1 Einleitung

Bei der Betrachtung der Benennung der Epochen in der menschlichen Geschichte ist bemerkbar, dass hier mehrmals die bedeutendste technische Errungenschaft aus diesem Zeitraum zur Namensgebung verwendet wird. Das ist natürlich sinnvoll da diese Entwicklungen im großen Ausmaß das Leben der Menschen beeinflussten und auch für den weiteren Verlauf der Geschichte ausschlaggebend sind. Diese Namen sind wie »Bronzezeit« recht selbsterklärend, hier wurde die Metallverarbeitung, vor allem mit Bronze erfunden und revolutionierte die Waffentechnik und ermöglichte auch viele andere neuartige Gegenstände.[1] Schwieriger wird es dann schon bei dem Titel des aktuellen Zeitabschnittes: »Digitales Informationszeitalter«. Nach Dr. Dr. Jörn Lengsfeld sind hierbei die »Informations- und Kommunikationstechnologien« die prägenden Technologien.[2] Diese Technik hat deshalb eine so große Bedeutung in unserem Leben, da sie uns durch das nicht mehr wegzudenkende Internet jederzeit Zugriff auf eine unfassbare Menge an Informationen verschafft. Allerdings werden auch diese Erfindungen leider nicht immer fortschrittsbringend eingesetzt, sondern sie haben genau wie die Erfindungen des Atomzeitalters ihre Schattenseiten, welche meist zwar um einiges unauffälliger sind, aber nicht immer auch ungefährlicher. Denn gerade diese riesige Reichweite macht das Internet so attraktiv für Angreifer und deshalb mussten Verfahren entwickelt werden um sich gegen Verbrecher, die im Hintergrund mitlesen oder schädliche Informationen verbreiten zu schützen. Aus diesem Grund wurden Verschlüsselungsverfahren entwickelt. Bei »Verschlüsselung« denkt man zwar schnell an Geheimnachrichten und ›top-secret‹ Dokumente, allerdings begegnen wir digitalen Verschlüsselungen inzwischen tagtäglich.

[1] *Bronzezeit in Europa – Deutschland in Geschichte | Schülerlexikon | Lernhelfer.*
[2] Dr. Dr. Jörn Lengsfeld, *Digitales Informationszeitalter.*

2 Verschlüsselung im Allgemeinen

2.1 Definition

Bei der Verschlüsselung handelt es sich um eine Form der Codierung, hierzu gehört zum Beispiel auch der *Morsecode* oder die allgegenwärtigen *Borcodes*, allerdings liegt die Zielsetzung bei der Verschlüsselung nicht nur einfach darin die Information in ein anderes Format zu übertragen, sondern hier will man »die Informationen systematisch so verfälschen, dass sie nicht rekonstruiert werden können, es sei denn, durch ausdrücklich hierzu Berechtigte.«[3] Die Verschlüsselung gehört zum Bereich der *Kryptographie*, womit die »Wissenschaft vom geheimen Schreiben«[4] gemeint ist.

2.1.1 Terminologie

Aus diesem Wissenschaftsbereich stammen noch mehrere Begriffe ab, die im folgenden von Bedeutung sein werden:

Chiffre Geheime Methode des Schreibens, also eine Form des Verschlüsselns

Klartext Der unverschlüsselte Text

Chiffretext Der verschlüsselte Text, bzw. Ausgangstext

Chiffrieren Das verschlüsseln des *Klartextes* zum *Chiffretext*

Dechiffrieren Das entschlüsseln des *Chiffretextes* um wieder den *Klartext* zu erhalten

[3] Dankmeier, *Grundkurs Codierung*, S. 263.
[4] Wätjen, *Kryptographie*, S. 1.

2.2 Ziele der Kryptographie

2.2.1 Geheimhaltung

Der wohl bekannteste und offensichtlichste Verwendungszweck der Verschlüsselung ist eine Nachricht geheim zu halten. Hierbei wird die zu übertragende Nachricht so entstellt, dass sie für jeden völlig unsinnig erscheint, außer für den beabsichtigten Empfänger, welcher den geeigneten Schlüssel besitzt, er ihm das Dechiffrieren ermöglicht.[5]

2.2.2 Authentikation

Bei der Authentikation liegt das Ziel darin, die Echtheit einer Identität oder Nachricht zu überprüfen, da wir uns in der digitalen Welt nicht einfach durch unser Aussehen oder unsere Stimme ausweisen können und auch bei Nachrichten ist nicht zweifelsfrei Festzustellen von wem sie versendet hat und ob sie auf ihrem Weg verändert wurden. Zur *Teilnehmerauthentikation* gehört unter anderem das eingeben der Geheimzahl am Geldautomaten, da nur der Besitzer der EC-Karte auch die dazu gehörige Nummer kennt und so seine Identität dem Geldautomaten nachweisen kann. Hier gilt das Prinzip:

> Ich weise meine Identität dadurch nach, dass ich nachweise, etwas zu haben, was kein anderer hat.[6]

Ähnlich funktioniert es bei der *Nachrichtenauthentikation*: hier verknüpft der Ersteller sein »Geheimnis« mit dem Dokument um es authentisch zu machen. Im Falle des Bankautomaten, muss allerdings zusätzlich zum Kontoinhaber logischerweise auch der Bankautomat die Geheimnummer kennen. Es gibt aber auch sogenannte *Signaturverfahren*, bei denen dies nicht notwendig ist.

[5] Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*.
[6] Beutelspacher, Schwenk und Wolfenstetter, *Moderne Verfahren der Kryptographie*.

2.2.3 weitere Ziele

Neben den beiden oben genannten Zielen für die die RSA-Verschlüsselung am häufigsten eingesetzt wird, gibt es auch noch weitere Ziele, die zwar weniger prominent sind, jedoch ähnliche Techniken nutzen. Bei dem Zeil der *Anonymität* wird die Identität verborgen, was bei einer digitalen Geschäftsabwicklung mit dem Zahlen mit Bargeld verglichen werden kann, aber auch oft zum Schutz der Privatsphäre eingesetzt wird. Wie die RSA-Verschlüsselung basieren *kryptographische Protokolle* größtenteils auf dem *Public-Key-Verfahren*. Mit einem Protokoll wird hierbei die zum Datenaustausch nötige Abfolge von auszuführenden Schritten bezeichnet. Somit ist es durch vorher festgelegte Protokolle möglich, dass sich eine große Anzahl von Teilnehmern miteinander verschlüsselt verständigen können. Ein *kryptografisches Protokoll* muss sich aber nicht auf den digitalen Nachrichtenaustausch beschränken, sondern auch schon das Bedienen eines Bankautomaten wird als solches bezeichnet.