



FOM Hochschule für Oekonomie & Management

university location Münster

Seminararbeit

in the study course Wirtschaftsinformatik

**im Rahmen der Lehrveranstaltung
Fallstudie/ Wissenschaftliches Arbeiten**

on the subject

**Kryptographie: Verwendung von mathematischen Methoden wie
Verschlüsselung und digitalen Signaturen zur Sicherung von
Webanwendungen**

by

Joshua-Volkan Gramatzki

Advisor: Prof. Dr. Gregor Hülsken
Matriculation Number: 647100
Submission: April 26, 2023

Contents

List of Figures	v
List of Tables	vi
List of Abbreviations	vii
List of Symbols	viii
Glossary	ix
1 ToDos	1
2 Einleitung	2
2.1 Zielsetzung	2
2.2 Aufbau der Arbeit	2
3 Grundlagen der Kryptographie	4
3.1 Grundbegriffe	4
3.2 Historische Entwicklung und grundlegende Konzepte	4
3.2.1 Caesar-Scheibe	5
3.2.2 Polyalphabetische Codes	6
3.2.3 Enigma	6
3.3 Kryptographische Verfahren und Algorithmen	7
3.4 Digitale Signaturen und Zertifikate	7
4 Anwendung von Kryptographie in Webanwendungen	8
4.1 Sicherheitsanforderungen an Webanwendungen	8
4.2 Verschlüsselung von Datenübertragungen	8
4.3 Passwortsicherheit	8
4.4 Authentifizierung und Autorisierung	8
4.5 Schutz vor Angriffen und Schwachstellen	8
5 Herausforderungen bei der Implementierung von Kryptographie in Webanwendungen	9
5.1 Performance- und Skalierbarkeitsprobleme	9
5.2 Komplexität und fehleranfälligkeit der Kryptographie	9
5.3 Benutzerfreundlichkeit und Usability-Aspekte	9
5.4 Abwägung von Sicherheitsanforderungen und Nutzerbedürfnissen	9

6 Fazit	9
Appendix	10
Bibliography	11

Todoverzeichnis

Dieses Kapitel muss vor Abgabe der Arbeit *unbedingt* entfernt werden 1

List of Figures

Figure 1: Caesar-Chifre am Beispiel eines Zeichenbandes	5
---	---

List of Tables

Table 1: Verschlüsselung mit Vigènere-Verfahren	6
---	---

List of Abbreviations

List of Symbols

Glossary

Algorithmus Exakte Handlungsvorschrift zur Lösung eines Problemes. 5

Kryptoanalyse Entschlüsselung von verschlüsselten Informationen und bewertung der Sicherheit von Verschlüsselungsverfahren. 4

Kryptographie Verschlüsselung von Informationen zum Schutz vor unbefugtem Zugriff. 4

Kryptologie Oberbegriff für Kryptographie und Kryptoanalyse zur Sicherheit von Informationen und Entwicklung von Techniken zur Verschlüsselung und Entschlüsselung von Daten. 4

monoalphabetisch Verschlüsselungsart, bei der der Schlüssel für jedes Zeichen gleich bleibt. 6

Steganographie Verbergen von Informationen in einer scheinbar harmlosen Nachricht. 4

1 ToDos

Dieses Kapitel muss vor Abgabe der Arbeit *unbedingt* entfernt werden

- Literaturrecherche
 - Angeben, was ich wann, wie, von wo als Literatur genutzt habe und wonach ich gesucht habe
- Eine gute Forschungsanalyse beinhaltet, dass neue Fragen entstehen
 - „Was bedeutet x für y?“
 - Zusammenfassung dieser im Fazit
- Literatur
 - Peer Reviewd Zeitschriften
 - Monographien
 - Lexika vermeiden

2 Einleitung

In der heutigen digitalen Welt ist die Sicherheit von Daten und Informationen von größter Bedeutung. Das Internet und Webanwendungen haben unser Leben erleichtert und verbessert, aber auch neue Herausforderungen in Bezug auf Datensicherheit und Datenschutz mit sich gebracht. Durch den Einsatz von Verschlüsselungs- und Signaturverfahren können Daten und Informationen sicherer übertragen und gespeichert werden. Das ist das Ziel der Kryptographie.

Kryptographie ist die Wissenschaft der Ver- und Entschlüsselung von Informationen. Sie umfasst mathematische Verfahren zur Sicherung von Daten und Informationen, die über das Internet oder andere Netzwerke übertragen werden. Die Verschlüsselung stellt sicher, dass die Informationen nur von autorisierten Personen gelesen werden können, während digitale Signaturen gewährleisten, dass die Informationen nicht manipuliert wurden.

2.1 Zielsetzung

In dieser Arbeit wird untersucht, wie mathematische Methoden, wie die Verschlüsselung und die digitale Signatur, eingesetzt werden, um Web-Anwendungen zu sichern. Webapplikationen werden immer häufiger zur Speicherung und Verarbeitung von Daten und Informationen verwendet und stellen daher ein attraktives Ziel für Angreifer dar. Durch den Einsatz von Kryptographie kann die Sicherheit von Webanwendungen erhöht werden.

2.2 Aufbau der Arbeit

Diese Ausarbeitung erläutert zunächst die Grundlagen der Kryptographie. Dazu gehört die Beschreibung verschiedener Verschlüsselungsverfahren wie symmetrische und asymmetrische Verschlüsselung. Anschließend werden digitale Signaturen und deren Funktionsweise erklärt. Im nächsten Schritt wird der Einsatz von Kryptographie in Webanwendungen betrachtet, einschließlich der Verwendung von SSL/TLS-Protokollen und der Public Key Infrastruktur.

Abschließend werden die Vor- und Nachteile der Kryptographie bei der Absicherung von Webanwendungen untersucht. Mögliche Angriffe und Schwachstellen von Verschlüsselungsverfahren und digitalen Signaturen werden aufgezeigt und mögliche Lösungen vorgestellt.

Insgesamt wird diese Arbeit zeigen, dass Kryptographie eine wichtige Rolle bei der Absicherung von Webanwendungen spielt und wie sie dazu beitragen kann, dass vertrauliche Daten und Informationen sicher über das Internet und andere Netzwerke übertragen und gespeichert werden können.

3 Grundlagen der Kryptographie

3.1 Grundbegriffe

Die folgende grundlegende Erklärung der Grundbegriffe der Kryptographie ist geschrieben in Anlehnung an Brinkmann, Kapitel 1.1.

Zu der **Kryptographie**, der Kunst Nachrichten oder Daten durch Verschlüsselung geheim zu halten, gibt es noch andere Wissenschaften, die sich mit Verschlüsselungen befassen. Bei der Kryptographie werden Nachrichten so unlesbar gemacht, dass sie nur von Empfängern mit einem geheimen Schlüssel wieder in den ursprünglichen Text umgewandelt werden können.

Parallel zu der Kryptographie gibt es die **Steganographie**, bei der die bloße Existenz der zu versteckenden Informationen verborgen wird. Dies wird dadurch ermöglicht, dass die geheimen Informationen in anderen, harmlos aussehenden Nachrichten versteckt werden, sodass sie nur von Eingeweihten entdeckt werden können.

Die **Kryptoanalyse** befasst sich, entgegen der Kryptographie, nicht mit der Verschlüsselung, sondern damit, verschlüsselte Nachrichten und kryptographische Verfahren zu analysieren. Dies wird mit dem Ziel gemacht, Verschlüsselungen zu brechen.

Die Wissenschaft, die Kryptographie und Kryptoanalyse vereint, ist die **Kryptologie**. Diese wird das Kernthema dieser Arbeit sein.¹

3.2 Historische Entwicklung und grundlegende Konzepte

Besonders in Zeiten des Krieges war es vonnöten, Informationen sicher von den Befehlshabern zu den Offizieren überbringen zu können. So wurden die ersten kryptographischen Konzepte für den militärischen und politischen Nutzen entwickelt.²

Eine grundlegende Erfindung für das Voranschreiten der Kryptographie war die Erfindung des Schlüssels. „Die Erfindung des variablen Schlüssels markiert die Geburtsstunde der Kryptographie“³. Durch variable Schlüssel ist es nun möglich, einfach zwischen verschiedenen Verschlüsselungen zu wechseln.

¹ compare Brinkmann, E., 2001.

² compare Beutelspacher, A., 2017.

³ Ibid.

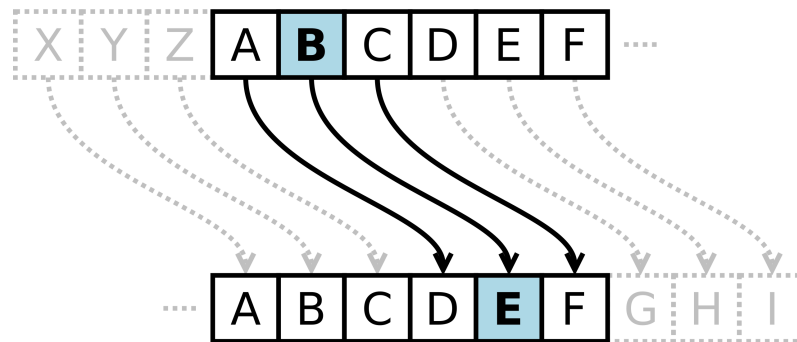


Figure 1: Caesar-Chiffre am Beispiel eines Zeichenbandes⁴

3.2.1 Caesar-Scheibe

Bei der Caesar-Scheibe (auch Caesar-Chiffre genannt) werden die Buchstaben des Alphabetes um einen bestimmten Wert, dem Wert des Schlüssels, rotiert. Dabei wird das 'z' als Buchstabe vor dem 'a' gesehen.

Die bevorstehende Abbildung zeigt, wie die Caesar-Chiffre mit dem **Schlüssel** 3 angewandt wird. Der Schlüssel bezeichnet bei der Caesar-Kodierung, um wie viele Zeichen das eingegebene Zeichen verschoben wird. Dieser Schlüssel ändert sich nicht für kommende Zeichen, sondern ist für die gesamte Nachricht identisch.

Die Figure 1 verbildlicht die Caesar-Chiffre mithilfe zweier Bänder, die mit den 26 Buchstaben des Alphabetes beschrieben wurden, die klassischere Darstellung ist die zweier Scheiben, welche im Mittelpunkt miteinander verbunden sind. Caesar nutzte für seine Verschlüsselungen immer den Schlüssel 3⁵, sodass aus CAESAR folglich FDHVDU wird. Dies bietet offensichtlich praktisch keine Sicherheit.

Da es sich durch die Jahrtausende hinweg immer wieder gezeigt hat, dass es fast unmöglich ist, Algorithmen geheim zu halten, kam mit der Zeit die Sorge auf, dass „[wer] das Verfahren kennt, insbesondere wer es erfunden hat, der kann es auch brechen.“⁶. Der Kryptologe Auguste Kerckhoffs formulierte 1833 in seinem zweiten der sechs Grundsätze zur Konstruktion eines sicheren Verschlüsselungsverfahrens⁷: „The system must not require secrecy and can be stolen by the enemy without causing trouble“⁸.

⁴ Eigene Graphik von Patricia.fidi (Wikipedia). Das Bild ist dem Gemeingut nach CC0 gewidmet.

⁵ compare *Beutelspacher, A.*, 2017.

⁶ Ibid.

⁷ *Petitcolas, F.*, n. d.

⁸ Übersetzt aus dem Französischen

3.2.2 Polyalphabetische Codes

Um 1500 wurde klar, dass monoalphabetische Codes keine wirkliche Sicherheit bieten. Im 16. Jahrhundert geschah ein Umdenken in der Verschlüsselung. Mehrere gelehrten hatten eine ähnliche Idee für eine neue Dimension dieser.⁹ Eines der bekanntesten polyalphabetischen Verfahren ist die Vigenère-Chiffre, benannt nach ihrem Entwickler, **Blaise de Vigenère**.

Bei der Vigenère-Chiffre wird sich, entgegen zu der Caesar-Chiffre, ein Schlüsselwort überlegt. Sollte dieses Wort kürzer sein, als der eigentliche Text, wird es so lange wiederholt, bis jedem Zeichen im Klartext ein Zeichen des Schlüssels zugeordnet ist. Anschließend wird jedes Zeichen im Klartext um das dazu assoziierte Zeichen des Schlüssels verschoben, sodass für jedes Zeichen ein anderes Zeichen im verschlüsselten Text herauskommt.

Klartext	D	i	e	s	i	s	t	e	i	n	v	e	r	s	c	h	l	u	e	s	s	e	i	t	e	r	T	e	x	t
Schlüssel (Alice)	A	L	I	C	E	A	L	I	C	E	A	L	I	C	E	A	L	I	C	E	A	L	I	C	E	A	L	I	C	E
Verschlüsselter Text	D	T	M	U	M	S	E	M	K	R	V	P	Z	U	G	H	W	C	G	W	S	P	T	V	I	R	E	M	Z	W

Table 1: Verschlüsselung mit Vigenère-Verfahren¹⁰

Durch diese nicht gleichmäßige Verschiebung bot die Vigenère-Chiffre eine deutlich sichere Verschlüsselung als die Caesar-Chiffre es bieten konnte. Aber vollständig sicher war sie allemal nicht. Man musste, sofern man den Schlüssel kennt, nur jeden Buchstaben des Verschlüsselten Textes in umgekehrter Reihenfolge entlang des Schlüssels verschieben.

Dies änderte dennoch nichts daran, dass polyalphabetische Verfahren stark waren und großes Potenzial hatten.

3.2.3 Enigma

Der Beginn des 20. Jahrhunderts läutete die Blütezeit der kryptographischen Maschinen ein. Diese wurden mit wachsender Komplexität der Verschlüsselungen immer notwendiger. Die wohl berühmteste Chiffriermaschine der Welt, die Enigma, wurde 1918 von ihrem Erfinder Arthur Schebius zum Patent angemeldet¹¹.

⁹ compare Beutelspacher, A., 2017.

¹⁰ Thielert, S., 2007, S. 6.

¹¹ Guo, J., Hu, Y., Wang, Y., 2022.

3.3 Kryptographische Verfahren und Algorithmen — symmetrische und asymmetrische Verschlüsselung, Hash-Funktionen etc.

3.4 Digitale Signaturen und Zertifikate

4 Anwendung von Kryptographie in Webanwendungen

**4.1 Sicherheitsanforderungen an Webanwendungen —
Vertraulichkeit, Integrität, Authentizität**

**4.2 Verschlüsselung von Datenübertragungen — HTTPS-Protokoll,
SSL/TLS-Verschlüsselung**

4.3 Passwortsicherheit — Salted Hashing, Key Derivation Function

4.4 Authentifizierung und Autorisierung — Token-Verfahren, OAuth

**4.5 Schutz vor Angriffen und Schwachstellen — SQL-Injection,
Cross-Site-Scripting**

5 Herausforderungen bei der Implementierung von Kryptographie in Webanwendungen

5.1 Performance- und Skalierbarkeitsprobleme

5.2 Komplexität und fehleranfälligkeit der Kryptographie

5.3 Benutzerfreundlichkeit und Usability-Aspekte

5.4 Abwägung von Sicherheitsanforderungen und Nutzerbedürfnissen

6 Fazit

Appendix

Appendix 1: Beispielanhang

Dieser Abschnitt dient nur dazu zu demonstrieren, wie ein Anhang aufgebaut sein kann.

Appendix 1.1: Weitere Gliederungsebene

Auch eine zweite Gliederungsebene ist möglich.

Appendix 2: Bilder

Auch mit Bildern. Diese tauchen nicht im Abbildungsverzeichnis auf.







Name	Änderungsdatum	Typ	Größe
 abbildungen	29.08.2013 01:25	Dateiordner	
 kapitel	29.08.2013 00:55	Dateiordner	
 literatur	31.08.2013 18:17	Dateiordner	
 skripte	01.09.2013 00:10	Dateiordner	
 compile.bat	31.08.2013 20:11	Windows-Batchda...	1 KB
 thesis_main.tex	01.09.2013 00:25	LaTeX Document	5 KB

Figure 2: Beispielbild

Bibliography

Brinkmann, Eilert (2001): VAK 03-794 Wintersemester 2000/01 Universität Bremen, in: (2001)

Guo, Jiaxin, Hu, Yichen, Wang, Yixuan (2022): Analysis and Illustration of the Enigma Machine. In: 2022 International Conference on Big Data, Information and Computer Network (BDICN), Big Data, Information and Computer Network (BDICN), 2022 International Conference on, BDICN (2022), pp. 807–819

Internet sources

Beutelspacher, Albrecht (2017): Eine kurze Geschichte der Kryptografie, bpb.de, (Accessed on 04/11/2023), <<https://www.bpb.de/shop/zeitschriften/apuz/259145/eine-kurze-geschichte-der-kryptografie/>> (2017-11-10) [Access: 2023-04-11]

Petitcolas, Fabian (n. d.): The information hiding homepage, Kerckhoffs's principles from « La cryptographie militaire », <<https://www.petitcolas.net/kerckhoffs/index.html>> (no Date) [Access: 2023-04-14]


Thielert, Sandra (2007): Kryptografische_Algorithmen.pdf, <https://www.hs-harz.de/dokumente/extern/Rechenzentrum/Grundschutz/Kryptografische_Algorithmen.pdf> (2007-05-11) [Access: 2023-04-19]

Declaration in lieu of oath

I hereby declare that I produced the submitted paper with no assistance from any other party and without the use of any unauthorized aids and, in particular, that I have marked as quotations all passages which are reproduced verbatim or near-verbatim from publications. Also, I declare that the submitted print version of this thesis is identical with its digital version. Further, I declare that this thesis has never been submitted before to any examination board in either its present form or in any other similar version. I herewith **agree/disagree** that this thesis may be published. I herewith consent that this thesis may be uploaded to the server of external contractors for the purpose of submitting it to the contractors' plagiarism detection systems. Uploading this thesis for the purpose of submitting it to plagiarism detection systems is not a form of publication.

Ahaus, 26.4.2023

(Location, Date)

A handwritten signature in black ink, appearing to read 'Gramsch', written over a horizontal line.

(handwritten signature)