LV-Nummer: 250115

Wintersemester 2009/2010

Ao. Univ.-Prof. Dr. Peter Schmitt

Seminar für LAK

Angewandte Mathematik

Martin Kletzmayr

Matrikelnummer: 0304008

Studienkennzahl: A 190 313 406

Email: martin.kletzmayr@gmx.net

Symmetrische Kryptografie

Das Geheimnis einen Text zu verschlüsseln, sodass diesen nur bestimmte Personen lesen konnten, die auch dazu berechtigt sind, haben die Menschheit schon immer fasziniert. So hatte die Kunst der Kryptografie auch einen großen Anteil in der Menschheitsgeschichte. Wir wollen uns aber nun ansehen, was es damit auf sich hat und wie die Verschlüsselung eines Textes funktionieren kann.

1. Kryptologische Grundlagen

Es geht als bei der Verschlüsselung von Texten um die Geheimhaltung von Nachrichten. Das bedeutet also, dass nur der Empfänger, der dazu berechtigt ist die Nachricht zu lesen, diese auch entschlüsseln kann. Im Gegensatz dazu kann kein Angreifer , der die Nachricht abfängt, diese auch lesen. Das bedeutet, dass der berechtigte Empfänger, dem vermeintlichen Angreifer eine Information voraus haben muss, damit er die Nachricht entschlüsseln kann. Diese Information nennt man Schlüssel. Man unterscheidet im Allgemeinen zwei verschiedene Arten der Verschlüsselung. In der klassischen, oder auch symmetrischen Kryptografie besitzt der Empfänger den gleichen Schlüssel wie der Sender, mit welchem auch die Nachricht verschlüsselt wurde. In der asymmetrischen Kryptografie unterscheiden sich die Schlüssel mit dem man die Nachricht verschlüsselt und mit dem man die Nachricht lesbar machen kann. Dieser Artikel wird sich im Folgenden ausschließlich mit der symmetrischen Kryptografie beschäftigen.

2. Definition einer symmetrischen Verschlüsselung

Man kann nun den Vorgang, der Verschlüsselung als mathematischen Algorithmus auffassen, den man wie folgt beschreiben kann: Ein symmetrischer Verschlüsselungsalgorithmus besteht aus einer Funktion f mit zwei Eingabewerten; dem Schlüssel k und dem Klartext m. Daraus entsteht ein Geheimtext c.

Formal: c:=f(k,m) oder auch $c := f_k(m)$

In der symmetrischen Verschlüsselung haben wir ebenfalls die Voraussetzung, dass der Algorithmus umkehrbar sein muss. Das heißt, dass es eine Funktion f* geben muss, die die Wirkung von f umkehrt. Das bedeutet, dass die die Funktion f*aus dem gleichen Schlüssel k wieder den Klartext rekonstruiert.

Formal: m:=f*(k,c)

Das heißt, dass man in der Praxis davon ausgehen muss, dass sowohl die Ver- als auch die Entschlüsselungsfunktion bekannt ist. Man nennt das das Kerkoffsches Prinzip.

3. Verschiedene symmetrische Algorithmen

Im Anschluss möchte ich nun einige verschiedene symmetrische Algorithmen beispielhaft vorstellen.

3.1. Monoalphabetische Substitution

Ein Beispiel für diesen Algorithmus ist die Cäsar-Chiffre. In dieser Verschlüsselungsform werden einfach die Buchstaben des Alphabets um eine bestimmte Anzahl an Stellen nach rechts verschoben. Man benötigte also einen Schlüssel. War dieser zum Beispiel k=3 dann wurden alle Buchstaben um 3 Stellen nach rechts verschoben. So wurden aus einem A ein D, oder aus einem H ein K. So musste der Empfänger der Nachricht nur den Schlüssel zu kennen. Dieses Verfahren fand mehrere Jahrhunderte lang Anwendung. Man sieht sofort, dass es ein sehr einfaches Verfahren ist, bei dem auch nur 25 verschiedene Varianten existieren einen Klartext zu verschlüsseln, was es für einen Angreifer relativ einfach macht.

3.2. Polyalphabetische Substitution

Ein Beispiel für einen solchen Algorithmus ist die Vigenère-Chiffre. Der große Unterschied zur monoalphabetischen Verschlüsselung besteht darin, dass man 26 Alphabete verwendete u den Text zu verschlüsseln. Das bedeutet, dass man mehrere monoalphabetische Verschlüsslungen im Wechsel anwendet und das Schlüsselwort das genaue Zeichen angibt, mit dem ein Buchstabe des Klartextes zu verschlüsseln ist. Das macht es möglich, dass ein Zeichen des Klartextes z.B. a durch mehrere Zeichen im Geheimtext dargestellt wird; z.B. s und u.

Ein weiteres erwähnenswertes System ist das One-Time-Pad Verfahren. Dieses neue Prinzip basierend auf dem Vigenère-Chiffre unterscheidet sich darin, dass beim One-Time-Pad das Schlüsselwort dieselbe Länge haben muss als der zu chiffrierende Text und er muss aus zufälligen Zeichen bestehen. Die Verschlüsselung basiert dann auf einer einfachen Addition von Klartext und Schlüsselzeichen modulo 26. Dieses Prinzip, so unglaublich es scheint, war eine fast perfekte Methode, natürlich solange kein Angreifer Zugriff auf das One-Time-Pad hatte. Das Problem dabei bestand aber in der schwierigen Anwendung.

3.3. Matrixverschlüsselung

Bei der Matrixverschlüsselung geht es um die Codierung eines Textes unter Zuhilfenahme von Matrizen – besser gesagt unter Zuhilfenahme von Matrix-Produkten. Die Matrixverschlüsselung ist eine Methode die relativ schnell von Hand aus durchgeführt werden kann und trotzdem sehr sicher ist. Dazu ordnet man jedem Buchstaben einer Zahl zu und bringt den Text in eine Form von symmetrischen Matrizen. Dieser Text wird anschließend mit einer Verschlüsselungsmatrix multipliziert. Dadurch erhält man einen Geheimtext, indem man keine eindeutige Zuordnung der einzelnen Einträge auf einzelne Zeichen erkennen kann. Zur Entschlüsselung muss man die Matrizen mit der inversen Verschlüsselungsmatrix multiplizieren um zum ursprünglichen Text zu gelangen. Da es unendlich viele (nxn)-Matrizen gibt ist es leicht einsichtig, dass man diesen Code durch probieren nur sehr unwahrscheinlich knacken kann.

3.4. Kombinierte Formen

Natürlich kann man die einzelnen Verschlüsselungsformen auch kombinieren bzw. hintereinander durchführen um eine höhere Sicherheit zu erhalten. Ein Beispiel dafür wäre die ADFGX-Verschlüsselung. Hierbei wird der Text zuerst in einen 5x5 Matrix gebracht und die Zeichen durch die Buchstaben ADFGX substituiert. Erst im Anschluss kommt es zu einer Transposition der Zeichen.

4. Kryptoanalyse

Bei der so genannten Kryptoanalyse handelt es sich um die Untersuchung eines Textes auf Regelmäßigkeiten, um herauszufinden wie der Text verschlüsselt wurde und um die Länge des Schlüsselwortes zu bestimmen. So kann man zum Beispiel durch den Kasiskitest einen Vigenère-verschlüsselten Text gleiche Zeichenfolgen suchen und so die Länge des

Schlüsselwortes bestimmen, indem man weiß, dass zwei gleiche Klartextfolgen(Z.B. das Wort ein) genau dann in gleiche Geheimtextfolgen verschlüsselt werden, wenn ihr Abstand ein Vielfaches der Schlüsselwortlänge ist. Wenn der Text also lange genug ist, um mehrere gleiche Zeichenfolgen zu finden ist es dadurch auch möglich hier mit der Kryptoanalyse anzusetzen. Ist ein Text nun polyalphabetisch verschlüsselt, so kann man dadurch die einzelnen Alphabete erkennen und diese sind dadurch relativ einfach zu entschlüsseln.

Eine andere Methode, um zu erkennen ob ein Text mono-, oder polyalphabetisch verschlüsselt wurde, ist der so genannte Friedmanntest. Die Grundidee besteht darin, dass der Koinzidenzindex eines Textes, der die Wahrscheinlichkeit angibt, mit der zwei zufällig herausgegriffene Buchstaben gleich sind, bei einem monoalphabetischen und einem polyalphbetischen Text verschieden ist.

5. Erfahrungsbericht

Die Entscheidung, mich mit diesem Thema zu beschäftigen, ist mir nicht schwer gefallen. Das hat vor allem den Grund, dass ich mich schon immer sehr für dieses Themengebiet interessiert habe und es vor allem noch heute brandaktuell ist. Auch hat mich begeistert, dass es im Schulunterricht sehr gut anwendbar ist, obwohl teilweise, je nachdem welche Verfahren man betrachtet, sehr viel Mathematik enthalten ist, diese aber trotzdem, oder gerade deshalb, nicht so sehr abstrakt erscheint, sondern im Gegenteil, sehr einleuchtend erscheint.

Zu meiner Begeisterung bin ich bei der Vorbereitung meines Vortrages für das Seminar noch auf sehr viele neue Dinge gestoßen, die mich ebenfalls sehr interessierten. So zum Beispiel auf den historischen Aspekt der Kryptografie. Da mein Zweitfach Geschichte ist habe ich auch versucht diese Gesichtspunkte in meinen Vortrag einzubauen. Besonders führen diese augenscheinlich vor wie bedeutend diese mathematischen Algorithmen in der Geschichte waren und zu welchen entscheidenden Wendungen diese auch beigetragen haben, wie zum Beispiel die These, dass es durch die Entschlüsselung der ADFGX-Chiffre durch die Franzosen, es den Deutschen im ersten Weltkrieg nicht gelang Paris einzunehmen.

Ich denke, dass eine solche fachliche Verknüpfung, auch wenn sie mir, wegen der Zeitknappheit bei meinem Seminarvortrag nicht ganz gelungen ist, eine große Chance ist, die Mathematik, sowie auch die Geschichte, im Unterricht an den Schule spannender zu gestalten, da die Fächer dadurch an Plastizität zulegen könnten und die Schüler dadurch mehr Anreize bieten könnte.

6. Literaturverzeichnis

- Albrecht *Beutelspacher*, Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln(^{8}2007 Wiesbaden)
- Albrecht *Beutelspacher*, Jörg *Schwenk*, Klaus-Dieter *Wolfenstetter*, Moderne Verfahren der Kryptografie. Vom RSA zu Zero-Knowledge(^{6}2006 Wiesbaden)
- Marion *Pilat,* Einführung in die Kryptologie: Von Cäsar bis RSA mit Übungsaufgaben. Eine Lehrunterlage für das Mathematik Wahlpflichtfach(2008 Diplomarbeit Fakultät für Mathematik Wien)