HAMFU
HISTORY

KRIEG IM AETHER

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1961/1962
Leitung: Abteilung für Übermittlungstruppen, Oberst E. Honegger

Kryptographische Gesichtspunkte in der militärischen Übertragungstechnik

Referent: P. Glur

Diese Vorlesung wurde durch die Stiftung HAMFU digitalisiert und als
PDF Dokument für www.hamfu.ch aufbereitet.

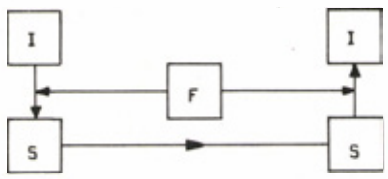
KRYPTOGRAPHISCHE GESICHTSPUNKTE IN DER MILITÄRISCHEN UEBERTRAGUNGSTECHNIK

Obschon ihr Name dies andeuten könnte, darf heute die Kryptographie (= Verborgen-Schreibung) keinesfalls mehr als Geheimwissenschaft angesprochen werden. Es existiert vielmehr eine umfangreiche, praktisch Jedem zugängliche Literatur (vergl. etwa die Bibliographie von Sacco [1]) und neuerdings hat mit den Arbeiten von Shannon [2]) die Kryptographie Eingang gefunden in die immer mehr sich ausbreitende Informationstheorie.

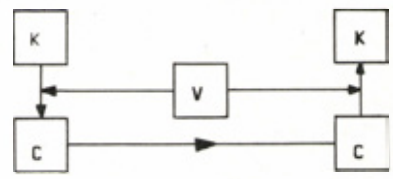
Im Folgenden soll deshalb zuerst eine einfachste allgemeine Betrachtungsweise über die Uebermittlung zitiert werden.

1. Das informationstheoretische Modell

Informationstheorie



Kryptographie



(1)

Hier bedeuten

I : die zu übermittelnde Idee
F : die Formulierung dieser Idee
S : das formulierte Signal (z.B. Sprache)

K : der zu übermittelnde Klartext
V : das Verschlüsselungsverfahren
C : der verschlüsselte Text

Die Uebermittlung wird richtig verstanden, wenn beide Partner dieselbe Formulierung beherrschen (z.B. "dieselbe Sprache sprechen") resp. dasselbe Verschlüsselungsverfahren vereinbaren.

Aus der Gleichartigkeit der beiden Modelle resultiert die Aehnlichkeit der Methoden; Informationstheorie im engern Sinne und Kryptographie unterscheiden sich aber in ihren Zielen :

Während die Informationstheorie durch zweckmässige Formulierungen (hier allgemein "Codierung" genannt) den Uebermittlungskanal

- entweder entlasten (durch Verminderung der Redundanz)
- oder gegen allfällige Störeinflüsse sichern (durch Vermehrung der Redundanz)

will, wobei die gewählte Formulierungsweise jedem Beteiligten bekannt sein darf, trachtet die Kryptographie danach

- einerseits geheime Formulierungen (= Verschlüsselungen) zu erfinden, welche für den Unberufenen schwer erkennbar sind,
- andererseits aus den verschlüsselten Texten allein die Klartexte und damit auch das a priori unbekannte Verschlüsselungsverfahren zu gewinnen (Dekryptierung).

Eingehendere Betrachtungen zeigen, dass auch hier die Grösse der Redundanz eine entscheidende Rolle spielt, doch steht die diesbezügliche kryptographische Forschung noch in den Anfängen [2].

Bemerkenswert für den Zusammenhang zwischen Informationstheorie und Kryptographie ist immerhin die Tatsache, dass die erste informationstheoretische Leistung des Kleinkindes eigentlich eine kryptographische ist :

Das Erlernen der Muttersprache aus gehörten Signalen ohne dass die zugehörige Formulierweise (eben die erst zu erlernende Muttersprache selbst) schon a priori bekannt wäre.

2. Die militärische Sachlage

Im militärischen Einsatz sind der Kryptographie im Erfinden und Anwenden von geheimen Verschlüsselungsverfahren Grenzen gesetzt.

Diese sind einmal gegeben durch das vorhandene Ordonnanzmaterial, das eine beschränkte Anzahl von Verschlüsselungsverfahren umfasst, welche an mehreren Stellen wiederholt angewendet werden und in deren Handhabung somit eine gewisse Einheitlichkeit beobachtet werden muss. Man wählt hier zweckmässig eine kleine Anzahl bewährter und deshalb mehr oder weniger allgemein bekannter Typen von Verschlüsselungsverfahren mit genügender Variationsfähigkeit (Schlüsselmannigfaltigkeit).

Ferner ist die Auswertung abgehörter Uebermittlungen nur eine Nachrichtenquelle unter vielen (Beobachtung, Aufklärung usw.), welche dem Gegner eine Beurteilung der Lage ermöglichen. Oft wird er auf Grund derselben die Klartexte zu verschlüsselten Uebermittlungen wenigstens teilweise vermuten können, und die Verschlüsselung kann nur mehr bezwecken, wenigstens diejenigen Klartextbestandteile geheim zu halten, welche dem Gegner noch nicht bekannt sind und seine Beurteilung der Lage ergänzen, bestätigen oder verneinen würden.

Diese beiden Umstände stellen recht hohe Anforderungen an die Sicherheit militärischer Verschlüsselungsverfahren und es ist verständlich, dass die in der Einleitung erwähnte Literatur in dieser Hinsicht eher zurückhaltend ist. Wie aber diesen Anforderungen Genüge geleistet werden kann, sollen die nachfolgenden Ausführungen darlegen.

3. Das kryptographische Modell

Es seien

$\mathfrak{K}$: die Menge aller für eine Uebermittlung in Frage kommenden Klartexte K ;

$\mathfrak{T}$: die Menge aller zur Verfügung stehenden Verschlüsselungsmöglichkeiten S ;

$\mathfrak{C}$: die Menge aller Chiffretexte C = S (K), welche durch Anwendung einer Verschlüsselung S auf einen Klartext K resultieren, formal $\mathfrak{C} = \mathfrak{T}\ (\mathfrak{K})$

Denkt man sich alle zugelassenen Klartexte, Verschlüsselungsmöglichkeiten und Chiffretexte numeriert

$$\begin{array}{lll} n(K_1) = 1 & n(S_1) = 1 & n(C_1) = 1 \\ n(K_2) = 2 & n(S_2) = 2 & n(C_2) = 2 \\ n(K_3) = 3 & n(S_3) = 3 & n(C_3) = 3 \\ \vdots & \vdots & \vdots \end{array} \qquad (2)$$

so lässt sich jedes Verschlüsselungsverfahren darstellen als Zuordnung zwischen diesen Nummern

$$f[n(K_\lambda);n(S_\mu)] = n(C_\nu) \qquad \text{oder kurz} \qquad f[\lambda : \mu] = \nu \qquad (3)$$

In der Fülle dieser Zuordnungsmöglichkeiten nimmt die Addition

$$\lambda + \mu = \nu \qquad (4)$$

eine derart hervorragende Stelle ein sowohl in der historischen Entwicklung als auch in der technischen Bedeutung, dass wir uns im Folgenden auf diese allein beschränken werden.

4. Das Additionsverfahren

Wir betrachten zuerst ein einfachstes Modell.

Es bestehe $\mathfrak{K}$ aus 4 zugelassenen Klartexten, z.B. aus den Zeitangaben

$$\begin{array}{l} K_1 = 0001 - 0600 \\ K_2 = 0601 - 1200 \\ K_3 = 1201 - 1800 \\ K_4 = 1801 - 2400 \end{array} \qquad (5)$$

für den möglichen Zeitpunkt einer täglich einmal durchzuführenden Aktion (z.B. Materialfassung, Absenden eines Kuriers, Ablösen eines Detachementes usw.).

$\mathfrak{T}$ bestehe aus den 4 möglichen Schlüsseln S_1, S_2, S_3, S_4 und es gelte

$$\underline{n(K) + n(S) \equiv n(C) \bmod 4} \qquad (6)$$

was der Zuordnungstabelle

	n(S)	1	2	3	4
n(K)	n(C)				
1		2	3	4	1
2		3	4	1	2
3		4	1	2	3
4		1	2	3	4

(7)

für die 4 Chiffretexte C_1, C_2, C_3, C_4 entspricht.

"Fassung zwischen 0601 - 1200" (= K_2) verschlüsselt mit Schlüssel S_3 ergibt demnach Chiffrat C_1.

Es sei nun dem Abhörenden aus andern Nachrichtenquellen (z.B. frühere Beobachtungen) bekannt, dass

- die 4 möglichen Zeiträume gemäss (5) ungleich häufig befohlen werden, z.B. mit den Wahrscheinlichkeiten

n(K)	p n(K)
1	0,1
2	0,3
3	0,2
4	0,4

(8)

- der Chiffreur eine Vorliebe für die Schlüssel mit gerader Nummer hat und diese mit den Wahrscheinlichkeiten

n(S)	q n(S)
1	0,1
2	0,4
3	0,1
4	0,4

(9)

wählt.

Wird jetzt die Uebermittlung des Chiffretextes C_v abgehört, so ergibt sich für die Wahrscheinlichkeit $\bar{p}_\lambda$ dafür, dass diesem Chiffrat der Klartext K_λ zugrunde lag, nach der Bayesschen Regel unter Berücksichtigung von $\lambda + \mu = V$ der Wert.

$$\bar{p}_\lambda = \frac{p_\lambda \, q_{v-\lambda}}{p_1 \, q_{v-1} + p_2 \, q_{v-2} + p_3 \, q_{v-3} + p_4 \, q_{v-4}} \qquad (10)$$

oder ausgerechnet

	n(C)	1	2	3	4
λ = n(K)	$\bar{p}_\lambda$				
1		0,21	0,03	0,21	0,03
2		0,16	0,39	0,16	0,39
3		0,42	0,06	0,42	0,06
4		0,21	0,52	0,21	0,52

(11)

Die ursprüngliche Beurteilung der Lage (8) wird also durch die Uebermittlung der Chiffrate C_2 oder C_4 gestützt, durch die Uebermittlung der Chiffrate C_1 oder C_3 in Frage gestellt, womit schon ein kleiner Dekryptiererfolg erzielt ist.

Würde der Chiffreur im Gegensatz zu (9) alle möglichen Schlüssel mit gleicher Wahrscheinlichkeit verwenden, so ergäbe sich

$$\bar{p}_\lambda = p_\lambda \qquad (12)$$

das heisst, die Uebermittlung eines Chiffrates verbessert die ursprüngliche Beurteilung der Lage (8) nicht.

Aber auch die gleichwahrscheinliche Verwendung der möglichen Schlüssel ermöglicht einen Dekryptiererfolg, wenn mehrere gleichgeschlüsselte Chiffretexte nacheinander übermittelt werden.

Es seien z.B. an 4 aufeinanderfolgenden Tagen die Chiffrate C_4, C_2, C_4, C_1 abgehört worden. Unter der Voraussetzung gleicher Schlüssel entsprechen diese den möglichen Klartextfolgen

	n(C)	4	2	4	1	$\bar{\bar{p}}_\mu$
μ = n(S)	n(K)					
1		3	1	3	4	0,113
2		2	4	2	3	0,507
3		1	3	1	2	0,042
4		4	2	4	1	0,338

(13)

mit den Wahrscheinlichkeiten $\bar{\bar{p}}$. Sehr wahrscheinlich wurde Schlüssel S_2 verwendet und die Klartexte K_2, K_4, K_2, K_3 übermittelt.

Derartige Ueberlegungen und eingehendere allgemeine Untersuchungen ergeben, dass sich auf dem Prinzip des Additionsverfahrens eine sichere Verschlüsselung (im Sinne der Anforderungen nach Ziff. 2) aufbauen lässt unter folgenden Voraussetzungen :

- die Menge $\mathfrak{S}$ der möglichen Verschlüsselungen muss mindestens soviele Elemente enthalten wie die Menge $\mathfrak{K}$ der zugelassenen Klartexte;
- alle möglichen Schlüssel S der Menge $\mathfrak{S}$ müssen mit gleichgrosser Wahrscheinlichkeit ausgewählt werden; (14)
- ein und derselbe Schlüssel S darf nur für die Verschlüsselung eines einzigen Klartextes K verwendet werden.

5. Anwendungen des Additionsverfahrens

Die direkte praktische Anwendung des Additionsverfahrens (im Sinne des Modells nach Ziff. 3) begegnet vorerst einer eigentümlichen Schwierigkeit: die Bestimmung der Menge $\mathfrak{K}$ der zugelassenen Klartexte K und deren Numerierung.

In der Regel behilft man sich so, dass die Klartexte in ihre Elemente (z.B. Buchstaben) zerlegt werden, welche man ein-

zeln numeriert und dann nach einem Additionsverfahren verschlüsselt.

Beispiele dafür sind :

5.1. Der klassische Additionschiffre

Die Buchstaben des Alphabets werden mit Ordnungsnummern versehen, z.B.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

und dann gemäss

$$n(K) + n(S) \equiv n(C) \mod 26 \qquad (15)$$

verknüpft.

So ergibt sich aus dem Klartext K = d i e s t r a s s e v o n ...
und dem Schlüsseltext S = t r k s i f b x r o l m s ...
das Chiffrat C = x a p l c x c q k t h b g ...

5.2. Die Impulschiffrierung

Die dualen 0/1 Impulse eines Telegraphieralphabetes werden gemäss

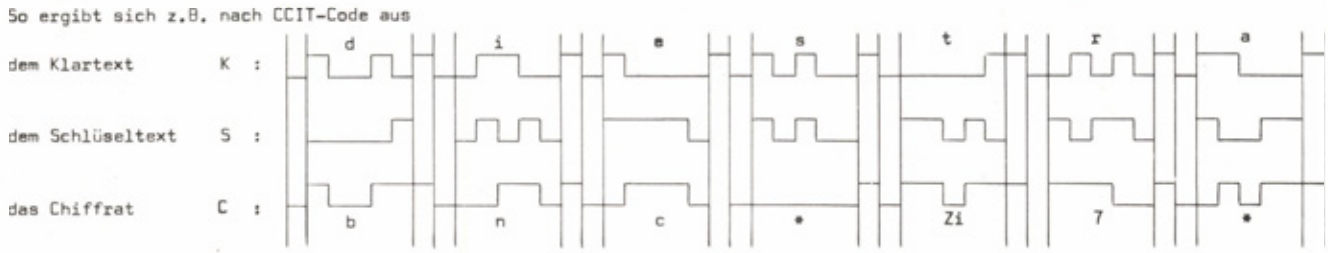
$$n(K) + n(S) \equiv n(C) \mod 2 \qquad (16)$$

das heisst nach der Tabelle

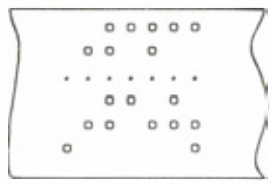
0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0

verknüpft.

So ergibt sich z.B. nach CCIT-Code aus



In der Regel wird der Schlüsseltext einem Lochstreifen entnommen (Vernam 1926 3), z.B.



5.3. Die Ueberlagerungschiffrierung

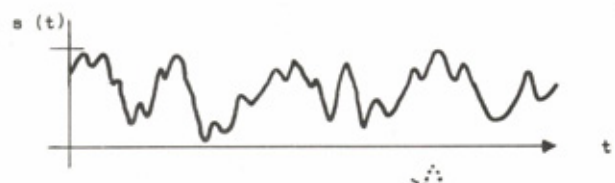
Einem als Zeitfunktion (z.B. Spannungsverlauf) dargestellten Klartextsignal wird ein Zusatzsignal überlagert gemäss

$$k(t) + s(t) \equiv c(t) \mod 1 \qquad (17)$$

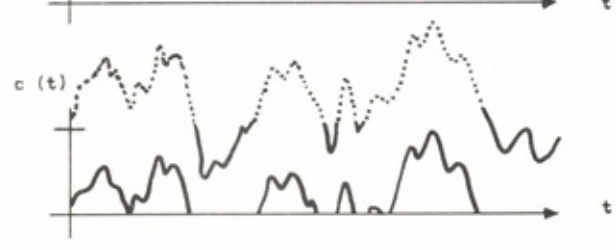
Dieses Verfahren findet Anwendung in der elektrischen Sprachchiffrierung.

Aus dem Klartextsignal

und dem willkürlichen Zusatzsignal

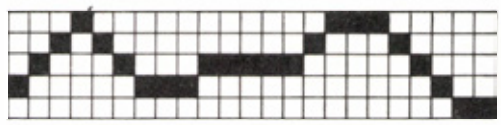


entsteht das Chiffretextsignal.

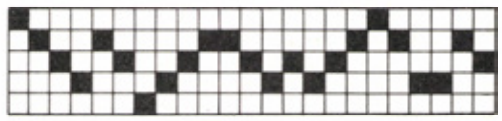


Um das infinitäre Verhalten der beteiligten Funktionen zu verwischen und aus technischen Gründen (Impulstechnik) wählt man in der Praxis eine Rasterung. In dieser Form ergibt sich wieder ein klassischer Additionschiffre gemäss Ziff. 5.1. :

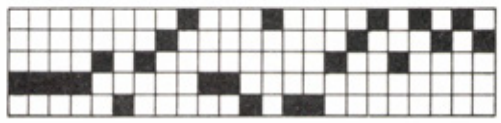
Klartext



Schlüsseltext



Chiffretext



Für eine naturgetreue Wiedergabe der Sprache benötigt man eine Rasterung, welche

- in der Abszisse ca. 1000 Teile der Sekunde,
- in der Ordinate ca. 100 Teile der Amplitude

auflöst. Das sind 100'000 Einheiten/Sekunde $\approx$ 17 bit/sec, was der Informationsleistung, welche durch die Uebermittlung von 384I Buchstaben/Sekunde geliefert wird, entspricht.
Durch geeignete Rasterung oder überhaupt durch andersartige Darstellung der Sprachsignale ist es der Informationstheorie gelungen, die für die Uebermittlung der Sprache notwendige Anzahl bit/sec zu reduzieren; die kryptographischen Konsequenzen derartiger Verfahren sind aber heute noch zu wenig bekannt.

Das eingangs der Ziff. 5 erwähnte Behelfsverfahren, die Klartexte in ihre Elemente zu zerlegen und dann diese einzeln zu numerieren, ist sehr übersichtlich und technisch leicht verwertbar, hat aber den Nachteil, dass auch beliebige sinnlose "Klartexte" wie (z.B. im Falle des klassischen Additionschiffre Ziff. 5.1.)

```
a a a a a a a a a a
b a a a a a a a a a
c a a a a a a a a a
. . . . . . . . . .
. . . . . . . . . .
. . . . . . . . . .
z a a a a a a a a a                                    (18)
a b a a a a a a a a
b b a a a a a a a a
c b a a a a a a a a
. . . . . . . . . .
. . . . . . . . . .
. . . . . . . . . .
x z z z z z z z z z
y z z z z z z z z z
z z z z z z z z z z
```

zugelassen sind und mitnumeriert werden.

Der Anteil der sinnvollen Texte unter den so zugelassenen "Klartexten" lässt sich grob abschätzen wie folgt :

Für die Bestimmung eines Buchstabens benötigt man

- in willkürlichem Text $\log_2 26 = 4{,}7$ bit
- in sinnvollem Text ca. 1,5 bit (empirisch bestimmter mittlerer Wert).

Dies entspricht einem Verhältnis von

$$q = 2^{1,5 - 4,7} = 2^{-3,2} \approx 1/10 \qquad (19)$$

das heisst unter den 26^N zugelassenen "Klartexten" von N Buchstaben befinden sich nur ungefähr $(26/10)^N$ sinnvolle.

Z.B. befinden sich unter den 26^{10} = 141'167095'653376 Zeilen der Liste (18) nur ungefähr 14117 sinnvolle Texte.

Da für ein sicheres Verschlüsselungsverfahren nach den Postulaten (14) die Auswahl an Schlüsseln mindestens so gross sein muss wie die Anzahl der zugelassenen Klartexte, ergibt sich die unwirtschaftliche Situation, dass für die Verschlüsselung der relativ wenigen $(26/10)^N$ allein in Frage kommenden sinnvollen Klartexte das Verschlüsselungsverfahren die ungeheure Mannigfaltigkeit von 26^N Schlüsseln umfassen muss.

Wie sich eine Beschränkung der Schlüsselmannigfaltigkeit auswirken würde, zeigt folgende Ueberschlagsrechnung :

Ein Verschlüsselungsverfahren mit der Mannigfaltigkeit von M Schlüsseln sei dem Gegner bekannt und es werde ein Chiffrat von N Buchstaben übermittelt. Der Gegner sei in der Lage, sämtliche M möglichen Schlüssel zur Dechiffrierung dieses Chiffrates durchzuspielen, er erhält so M zugehörige, meist sinnlose "Klartexte". Die Wahrscheinlichkeit w(x) dafür, dass sich unter diesen M "Klartexten" allein durch das Spiel des Zufalls x sinnvolle befinden, berechnet sich nach der binomischen Formel zu

$$w(x) = \binom{M}{x} . 10^{-Nx} . (1 - 10^{-N})^{M-x} \qquad (20)$$

mit dem Erwartungswert $M.10^{-N}$, das heisst unter den M dechiffrierten "Klartexten" werden sich voraussichtlich $M.10^{-N}$ sinnvolle, aber falsche befinden.

Für $M = 26^{10}$ findet man

N	$M.10^{-N}$
10	14117
11	1412
12	141
13	14
14	1
15	0,1
.	.
.	.
.	.

(21)

Für N≫ 14 werden sich also unter den M dechiffrierten "Klartexten" keine sinnvollen falschen Klartexte befinden, sondern nur mehr ein sinnvoller Text: der richtige Klartext.

Damit ist gezeigt, dass selbst die respektable Mannigfaltigkeit von 26^{10} möglichen Schlüsseln nur für die wirksame Chiffrierung eines Textes von höchstens 14 Buchstaben ausreicht; andernfalls wäre man in der Lage, durch systematisches Probieren (das mit der Entwicklung moderner Rechenautomaten allmählich in den Bereich des Möglichen rückt) den richtigen Klartext zu finden.

Der Wunsch, die Mannigfaltigkeit der notwendigen Schlüssel dennoch zu reduzieren, ist verständlich. Möglichkeiten dazu bestehen :

- in der Einführung einer variablen Zuordnung der Ordnungsnummern zu den Elementen des Klartextes, womit beim klassischen Additionschiffre (Ziff. 5.1) und bei der Ueberlagerungschiffrierung (Ziff. 5.3) eine beschränkte Verbesserung der Wirtschaftlichkeit erzielt werden kann. Bei der dualen Impulschiffrierung (Ziff. 5.2) ist eine variable Zuordnung praktisch unwirksam.
- in der weitgehenden Redundanzreduzierung der für die Uebermittlung der Klartexte gewählten Signale. Diese Forderung steht in gewissem Widerspruch zur Forderung der Uebermittlungssicherheit und kann nur erfüllt werden durch eine bis heute noch nicht realisierte Zusammenarbeit Informationstheorie/Kryptographie.
- im Verlassen des Additionsprinzips. Diesbezügliche Ausführungen würden aber über den gewählten Rahmen dieser Arbeit hinausgehen.

Interessant ist die Tatsache, dass die historische Entwicklung bezüglich der Mannigfaltigkeit der Schlüssel den umgekehrten Weg gegangen ist. Sie hat begonnen mit primitiv beschränkten Schlüsselmannigfaltigkeiten, um dann, angeregt durch die unliebsamen Erfahrungen mit unberufenen Dekrypteuren, immer kompliziertere und umfassendere Mannigfaltigkeiten einzuführen bis zum Stand der heutigen Erkenntnis. -

Die nachfolgend aufgeführten Marksteine in der Entwicklung der Additonschiffre sollen diese Sachlage illustrieren.

6. Die historische Entwicklung

6.1. Der Cäsar
(101 - 44 v.Chr.)

Schlüsseltext konstant :

```
K = d i e s t r a s s e v o n . . .
S = 4 4 4 4 4 4 4 4 4 4 4 4 4 . . .
C = h m i w x v e w w i z s r . . .
```

6.2. Der Sprungchiffre

(bis 1914-1918, eigentlich ein Anachronismus, vergl. Figl [4])

Schlüsseltext sequenzweise konstant :

```
K = d i e s t r a s s e v o n . . .
S = 7 7 7 7 7 2 2 2 2 2 4 4 4 . . .
C = k p l z a t c u u g z s r . . .
```

6.3. Der Vigenère

(1586 [5])

Schlüsseltext periodisch :

```
K = d i e s t r a s s e v o n . . .
S = 4 712 5 4 712 5 4 712 5 4 . . .
C = h p q x x y m x w l h t r . . .
```

Dieses Verfahren hat fast 3 Jahrhunderte lang den Ruf des "chiffre indéchiffrable" behaupten können, bis schliesslich Kasiski [6] 1863 eine fast unfehlbare Dekryptiermethode dazu angab. Bemerkenswert ist insbesondere die Tatsache, dass zur Zeit Kasiskis der Vigenère als der (einzige) Chiffre galt.

Zur Illustration der Methode von Kasiski sei folgendes Beispiel angeführt :

```
C :   u u k b r   i h l j j   v h v j k   b x q n f   u c y f t
      a k p n x   k y s v y   t x c n f   j y a o s   k m h r u
      y h s f n   h m t g k   z y o b x   u g c r u   y n f f a
      i h c m w   i h z b z   j x c e g   e u f g g   d z p w k
      v c f f s   t n b y x   v l w o k   x k v n a   q y a o k
      d l i a s   y f w o j   u g h l z   n o f h b   u k a r w
      y y f
```

1. Schritt : Bestimmung der Periodenlänge.
Das Hauptverdienst von Kasiski bestand in der Erkenntnis, dass im Chiffrat sich wiederholende Buchstabenpaare (Bigramme) vorzugsweise um ganzzahlige Vielfache der Periodenlänge auseinander liegen. Im vorliegenden Chiffrat wird beobachtet

Bigr.	Abstand	Bigr.	Abstand	Bigr.	Abstand
ao	80	kv	17	uy	20
bx	48	nf	20 53 33	wo	20
ff	30	ok	10	xc	50
hl	131	ru	20	xk	86
ih	70 75 5	ug	70	ya	80
kb	12	uk	144	yf	108 129 21

Von diesen 24 Abstandszahlen sind folgende Anzahlen durch n teilbar

n	Anzahl	Reduktion	Ueberschuss
1	24	24	0
2	16	12	4
3	9	8	1
4	10	6	4
5	13	5	8
6	5	4	1
7	3	3	-
8	4	3	1
9	2	3	-
10	11	2	9
11	1	2	-
12	4	2	2
13	0	2	-
14	2	2	0
15	2	2	0
usf.			

(Reduktion = 24/n)

Das Maximum liegt bei 10, woraus die Periodenlänge 10 geschlossen wird.

2. Schritt : Periodenanordnung des Chiffrates.

```
u u k b r i h l j j
v h v j k b x q n f
u c y f t a k p n x
k y s v y t x c n f
j y a o s k m h r u
y h s f n h m t g k
z y o b x u g c r u
y n f f a i h c m w
i h z b z j x c e g
e u f g g d z p w k
v c f f s t n b y x
v l w o k x k v n a
q y a o k d l i a s
y f w o j u g h l z
n o f h b u k a r w
y y f
```

Sofern die Hypothese der Periodenlänge 10 richtig ist, sind nun die Buchstaben aus ein und derselben Kolonne entstanden aus den Klarbuchstaben durch Addition ein und derselben Schlüsselzahl.

Zur Bestimmung dieser Schlüsselzahlen werden die Häufigkeiten der Buchstaben in jeder Kolonne festgestellt und mit den für die Klarbuchstaben empirisch bekannten "normalen Häufigkeiten" verglichen (dieses Verfahren war schon lange vor Kasiski bekannt).

a	0	0	2	0	1	1	0	1	1	1	r
b	0	0	0	3	1	1	0	1	0	0	s
c	0	2	0	0	0	0	0	4	0	0	t
d	0	0	0	0	0	2	0	0	0	0	u
e	1	0	0	0	0	0	0	0	1	0	v
f	0	1	5	4	0	0	0	0	0	2	w
g	0	0	0	1	1	0	2	0	1	1	x
h	0	3	0	1	0	1	2	2	0	0	y
i	1	0	0	0	0	2	0	1	0	0	z
j	1	0	0	1	1	1	0	0	1	1	a
k	1	0	1	0	3	1	3	0	0	2	b
l	0	1	0	0	0	0	1	1	1	0	c
m	0	0	0	0	0	0	2	0	1	0	d
n	1	1	0	0	1	0	1	0	4	0	e
o	0	1	1	4	0	0	0	0	0	0	f
p	0	0	0	0	0	0	0	2	0	0	g
q	1	0	0	0	0	0	0	1	0	0	h
r	0	0	0	0	1	0	0	0	3	0	i
s	0	0	2	0	2	0	0	0	0	1	j
t	0	0	0	0	1	2	0	1	0	0	k
u	2	2	0	0	0	3	0	0	0	2	l
v	3	0	1	1	0	0	0	1	0	0	m
w	0	0	2	0	0	0	0	0	1	2	n
x	0	0	0	0	1	1	3	0	0	2	o
y	4	5	1	0	1	0	0	0	1	0	p
z	1	0	1	0	1	0	1	0	0	1	q

Man findet so z.B. in der zweitletzten Kolonne mit der auf dem Papierstreifen angedeuteten Lage die beste Uebereinstimmung; dies liefert dort die Schlüsselzahl a-r = 9.

Ebenso findet man in den andern Kolonnen die Schlüsselzahlen

17 20 18 01 06 16 19 15 09 18

mit dem Klartext

d a s a l s o w a r
e n d i e l e b e n
d i g e n k r a e f
t e a u s d e n e n
s e i n m u t s i c
h n a e h r t e x s
i e w a r e n n i c
h t n e u s o n d e
r n h a t t e n v o
n a n f a n g a n s
e i n e m d u m p f
e r e n e h r g e i
z e i n e n s t r a
h l e n d e n s c h
w u n g v e r l i e
h e n

Betrachtet man die Einfachheit dieser Dekryptiermethode, so ist es eigentlich kaum verständlich, dass das Chiffrierverfahren von Vigenère sich so lange halten konnte; umso mehr, als nach heutiger Auffassung eine spezielle Periodenbestimmung ja gar nicht notwendig war, sofern man nur die möglichen Perioden 1, 2, 3, 4, 5, ... sukzessive durchprobieren würde.
Offenbar hat man vor Kasiski gar nicht an die Möglichkeit einer Dekryptierung geglaubt und die Untersuchungen einfach eingestellt. So stellt Kasiski eigentlich den ersten Anfang einer modernen Kryptographie dar.

6.4. Der Cadran

(Kryha, Hamel [7] 1927)

Differenz der Schlüsselfolge periodisch :

K =	d	i	e	s	t	r	a	s	s	e	v	o	n	...
S =	4	1	6	4	1	6	4	1	6	4	1	6	4	...
	8	12	13	19	23	24	4	8	9	15	19	20	26	...
C =	l	u	r	l	q	p	e	a	b	t	o	i	n	...

6.5. Chiffrierung nach einem Buch

(dekryptiert von Bazeries [8] 1901)

Schlüsselfolge nach einem vereinbarten Buchtext :

K =	d	i	e	s	t	r	a	s	s	e	v	o	n	...
S =	f	e	s	t	g	e	m	a	u	e	r	t	i	...
C =	j	n	x	m	a	w	n	t	n	j	n	i	w	...

6.6. Der Buchstabenwurm

(Vernam [3] 1926)

Schlüsselfolge willkürlich : vergl. Ziff. 5.1

Dieses Verfahren setzt voraus, dass beide miteinander verkehrenden Partner über einen genügenden Vorrat an vorbereiteten gleichlautenden Schlüsseltexten verfügen. Würde ein und derselbe Schlüsseltext zweimal verwen-

det, so reduziert sich dieses Verfahren praktisch auf dasjenige nach Ziff. 6.5.

Nach den Ausführungen in Ziff. 5 genügt der Buchstabenwurm, richtig angewendet, den Anforderungen nach den Postulaten (14), er ist jedoch kryptographisch unwirtschaftlich und wird deshalb nur für höchste Sicherheitsansprüche (Diplomatie u.s.w.) eingesetzt.

Gerade die Schwierigkeit, im militärischen Einsatzbereich eine genügende Anzahl gleichlautender Schlüsseltexte bereitzustellen und nachzuschieben, hat (ausserhalb der oben angegebenen historischen Reihe) zu Konstruktionen Anlass gegeben, welche auf maschineller Basis angenähert willkürlich erscheinende Schlüsseltexte produzieren. Solche Maschinen sind neben dem unwirtschaftlichen Zahlenwurm immer noch konkurrenzfähig, sind aber mehr oder weniger den durch die Ueberschlagsrechnung (20) aufgezeigten Beschränkungen unterworfen.

P. Glur

Literatur :

1 L. Sacco : Manuel de Cryptographie, Paris 1951

2 C.E. Shannon : Communication Theory of Secrecy Systems, the Bell System Technical Journal 1949, S. 656-715

3 Cartier : Les Secrets en T.S.F., Radioélectricité, Paris 1926

4 Figl : Systeme des Chiffrierens, Graz 1926

5 B. de Vigenère : Traictés des chiffres ou secrètes manières d'escrire, Paris 1586

6 F.W. Kasiski : Die Geheimschriften und die Dechiffrierkunst, Berlin 1863

7 G. Hamel : Die Chiffriermaschine System Kryha, Berlin 1927

8 Bazeries : Les chiffres secrets dévoilés, Paris 1901