Softwarepraktikum: Enigma

Martin Steffen

Sommersemester 2003

Abschnitt I

Kryptographische Angriffe

Inhalt: die Achillesfersen der Enigma · Streifenmethode · Schlüsselverteilung und 2 Indikatorsysteme · Rejewki-Angriff für die Spruchschlüssel · Angriff über die Zyklenstruktur · Females · Zygalksi-Roste · die polische Bombe · die Britische Bombe und das Diagmonalboard

Literatur: Material über die Angriffe auf die Enigma findet sich in [DK85, Kapitel III], ein wenig auch in [Bau91]. Die Streifenmethode ist detailliert beschrieben in [Dea80].

Die zweite Attacke ist oft beschrieben worden, z.B. von einem ihrer ursprünglichen

Entdecker, Marian Rejewski, in [Rej89]. Einiges an Material auch in [Bau91].

The Code&Ciphers-Seite ist auch sehr hilfreich, wenn auch manchmal mit Fehlern behaftet.

Angriffsmöglichkeiten

- inhärente Schwächen der Bauart: Achillesferse: bei gegebenem Zustand: Substitution ist
  - selbstinvers
  - fixpunktfrei: kein Buchstabe wird auch sich selbst abgebildet
- Schwächen der "Kommunikationsprotokolle"/Schlüsselübermittlung
- (individuelle und systematische) Dummheiten und Schlampereien (Schlüsselauswahl, parallele Netze)
- Kriegshandlungen (Spionage, erbeutete Maschinen)
- Unterschätzung des Gegners

Angriffe

- Unterschieden nach Enigmavariante (mit oder ohne Steckerbrett, Steckerbrett mit nur wenigen Verbindungen)
- was ist gegeben?
  - z.B. bekannter/wahrscheinlicher Klartext?
  - eine Nachricht, viele Nachrichten
- was will man bestimmen?
  - Walzenstartposition
  - Grundstellung
- Angriff über das Indikatorsystem

Streifenmethode

- einfacher Angriff
- *methode de bâton*, *cliques on the rods*, *Isomorphiemethode*
- Annahmen
  - kein Steckerbrett!
  - bekannter Klartext ("known plaintext attack"), Klartext-Geheimtext-Kompromittierung
  - bekannter Walzenvorrat und -verdrahtung
- Ziel: Bestimmung der Walzenlage
- Ausnutzung von: Spezifika der Enigma: Fixpunktfreiheit und Selbstinversität lassen Rückschlüsse zu.

Streifenmethode: Verschlüsselungsgleichung

- Verschlüsselungsgleichung (c = Schlüsseltext, p = Klartext, R_i Substitutionen der einzelnen Walzen,[1] R = Umkehrwalze)

$$c = pR_0R_1 \dots R_nRR_n^{-1} \dots R_1^{-1}R_0^{-1} \tag{1}$$

- Bestimmung der Walze R_0:

$$cR_0 = (pR_0)(R_1 \dots R_nRR_n^{-1} \dots R_1^{-1}) \tag{2}$$

Annahme: bei der Verschlüsselung von p nach c ändern sich $R_1 \dots R_n$ nicht $\Rightarrow$

$$c' = p'R_1 \dots R_nRR_n^{-1} \dots R_1^{-1} \tag{3}$$

ist monoalphabetisch

[1] die R_i sind natürlich auch vom momentanen Enigma-Zustand abhängig und schalten sich mit jedem Buchstaben fort.

- Eigenschaften von $R_1 \dots R_n R R_n^{-1} \dots R_1^{-1}$
  - Permutation, keine fixpunkte, selbstinvers!

- Ausschlußsverfahren: für alle Walzen und alle Anfangspositionen: pR_0 und cR_0: isomorph? d.h.

  Verschlüssele c und r und teste, ob die Ergebnisse cR_0 und pR_0 über eine fixpunktfreie, selbstinverse Permutation zusammenhängen oder nicht

- Streifenmethode: die Tabellen wurden auf Streifen geschrieben, die manuell gegeneinander verschoben wurden.

Angriff über das Indikatorsystem

- die "berühmtesten" und wertvollsten Angriffe: über das Indikatorsystem
- fataler Fehler im Verfahren der Schlüsselverteilung
- "Hilfsmittel": Permutationstheorie, erste elektromechanische Computer
- Ursprung: polnische Mathematiker vor dem Krieg (Marian Rejewski, Jerzy Różycki, Henryk Zygalski)[2], Wissenstransfer nach Bletchley Park
- Enigma mit Steckerbrett
- Ziel: Bestimmung des Nachrichtenschlüssels (und damit Entschlüsselung), zunächst aber: Bestimmung des Klartext-Indikators, d.h. Bestimmung der Startstellung der Rotoren

[2] vielleicht mehrfach entdeckt, wie die Streifenmethode auch.

- gegeben: Walzenverdrahtung, allgemeines Protokoll, viele Nachrichten, Vermutungen über wahrscheinliche Startpositionen/Schlüssel

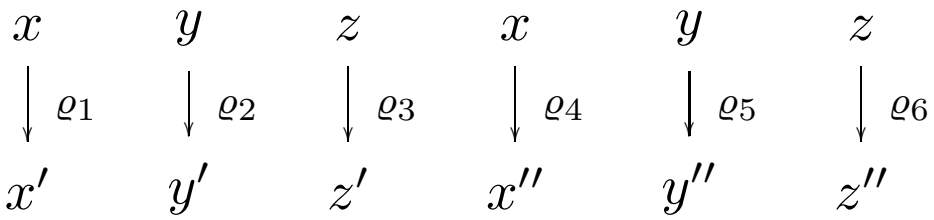
Zustand der Engima und Schlsselbermittlung

- zur Kommunikation: Sender und Empfänger im selben Anfangszustand
- Zustand:
  - Walzenlage = Auswahl und Anordnung der Walzen
  - Ringstellung = relat. position Walzenkern vs. Alphabetring
  - Steckerbrett
  - Startposition, sichtbar im oberen Fenster
- Anfangszustand konzeptionell zweigeteilt:
  - individuell pro Nachchricht festgelegt (durch Sender): Startposition
  - vorher festgelegt (pro 24h zum Beispiel)

Rejewski-Angriff

- gegeben 60–100 Nachrichten
- Geheimtext-Geheimtextkompromittierung
- Angriffspunkt:
  - zweimalige verschlüsselte bermittlung der selbstgewählten Rotorpositionen (= Nachrichtenschlüssel)

  $\Rightarrow$ Ausnutzen der festen Beziehungen der ersten Buchstaben



- fester Zusammenhang: für alle Nachrichten, wenn einmal $x' = \texttt{r}$ und $x'' = \texttt{f}$, konstant in allen Vorspannen.

$\Rightarrow$ fasse den festen Zusammenhang von $x' \mapsto x''$ ... als Abbildung auf

$\Rightarrow$ ernte genügend Nachrichten/Vorspänne zur Bestimmung der drei 3 Abbildungen π_0, π_1, π_2

- Es gilt

$$\pi_0 = \varrho_0^{-1}\varrho_3 \qquad \pi_1 = \varrho_1^{-1}\varrho_4 \qquad \pi_2 = \varrho_2^{-1}\varrho_5 \tag{4}$$

Beispiel 1. *Folgende Nachrichtenpräfixe seien gegeben:*

```
gab hfz
gcd hpq
acf jpe
....
```

Nach Auswertung dieser drei 6Tupel bekommt man als Teil der Permutationen

$$\pi_0 = \{g \mapsto h, a \mapsto j\} \quad \pi_1 = \{a \mapsto f, c \mapsto p\} \quad \pi_2 = \{b \mapsto f, d \mapsto q, f \mapsto e\}$$

- Eigenschaften von ϱ_i: Transpositionen = nur Zyklen der Länge 2!
- wichtig: Zyklenschreibweise von Permutationen
- Bedeutung: Zyklenstruktur (Anzahl von Zyklen bestimmter Größe) ist "charakteristisch" für eine Permutation, inbesondere

  "Das Theorem das den 2. Weltkrieg gewann": π und $\varphi^{-1}\pi\varphi$ haben die selbe Zyklenstruktur

$\Rightarrow$ Informationen über die Enigma unabhängig vom Steckerbrett

Ernten der Permutationen als Zyklen

Beispiel 2. [Zyklen] *Gegeben sei folgende Anzahl an Nachrichten*

```
DMQ VBN
VON PUY
PUC FMQ
....
```

Vervollständigt, könnte dies folgende Permutationen in Zykelschreibweise ergeben

$$\begin{aligned}\pi_0 &= (\underline{DVPF}KXGZYO)(EIJMUNQCHT)(BL)(RW)(A)(S)\\ \pi_1 &= (\underline{B}LFQVE\underline{OUM})(HJPSWIZRN)(AXT)(CGY)(D)(K)\\ \pi_2 &= (ABVIKTJGF\underline{CQNY})(DUZREHLXWPSMO)\end{aligned}$$

- *Beobachtung: Anzahl der Zyklen gegebener Länge*[3]
  - π_0*: 2 der Länge 10, 2 der Länge 2, 2 der Länge 1*
  - π_1*: 2 der Länge 9, 2 der Länge 3, 2 der Länge 1*
  - π_2*: 2 der Länge 13*

[3] Klarerweise: Wenn man die Zyklenschreibweise auf eine beliebige Permutation anwendet, muß nicht notwendigerweise zu den Beobachtunge wie hier führen, daß die Anzahl der Zyklen gleicher Länge immer gerade ist. Dies (konstruierte) Beispiel ist so gewählt, daß es die Charakteristika der Enigma-π's aufweist.

Ein weiteres Theorem was im 2. Weltkrieg hilfreich war ...

Lemma 1. *Gegeben: Permutationen φ und ψ von ungerader Anzahl an Transpositionen.*[4]

Sei $\alpha = \varphi \circ \psi$.

1. *Anzahl der Zyklen gegebener Länge in α ist gerade*

2. *(a, b) = Zykel von φ oder $\psi \Rightarrow a$ und b kommen in α in verschiedenen Zyklen gleicher Länge vor*

3. *kommen zwei Buchstaben unterschiedlicher Zykel in α von der selben Transposition in φ (resp. ψ) $\Rightarrow$ auch der Buchstabe links von a und rechts von b stammen aus einer Transposition*

[4] Transposition = Permutation bei der alle Zyklen der Länge 2 sind. Insbesondere: $\pi = \pi^{-1}$. Hier: ungerade Anzahl $= 13 = 26/2$

Anwendung des Lemmas

Beispiel 3. [Wahrscheinliche Worte] *Fortsetzung von Beispiel 2.*

- *Analyse der Verkehrs ergibt gewisse Häufungen, z.B. nehmen wir an, es träten folgende Tupel auffallend oft auf:*

  1. *SUG SMF*
  2. *SJM SPO*
  3. *SYX SCW*

- *Beachte: alle 3 6tette realisieren (natürlich) ein Teil der Permuation in Zykelschreibweise aus Beispiel 2, insbesondere* $\mathtt{S} \mapsto \mathtt{S}$ *als 1erzykel.*

- *Annahme: Verschlüsseler wählte* AAA[5]

[5] oder eine weitere beliebte Startposition wie BBB ..., QWE .... Allerdings, bei genauerem Hinsehen: in allen drei Chiffretext-Verdachstfällen ist von allen Klartexttriplets mit dreifach-gleichem Buchstaben nur AAA möglich! Der Chiffretextbuchstabe S und der Klartextbuchstabe A bilden einen Zweierzyklus in sowohl ϱ_0 als auch ϱ_3. S ist in π_0 ein Einerzyklus, und der einzige zweite Einerzyklus in π_0 ist der von A.

- *Wende Punkt 2 des Lemmas 1 an*

- *Für alle drei obigen Sechstupel: in allen drei Fällen:* $\varrho_0, \varrho_3 : A \mapsto S$ *(konsistent mit* π_0 *mit dem Lemma).*

  1. *betrachte* U *(d.h.* ϱ_1 *als Teil von* $\pi_1 = \varrho_0^{-1}\varrho_3$*).* $\varrho_1 : \mathtt{A} \mapsto \mathtt{U}$*. Widerspruch:* A *und* U *sind in verschiedenen Zyklen in* π_0 *(weitere Widersprüche ergeben sich für* M *und* F*, nicht aber für* G*)*
  2. $\varrho_1 : \mathtt{A} \mapsto \mathtt{J}$
  3. $\varrho_1 : \mathtt{A} \mapsto \mathtt{Y}$*: ok,* A *und* Y *kommen in zwei Zyklen passender Länge (=3) vor. die anderen* ϱ_2*,* ϱ_4*,* ϱ_5 *passen auch. D.h. Fall drei ist mglich.*

Beispiel 4. *Das folgende Beispiel ist ausu [DK85, Seite 108ff]. Es ist ein wenig komplexer als das vorige hier auf den Folien.*

```
(DP) (SY) (ABQHZUIWOXL) (MNJRVTGCKEF)    : pi0, 2,2 11,11
(AJV) (HNY) (BFZSWGCIMO) (DKTLRXEQUP)    : pi1, 3,3,10,10
(AXJBLREONDZCS) (IUYHWQVMFTPGK)          : pi2  13,13
```

Verdachtsfall (mit gehäuftem Auftreten im Chiffrat) `YSG SWK`

1. betrachte π_0*: eine Teil* $\mathtt{Y} \mapsto \mathtt{S}$ *kommen in* π_0 *vor und natürlich auch im selben*

Zykel und zwar hintereinander. Das ist klar nach Definition. Glück haben wir insofern als daß der Zykel klein ist (von der Länge 2) und daß es nur noch einen weiteren Zykeln von dieser Länge gibt.

Das ist deswegen gut, weil uns das Theorem 1(2) bereits sehr einschränkt.

Wir wissen, Y *und* S *stammen aus dem selben Klartextbuchstaben* x*,* $(x\mathtt{Y})$ *und* $(x\mathtt{S})$ *sind sind 2 2erzyklen/Transpositionen aus* ϱ_0 *bzw.* ϱ_3*. D.h.,* x *kommt in einem* anderen 2er Zyklus *von* π_0 *vor als* Y *(und gleichfalls ein einem andere 2er Zyklus als* S*, aber das ergibt nichts neues). Damit gibt es 2 Kandidaten für* x*:* P *und* D

2. *Aus der Tatsache, daß das 6Tupel vermehrt auftrat, nehmen wir hypothetisch an, daß die Stellung eine dreifache Wiederholung darstellt, also nehmen wir an*

   PPP oder DDD

   Die dritte Permutation π_2 *zeigt, daß es nicht* PPP *sein kann da* P *im selben Zykel von* π_2 *vorkommt wie* Y *und* S*. Alternativ kann man* PPP *mittels* π_1 *ausschließen:* P *und* S *(bzw.* W*) kommen im selben Zyklus von* π_1 *vor, was nicht sein kann.*

3. *Nachdem wir nun (hypothetisch)* DDD *bestimmt haben, was nun?*

Aus dem Überlagern der Zyklen kann man anfangen, die eigentlichen Abbildungen zu ernten. Es wird ein Zyklus aus gewählt und der (oder die) anderen passender Länge in umgekehrter Richtung untereinandergeschrieben.

```
      pi0 |    pi1                pi2

     (YS) | (SWGCIMOBFZ) |    (GKIUYHWQVMFTP)
-----     |              |
     (DP) | (DPUQEXRLTK) |   (DNOERLBJXASCZ)
     (PD) | (KDPUQEXRLT) |   (ZDNOERLBJXASC)
```

Liest man nun die Spalten,[6] *bekommt man (Teile) der Abbildung an der man eigentlich interessiert ist, nämlich die ϱ_i als Faktoren der π_j.*

Von allen möglichen Verschiebungen betrachtet man gerade diese beiden (jeweils), weil es uns gelungen ist, bereits den Buchstaben `D` als Schlüssel fest zu bestimmen.

Wir brauchen für jeden der Zyklen 2 Verschiebungen, für ϱ_i und ϱ_{i+3}.

Im der ersten Spalte ist es egal, es sind ohnehin nur zwei möglich, D.h., man bekommt daraus für ϱ_0 und ϱ_3.

[6] Die Zeilen hängen nicht zusammen, "Zeile 1" hat keine Bedeutung.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
                    P     D : rho0
                    D     P : rho3
```

Für ϱ_1 und ϱ_4, die kombiniert in π_1 eine Zykellänge von 10 haben, gibt es damit prinzipiell 10 Verschiebungen. Durch die Buchtstaben `SW` *zu Beginn, die selbstverständlich Teil der π_1 Zyklus sein müssen und deswegen hintereinander stehen, ist die Positionen von* `D` *für die zwei Verschiebungen festgelegt.*

Für die verbleibenden 2 Paare von Abbildungen bekommt man:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
--------------------------
 LQ  TU E   X R   D   P  K : rho1

 RU  LP Q   E X   K   D  T : rho4
```

und

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

```
------------------------
     SDLO N A  ZJ  CEXB R
     AZRN D X  CB  SOJL E
```

In Zykelschreibweise (was natürlich auch direkt aus den zwei verschobenen Zyklenpaaren von oben hervorgeht):

```
(YD)(SP)  : rho0
(YP)(SD)  : rho3

(SD)(WP)(GU)(CQ)(IE)(MX)(OR)(BL)(FT)(ZK)   : rho1
(SK)(WD)(GP)(CU)(IQ)(ME)(OX)(BR)(FL)(ZT)   : rho4

(GD)(KN)(IO)(UE)(YR)(HL)(WB)(QJ)(VX)(MA)(FS)(TC)(PZ)  : rho2
(GZ)(KD)(IN)(UO)(YE)(HR)(WL)(QB)(VJ)(MX)(FA)(TS)(PC)  : rho5
```

4. *Wie geht es nun weiter? Wir haben natürlich von den Abbildungen ϱ_i nur einen Teil geerntet, speziell ϱ_0 und ϱ_3 sind mit zwei Werten noch sehr lückenhaft vertreten. Wir können natürlich mit den bereits festen Informationen auf andere abgefangene Indikatoren anwenden. Z.B. liefert*

UQJ IUP

als Position

?CC

D.h., die Zerlegung von π_1 und π_2 ist konsistent mit den bisherigen Annahmen, die Zerlegung von π_0 ist mit Werten noch zu unvollständig, aber zumindest ist auch dieser Wert konsistent. Die Buchstaben `U` und `I` für π_0 kommen diesmal in einem der langen Zyklen vor —die zwei 2er-Zyklen sind auch bereits ausgewertet— und zusätzlich taucht `C` in dem langen Partnerzyklus auf. Wir raten damit das Fragezeichen zu `C`, und bekommen

```
UIWOXLABQHZ

CGTVRJNMFEK   :rho_0
KCGTVRJNMFE   :rho_3
```

Wenn wir weiter so raten, kriegen wir sicher die Zerlegung raus. Was haben wir damit gewonnen?

- *Wir kennen das Steckerbrett nicht.*
  - *nicht so schlimm, kann man raten*
- *Walzenlage: bei 60 Möglichkeiten kann man es zur not ausprobieren*
- *Wir kennen die Position des Alphabetrings nicht: d.h., das Wissen um die Klartext-Indikatorbuchstaben* bringt nichts[7]

[7] Beachte: wir haben die Klartextindikatoren Entschlüsselt *ohne* Kenntnis der Walzenverdrahtung!

Bestimmung der Walzenanorndung

- zumindest Identität der Rechten Walze bekannt[8]
- Annahme: nur 6 Stecker, d.h. nur 12 Buchstaben vom Steckerbrett betroffen
- $6 * 26 * 26$ für Positionen I und II

[8] manchmal mehr

Übersicht: Entschlüsselung bei fester Grundstellung

Wir haben nicht alle Angriffe gemacht, auch sind wir nicht direkt drauf eingegnagen, daß man mit dem Klartext-Spruchschlüssel gar nicht viel anfangen kann, bzw. wie es dann weiter geht. Deswegen hier die Üersicht, in welcher Reihenfolge die Bestanddeile der Enigma in Historische Folge entzifffert wurden.

1. Entschlüsselung der Klartext-Spruchschlüssel

   - geg: Verschlüsselungssystem, Indikatoren des gesamten Verkehrs[9].
   - Ausnutzung:
     - Eigenschaften der Enigmapermutationen,
     - Verdoppelung der Spruchschlüssels,
     - Annahmen über beliebte Buchstabenkombinationen

2. (innere Verdrahtung der Rotoren, (Różicki), Eingangspermutation)[10]

[9] Nicht gebraucht: Verdrahtung, Walzenlage, Steckerbrett

[10] Das haben wir nicht besprochen. Zum beispiel wurden hier auspionierte Schlüsselunterlagen ausgenuzt. Die eingangspermutation würde per Intuition geraten.

3. Walzenlage + Kernposition (absolute Walzenposition) (d.h. Anfangszustand modulo Ringstellung und ohne Steckerbrett)

   - geg: wie unter 1, dazu Vorrat der Rotoren + Verdrahtung (nicht notwendig: Steckerbrett)
   - Ausnutzung:
     - Verdoppelung der Sprachschlüssel $\Rightarrow$ die π's
     - Invarianz der Zyklenstruktur vom Steckerbrett Katalog der charakteristischen Zyklen pro Walzenlagen und Kernposition[11]
   - Elekromechanische Hilfe: Cyclometer

4. (Ringstellung + Steckerbrett):[12]

   - Annahmen über wahrscheinliche Texte/Textanfänge.
   - "Vertauschte" Buchstaben in ansonstem vernünftigem Text $\Rightarrow$ Steckerbrett
   - Beachte: Ringstellung und Steckerbrett fest für den gesamten Verkehr $\Rightarrow$ ein entschlüsselter Text kompromittiert alle anderen

[11] Kernposition = "physikalische" Stellung der Rotorkerne. Die Ringstellung und die Startposition kann man natürlich natürlich über die π's nicht bestimmen.

[12] Auf das haben wir nicht besprochen

Variable Grundstellung

- Ab 15. September 1938
- Indikator mit Schlüssellänge 9
  - Grundstellung in Klartext
  - Doppelte, verschlüsselte Startposition wie zuvor
- zwei Methoden, beide mit females
- female: zweimal der selbe Buchstabe als Verschlüsselung des selben (unbekannten) Klartextbuchstabens aus dem Nachrichtenindikator
  - gibt ein winziges Bisschen an "characteristischer" Information preis:

  $\Rightarrow$ Zyklus der Länge 1 für die π_i/ Fixpunkt existiert bei der entsprechenen Enigma-Kernposition/Walzenlagen, festgelegt durch die ersten 3 Buchstaben des Indikators

- Problem: Grundposition im Klartext übertragen, aber Kernposition relativ zur Ringstellung!
- Variable Startposition: Verschieben der Females $\Rightarrow$ bei fester (unbekannter) Ringstellung: Muster von Females, verschoben gemäß den ersten 3 Buchstaben des Indikators/Startposition der Grundstellung

Zygalski-Roste

- Lochblattverfahren, auch Jeffrey-Sheets
- gegeben: Indikatoren eines Tages[13] mit ihren females (10–12 sind ausreichend)
- Ausnutzung: Wie bei der Bestimmung der Walzenlage/Kernposition beim Angriff mit fester Grundposition:
  - Verdoppelung der Schruchschlüssel $\Rightarrow$ Muster der Fixpunkte der π's
  - Invarianz der Zyklenstruktur unterm Streckerbrett
- Notwendig: anstelle eines Katalogs der charakt. Zyklenstruktur:
  - Katalog der charakteristischen Fixpunktstruktur: Existiert ein Fixpunkt bei gegebener
    * Walzenlage

[13] dazu natürlich das Verschlüsselungssystem, der Walzenvorrat und ihre Verdrahtung

    - ∗ Kernposition
  - Methode des schnellen Abgleichs mit den geg. Fixpunkten des Verkehrs, "Parallelverarbeitung", Hauptproblem: Herausrechnen des Offsets der unbekannten Ringstellung

- $26^3 * 6 = 10456$ Eintrage (Bits)[14]

- Verwendung der Existenz von females ⇒ unabhängig vom Steckerbrett,[15] ⇒ auch brauchbar mit 11 Steckverbindungen

[14] bei 3 Walzen zur Auswahl. Bei 5 sind es 10 mal soviel.

[15] Die Characteristic eine Stellung ist unabhängig vom Steckerbrett, d.h., die *Existenz* einer Fixpunktes/Einerzyklusses/Females bleibt erhalten.

Zygalski-Roste

- für jede Walzenlage und jede Kern-Grundstellung: existiert im Alphabet ein Fixpunkt, d.h., ist female moglich

- Aufgabe im Prinzip:
  - gegeben
    - das "Bitmuster" (Fixpunkt/kein Fixpunt)[16] für alle Walzenstellungen
    - aktuelles Bitmuster des Verkehrs, relativ zu Grundstellungen, aber für alle

  $\Rightarrow$ Mustervergleich, Eindimensinale Anordung möglich, aber unpraktikabel

- Anordnung in Lochblättern
  - Auspaltung nach Walzenlage $\Rightarrow$ 6 getrennte "Kataloge" = Lochkartensets
  - "Abspalten" des ersten Positionen $\Rightarrow$ 26 Blätter einer Binären Matrix der Größe 26*26

[16] Die Existenz eines Fixpunktes heißt noch nicht, daß im Verkehr ein female auftraucht, nur das es möglich ist.

  - Zum besseren Überlapp/Verschieben: Verdoppelung der Alphabete für den 2ten und 3ten Position

⇒ Lochblatt der Größe $51 * 51$, effektive Information natürlich dennoch $26 * 26$

  - Female als Loch in Karte, genauer gesagt (meist) 4 Löcher durch die Duplizierung[17]

- Vorgehen: für alle

  - 6 Walzenlagen
  - 26 Ringstellungen der ersten Position

  Tue folgendes

  - Wähle das Blatt gemäß der Walzenlagen und der Ringstellung
  - Finde eine 1-4 Female:
  - Bestimme die absolute Grundstellung der erster Walze (aus Klartext-Startposition und (angenommene) Ringstellung)

⇒ legt die Auswahl des 2te Blattes fest

  - Verschieben des Blattes gemaß der 2 verbleibenden Buchstaben der Grundstellung

[17] wahrscheinlichkeit für ein female: ca. 40%

Zygalski-Rost, 6 Buchstaben-Alphabet

```
   A B C D E F | A B C D E
-+------------+----------
A| 0   0 0   0 | 0   0 0
B|   0 0 0     |   0 0 0
C| 0           | 0
D|   0       0 |   0
E|         0 0 |         0
F| 0 0         | 0 0
-+------------+----------
A| 0   0 0   0 | 0   0 0
B|   0 0 0     |   0 0 0
C| 0           | 0
D|   0       0 |   0
E|         0 0 |         0
-+-----------=-+----------
```

Zygalski

```
Sheet: wheels 132
       left ring P
       left wheel set to A

. 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
A . . . O . O O . . . . . . O . . . . . . . O O . . O
B . O . . O . . . . O . . . . O . O . . . . O . . . .
C . O O O . . O . . . . . O . . . . O . O O O . . O .
D . O . . O O O . . . O O . . O O . . . O O . O . . .
E . . . O . . . O O . O . . O O . . O . . . O . . . .
F O . O . . . . O O . O . . . . O O . O O O O O O . .
G O . O . O O . . O . . . O O . . O . . . . . O . O .
H . . O . . . . . . . O O O O O . O O . . O O O O O O
I . O . O . . . O . . . O O O O . . O O O . . . O O .
J . . O . O O O . O O . O . . O . . O O . O . O O . O
K O O . O . O O . . O . . . O O . . . O . O O . . . .
L O . . . . . . . O O . O O . . O O . . . O . . . O . .
```

```
M . O . O . . . . O . O . . O . O O . O . . . O . . .
N O . . . O O O . . . O O . O . . . . . O O . . . . .
O O O . O . O . O O . . O . O O O . . . . . . . . . .
P . . . . . O O . O . O O . . . O . . . O . O . O . O
Q . . O . O . O O O O . . . O . . O O O . O . . . . O
R O O . . O . . O . . . O O O O O O . O O O O . . O O
S O . . O . O . . . . . . . . . O O O . . O O . . O O
T . . O . O . . . . O . . O . . O . O . . . . O . . .
U . . . . . O O O . O . . O O O O O . O . . . O . . .
V . . . O O . O O . . . O . . O . . . . . O O O O O O
W . . . O . . O O O O . . . O . . . . O . . . O O O .
X . . . . . O O O . O . . O O O . O O . O . . . . O .
Y O O O O . O O . . . . O . . . . O . . O O . . O . .
Z O . O O O . . O . . . . . O O . O . . . O O . O O O
```

277

Beispiel

```
bkr BWB RIG
eme SQS CQZ
ens VYY VWO
gvu RLG CLO
nna AGW UGC
oxw UPZ TEX
vyw WOI WNA
```

- Wähle Walzenlage, wähle Ringstellung (als Beispiel 132 und Q) für erste Walze $\Rightarrow$ erstes Blatt $\mathbf{Z}_{132}^{D}$
- das die Walzenlagen fest ist, sind nun Zettel aus $\mathrm{Z}_{132}^{?}$ ebenfalls fest.
  - Finde ein female an 1-4 Position: z.B.vyw WOI WNA
  - Wir testen: Walzenlagen + Ringstellung 1
  - Auswahl der Blattes: Ringstellung + Klartextbuchstabe 1 legt Blatt fest

  - Übernanderlegen

- 2 Females an erster Stelle: und `ens VYY VWO`

$\Rightarrow$ Übernanderlegen der Blätter 0 und 17[18], Verschieben der x und y-Achsen um die errechneten Differenzen

- verbleibende übereinanderliegende Löcher: Bislange kein Widerspruch.

- Fortsetzten der Prozedur mit weiteren Females, bis
  - kein gemeinsames Loch $\Rightarrow$ Widerspruch, d.h., Walzenlage verkehrt
  - genau ein Loch
    - $\Rightarrow$ (vermutlich) richtige Stellung gefunden

    $\Rightarrow$ Walzenlage klar, relative Walzenpositionen klar
    - Herausrechnnen der Ringstellung

[18] Oder 1 und 18 etc.

Literatur

[Bau91] Friedrich L. Bauer. *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Springer-Verlag, 1991.

[Dea80] C. A. Deavours. La methode des batons. *Cryptologia*, IV, October 1980.

[DK85] Cipher A. Deavours and Louis Kruh. *Machine Cryptography and Modern Cryptanalysis*. IPF. Artech House Books, 1985.

[Rej89] Marian Rejewski. Mathematical solution of the Enigma cipher. IPF, pages 310–327. Artech House Books, 1989. Translation of an article in Polish, 1979.