Von der Enigma zur Quantenkryptographie

Beziehung von Verschlüsselung zu Entschlüsselung

Donnerstag, 8. Juni 19:30 Uhr, KHG Graz

Über Jahrtausende hinweg veränderten des Öfteren geheime Botschaften, versteckte Nachrichten und strategische Informationen den Lauf der Geschichte. Dabei waren meist die Stärke der Verschlüsselung dieser Informationen oder die Raffinesse in der Entschlüsselung von entscheidender Bedeutung. Dieser kurze Beitrag diskutiert die spannende Beziehung von Verschlüsselung und Entschlüsselung im Laufe der Geschichte und die womöglich finale Entscheidung im Kampf Kryptograph versus Kryptoanalytiker.

Schon in der Antike entwickelten sich erste Formen der Verschlüsselung, so wird von Gaius Julius Caesar durch Sueton berichtet, er hätte eine einfache Substitutionsmethode verwendet, indem jeder Buchstabe durch den drei Buchstaben folgenden Buchstaben ersetzt wird.

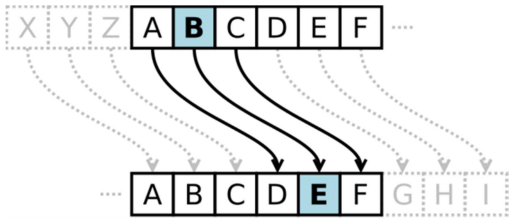

Abbildung 1: Von Cepheus - Eigenes Werk, Gemeinfrei, https://commons.wikimedia.org/w/index.php?curid=1235339

Diese Art der Verschlüsselung kann jedoch durch eine einfache statistische Textanalyse dechiffriert werden, indem die Häufigkeit der Zeichen gezählt wird.

Besonders relevant wurden Kryptographie und Kryptoanalyse im 18. und 19. Jahrhundert, als Nachrichten über weite Strecken per kabelgebundener und drahtloser Telegraphie übertragen werden konnten. Da es ein Leichtes war, solche Verbindungen mit einfachen Kabeln oder Antennen anzuzapfen und mitzuhören, wurde eine wirkungsvolle Verschlüsselung schnell sehr bedeutend, um Nachrichten geheim zu halten.

Die eingangs erwähnte Methode der statistischen Textanalyse trug so im ersten Weltkrieg wesentlich zur Entschlüsselung der ADFGX Verschlüsselung, der Geheimschrift der deutschen Funker und der deutschen Militärs, einem zweistufigen Verschlüsselungsverfahren, im Frühjahr 1918 vor der Frühjahrsoffensive bei.
48 Jahre nach dem ersten Weltkrieg trafen der Erfinder der ADFGX Verschlüsselung Fritz Nebel (der Kryptograph) und der Entschlüsseler Georges Painvin (der Kryptoanalytiker) freundschaftlich aufeinander und stellten fest, dass die Verschlüsselung von Nebel nach ursprünglichem aufwändigerem Verschlüsselungsschema von Painvin nicht geknackt hätte werden können.

Eine etwas kompliziertere Verschlüsselung, die im ersten Weltkrieg unter anderem von deutschen Diplomatenkreisen eingesetzt wurde und auf einer Codeverschlüsselung (Verschlüsselung ganzer Wörter durch bestimmte Zahlenfolgen) beruhte, war schon zu Beginn des ersten Weltkrieges wirkungslos, da die Codebücher (Schlüssel) bereits 1914 in die Hände der Alliierten fielen. Den Deutschen war bis zum Ende des ersten Weltkrieges nicht bewusst, dass ihre Verschlüsselung geknackt wurde.
Die Blamage der deutschen Verschlüsselung gipfelte in der Zimmermann Depesche, die Mexiko zum

Krieg gegen die USA aufstacheln wollte und die USA letztendlich bewog, an der Seite der Alliierten in den ersten Weltkrieg einzutreten.

Diese aus deutscher Sicht kryptographische Katastrophe des ersten Weltkrieges führte in Deutschland bis zum zweiten Weltkrieg zur Entwicklung der Enigma, einer ersten Realisierung maschineller Verschlüsselung in Schreibmaschinenform.
Die Stärken der Enigma beruhten zunächst auf dem großen Schlüsselraum, der es einem unmöglich machte, die Verschlüsselung manuell zu knacken. Dem Polen Marian Rejewski und dem Engländer Alan Turing, gelang es jedoch mit mathematischer Raffinesse und mit einer mechanischen Maschine, genannt Turing Bomb, dem Vorläufer der heutigen Computer, gegen Ende des zweiten Weltkrieges die Enigma zu entschlüsseln.
Entscheidend dabei waren zwei Fehler von deutscher Seite: der eine konstruktionsbedingt, der andere ein Bedienungsfehler.
Ein Buchstabe wurde von der Enigma nie mit demselben Buchstaben verschlüsselt (zB: aus dem Buchstaben A konnte nie ein A werden). Diese Tatsache konnte ausgenutzt werden, um einen zweiten Fehler der Deutschen auszunützen. Die deutschen Soldaten waren bekannt für ihren Ordnungssinn und exakten Tagesablauf, der ihre Funksprüche berechenbar machte und gewisse Wörter in regelmäßigen Abständen zu erwarten waren. Die Wortfolge OBERKOMMANDODERWEHRMACHT oder WETTERVORHERSAGEBEREICHSIEBEN stellte eine pünktlich zu erwartende Wortfolge dar, die ausschlaggebend für die Entschlüsselung der Enigma und damit sämtlicher deutscher Funksprüche im zweiten Weltkrieg war.

Die Auswirkung der Entschlüsselung auf den zweiten Weltkrieg wird von Historikern unterschiedlich bewertet, während die einen von einer Reduktion der Kriegsdauer um mindestens zwei Jahre sprechen, halten andere die Entschlüsselung der Enigma für kriegsentscheidend.

Die erfolgreiche Entschlüsselung der Enigma durch die Engländer und Polen war eines der am besten gehüteten Geheimnisse Großbritanniens bis in die 70er Jahre hinein.

Ab der Mitte des 20. Jahrhunderts änderten sich die Verschlüsselungstechniken grundlegend. Bis dato verwendeter Standard war es, einen Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln zu verwenden. Die größte Schwierigkeit beim Aufbauen einer Verschlüsselung war es, eben diesen Schlüssel zuvor auszutauschen.
Ein neuer Verschlüsselungsalgorithmus, der parallel im britischen Nachrichtendienst (GCHQ) und von den Wissenschaftler Ronald L. Rivest, Adi Shamir und Leonard M. Adleman entwickelt wurde, revolutionierte diesen Schlüsselaustausch. Es wurden nun zwei Schlüssel verwendet, ein öffentlicher Schlüssel, der zum Verschlüsseln diente und mit dem ein Entschlüsseln alleine nicht mehr möglich ist und ein privater Schlüssel, der notwendig ist, um die Nachricht tatsächlich zu entschlüsseln.
Dies erleichterte den Schlüsselaustausch natürlich immens. Zwei Personen mussten vorher gar keinen Schlüssel ausgetauscht haben, sondern nur den jeweils anderen öffentlichen Schlüssel (zB. von einer Homepage) kennen um miteinander verschlüsselt zu kommunizieren.
Grundlage dieser asymmetrischen Verschlüsselung ist eine mathematische Operation, deren Umkehrung extrem zeitaufwändig und damit faktisch unmöglich wird.
Als Beispiel sei hier die Primfaktorzerlegung angeführt. Dabei geht es im Prinzip um folgende zwei mathematische asymmetrische Operationen.
Die leichte Operation lautet folgendermaßen: Man nehme zwei Primzahlen und multipliziere sie. Die so entstandene Zahl nennen wir N.

Die schwierige Operation besteht darin herauszufinden, aus welchen Primzahlen die Zahl N besteht. Da prinzipiell die einzige Möglichkeit darin besteht, alle Primzahlen als Teiler auszuprobieren, stellt diese zweite Operation eine schwer umkehrbare Operation dar.
Ein Angreifer müsste diese Operation durchführen, um die Nachricht zu entschlüsseln.

Alle bis jetzt besprochenen Verfahren sind knackbar, das heißt es besteht die Chance die Verschlüsselung mit einer gewissen Anstrengung zu brechen. In den letzten Jahrzehnten änderte sich dieses Dogma (Verschlüsselungen sind prinzipiell knackbar) grundlegend.
Die Quantenmechanik ermöglicht mit ihrem neuen eigenartigen Wesen eine nicht knackbare Verschlüsselung, die von physikalischen Gesetzen garantiert wird.
Verwendet werden verschränkte Photonen, die ein identisches Paar Photonen darstellen, diese werden vom Verschlüssler (Alice) erzeugt und können nicht kopiert werden. Ein Angreifer (Eve) kann es nicht schaffen die Kommunikation abzuhören. Wenn Eve mithört, vernichtet er die Photonen und Alice und Bob (der Adressat) wissen, dass ihre Leitung abgehört wird.

Diese Technologie stellt im Prinzip den Sieg der Kryptographen über die Kryptoanalytiker dar. Die Technologie wird heutzutage schon in Glasfaserkabeln eingesetzt und Banktransaktionen werden zum Beispiel schon auf diese Weise durchgeführt.
Sogar die Satellitenkommunikation über genau eingestellte Laser werden derzeit angedacht und sind Gegenstand aktueller Forschung.

Den Kryptoanalytikern bleiben jedoch immer noch andere Wege (zB. Tastatur) um geheime Nachrichten abzufangen.