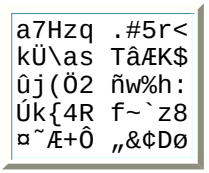
Kryptologie

Ansätze zur Kryptoanalyse von Rotor-Maschinen



Die Kryptoanalyse ist sehr komplex und von den Details der jeweiligen Maschine abhängig. Hier werden nur einige allgemeine Ansätze behandelt. Für eine ausführliche Darstellung sei auf das Buch von Deavours und Kruh im Literaturverzeichnis verwiesen.

Superimposition

… ist anwendbar, wenn mehrere Geheimtexte vorliegen, die mit dem gleichen Schlüssel erstellt wurden. Diese werden untereinander geschrieben. Dabei entstehen monoalphabetisch verschlüsselte Kolonnen.

In der Praxis wird dies durch den mit jeder Nachricht wechselnden Spruchschlüssel (= variabler Anfangszusatnd) verhindert. Aber auch dann treten bei hohem Nachrichtenaufkommen immer wieder Abschnitte in verschiedenen Nachrichten auf, die mit dem gleichem Schlüssel verschlüsselt wurden. Mit Zeichenkoinzidenz-Bestimmung werden solche Abschnitte zuverlässig erkannt.

Dieser Ansatz benötigt so weit keinen bekannten Klartext.

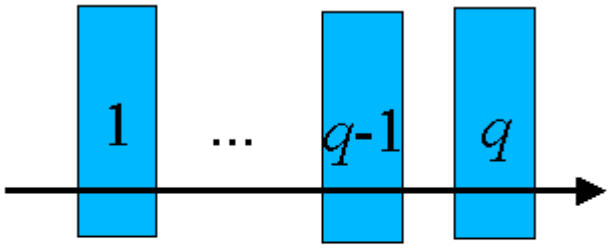
Erkennen eines schnellen Ausgangsrotors

Hier wird angenommen, dass die Menge der Rotoren, also der Walzenkorb, bekannt ist, aber nicht die verwendete Auswahl von Rotoren. Bekannter Klartext wird nicht benötigt.

Der Angriff ist durchführbar, wenn der Ausgangsrotor sich bei jedem Schritt um eine Position weiterdreht, die anderen Rotoren wesentlich seltener.

Die Rotoren seien von 1 (= Eingangsrotor) bis q (= Ausgangsrotor) nummeriert; in dieser Reihenfolge sollen sie auch durchquert werden.

Nun sei ein Abschnitt der Länge m gegeben, in dem nur der Rotor q bewegt wird. Die Substitution μ, die von den Rotoren 1 bis q-1 bewirkt wird, ist dann in diesem Abschnitt konstant. Die Verschlüsselung folgt, wenn die Indizes der Einfachheit halber in diesem Abschnitt als 1 bis m gewählt werden, dann dem Schema



$$a_i \xrightarrow[\mu]{} b_i \mapsto c_i$$

$$\begin{aligned}
a_1 &\to b_1 := \mu(a_1) &&\to \rho_q^{(z_1)}\mu(a_1) = c_1\\
a_2 &\to b_2 := \mu(a_2) &&\to \rho_q^{(z_1+1)}\mu(a_2) = c_2\\
&\dots \quad \dots && \dots\\
a_m &\to b_m := \mu(a_m) &&\to \rho_q^{(z_1+m-1)}\mu(a_m) = c_m
\end{aligned}$$

Somit ist $b = (b_1,\dots,b_m) \in \Sigma^m$ monoalphabetisches Bild von $(a_1,\dots,a_m)$. Es ist aber auch

$$\begin{aligned}
b_1 &= [\rho_q^{(z_1)}]^{-1}(c_1),\\
b_2 &= [\rho_q^{(z_1+1)}]^{-1}(c_2),\\
&\dots\\
b_m &= [\rho_q^{(z_1+m-1)}]^{-1}(c_m).
\end{aligned}$$

Damit lässt sich eine reduzierte Exhaustion für den Rotor q mit p Möglichkeiten und seine Anfangsstellung z_1 im betrachteten Abschnitt mit jeweils n Möglichkeiten durchführen.

- Bei falscher Wahl des Rotors oder seiner Anfangsstellung wird b wie ein zufälliger Text aussehen, also den Koinzidenzindex $\varphi(b) \approx 1/n$ haben.
- Bei richtiger Wahl hingegen ist b ein monoalphabetisch verschlüsselter sinnvoller Text, wird also den Koinzidenzindex $\varphi(b) \approx \kappa_M$ der Sprache M haben.

Damit ist der Ausgangsrotor und sein Zustand im betrachteten Abschnitt identifiziert. Der Aufwand hierzu bestand aus $n \cdot p$ Bestimmungen von Koinzidenzindizes von Texten der Länge m.

Bemerkungen

1. Die Methode wird in der Regel am Anfang eines Textes angewendet.
2. Falls im gewählten Abschnitt nicht alle anderen Rotoren still stehen, aber doch nur *ein* weiterer Rotor genau einmal die Position ändert, besteht b aus zwei verschiedenen monoalphabetischen Stücken. Auch dies ist in der Regel noch am Koinzidenzindex $\varphi(b)$ erkennbar.

Weiterführung des Angriffs

Sobald der schnelle Rotor identifiziert ist, kann man den durch ihn bewirkten Effekt wie eine Überverschlüsselung abstreifen. Der oben verwendetete »Zwischen-Geheimtext« $b_1, \ldots, b_m$ wird dadurch zu einem Geheimtext $c' \in \Sigma^r$ verlängert, der mit einer wesentlich einfacheren Maschine erstellt wurde.

Ist die Steuerlogik z. B. ein Zählwerk und der Text lang genug (etwa mindestens $\approx n^2$), so lassen sich sukzessiv weitere Rotoren erkennen und abstreifen.

Oder man versucht, die monoalphabetischen Stücke, aus denen c' zusammengesetzt ist, einzeln zu dechiffrieren. Das sind z. B. $[r/n]$ Stücke der Länge n und ein Reststück der Länge r mod n.

Angriff mit bekanntem Klartext

(oder mit wahrscheinlichem Wort)

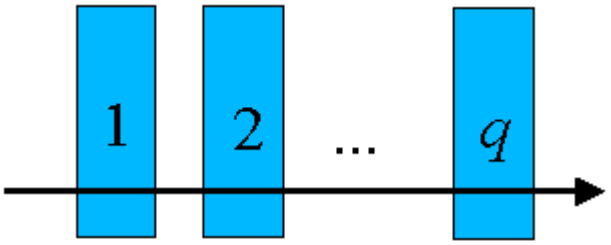
Erkennen eines schnellen Ausgangsrotors

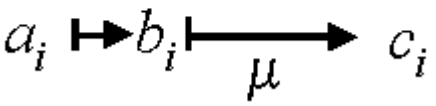
… ist damit wie oben, aber ohne Berechnung von Koinzidenzindizes, möglich: Man prüft, ob $b_1, \ldots, b_m$ dasselbe numerische Muster zeigt wie $a_1, \ldots, a_m$.

Die Angriffsmethode, einen Zwischenschritt einer Verschlüsselung von beiden Seiten aus zu betrachten, nennt man auch »Meet in the Middle«.

Erkennen eines schnellen *Ein*gangsrotors

Analog zu oben ist die Situation hier:





$$
\begin{aligned}
a_1 &\to b_1 := \rho_1^{(z_1)}(a_1) &&\to \mu(b_1) = c_1\\
a_2 &\to b_2 := \rho_1^{(z_1+1)}(a_2) &&\to \mu(b_2) = c_2\\
\ldots &\quad \ldots &&\quad \ldots\\
a_m &\to b_m := \rho_1^{(z_1+m-1)}(a_m) &&\to \mu(b_m) = c_m
\end{aligned}
$$

Damit ist $(b_1,\ldots,b_m)$ monoalphabetisches Bild von $(c_1,\ldots,c_m)$.

Also hat man nur alle p Rotoren mit jeweils allen n Anfangsstellungen durchzuprobieren, bis die

numerischen Muster von (b_1,…,b_m) und (c_1,…,c_m) übereinstimmen. Da Texte mit gleichem numerischen Muster auch »Isomorphe« genannt werden, nennt man dieses Vorgehen »Methode der Isomorphe«.

Die kommerzielle Enigma

… ohne Steckerbrett - die Substitution reduziert sich auf

$$c_i = \sigma_z^{-1}\, \pi\, \sigma_z\, (a_i)$$

In einem Abschnitt, wo sich nur der Rotor 1 bewegt, bewirken die beiden inneren Rotoren zusammen mit der Umkehrwalze eine konstante Involution $\pi^{\sim}$. In diesem Abschnitt bestehen dann Gleichungen

$$\begin{aligned} c_1 &= [\rho_1^{(z_1)}]^{-1}\, \pi^{\sim}\, \rho_1^{(z_1)}\, (a_1), \\ c_2 &= [\rho_1^{(z_1+1)}]^{-1}\, \pi^{\sim}\, \rho_1^{(z_1+1)}\, (a_2), \\ &\dots \\ c_m &= [\rho_1^{(z_1+m-1)}]^{-1}\, \pi^{\sim}\, \rho_1^{(z_1+m-1)}\, (a_m). \end{aligned}$$

Also ist für $i = 1, \dots, m$

$$c_i' = \rho_1^{(z_1+i-1)}\, (c_i) = \pi^{\sim}\, \rho_1^{(z_1+i-1)}\, (a_i) = \pi^{\sim}\, (a_i')$$

monoalphabetisches Bild von $a_i' = \rho_1^{(z_1+i-1)}\, (a_i)$.

Auch hier ist durch Mustervergleich beim Durchprobieren aller Rotoren und Ausgangsstellungen der schnelle Rotor und sein Zustand identifizierbar.

Um diesen Angriff zu verhindern, wurde beim Übergang zur Wehrmachts-Enigma das Steckerbrett eingeführt.

Besonderheiten der Enigma

- Die Zykelzerlegung jeder Substitution ρ_z wird durch das Steckerbrett nicht geändert; die Substitution wird ja einfach nur mit η konjugiert.
  - Bei genügend viel bekanntem Klartext lassen sich Zykeln finden.
  - Die verschiedenen Walzenlagen unterscheiden sich durch ihre Zykeltypen [TURINGs »Klassen«].
  - Auf diese Weise kann man Informationen über die Walzenlage gewinnen.
- Negative Mustersuche
  - ermöglicht, die Lage von bekanntem Klartext einzugrenzen,
  - führte zur Entdeckung eines italienischen Testfunkspruchs, der nur aus `LLL...LLL` bestand.
    [Ein Genieblitz der Kryptoanalytikerin Mavis LEVER, der aufgefallen war, dass der Geheimtext kein `L` enthielt; er trug wesentlich zur Aufdeckung der Verdrahtung der Rotoren bei.]

Historische Daten zur Kryptoanalyse von Rotormaschinen

- Friedman kryptoanalysiert 1925 die Hebern-Maschine erfolgreich. Sie wird als Folge davon nicht für die US-Army übernommen, erst eine spätere Weiterentwicklung, die HCM bzw. ECM.

- Beurling bricht 1931 die B21 von Hagelin. Eine Weiterentwicklung, die unter der Bezeichnung M-209 im zweiten Weltkrieg von der US Army eingesetzt wurde, wurde von deutschen Kryptologen unter der Leitung von Erich Hüttenhain [Bild] gebrochen. Dies entdeckten die Amerikaner 1942 in einer von Ihnen dechiffrierten Nachricht der italienischen Marine. Sie führten sofort ein neues Verfahren ein, das von den Deutschen, wie erst kürzlich bekannt wurde [Artikel in Telepolis] auch wieder gebrochen werden konnte. Hierzu entwickelte Reinold Weber ein elektromechanisches Hilfsgerät - ähnlich der polnischen »Bomba« (s. u.) -, das zu Kriegsende vernichtet wurde.

- Die japanischen Rotor-Maschinen der Vorkriegszeit werden in den dreißiger Jahren von den Amerikanern (Kullback, Rowlett), Deutschen (Kunze) und Engländern gebrochen. Weiterentwicklungen davon werden von den Amerikanern im 2. Weltkrieg fortlaufend gebrochen.

- Die Polen Marian Rejewski [Bild], Henryk Zygalski, Jerzy Rózycki brechen die kommerzielle Enigma und die Vorkriegsversion der Wehrmachts-Enigma. Insbesondere finden sie die innere Verdrahtung der einzelnen Rotoren heraus. Sie finden Möglichkeiten, mit bekanntem oder vermutetem Klartext (Stereotypen) den Schlüsselraum zu reduzieren. Zu parallelen Abarbeitung der vollständigen Suche in diesem reduzierten Schlüsselraum entwickeln sie die »Bomba«, eine elektromechanische Simulation eines Teils der Enigma-Operation. Mit Beginn des zweiten Weltkriegs übergeben sie ihre Erkenntnisse, insbesondere ihren Nachbau der Enigma, den Briten.

- Während des gesamten zweiten Weltkriegs brechen die Briten fortlaufend die Enigma-verschlüsselten Nachrichten, auch jeweils mit etwas Zeitverzug nach Weiterentwicklung der Maschinen. Die mathematischen Köpfe hinter diesem Unternehmen sind Gordon Welchman und Alan Turing (1912-1954) [Bild]. Auch bei ihnen wird die vollständige Suche durch geeignete Geräte, die »Turing-Bomben«, unterstützt. Öffentlich bekannt wurde das alles erst 1974; bis dahin hatten die Öffentlichkeit und selbst die deutschen Kryptologen die Enigma für sicher gehalten.

- Als die Einführung der vierten Walze für die Marine-Enigma die Leistungsfähigkeit der britischen »Bomben« überforderte, sprangen die USA ein und ließen bei NCR (National Cash Register Company) unter der Leitung von Joseph Desch Hochleistungsanlagen (»US Navy Bomb«) konstruieren, mit deren Hilfe nach fast einem Jahr vergeblichen Bemühens die Geheimtexte der deutschen Marine wieder routinemäßig gebrochen werden konnten.

- Basierend auf dem Know-How der Engländer - und damit indirekt auf dem der längst ausgebooteten Polen - konnten auch die Amerikaner verschiedene Versionen der Enigma brechen und teilten sich dabei die Arbeit mit den Engländern. Die Arbeitsteilung betraf hauptsächlich die Konstruktion bzw. Konfiguration der jeweils passenden »Bomben«.

- Ebenfalls von den Briten (William Tutte [Bild], Maxwell Newman, Tom Flowers) wird 1943 der »COLOSSUS«, der erste funktionierende elektronische Rechner entwickelt, um die Kryptoanalyse der Chiffrier-Fernschreiber von Lorenz (»Schlüsselzusatz«, SZ-Serie) mit

Erfolg zu unterstützen. Weitere bekannte Mathematiker, die an diesem oder verwandten Projekten beteiligt waren, waren P. J. Hilton und I. J. Good.

- In Schweden bricht Arne Beurling [Bild] 1940 die Verschlüsselung des Siemens-Geheimschreibers; auf den über das neutrale Schweden laufenden deutschen Fernschreibverbindungen nach Norwegen fand sich reichlich Material dazu. Beurling hatte nur diese abgefangenen Geheimtexte; er hatte keine Ahnung, wie die zugehörige Chiffriermaschine aussah. Dieses ist wohl die verblüffendste Einzelleistung in der Geschichte der Kryptoanalyse. Als Folge konnten die Schweden während des zweiten Weltkrieges fast die gesamten strategischen Nachrichten der Deutschen mitlesen. Bekannt wurde dies erst in den 90-er-Jahren.

Zum letzten Punkt:

- Bengt Beckman: *Codebreakers: Arne Beurling and the Swedish Crypto Program During World War II.* AMS 2002, ISBN 0-8218-2889-4.

Interessant ist es auch, eine Enigma und zugehörigen »Bomben« in dem gleichnamigen Film in Aktion zu sehen. (Kurzbesprechung hier.)

Typisch ist, dass im zweiten Weltkrieg erstmals in vielen Ländern führende Mathematiker in größerer Zahl als Kryptoanalytiker beschäftigt waren. Dennoch entstand daraus in der Nachkriegszeit (bis etwa 1975) kein aktives mathematisches Forschungsgebiet, hauptsächlich wohl, weil die Vorgänge aus dem Krieg noch lange Zeit geheimgehalten wurden - oder in der Sprache der Amerikaner und Engländer »classified« waren.

Folgerungen

- Das Prinzip von KERCKHOFFS (1883) ist unbedingt zu beachten: Ein Chiffrierverfahren muss so sicher sein, dass es nicht schadet, wenn der Gegner es kennt. Anders ausgedrückt: *Bei einem gut gemachten Chiffrierverfahren muss nur der Schlüssel geheim gehalten werden.* »Il faut qu'il puisse sans inconvéniant tomber entre les mains de l'ennemi.«
  [François KERCKHOFFS VAN NIEUWENHOFF, 1835-1903]
- Man kann das KERCKHOFFS-Prinzip auch so formulieren:
  > *Parameter, die sich nicht jederzeit sofort ändern lassen, sind als Schlüssel ungeeignet.*
- Ebenfalls muss ein Chiffrierverfahren so gut sein, dass es auch bei »Chiffrierfehlern« - Nachlässigkeiten, Abweichen von strengen Vorschriften, Bequemlichkeit, Gedankenlosigkeit - der Kryptoanalyse standhält.
- Rotor-Maschinen können nur sicher sein, wenn sie eine komplexe Steuerlogik haben.

Rotor-Maschinen *können* also offenbar starke Chiffren produzieren. Ein denkbarer moderner Ansatz, algorithmisch, also durch Computer-Simulation zu verwirklichen, wäre etwa der folgende (**Projektidee**):

- Verwendung von 256-Buchstaben-Rotoren (für das Alphabet $\mathbf{F}_2^8$ der Oktette).
- Antrieb durch eine Steuerlogik, die einen (nicht ganz schlechten) Pseudozufallsgenerator verwendet.

Das ursprüngliche `crypt`-Kommando unter Unix war so implementiert, allerdings nicht besonders stark.

Forschungsproblem: Kriterien für die Sicherheit einer solchen Rotor-Maschine:

1. Wie nimmt die Sicherheit mit der Zahl p der verwendeten Rotoren zu?
   Hier könnte man ähnliche Kriterien entwickeln wie für die Zahl der Runden einer Bitblock-Chiffre.
2. Welche Qualität muss der Pseudozufallsgenerator haben?
   Hier sollte man die Kriterien verwenden, die im Zusammenhang mit Bitstrom-Chiffren vorgeschlagen wurden.

Autor: Klaus Pommerening, 13. Februar 2000; letzte Änderung: 10. Januar 2005.