

Bitte vertraulich behandeln – Verschlüsselung von Daten

Es gibt eine Vielzahl von Programmen, mit denen Dateien durch Verschlüsselung vor unberechtigten Blicken geschützt werden können. Einige dieser Programme sollen in diesen und in weiteren ZPG-Mitteilungen vorgestellt werden. Dieser Artikel versucht die zu Grunde liegenden Prinzipien darzustellen sowie die wichtigsten Begriffe rund um das Thema Kryptographie zusammenzufassen.

Problembewusstsein

Der Inhalt eines im Klassenzimmer liegen gelassenen Memory-Sticks kann in kürzester Zeit ohne Spuren zu hinterlassen kopiert werden. Über das Internet ist es ein Leichtes, die so gewonnenen Daten zu verteilen. Ein auf dem Memory-Stick gespeicherter Entwurf einer Prüfungsaufgabe kann damit als veröffentlicht angesehen werden und ist somit wertlos. Ähnliches gilt für Notenlisten und andere persönliche Schülerdaten – auch sie haben nichts im Internet verloren.

Werden diese sensiblen Daten verschlüsselt auf dem Stick abgelegt, können sie zwar genauso leicht kopiert werden, aber der Datendieb kann nichts mit ihnen anfangen. Gleiches gilt für den Versand als E-Mail Anhang. Egal welchen Weg die E-Mail durch das Internet nimmt, der Inhalt der angehängten Datei bleibt geheim.

Steganographie

Der Begriff Steganographie leitet sich von den beiden griechischen Begriffen „steganós“ (bedecken) und „gráphein“ (schreiben) ab und bedeutet sinngemäß verstecktes Schreiben. Die zu übermittelnde Nachricht wird so versteckt, dass sie dem Betrachter nicht auffällt. Ganz so wie im Film „Arabeske“ mit Sophia Loren und Gregory Peck, in dem die eigentliche Nachricht als Mikroschrift in einem Punkt auf einem ansonsten wertlosen Stück Papier versteckt wurde. Heutzutage werden Informationen gerne in Bilddateien versteckt.

Wer das einmal ausprobieren möchte, sollte sich das Open Source Programm OpenStego mal genauer ansehen. Mit diesem Programm kann die zu übermittelnde Nachricht zusätzlich noch verschlüsselt werden.

Kryptographie

Der Begriff Kryptographie kommt aus dem griechischen und wurde von den beiden Wörtern kryptos (verborgen) und graphein (schreiben) abgeleitet. Im Gegensatz zur Steganographie geht es hier nicht darum die Nachricht zu verstecken, sondern sie zu verschleiern. Oft werden beide Verfahren auch in Kombination eingesetzt. Eine versteckte Nachricht weckt erst mal keine Begehrlichkeiten. Wird sie trotzdem entdeckt, ist ihr Inhalt für den Angreifer wertlos.

Bsp. Cesar-Verschlüsselung

Wie eine Nachricht verschlüsselt werden kann, lässt sich am besten anhand der einfachen Cesar-Verschlüsselung nachvollziehen. Der große Stratege Cesar verwendete für die Verschlüsselung seiner Nachrichten eine einfache Methode. Er verschob zum Schreiben einer Nachricht einfach alle Buchstaben des Alphabets um einen festen Wert.

In der Kryptographie ist es zur einfacheren Unterscheidung üblich, den Klartext in Kleinbuchstaben und den Geheimtext in Großbuchstaben anzugeben. Bei einer Verschiebung um drei Buchstaben ergibt sich folgendes Geheimtextalphabet:

Klartextalphabet	a b c d e f g h i j k l m n o p q r s t u v w x y z
Geheimtextalphabet	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Jedem Buchstaben des Klartextalphabets ist ein fester Buchstabe des Geheimtextalphabets zugeordnet

Soll nun die Nachricht „Angriff im Morgengrauen“ verschickt werden, werden einfach die Buchstaben des Klartextes durch die entsprechenden Buchstaben des Geheimtextalphabetes ersetzt.

Klartextalphabet	a	n	g	r	i	f	f	i	m	m	o	r	g	e	n	g	r	a	u	e	n
Geheimtextalphabet	D	Q	J	U	L	I	I	L	P	P	R	U	J	H	Q	J	U	D	X	H	Q

Diese verschlüsselte
Botschaft ist relativ leicht
zu entschlüsseln

Ein solches Verfahren, bei dem einzelne Buchstaben durch andere Buchstaben ersetzt werden, wird als Substitution bezeichnet. Eine andere grundlegende Möglichkeit besteht darin, die Position der Buchstaben zu verändern. In diesem Fall spricht man von der Transposition. Gerne werden beide Verfahren miteinander kombiniert.

Der Empfänger der Nachricht muss zum Entschlüsseln zwei Dinge wissen. Zum einen muss er das Verschlüsselungsverfahren selbst kennen und zum anderen benötigt er die Anzahl an Buchstaben, um die das Geheimtextalphabet verschoben wurde. Das Verfahren selbst wird als Verschlüsselungsalgorithmus und die Anzahl der Buchstaben als Schlüssel bezeichnet. Nur wer beides kennt, kann eine Nachricht ver- bzw. entschlüsseln. Der Gedanke, sowohl den Algorithmus wie auch den Schlüssel geheim zu halten, liegt nahe. Heutzutage sind sich die Experten aber darüber einig, dass es bei einem guten Algorithmus genügen muss, nur den Schlüssel geheim zu halten.

Kryptoanalyse

Der Versuch, hinter das Geheimnis einer verschlüsselten Nachricht zu kommen, wird als Kryptoanalyse bezeichnet. Der Kryptoanalytiker muss zum Entschlüsseln einer Nachricht sowohl den verwendeten Algorithmus wie auch den eingesetzten Schlüssel herausbekommen. Je nach verwendetem Algorithmus ist das unterschiedlich schwer. Bei der oben beschriebenen Cesar-Verschlüsselung kann beispielsweise eine einfache Häufigkeitsanalyse schon zum Erfolg führen. Hierbei wird die Häufigkeit der im Text vorkommenden Buchstaben erfasst und mit der durchschnittlichen Häufigkeit in Texten derselben Sprache verglichen. In deutschen Texten ist der Buchstabe e der am häufigsten vorkommende Buchstabe. Kommt in einem zu entschlüsselnden Geheimtext der Buchstabe h am häufigsten vor, so kann

man davon ausgehen, dass h für ein e steht und somit das Geheimtextalphabet um 3 Buchstaben gegenüber dem Klartextalphabet verschoben wurde.

Ebenfalls sehr hilfreich sind typische Wörter der verwendeten Sprache. So wird es sich bei aus drei Buchstaben bestehenden Wörtern eines deutschen Geheimtextes, aller Wahrscheinlichkeit nach, um Wörter wie *der*, *die*, *das* oder *ein* handeln.

Bei der Entwicklung eines Algorithmus müssen die Möglichkeiten und Verfahren zur Kryptoanalyse berücksichtigt werden. Beide Wissenschaften stehen sozusagen in einem ständigen Wettstreit.

Advanced Encryption Standard - AES

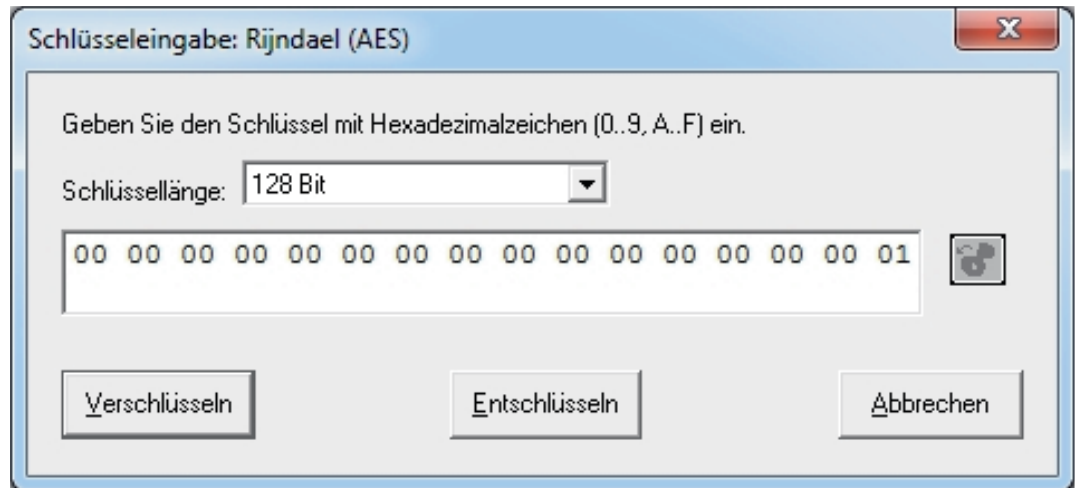
Zurzeit gilt der aus einer Ausschreibung des amerikanischen Handelsministeriums vom 2. Januar 1997 hervorgegangene Rijndael Algorithmus als sicher. Der Algorithmus ist frei verfügbar und erhielt den Namen Advanced Encryption Standard oder kurz AES. AES verwendet mindestens eine Schlüssellänge von 128 Bit (AES 128).

Bei dieser Schlüssellänge wäre ein Cluster von einer Billion PC's, von denen jeder eine Billion Schlüssel pro Sekunde ausprobieren kann, immerhin zehn Millionen Jahre beschäftigt (vgl. *Bachfeld, Daniel; c't Nr. 19; 29.08.2011; Weiterer Kratzer für Kryptoalgorithmus AES*). Wer also bereits nach einer Million Jahren das richtige Passwort gefunden hat, kann sich glücklich schätzen.

Auch wenn andere Angriffe auf den Algorithmus selbst bisher schon einige mögliche Schwachstellen aufgezeigt haben, gilt der Algorithmus bisher trotzdem als sicher.

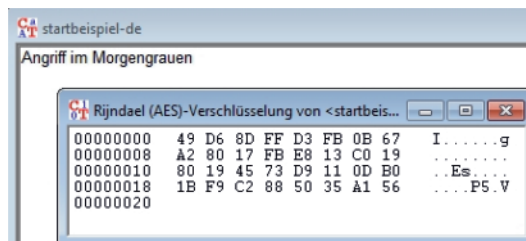
Im folgenden Beispiel wurde der Text „Angriff im Morgengrauen“ mit einem 128 Bit langen Schlüssel bestehend aus 127 Nullen gefolgt von einer 1 verschlüsselt.

128 Bit langer Schlüssel

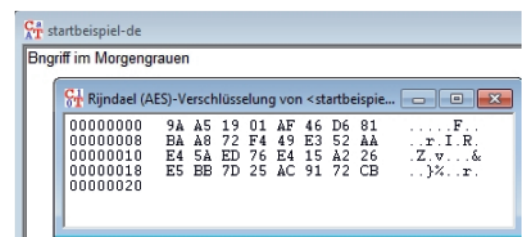


Screenshots CryptTool

Zwei fast identische Begriffe verlieren jede Ähnlichkeit



„Angriff im Morgengrauen“ AES verschlüsselt



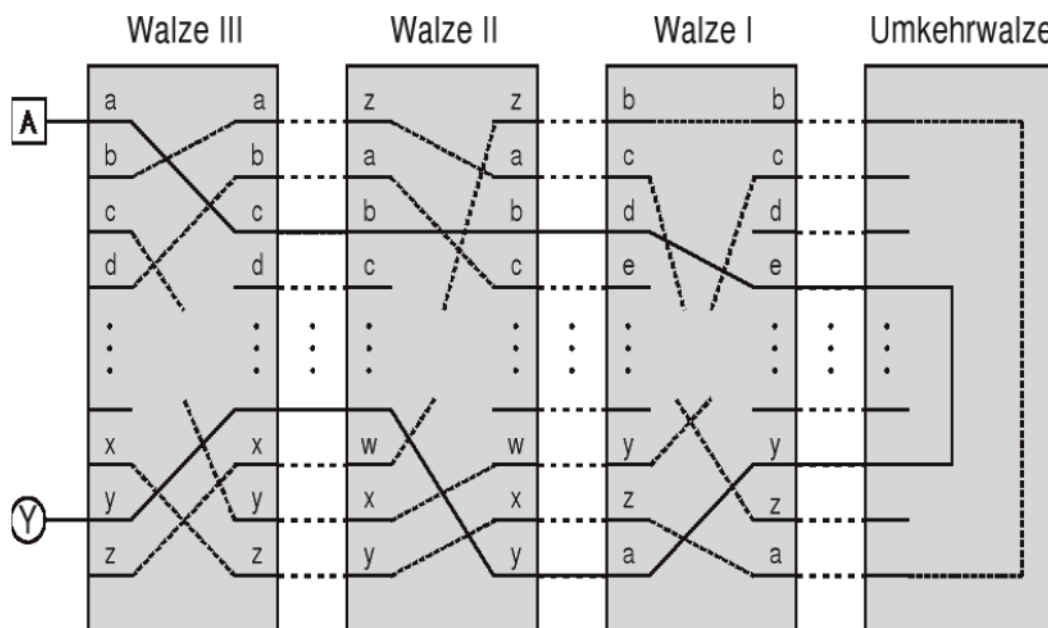
„Bngriff im Morgengrauen“ AES verschlüsselt

Zum Vergleich wurde im Text nur der erste Buchstabe in ein B geändert. Es ist zu erkennen, dass die beiden Ergebnisse der Verschlüsselung keine Gemeinsamkeiten aufweisen.

Beispiel Enigma

Im zweiten Weltkrieg setzten die Deutschen für die Verschlüsselung ihrer Nachrichten die Enigma (gr. Rätsel) ein. Die Enigma hatte eine Schreibmaschinentastatur mit der die einzelnen Buchstaben der zu verschlüsselnden Nachricht, eingegeben wurden. Auf einem Ausgabefeld leuchtete dann der Buchstabe auf, mit dem der Eingebene zu ersetzen war. Nach dem Verschlüsseln der Nachricht wurde diese dann, ohne Leerzeichen zu verwenden, durch Morsen übertragen. Zum Entschlüsseln wurde die empfangene Nachricht Buchstabe für Buchstabe wieder in eine Enigma eingetippt, die dann die richtigen Buchstaben anzeigte.

Die Enigma arbeitete nach dem Prinzip der Transposition. In fest verdrahteten Walzen wurde jeder Buchstabe des Alphabets auf einen anderen Buchstaben abgebildet. Der Trick der Enigma bestand nun darin, mehrere Walzen hintereinander zu schalten und die Stellung der Walzen, ähnlich einem mechanischen Kilometerzähler, nach jedem Tastendruck zu ändern. So wurde erreicht, dass derselbe Buchstabe immer durch einen anderen Buchstaben ersetzt wurde. Entscheidend für die Ver- und Entschlüsselung war die Auswahl und Grundstellung der Walzen. Dieser „Schlüssel“ musste Sender und Empfänger der Nachricht bekannt sein.



Bildquelle: Harald Baurle

Stark vereinfachte Darstellung des Funktionsprinzips der Enigma. Entsprechend der Walzenstellung leuchtet beim Betätigen der Taste A die Anzeigeleuchte für Y. Durch eine Änderung der Walzenstellung ändert sich auch die Chiffrierung des Buchstaben A.

Problem der Schlüsselverteilung

Genau hier lag das Problem. Um den gegnerischen Codebrechern die Arbeit zu erschweren, wurde der Schlüssel, also die Auswahl und Grundstellung der Walzen, täglich geändert. Wie aber konnte man dem Empfänger einer Nachricht den Schlüssel zukommen lassen, wenn keine Möglichkeit einer abhörsicheren Kommunikation bestand? Die deutsche Marine löste dieses Problem, indem sie für jeden Tag den zu verwendenden Schlüssel im Voraus festlegte und den Schiffen und U-Booten diese Schlüssel in sogenannten Schlüsseltafeln mitgab. Natürlich waren diese streng geheim und dementsprechend begehrt.

In der Literatur wird zur Verdeutlichung des Problems der Schlüsselverteilung gerne von Alice, Bob und Eve gesprochen. Alice möchte Bob eine Nachricht zukommen lassen. Eve (engl. Eavesdropper – Lauscher) versucht alles, um an die Nachricht zu gelangen. Solange Alice und Bob die Möglichkeit besitzen einen geheimen Schlüssel zu vereinbaren, können sie sich anschließend ungehindert verschlüsselte Nachrichten zukommen lassen. Auch wenn Eve die verschlüsselte Nachrichten mitlesen kann, hat sie keine Möglichkeit an deren Inhalt zu gelangen – eine gute Verschlüsselung vorausgesetzt. Wie aber sieht es aus, wenn keine Möglichkeit zu einem sicheren Schlüsselaustausch besteht? Bob könnte zum Beispiel in einem fernen Land leben, aus dem er nicht ausreisen darf und alle Kommunikationsmittel durch Geheimdienste überwacht werden.

Unabhängig hiervon stößt das System mit jedem Kommunikationspartner geheime Schlüssel zu vereinbaren schnell an seine Grenzen, wenn die Anzahl der teilneh-

menden Personen zunimmt. Damit sich z. B. zehn Lehrerinnen und Lehrer einer Abteilung untereinander verschlüsselte Nachrichten zu-senden können, sind bereits 45 Schlüssel nötig.

Öffentlicher und privater Schlüssel

Das Problem der Schlüsselverteilung ließ den Amerikanern Martin Hellmann und Whitfield Diffie keine Ruhe. Zusammen mit Ralf Merkle veröffentlichten sie 1976 ein theoretisches Modell zu Lösung dieses Problems. Im August 1977 stellten die Amerikaner Rivest, Shamir und Adleman ihre darauf aufbauendes RSA-Verfahren zur Verschlüsselung der Öffentlichkeit vor.

Der Trick besteht in einer asymmetrischen Verschlüsselung. Bei den bisher besprochenen Verfahren handelte es sich immer um sogenannte symmetrische Verschlüsselungen. Das bedeutet, dass zum Ver- und Entschlüsseln immer der gleiche Schlüssel verwendet wird. Die Idee hinter der asymmetrischen Verschlüsselung ist, dass es zwei zusammengehörende Schlüssel gibt. Wird mit dem einem Schlüssel verschlüsselt, kann nur mit dem anderen Schlüssel wieder entschlüsselt werden – und umgekehrt.

Einer der Schlüssel, der Privat Key, wird geheim gehalten. Der andere Schlüssel, der Publik Key, wird veröffentlicht. Wenn nun Alice Bob eine Nachricht zukommen lassen will, verschlüsselt sie diese einfach mit Bobs öffentlichem Schlüssel und schickt sie ihm zu. Bob entschlüsselt die Nachricht mit seinem geheimen privaten Schlüssel. Da nur Bob im Besitz des geheimen Schlüssels ist, kann auch nur er die für ihn bestimmte Nachricht lesen.

Um mehr über die geheime Unterhaltung zwischen Alice und Bob zu erfahren könnte sich Eve als Alice ausgeben und Bob ebenfalls eine mit seinem öffentlichen Schlüssel verschlüsselte Nachricht zukommen lassen. Zwar kann auch diese Nachricht nur Bob mit seinem privaten Schlüssel entschlüsseln, er kann aber nicht mit Sicherheit

sagen, dass die Nachricht tatsächlich von Alice stammt. Hier kommt nun der öffentliche Schlüssel von Alice ins Spiel. Wenn Alice eine Nachricht mit ihrem geheimen privaten Schlüssel verschlüsselt, kann sie von allen, die ihren öffentlichen Schlüssel besitzen, entschlüsselt werden. Damit ist der Inhalt der Nachricht natürlich nicht mehr als geheim anzusehen. Aber es ist sicher, dass die Nachricht von Alice stammt, da nur sie den zugehörigen privaten Schlüssel besitzt.

Für eine sichere Kommunikation muss also Alice zuerst ihre Nachricht mit ihrem eigenen privaten Schlüssel verschlüsseln und anschließend die so verschlüsselte Nachricht zusätzlich noch mit Bobs öffentlichem Schlüssel verschlüsseln. Die zweimal verschlüsselte Nachricht kann dann bedenkenlos über jedes unsichere Medium übertragen werden, denn nur Bob ist mit seinem geheimen privaten Schlüssel in der Lage, die verschlüsselte Nachricht zu entschlüsseln. Nachdem Bob die Nachricht mit seinem privaten Schlüssel entschlüsselt hat, entschlüsselt er die dann immer noch mit dem privaten Schlüssel von Alice verschlüsselte Nachricht zusätzlich mit ihrem öffentlichen Schlüssel. So kann er mit Sicherheit sagen, dass die Nachricht tatsächlich von Alice stammt. Alice und Bob können also ohne sich jemals irgendwo getroffen zu haben nur durch den Austausch ihrer öffentlichen Schlüssel sicher miteinander kommunizieren.

Das als RSA (Rivest, Shamir, Adleman) bezeichnete Verfahren zur asymmetrischen Verschlüsselung dient somit nicht nur zum Ver- und Entschlüsseln von Nachrichten sondern kann auch im Prinzip zu deren digitalen Signatur eingesetzt werden.

Dies geschieht zum Beispiel beim Zugriff auf eine HTTPS-Seite. Da asymmetrische Verfahren deutlich rechenintensiver sind als symmetrische, erfolgt die eigentliche Kommunikation zwischen Browser und Server symmetrisch. Der dazu notwendige geheime Schlüssel wird über eine asymmetrische Verschlüsselung übertragen, wobei der Browser über den öffentlichen Schlüssel des Servers dessen Authentizität überprüfen kann.

Es bleibt noch anzumerken, dass den beiden Engländer James Ellis und Clifford Cocks mittlerweile die Entdeckung der asymmetrischen Verschlüsselung zugesprochen wird. Bereits einige Jahre vor den Amerikanern entwickelten sie ein Verfahren zur

asymmetrischen Verschlüsselung. Da ihre Arbeit der Geheimhaltung unterlag, haben die Amerikaner unabhängig davon ihr System entwickelt.

Zusammenfassung

Personenbezogene Daten sollten auf keinen Fall unverschlüsselt gespeichert werden. Die Verschlüsselung sollte durch einen als sicher einzustufenden offenen Algorithmus wie z. B. AES erfolgen. Werden zum Ver- und Entschlüsseln Open Source Programme eingesetzt, sind auch die Programmquellen einsehbar. Ein Umstand, der die Wahrscheinlichkeit einer fehlerfreien Implementierung stark erhöht. Durch die Verwendung eines offengelegten Algorithmus liegt die Sicherheit der Verschlüsselung allein im verwendeten Passwort. Dieses sollte aus mindestens 12 Zeichen bestehen und neben Groß- und Kleinbuchstaben auch Satz- und Sonderzeichen enthalten. Natürlich darf das Passwort auch in keinem Wörterbuch stehen.

Symmetrisch verschlüsselte Dateien können z. B. auch als Mailanhang über das Internet verschickt werden. Mit dem Empfänger sollte hierzu ein eigenes streng geheimes Passwort vereinbart werden.

Besteht mit dem Kommunikationspartner keine Möglichkeit für einen sicheren Schlüsselaustausch oder nimmt die Anzahl der Kommunikationspartner überhand, kann über eine asymmetrische Verschlüsselung mit einem privaten und einem öffentlichen Schlüssel eine sichere Kommunikation hergestellt werden, die zusätzlich die Möglichkeit einer digitalen Signatur bietet.

Wer sich für das Thema Kryptographie interessiert, findet im Internet zahlreiche Informationen hierzu. Weitere Informationen liefert z. B. das Buch „Geheime Botschaften“ von Simon Singh und Übungsmöglichkeiten bietet z. B. die von der Universität Siegen und Darmstadt entwickelte Open-Source-Software CrypTool (www.cryptool.org).

Harald Bäurle