Kryptoanalyse

Autor(en): **Glur, P.**

Objekttyp: **Article**

Zeitschrift: **Pionier : Zeitschrift für die Übermittlungstruppen**

Band (Jahr): **44 (1971)**

Heft 10

PDF erstellt am: **11.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-562907

mann an, so braucht man, um eine Minute sprechen zu können, etwa eine Million Chiffrierimpulse und hat zudem Probleme mit der Synchronisation.
Ein Vocoder braucht weniger Impulse zur Sprachübertragung, da er ja nicht die Sprache, sondern nur die Steuerimpulse überträgt; also kann man auch mit kleinerem Aufwand chiffrieren, und zudem ist die Redundanz weggelassen. Computer kann man hier dafür einsetzen, die Kombination Vocoder/Chiffriersystem zu simulieren, um die Wirksamkeit zu testen.

Pi Motf R. Mäder

Kryptoanalyse

Die Kryptoanalyse befasst sich mit der Aufgabe der Dekryptierung, das heisst mit dem Aufbrechen von aufgefangenen Chiffraten ohne Kenntnis der verwendeten Schlüssel. Im folgenden sei ein Beispiel für den Einsatz von Computern für derartige kryptoanalytische Aufgaben gegeben.
Wir gehen aus von einem konkreten handelsüblichen konventionellen Chiffriergerät. Ein solches präsentiert sich in folgender Form:

Ein Gerät mit
- einer Einrichtung für die Einstellung des Schlüssels (6 zweistellige Zahlen);
- einer Eingabemöglichkeit des zu chiffrierenden oder zu dechiffrierenden Textes (Tastatur);
- einer Schreib- oder Lesevorrichtung für den zugehörigen Chiffre- oder Klartext (Schreibstreifen).

Dieses Gerät führt im Innern Operationen aus (Ersetzen von Buchstaben nach einem arithmetischen oder Booleschen Formalismus), welche auch von einem Computer ausgeführt werden können. Es ist also durchaus möglich, einen Computer so zu progammieren, dass er dieses Chiffriergerät vollwertig simuliert oder sogar ersetzt.

Das notwendige zugehörige Programm umfasst
- das eigentliche Chiffrierprogramm, welches die inneren Funktionen des Chiffriergerätes enthält;
- die Eingabe des zu wählenden Schlüssels;
- die Eingabe des zu chiffrierenden Textes.

Über diese Verwendung als Chiffrierprogramm hinaus stellen wir nun die folgende kryptoanalytische Aufgabe:
Es sei ein Chiffrat aufgefangen worden, von dem wir wissen, dass es mit diesem Gerät hergestellt wurde, der dafür gewählte Schlüssel aber sei uns unbekannt. Bei bekanntem Schlüssel wären Chiffriergerät und Computer, abgesehen von der verschiedenen Arbeitsgeschwindigkeit, gleichwertig für die Dechiffrierung. Da wir aber in unserer Aufgabe den verwendeten Schlüssel zuerst suchen müssen, bietet uns der Computer dank seiner grossen Geschwindigkeit die naheliegende Möglichkeit, sämtliche Schlüssel des Gerätes systematisch abzusuchen.
Den Auftrag dazu geben wir dem Computer mit einem übergeordneten Such- oder Dekryptierprogramm mit folgendem Arbeitszyklus:

- Stelle einen ersten Schlüssel ein.
- Dechiffriere damit das aufgefangene Chiffrat.
- Prüfe auf Klartext, das heisst das Auftreten eines verständlichen Sinnes der Meldung.
- Entscheide:
  wenn ja: drucke den Klartext heraus;
  wenn nein: stelle den nächsten Schlüssel ein,

womit der Zyklus wieder anfängt.

Machen wir eine Zeitbilanz: Das Gerät hat eine Mannigfaltigkeit von $2{,}75 \cdot 10^9$ möglichen Schlüsseln. Diese Zahl entspricht
- in msec gemessen 32^d
- in µsec gemessen 46^m

Bei der für einen der oben beschriebenen Arbeitszyklen benötigten Zeit (Grössenordnung msec) haben wir also mit einer Computerzeit von mehreren Tagen zu rechnen. Diese Dauer gibt uns übrigens einen Hinweis auf die Güte des gewählten Chiffriergerätes.
Das Absuchen können wir durch folgende Ergänzung beschleunigen:
Wir nehmen an, in unserem aufgefangenen Text komme ein bestimmtes Klarwort vor (es ist dies die Methode des «mot probable» in der Kryptologie). Solche Annahmen sind bei militärischen Texten naheliegend, wir wählen für unseren Fall das meistverwendete Wort «Angriff».
Der Umstand, dass der Computer nun nicht mehr irgendeinen Klartext, sondern einen bestimmten Klartextausschnitt zu suchen hat, erlaubt im vorliegenden Chiffrierverfahren ein gezieltes Absuchen der möglichen Schlüssel, so dass wir statt der ursprünglichen $2{,}75 \cdot 10^9$ Fälle nur mehr deren 50 000 zu prüfen haben. Damit sind wir im Bereiche des hier Möglichen.
Wir geben nun dem Computer über das Terminal den Auftrag:

- Lies das aufgefangene Chiffrat.
- Lege das Klarwort «Angriff» an die erste Stelle desselben.
- Prüfe, ob einer der noch zugelassenen möglichen Schlüssel die Zuordnung Chiffrat–Klarwort erlaubt.
- Entscheide:
  wenn ja: dechiffriere das ganze Chiffrat und drucke den Text heraus;
  wenn nein: lege das Klarwort an die zweite Stelle,

und so fort.

Der Computer liefert uns die Antwort, bestehend aus 8 möglichen Texten, die alle das Klarwort «Angriff» enthalten. Einer dieser Texte scheint uns einen vernünftigen Inhalt zu liefern («allgemeine Lage: Rot der durch einen starken Angriff von Grün im Raume ...»), das wir als richtigen Klartext für unser aufgefangenes Chiffrat ansprechen dürfen. Die sieben anderen Texte scheiden wegen Unverständlichkeit aus.
Wir haben bei diesem Beispiel Glück gehabt, dass wir nur eine Auswahl von 8 Texten auf vernünftigen Sinn prüfen mussten. Was ist aber zu tun, wenn statt nur 8 deren 8000 oder noch mehr Texte zur Auswahl herausgedruckt würden, was bei einem stärkeren Chiffriergerät mit grösserer Schlüsselmannigfaltigkeit ohne weiteres zu erwarten wäre? Das Absuchen durch den Menschen auf vernünftigen Text ist dann hoffnungslos.
Wir helfen uns, indem wir dem Computer ein Klartextkriterium einbauen. Zwar ist der Computer nicht imstande, auftretende Dechiffrate intelligenzmässig zu verstehen; wir können ihn aber so programmieren, dass er auf bestimmte Klartextmerkmale achtet und sie zweckmässig bewertet. Im allgemeinen werden wir den Computer nur die höchstbewerteten Texte ausdrucken lassen. So haben wir dann nur noch wenige Fälle intelligenzmässig auf vernünftigen Sinn zu prüfen.
Im vorliegenden Beispiel liegt zwischen der Eingabe unseres Auftrages an den Computer und dem Herausdrucken seiner Antwort eine Rechenzeit von 65^m. Diese Rechenzeit ist hauptsächlich bedingt durch die Zugriffszeit des für diese Aufgabe benötigten externen Speichers; sie lässt sich bei moderneren Anlagen wesentlich verkürzen.
Diese Zeitspanne dient uns als Mass für die Sicherheit eines Chiffriergerätes. Nach heutiger Auffassung handelt es sich um ein konventionelles Chiffrierverfahren mittlerer Kapazität, die sich durch Verwendung weiterer Bauelemente um mehrere Zehnerpotenzen verbessern liesse. Damit ist gezeigt, dass der Wettlauf zwischen Chiffrierverfahren und Computer noch nicht entschieden ist.

Major P. Glur