Machine Learning for Cryptanalysis

Marcus Jan Almert, Vincent Mann, Vladimir Spassov

Professur für Mediensicherheit

Chiffre

Eine Chiffre verschlüsselt eine Nachricht unter einem Schlüssel zu einem Chiffretext. Der Chiffretext einer Chiffre sollte idealerweise wie zufälliger Text aussehen, damit keine Relationen zwischen Klar- und Chiffretext hergestellt werden können. Nur mit dem gleichen Schlüssel, welcher beim Verschlüsseln benutzt wurde, kann man den Chiffretext wieder entschlüsseln.

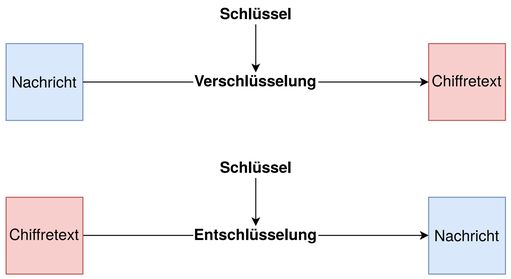

Abbildung 1. Ver- und Entschlüsselung.

Kryptanalyse

In der Kryptanalyse untersuchen wir Chiffren, um Schwachstellen in ihrem Aufbau und ihrer Funktionsweise zu erhalten. Es gilt einen Zusammenhang zwischen den Klar- und Chiffretexten zu erschließen um darauf basierend zum Beispiel den verwendeten Schlüssel zu ermitteln.

Differentielle Kryptanalyse

In der differentiellen Kryptanalyse betrachtet man Differenzen zwischen Nachrichten und Chiffretexten. Erzeugt eine bestimmte Differenz in den Nachrichten mit signifikanter Wahrscheinlichkeit eine bestimmte Chiffretext-Differenz, so kann man einen Zusammenhang zwischen Nachrichten und Chiffretexten herstellen.

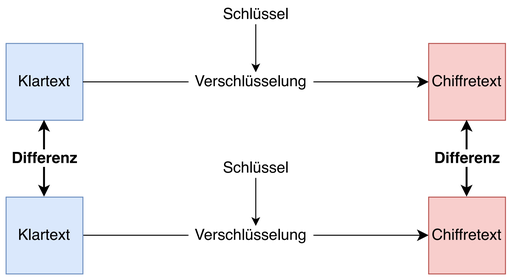

Abbildung 2. Differenzen zwischen Texten.

Maschinelles Lernen

Beim maschinellen Lernen werden Algorithmen welche durch Erfahrung lernen genutzt. Sie verarbeiten hierbei Trainingsdaten, um Muster in diesen zu erkennen und in ein statistisches Modell zu übersetzen. Nach der Lernphase können sie das Gelernte auf echte Daten anwenden, ohne explizit auf ein bestimmtes Problem programmiert zu werden.

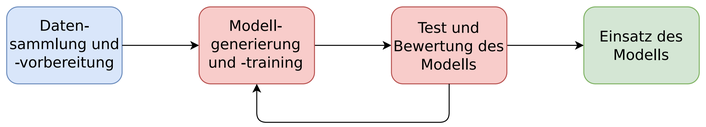

Abbildung 3. Prozess des Maschinellen Lernens.

Künstliche Neuronale Netzwerke

Künstliche neuronale Netzwerke sind eine Art des maschinellen Lernens. Als Vorbild dient das menschliche Nervensystems.

Das Neuron ist der Grundbaustein des neuronalen Netzes. Die Eingaben werden unterschiedlich gewichtet aufaddiert. Eine sogenannte Aktivierungsfunktion berechnet auf dieser Summe basierend die Ausgabe des Neutrons.

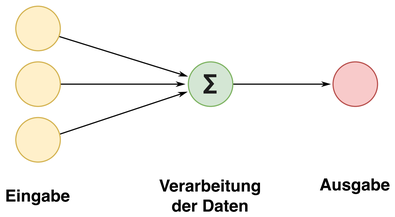

Abbildung 4. Aufbau eines Neurons.

Ein Netzwerk aus Neuronen besteht aus Ebenen, welche ein oder mehrere Neuronen enthalten. Die Eingabe-Ebene nimmt den Input entgegen. Es können mehrere versteckte Ebenen folgen, welche die Neuronenanzahl erhöhen, um komplexe Sachverhalte zu modellieren. Die Ergebnisse der Verarbeitung werden dann von der Ausgabe-Ebene ausgegeben.

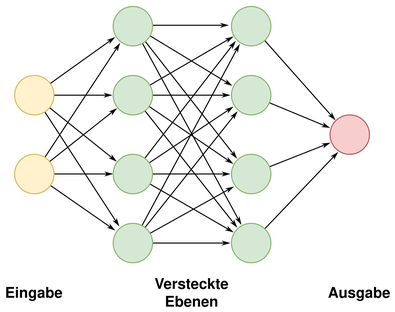

Abbildung 5. Aufbau eines neuronalen Netzwerks.

Kryptanalyse mit neuronalen Netzwerken

Ziel ist es, mittels neuronalen Netzwerken Muster und Strukturen in Chiffretexten zu erkennen und diese für Angriffe auf die Chiffre auszunutzen.

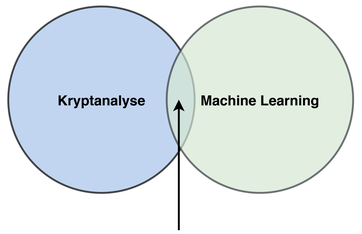

Abbildung 6. Überschneidung von Maschinellen Lernen und Kryptanalyse.

Um neuronale Netzwerke in der Kryptanalyse einsetzen zu können, muss man ihnen Zugriff auf die Ein- und Ausgabe der Chiffre geben. Von Interesse sind nicht nur Angriffe, welche allein mit Hilfe neuronaler Netzwerke durchgeführt werden, sondern auch Mischformen mit klassischen Angriffstechniken, bei denen neuronale Netzwerke in unterstützender Rolle auftreten.

Ausgangspunkt unserer Arbeit sind dabei die bisherigen Erkenntnisse von Aron Gohr auf diesem Gebiet [1].

Ausblick

Neuronale Netzwerke scheinen Eigenschaften außerhalb der uns bekannten Strukturen und Muster der Chiffren erkennen und erlernen zu können und damit Unterscheidungen möglich zu machen, welche mit den traditionellen Vorgehensweise der Kryptanalyse nicht möglich scheinen.

Ein interessanter Forschungsaspekt ist es, diese neuen Strategien zu erkennen und in effizientere Analysetools umzuwandeln. Um dies zu tun, möchten wir in diesem Projekt die Erkenntnisse von Gohr auf weitere Chiffren und andere kryptographische Primitive anwenden und Werkzeuge entwickeln, welche diesen Prozess automatisieren. Dadurch kann die wissenschaftliche Gemeinschaft mehr Daten auswerten und einfacher neue Experimente starten.

Referenzen

[1] Aron Gohr. „Improving Attacks on Round-Reduced Speck32/64 Using Deep Learning“. In: *CRYPTO 2019*. LNCS. Springer, 2019, S. 150–179.