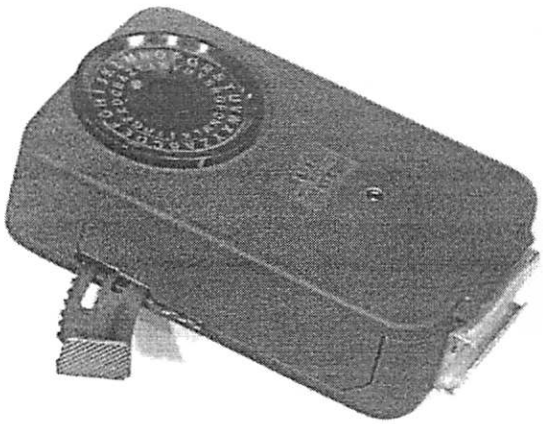
Übung zu Angewandter Systemtheorie: Kryptographie

SS 1997 – Übungsleiter: Dr. Josef Scharinger

Taschenchiffriergerät CD-57



Michael Topf, Matr.Nr. 9155665, Kennz. 880

Johannes Kepler Universität Linz
Institut für Systemwissenschaften
Abteilung für Systemtheorie und Informationstechnik

Inhaltsverzeichnis

Einleitung

Der geistige Vater des betrachteten Chiffriergeräts sowie einer Reihe verwandter Geräte ist der Schwede Boris Hagelin. Daher sollen einleitend er, die Familie der Rotor-Kryptographierer sowie die von ihm gegründete Schweizer Firma Crypto AG, vorgestellt werden.

Boris Hagelin

Boris Hagelin war ein Visionär, der bereits zu seiner Zeit die Probleme der Informationstechnologie erkannte. [CRYP97]

Basierend auf den kryptographischen Erfindungen des Ingenieurs Arvid Gerhard Damm wurde 1916 in Stockholm, Schweden, die Firma A. B. Cryptograph gegründet. Nach anfänglichen finanziellen Schwierigkeiten zeigte die bekannte Familie Nobel Interesse an der Firma und übernahm 1920 deren Finanzierung. 1922 setzte die Familie Nobel Boris Hagelin als Sachverwalter in der Firma ein. Schon bald begann dieser, sich für Kryptographie zu interessieren und begann selbst, kryptographische Maschinen zu entwerfen. Seine C-36 wurde als M-209 von den amerikanischen Streitkräften während des zweiten Weltkrieges intensiv genutzt. Einige Jahre nach dem Krieg ging Hagelin in die Schweiz, wo er am 15. Mai 1952 in Zug die Firma Crypto AG gründete. Eine der ersten Konstruktionen, die er in der Schweiz baute, war der Chiffrierer CX-52 [ANDE96]

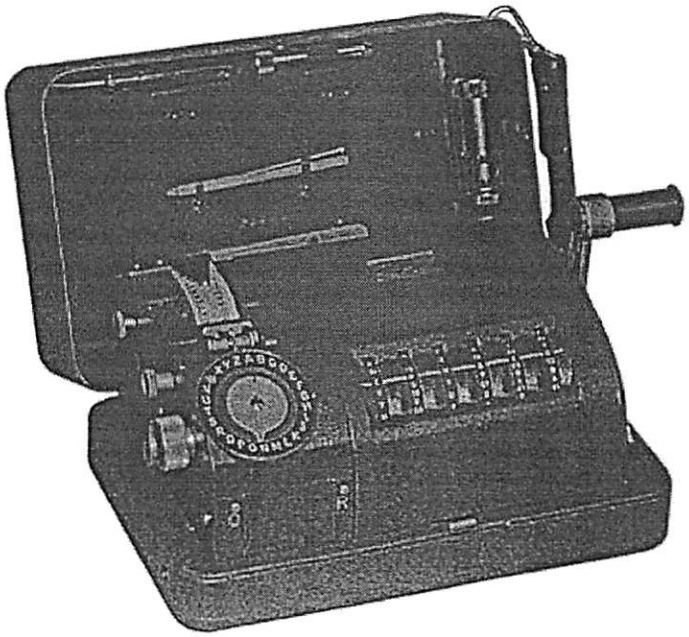


Abbildung 1: Der Hagelin Chiffrierer CX-52 [ANDE96]

Die Hagelin M-209 Rotormaschine

Sehr verwandt mit der zu betrachtenden CD-57 ist die C-48, die es zu großer Bekanntheit beim amerikanischen Militär gebracht hat.

Die Hagelin C-48, besser bekannt als M-209 wurde in einigen Varianten hergestellt, unter anderem für die amerikanische Navy, wo sie CSP-1500 hieß. Sie hat sechs Codescheiben (Rotoren), bot aber relativ geringe Sicherheit. [IACR95]

Die M-209 ist ein portables, handbetriebenes Chiffrier- und Dechiffriergerät für taktische Meldungen, das auf einem Papierstreifen druckt. Ihr kryptographisches Prinzip beruht auf reziproker Substitution von Alphabeten. Ein Alphabet in normaler Reihenfolge wird gegen eines mit umgedrehter Reihenfolge verschoben. Das wird durch einen Satz Räder mit einer unterschiedlichen Anzahl von Stiften erreicht, die aktiviert oder deaktiviert werden können und über Abtasthebel eine sehr unregelmäßige Verschiebung der Alphabete erzeugen. [NMMA97]

Die Maschine wurde als Ersatz für die M-94 (Navy: CSP-885) für taktische Situationen entwickelt. Sie basiert auf einer von B. Hagelin in den späten 30er Jahren gebauten Entwicklung. 1940 wurden einige Geräte von der Army Signal Corp. gekauft. Nachdem sie im Hinblick auf leichtere Produzierbarkeit modifiziert und robuster gemacht wurde, begann die Herstellung in den Vereinigten Staaten. Während der Afrikanischen Invasion im November

1942 war der erste breite Einsatz der M-209. Im Zweiten Weltkrieg wurden über 140.000 Einheiten von ihr produziert. [NMMA97]

Abbildung 2: Die Hagelin M-209-B Rotormaschine wiegt 2,7kg. [IACR95]
Circa 30 Zeichen pro Minute konnten mit ihr ver- oder entschlüsselt werden.

Ihre Beliebtheit in der Army verdankte sie ihren kleinen Abmessungen, ihrem geringen Gewicht und der leichten Erlernbarkeit ihrer Bedienung. Darüber hinaus waren für das Gerät selbst keine besonderen Sicherheitsvorkehrungen zu treffen. Allerdings war es kryptographisch nie sicher und konnte daher nur auf unteren taktischen Ebenen verwendet werden, wo es lediglich notwendig war, einen Feind um einige Stunden hinzuhalten. [NMMA97]

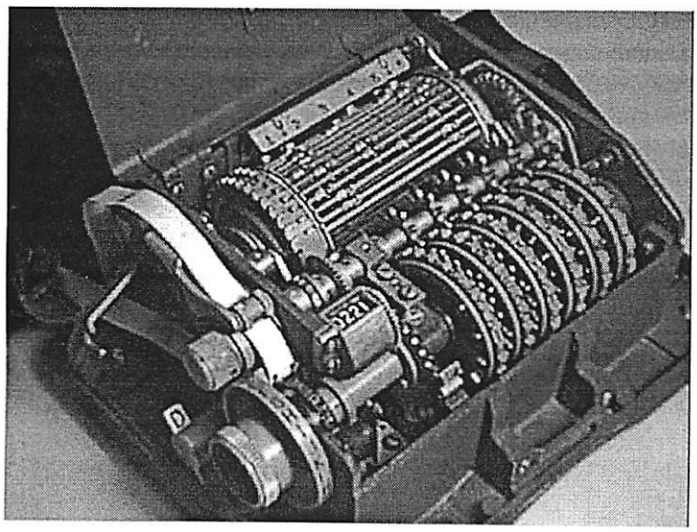


Abbildung 3: Die Hagelin M-209-B Rotormaschine im geöffneten Zustand [IACR95]

Das Taschenchiffriergerät CD-57

Der steigende Bedarf an Taschenchiffriergeräten hat zur Entwicklung des CD-57 geführt. Dieses Gerät ist für solche Anwendungsfälle gedacht, wo Kleinheit die Hauptforderung darstellt und wo auf gedruckte Meldungen verzichtet werden kann.

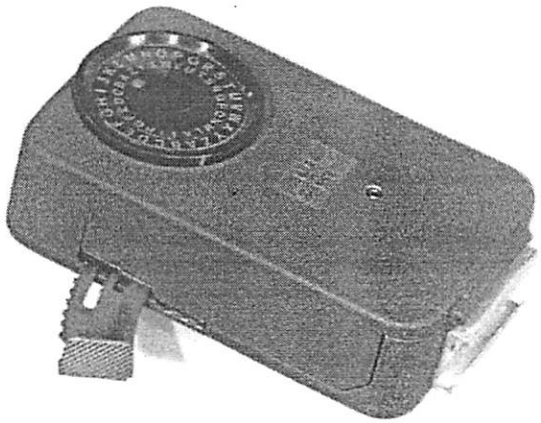


Abbildung 4: Das Taschenchiffriergerät CD-57

Gegenüber den vorher bekannten Taschenchiffriergeräten weist das CD-57 eine größere Sicherheit auf. Sie bietet außerdem die Möglichkeit, mit größeren – druckenden – Geräten der Firma Crypto AG (C-4 und C-52/CX-52) zusammenzuarbeiten, was beim Aufbau von Nachrichtenorganisationen von Vorteil ist. Da kein Druckmechanismus vorliegt, fällt das Einstellen der Buchstaben weg. Es wird lediglich abgelesen und, falls nötig, von Hand notiert, in vielen Fällen aber direkt in das Telephon oder das Funkgerät diktiert. [CRYP63]

Die Crypto AG

Hersteller des Taschenchiffriergerätes CD-57 war die 1952 von Boris Hagelin gegründete Firma Crypto AG mit Sitz in Zug in der Schweiz. Heute baut Crypto AG auf 45 Jahre Erfahrung und beliefert Kunden in über 130 Ländern auf allen Kontinenten. Sie baut Sicherheitssysteme für Kommunikation und Management auf individueller Basis, die im Diplomatendienst, beim Militär, bei Polizei und Behörden sowie bei zahlreichen Firmen im Einsatz stehen. 1985 erhielt sie die ISO 9001 Qualitätsmanagement Zertifizierung. [CRYP97]

Anfang der achtziger Jahre bekam die Crypto AG allerdings mit negativen Schlagzeilen einen unangenehmen Beigeschmack. Sie wurde beschuldigt, Verfahren und Schlüssel an den amerikanischen Geheimdienst National Security Agency NSA verkauft zu haben. Am 18. März 1992 nahm der Teheran den Verkaufsführer der Crypto AG, Hans Bühler, fest, um zu erfahren, an wen er die Teheraner Codes und die Schlüssel Libyens verraten habe. Auch die Besitzverhältnisse der Firma waren mehrmals fragwürdig. Gerüchten zufolge gab es innige Bindungen mit dem Bundesdeutschen Geheimdienst BND sowie mit der Siemens AG, bei der mehrere der wechselnden Geschäftsführer vorher beschäftigt waren. Auch den Aussagen eines früheren Beschäftigten der Crypto zufolge wurden bei manchen Kunden entweder abgemagerte Chiffrierverfahren eingesetzt oder aber dem Chiffrat Zusatzinformation beigefügt, die den Code für Eingeweihte spielend leicht zu errechnen gestatteten. [SPIE96]

Funktionsweise

Kryptographisches Prinzip

Losgelöst von der mechanischen Realisierung, auf die später noch eingegangen wird, soll hier der logische Aufbau des CD-57 gezeigt werden.

Das Taschenchiffriergerät CD-57 bedient sich eines symmetrischen Chiffrierverfahrens, der Schlüssel muß also geheim gehalten werden. Als Pseudo-Zufallszahlengenerator werden sechs einfach rückgekoppelte binäre Schieberegister verwendet. Die Codierungsfunktion ist so beschaffen, daß die Ausgänge der Schieberegister gewichtet und gemeinsam mit dem Primärtext (Klartext / Chiffrat) summiert und Modulo 26 dividiert werden. Zusätzlich erlaubt das CD-57 noch eine Konstante (Relativlage) dazuzuaddieren.

Das CD-57 soll auf die gleiche Weise ver- und entschlüsseln können. Dazu ist es notwendig, daß das Verfahren reziprok ist, was man durch Zuordnung eines Alphabets in richtiger Reihenfolge zu einem in umgekehrter Reihenfolge erreicht, also den Primär- oder Sekundärtext mit einem negativen Vorzeichen behaftet, das sich beim zweiten Verarbeiten wegkürzt.

Allgemein:	Ausgabe = -Eingabe + Pseudozufall (f)
Verschlüsseln:	Chiffrat (C) = -Klartext (P) + f
Entschlüsseln:	$P = -C + f$ mit $C = -P + f \Rightarrow P = -(-P + f) + f = P$

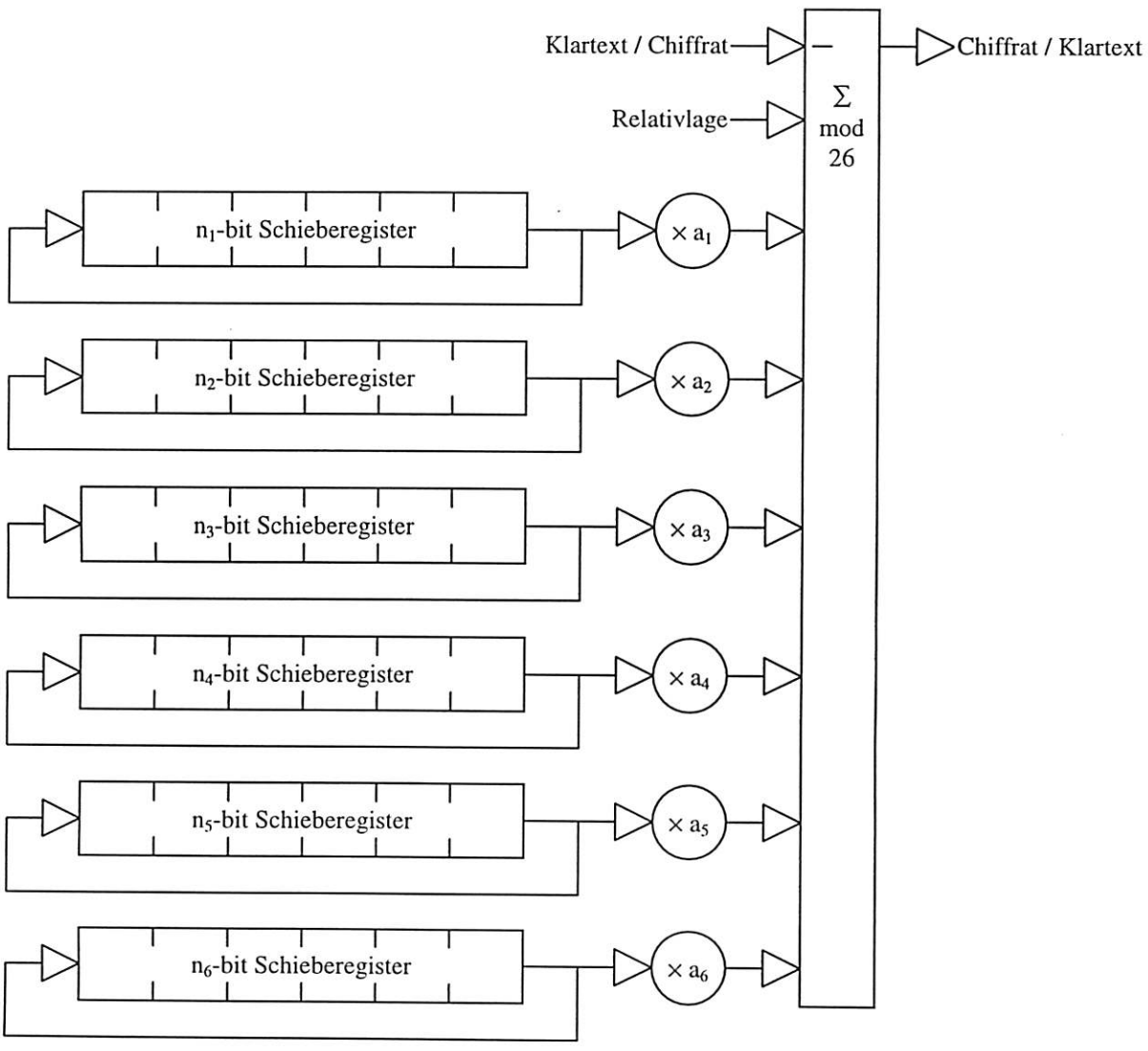


Abbildung 5: Blockschaltbild des CD-57

Es werden zwei Arten von Schlüsseln unterschieden:

- Der innere (Grund-)Schlüssel
  - Anfangszustand der Schieberegister
    Der Anfangszustand wird durch die Lage der Stifte auf den Stifträdern bestimmt. zusätzlich kann man die Stiftträder in unterschiedliche Ausgangspositionen stellen, was aber keine zusätzliche Sicherheit bringt, denn dieser Effekt wäre durch andere Stiftanordnung ebenso erzielbar.
  - Gewichtung der Schieberegister-Ausgänge a_1-a_6
    Jeder Schieberegister-Ausgang kann mit einer Zahl von 1 bis 16 gewichtet werden. Als Beschränkung gilt aber aus Realisierungsgründen, daß die Summe der Gewichte 40 nicht übersteigen darf.
  - Länge der Schieberegister n_1-n_6
    Es gibt fertige Schieberegister mit den Längen 29, 31, 37, 41, 43 und 47, die untereinander austauschbar sind. Die Längen sind Primzahlen, um bei der Kombination am Ausgang möglichst lange Perioden zu erreichen. Das Vertauschen der Schieberegister ist allerdings nichts anderes, als eine Umstellung der Gewichtungen und somit eigentlich überflüssig. Es trägt nicht dazu bei, die Verschlüsselung sicherer zu machen.
- Der äußere (Ausgangs-)Schlüssel
  - Startschritt
    Der Startschritt bestimmt die Anzahl der Codierungsschritte, die ausgeführt werden, bevor mit der Übertragung der eigentlichen Nachricht begonnen wird.
  - Relativlage
    Die Relativlage ist lediglich eine fest eingestellte Verschiebung des Primäralphabets zum Sekundäralphabet und trägt zur Sicherheit des Codes nichts bei. Bestenfalls kann sie als Verschleierung gelten.

Mechanische Realisierung

Das beschriebene kryptographische Prinzip ist in einem Kästchen realisiert, das wir erst von außen betrachten wollen

Black-Box-Betrachtung

Geht man davon aus, daß der korrekte Schlüssel bereits eingestellt ist, so kann man das Chiffriergerät als geschlossenes Kästchen betrachten, und sein Verhalten bzw. seine Bedienung beschreiben.

Von außen sind ein Buchstabenring und eine Buchstabenscheibe sichtbar. Auf dem Ring wird die Relativlage eingestellt und der Primärbuchstabe gesucht, auf der Scheibe der Sekundärbuchstabe abgelesen. Beim Verschlüsseln ist das das Chiffrat, beim Entschlüsseln der Klartext.

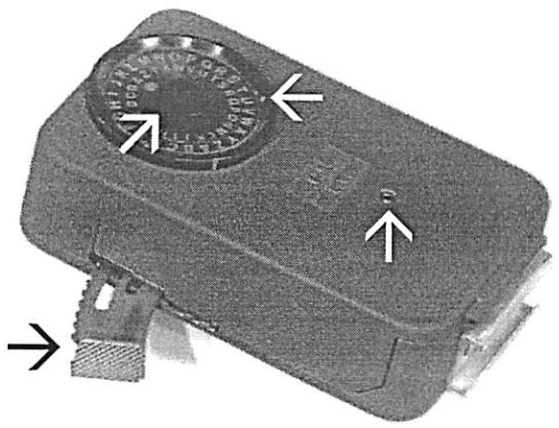


Abbildung 6: Die Bedienungselemente des CD-57
←: Buchstabenring
↗: Buchstabenscheibe
→: Antriebsbügel
↑: Schlitz für Hilfskurbel

Ein Hebel (der Antriebsbügel) dient dem Weiterschalten der Buchstabenscheibe zwischen den Zeichen des Primärtextes. Der Vorgang zum Ver- bzw. Entschlüsseln einer Nachricht lautet also: Den Hebel drücken und wieder loslassen, dann den Primärbuchstaben am Buchstabenring suchen und den Sekundärbuchstaben auf der Buchstabenscheibe ablesen. Den Hebel drücken...

Um den Startschritt einzustellen, liegt dem Gerät eine Hilfskurbel bei, damit man nicht hunderte male den Hebel betätigen muß. Die Kurbel wird in den entsprechenden Schlitz gesteckt, ein Zähler auf der rechten Gehäuseseite zeigt dabei die Schritte an.

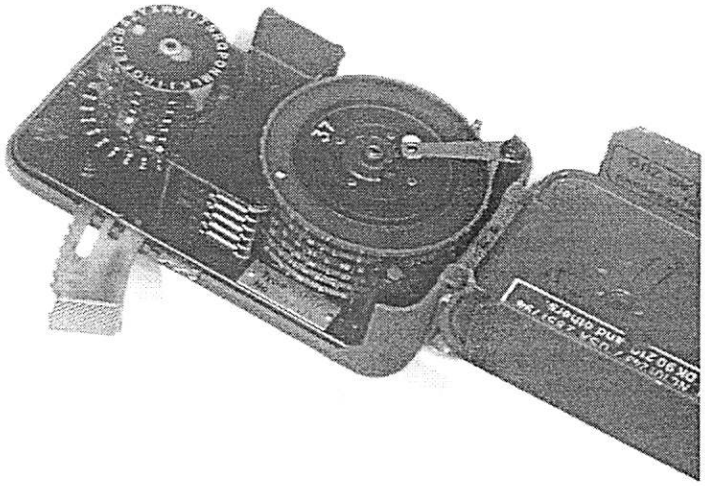


Abbildung 7: Ein Blick ins Innere

Schieberegister

Die Schieberegister bestehen aus Rädern, an deren Umfang umlegbare Stifte angebracht sind (siehe Abbildung 8). Einen Stift, der zum Radmittelpunkt zeigt, nennt man inaktiv, einen der nach außen zeigt, aktiv. Ein Abtasthebel (siehe Abbildung 9) wird durch Federkraft in Richtung des Stiftrades gedrückt und ermittelt, ob an der Stelle, die als « Ausgang » definiert ist, ein aktiver Stift vorhanden ist.

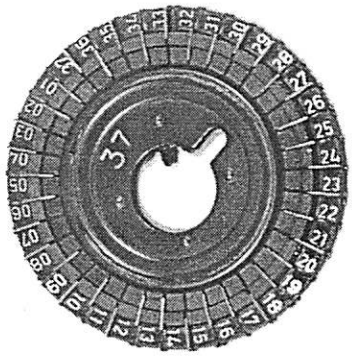


Abbildung 8: Stiftrad mit 37 Teilungen

In der Mitte der Stifträder dreht sich ein Vorschubkreuz, das bei jedem Schritt eine Viertelumdrehung weitergedreht wird. Dieses Kreuz greift in die Antriebszahnräder der Stifträder ein. Jedes Stiftrad hat eine eigene Übersetzung, die es bei jedem Schritt genau um einen Winkel von 360° / Teilungszahl weiterbewegt. Dadurch liegt der nächste Stift vor dem Abtasthebel.

Ausgangsgewichtung und Summierung

Mechanisch relativ aufwendig ist die Gewichtung der Schieberegister-Ausgänge. Die Summierung und Modulo-Bildung der gewichteten Ausgänge und des Primärtextes (Klartext oder Chiffrat) erfolgt durch Drehung der Buchstabenscheibe (siehe Abbildung 9). Diese Buchstabenscheibe sitzt auf einer Achse, die durch Federkraft angetrieben wird. Außerdem sind auf dieser Achse sechs Anschläge montiert, für jedes Stiftrad einer. Diese Anschläge geben an, wie weit sich die Buchstabenscheibe im Falle eines aktivierten Stiftes drehen kann, stellen also die Gewichtung dar. Bei einem inaktiven Stift löst der Abtasthebel eine Arretierung beim entsprechenden Anschlag aus, so daß sich die Buchstabenscheibe nicht weiterdrehen kann. Bei einem ativen Stift kann sich die Buchstabenscheibe bis zum Anschlag drehen, also um die Gewichtung des entsprechenden Stiftrades.

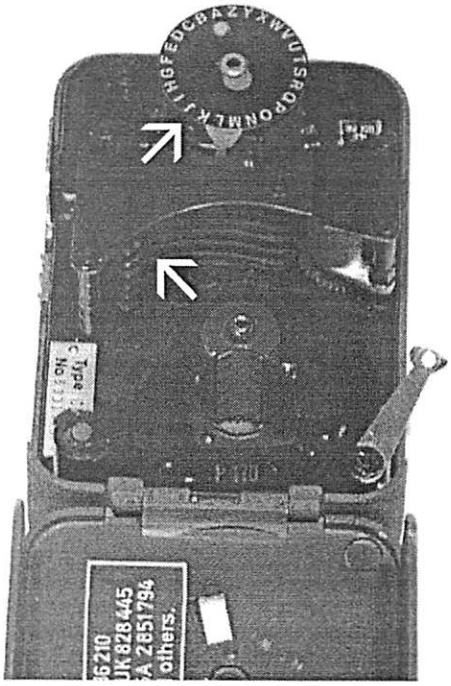


Abbildung 9: CD-57 ohne Stifträdern
↗: Die Buchstabenscheibe
↖: Die Abtasthebel

Daten

Abmessungen.....80 × 130 × 80 mm
Gewicht.....650g
Geschwindigkeit .....bis 40 Zeichen pro Minute
Max. Periode.....$29 \times 31 \times 37 \times 41 \times 43 \times 47 = 2.756.205.443$ (Nach so vielen Zeichen stehen die Stifträder wieder in der Ausgangslage.)
mögliche Schlüssel...$2^{29+31+37+41+43+47} = 2^{228} = 4{,}313591466744 \times 10^{68}$ (So viele Kombinationen der Stiftlagen i.e. Anfangszustände der Schieberegister sind möglich.)

Anfangszustand der Schieberegister (Stiftposition)

Um sicherzustellen, daß der Pseudo-Zufallszahlengenerator möglichst gute Zahlenfolgen liefert, schlägt die Crypto AG vor, daß zwischen 40 und 60% der Stifte aktiv sein sollen. Zusätzlich soll gewährleistet sein, daß nicht mehr als 5 Stifte hintereinander die gleiche Lage einnehmen. Das schränkt den Schlüsselvorrat von circa 4×10^{68} auf etwa 10^{15} Möglichkeiten ein. [CRYP63]

Gewichtung der Schieberegister-Ausgänge (Position der Anschläge)

Die Verschiebung zwischen dem Alphabet des Klartextes und dem des Chiffrats soll über die Schritte hinweg möglichst gleichmäßig verteilt sein. Wir suchen eine Gewichtzuteilung, die diese Anforderung erfüllt.

Jeder Schieberegister-Ausgang kann mit einem Gewicht von 1 bis 16 belegt werden. Die Summe der Gewichte darf jedoch 40 nicht überschreiten. Eine gute Belegung wäre z.B.:

Platz	Gewicht
1	1
2	2
3	4
4	7
5	8
6	10

Tabelle 1: Eine gute Gewichtsbelegung

Für diese Belegung wollen wir die resultierende Häufigkeitsverteilung für die möglichen Verschiebungen von 0 bis 25 überprüfen, wobei durch die Modulo-26 Division 26 wieder als 0, 27 wieder als 1 usw. zu betrachten ist. Wir überlegen zuerst, welche Verschiebung bei welcher Kombination der Schieberegister-Ausgänge zustande kommt:

aktive Stifte	Verschiebung	aktive Stifte	Verschiebung	aktive Stifte	Verschiebung	aktive Stifte	Verschiebung
000000	0	010000	8	100000	10	110000	18
000001	1	010001	9	100001	11	110001	19
000010	2	010010	10	100010	12	110010	20
000011	3	010011	12	100011	13	110011	22
000100	4	010100	15	100100	14	110100	25
000101	5	010101	11	100101	15	110101	21
000110	6	010110	13	100110	16	110110	23
000111	7	010111	16	100111	17	110111	26 = 0
001000	7	011000	14	101000	17	111000	27 = 1
001001	8	011001	17	101001	18	111001	27 = 1
001010	9	011010	19	101010	19	111010	29 = 3
001011	11	011011	15	101011	21	111011	25
001100	10	011100	18	101100	20	111100	28 = 2
001101	12	011101	20	101101	22	111101	30 = 4
001110	13	011110	21	101110	23	111110	31 = 5
001111	14	011111	22	101111	24	111111	32 = 6

Tabelle 2: Verschiebungen in Abhängigkeit von den Schieberegister-Ausgängen

Jetzt können wir ein Histogramm der möglichen Verschiebungen zeichnen, das uns die Häufigkeitsverteilung anzeigt:

Verschiebung	0	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
Häufigkeit	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	2	3	3	3	3	3	3	2	2	2

Tabelle 3: Häufigkeitsverteilung bei der gewählten Gewichtsbelegung

Eine exakt gleichförmige Häufigkeitsverteilung ist unmöglich, denn dann müßte jede Verschiebung genau 64 / 25 = 2,56 mal vorkommen.

Softwaremodell

Das C-Programm « CD-57.c » überprüft die Korrektheit der vorangegangenen Analyse. Es erzeugt aus einem Primärtext einen Sekundärtext, welcher dann mit dem vom CD-57 erzeugten Chiffrat verglichen werden kann.

Quelltext « CD-57.c »

```
/*********************************************************************
* CD-57.c
* Michael Topf, 17. April 1997
*--------------------------------------------------------------------
* Simulation des Taschenchiffriergeraetes CD-57
*********************************************************************/

#include <stdlib.h>
#include <stdio.h>

#define STIFTRAEDER 6 /* Anzahl der Stiftraeder */
#define MAXTEILUNG 47 /* Maximale Stiftanzahl eines Stiftrades */

int stiftraederTeilung[STIFTRAEDER]; /* Anzahl der Stifte */
int stifte[STIFTRAEDER][MAXTEILUNG]; /* Stellung der Stifte */
int stellung[STIFTRAEDER];           /* Stellung der Stiftraeder */
int anschlaege[STIFTRAEDER];         /* Stellung der Anschlaege */
int relativlage;                     /* Stellung des feststehenden
                                        Buchstabenringes */

void SchluesselLesen(char *dateiname) {
    FILE *schluessel;
    int stiftrad;
    int stift;
    char zeichen;
    int korrektur;

    schluessel = fopen(dateiname, "r");
    if (!schluessel) {
        perror("Fehler beim Oeffnen des Schluessels");
        exit (-1);
    }
    /* Lesen der Auswahl und Anordnung der Stiftraeder und der
    Stellung der Stifte */
    for (stiftrad = 0; stiftrad < STIFTRAEDER; stiftrad++) {
        fscanf(schluessel, "%d", &(stiftraederTeilung[stiftrad]));
        for (stift = 0; stift < stiftraederTeilung[stiftrad]; stift++)
            stifte[stiftrad][stift] = (fgetc(schluessel) == '+');
    }
    /* Lesen der Anschlagpositionen */
    for (stiftrad = 0; stiftrad < STIFTRAEDER; stiftrad++)
        fscanf(schluessel, "%d", &(anschlaege[stiftrad]));
    /* Lesen der Stellung der Stiftraeder */
    for (stiftrad = 0; stiftrad < STIFTRAEDER; stiftrad++) {
        fscanf(schluessel, "%d", &(stellung[stiftrad]));
        /* Da die Bezugslinie nicht mit den Abtastlinie zusammen-
        faellt, muss diese Verschiebung beruecksichtigt werden.
        "korrektur" ist die Nummer jenes Stiftes, der abgetastet
        wird, wenn sich die Stiftscheibe in Stellung 1 ("A") be-
        findet. */
        switch (stiftraederTeilung[stiftrad]) {
        case 29: korrektur =  9; break;
        case 31: korrektur =  9; break;
        case 37: korrektur = 11; break;
        case 41: korrektur = 12; break;
        case 43: korrektur = 12; break;
        case 47: korrektur = 14; break;
        default:
            printf("Stiftraederteilung %d unbekannt.\n",
                   stiftraederTeilung[stiftrad]);
            exit (-1);
        }
        stellung[stiftrad] += korrektur - 2;
    }
    /* Lesen der Relativlage des feststehenden Buchstabenringes */
    fscanf(schluessel, "%1s", &zeichen);
    relativlage = (int)toupper(zeichen) - 'A';

    fclose(schluessel);
}

int Codieren(int buchstabe) {
```

```
    int stiftrad;
    int umstellung;

    umstellung = 0;
    for (stiftrad = 0; stiftrad < STIFTRAEDER; stiftrad++) {
        if (stifte[stiftrad][stellung[stiftrad]])
            umstellung += anschlaege[stiftrad];
        stellung[stiftrad] = (stellung[stiftrad] + 1) %
                             stiftraederTeilung[stiftrad];
    }
    return (umstellung - toupper(buchstabe) + relativlage + 'A' + 26)
           % 26 + 'A';
}

void main (int argc, char *argv[]) {
    FILE *primaer, *sekundaer;
    int buchstabe;

    if (argc != 4) {
        printf("korrekter Aufruf: CD-57 <schluesseldatei> " \
               "<primaertextdatei> <sekundaertextdatei>\n");
        exit (-1);
    }

    SchluesselLesen(argv[1]);

    /* Dateien oeffnen */
    primaer = fopen(argv[2], "r");
    if (!primaer) {
        perror("Fehler beim Oeffnen des Primaertextes");
        exit (-1);
    }
    sekundaer = fopen(argv[3], "w");
    if (!sekundaer) {
        perror("Fehler beim Oeffnen des Sekundaertextes");
        exit (-1);
    }

    /* Verschluesseln / Entschluesseln */
    /* Laut Bedienungsanleitung wird vor dem eigentlichen Codieren
    einmal der Antriebsbuegel betaetigt */
    Codieren('A');
    buchstabe = fgetc(primaer);
    while (!feof(primaer)) {
        buchstabe = toupper(buchstabe);
        if (ferror(primaer)) {
            perror("Fehler beim Lesen des Primaertextes");
            exit (-1);
        }
        if ((buchstabe >= 'A') && (buchstabe <= 'Z'))
            buchstabe = Codieren(buchstabe);
        fputc(buchstabe, sekundaer);
        if (ferror(sekundaer)) {
            perror("Fehler beim Schreiben des Sekundaertextes");
            exit (-1);
        }
        buchstabe = fgetc(primaer);
    }
    fclose (primaer);
    fclose (sekundaer);
    exit (0);
}
```

Beispiel

Schlüsseleinstellungen « Schluessel.txt »

```
31+++--+-+-+++++-+--++++++++--
47+-++++-+++-+--+-++++-+++-+++-+++-+++++++++----+
41-+-+--++-+++-+----++++---+--+-++-+++-+-+-
43-+-+--+--+--+---+++-+--+--+-+--+++-+----++-
29+---++----+--++---+--+--+-+--
37--++--++-+-+--+--+--+-+++-+-+++-+--+-+
1 2 4 7 8 10
1 1 1 1 1 1
K
```

Teilungszahl und Stiftstellung des ersten Stiftrades
Teilungszahl und Stiftstellung des zweiten Stiftrades
Teilungszahl und Stiftstellung des dritten Stiftrades
Teilungszahl und Stiftstellung des vierten Stiftrades
Teilungszahl und Stiftstellung des fünften Stiftrades
Teilungszahl und Stiftstellung des sechsten Stiftrades
Position der Anschläge
Ausgangsstellung der Stifträder (1 = A)
Relativstellung des feststehenden Buchstabenringes

Primärtext « Klartext.txt »

```
Dieses Geraet ist fuer solche Anwendungsfaelle zu empfehlen, wo Kleinheit die Hauptforderung
darstellt und wo auf gedruckte Meldungen verzichtet werden kann.
```

Programmaufruf

```
CD-57 Schluessel.txt Klartext.txt Geheimtext.txt
```

Sekundärtext « Geheimtext.txt »

```
ZQHFYK ZLEIJJ WYY XEZK GEUUOW IZVZPTRUZIWRZODX WX ZGXXSBDNG, AF EKIPIYXCV VKA UAUGJQQITXXLGL
FLDXUTRZF HKL PX RHO YNBFUHRGN KLGWAQTIS XHQWEOREXW WAWAED PAMP.
```

Dieses Ergebnis stimmt mit dem vom CD-57 generierten Chiffrat überein.

Abbildungsverzeichnis

Tabellenverzeichnis

Quellenverzeichnis

[ANDE96] Andersson, Torbjørn: Toby's Cryptopage, The HAGELIN cryptographer CX-52; http://hem.passagen.se/tan01/CX52.HTM; Visby, Schweden; 1997

[CRYP63] Crypto AG: Taschenchiffriergerät CD-57, Techn. Beschreibung; Zug, Schweiz; 1963

[CRYP97] Crypto AG: Welcome to CRYPTO AG; http://www.crypto.ch/; Zug, Schweiz; 1997

[IACR95] International Association for Cryptologic Research: The Hagelin M-209-B Rotor Machine; http://www.iacr.org/m209/; Albuquerque, New Mexico, USA; 1995

[MORR78] Morris, Robert: The Hagelin Ciper Machine (M-209): Reconstruction of the Internal Settings; in: Deavours, Cipher; Cryptology, Yesterday, Today and Tomorrow; Seite 201; Artech House; Norwood, Massachusetts, USA; 1987

[NMMA97] National Maritime Museum Association: CSP-1500; http://www.maritime.org/csp1500.htm; USA; 1997

[SPIE96] DER SPIEGEL 36/96; Seite 206; Hamburg, Deutschland; 1996