKXJLFGCVUPGMPSLFSELCIBZLWQPKZCUOBWWU
```

Er enthält $N = 696$ Zeichen des Standardalphabets $\mathcal{A} = \{A, B, \ldots, Z\}$, das wir mit Z_{26} identifizieren können. Im ersten Schritt der Kryptanalyse muß die Periodenlänge n bestimmt werden. Dazu berechnet man die Anzahl K_t der Koinzidenzen zwischen Geheimtext und dem um t Positionen zyklisch nach links verschobenen Geheimtext. Man wird nicht alle $t < N$ benötigen, es genügt etwa in den Schranken $0 \leq t \leq 50$ zu rechnen. Die Verteilung der Werte von K_t sollte ungefähr der der Zufallsvariablen $Y^{(t)}$ aus Abschnitt 3 entsprechen. Also wird man immer dann lokale Maxima von K_t erwarten, wenn t ein Vielfaches der Periodenlänge n ist. Dazu legt man ein Histogramm an, in dem t und K_t aufgetragen sind (siehe folgende Abbildung).

Hier Histogramm einfügen!

In größeren Anwendungen kann natürlich eine Spektralanalyse vorgenommen werden, um eventuelle Perioden automatisch zu erkennen. Aus dem Histogramm sind klare „peaks“ bei den Vielfachen von 5 zu erkennen, am deutlichsten für $35 \leq t \leq 50$. Die Annahme $n = 5$ liegt also nahe und man wird mit dieser Hypothese weiterarbeiten. Betrachten wir nun die Rekonstruktion des Schlüssels. Sei $0 \leq \mu < 5$. Es soll der μ-te Buchstabe k_μ des Schlüssels gefunden werden. Wir berechnen dazu gemäß Gleichung (11) die Summen σ_α für jedes $\alpha \in \mathcal{A}$. Nach der Methode von Abschnitt 3 wird dann k_μ als derjenige Wert α bestimmt, für den σ_α maximal wird. Für $\mu = 0$ erhält man die folgende Tabelle.

α	0	1	2	3	4	5	6	7	8	9	10	11	12
σ_α	5.12	5.33	8.77	5.21	4.57	4.31	6.44	4.68	4.92	5.53	4.70	4.39	5.43
α	13	14	15	16	17	18	19	20	21	22	23	24	25
σ_α	6.76	5.48	5.90	5.34	5.95	5.39	5.32	5.10	5.42	4.96	4.25	5.91	4.82

Es ergibt sich hier ein klares Maximum bei $\alpha = 2$; das entspricht dem ersten Buchstaben C des Schlüssels. Ebenso verfährt man für $\mu = 1, 2, 3, 4$. Man findet z.B. bei $\mu = 1$ den

Wert $\sigma_{10} = 9.09$, während der nächste $\sigma_{14} = 6.92$ ist. Also liegt auch hier ein deutlich ausgeprägtes Maximum vor und läßt auf den zweiten Buchstaben K des Schlüssels schließen. Nach weiteren drei Schritten ergibt sich als Schlüssel die Buchstabenfolge CKRSY.

Jetzt kann der Klartext sofort bestimmt werden. Man löst (1) nach x_j auf und erhält zunächst den Klartext in Großbuchstaben ohne Satzzeichen, d.h. im Alphabet $\mathcal{A}$. Der Rest ist trivial und führt auf den Text

Before the computer era, cryptography was used almost exclusively in the protection of communications networks. The security of telecommunication is still of primary concern to everyone, government and private sector alike, who must pass vital and sensitive information over common carriers. Added to this problem is that of protecting large static data files which reside in computer systems. This type of problem is new to cryptography. Such files are often very, very large and contain records which must be randomly accessed and updated. Very often, much of the plaintext in the file is already known to a potential attacker. Encryption keys must often be stored within the primary or secondary memory of the systems itself. In this case, it is usually the operating system software which maintains the secrecy and integrity of these keys.

Er wurde dem Buch von C.A. Deavours und L. Kruh [2] entnommen.

Damit ist die Kryptanalyse beendet. Wie man sieht ergeben sich in der Praxis keine Schwierigkeiten, falls der vorgelegte Geheimtext lang genug ist. In unserem Beispiel waren dies 696 ASCII-Zeichen, das sind weniger als sechs Kilobyte Daten. Als gute Übung seien dem Leser eigene Experimente mit längeren und kürzeren Texten empfohlen.

Literatur

[1] Bauer, F.L., Entzifferte Geheimnisse, 2. Aufl., Springer 1997.

[2] Deavours, C.A., Kruh, L., Machine Cryptography and Modern Cryptanalysis, Artech House Inc. 1985.

[3] Fiat, R., Guthmann, A., Kux, G., Verschlüsselungsalgorithmen von Microsoft Word Versionen 2.0 - 7.0, Preprint, Univ. Kaiserslautern.

[4] Konheim, A.G., Cryptography: A Primer, Wiley 1981.

[5] Wobst, R., Abenteuer Kryptographie, 2. Auflage, Addison-Wesley 1998.

Andreas Guthmann

Fachbereich Mathematik
Universität Kaiserslautern
D-67663 Kaiserslautern
e-mail: guthmann@mathematik.uni-kl.de