# LaTeX-Vorlage für diverse Ausarbeitungen – oder so ähnlich

# Projekt-/Studien-/Bachleorarbeit

für die Prüfung zum

Bachelor of Science

des Studienganges Informatik / Informationstechnik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

**Max Mustermann**

Abgabedatum 1. April 2090

| | |
|---|---|
| Bearbeitungszeitraum | 12 Wochen |
| Matrikelnummer | 4711 |
| Kurs | tinf17b3 |
| Ausbildungsfirma | Firmenname<br>Stadt |
| Betreuer der Ausbildungsfirma | Titel Vorname Nachname |
| Gutachter der Studienakademie | Titel Vorname Nachname |

## Erklärung

Ich versichere hiermit, dass ich meine Projekt-/Studien-/Bachleorarbeitmit dem Thema: »LaTeX-Vorlage für diverse Ausarbeitungen
–
oder so ähnlich« selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt. _____

_____

Ort Datum Unterschrift

*Sofern vom Dualen Partner ein Sperrvermerk gewünscht wird, ist folgende Formulierung zu verwenden:*

## Sperrvermerk

Der Inhalt dieser Arbeit darf weder als Ganzes noch in Auszügen Personen außerhalb des Prüfungsprozesses und des Evaluationsverfahrens zugänglich gemacht werden, sofern keine anderslautende Genehmigung vom Dualen Partner vorliegt.

**Zusammenfassung**

Dieses LaTeX-Dokument kann als Vorlage für einen Praxis- oder Projektbericht, eine Studien- oder Bachelorarbeit dienen.

Zusammengestellt von Prof. Dr. Jürgen Vollmer <juergen.vollmer@dhbw-karlsruhe.de>
`https://www.karlsruhe.dhbw.de`. Die jeweils aktuellste Version dieses LaTeX-Paketes ist immer auf der *FAQ-Seite* des Studiengangs Informatik zu finden: `https://www.karlsruhe.dhbw.de/inf/studienverlauf-organisatorisches.html` → *Formulare und Vorlagen*.

Stand `$Date: 2020/03/13 15:07:45 $`

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Liste der Algorithmen

# Formelverzeichnis

# Abkürzungsverzeichnis

# Kapitel 1

# Grundlagen

In diesem Kapitel werden die theoretischen Grundlagen der Kryptologie, Mathematik, Zahlentheorie und der IT-Sicherheit erläutert, die in dieser Arbeit eine Rolle spielen. Aus diesen sollen die grundlegenden Funktionen eines kleptographischen Angriffes und dessen Folgen abgeleitet werden.

## 1.1 Kryptologie

Die Kryptologie ist die wissenschaftliche Disziplin für den Schutz von Daten. Unter ihr stehen die zwei Felder der Kryptographie und der Kryptoanalyse.

### 1.1.1 Kryptographie

Die Kryptologie befasst sich mit der Entwicklung von Verfahren und Techniken für den sicheren Austausch von Daten. Dabei stehen zwei Eigenschaften [Beutelspacher, Schwenk und Wolfenstetter 2015] im Fokus:

#### Eigenschaften

**Geheimhaltung** Durch Geheimhaltung (Datenintegrität) sollen, bei der Übertragung von Daten zwischen Teilnehmern, Unbeteiligte keine Erkenntnisse über den Inhalt erlangen. Dies kann durch physikalische oder organisatorische Maßnahmen erreicht werden, wobei Unbeteiligten der Zugang zu den übertragenen Daten verwehrt wird. Diese Maßnahmen sind sinnvoll bei der Übergabe der Daten in einer nicht digitalen Welt. Bei der Kommunikation in digitalen Netzen, wie u.a. dem Internet, sind diese Maßnahmen nur schwer zu implementieren. Dies gilt nicht für kryptographische Maßnahmen. Dabei ist es nicht mehr das Ziel, Unbeteiligten den Zugang zu den übertragenen Daten zu erschweren, sondern den Inhalt der Daten während der Übertragung zu verschlüsseln. Dadurch soll es Unbeteiligten nahezu unmöglich sein, aus den mitgehörten oder abgefangenen Daten, Rückschlüsse auf deren Inhalt zu erlangen.

**Authentifikation** Durch Authentifikation soll es den Teilnehmern einer Kommunikation möglich sein, die anderen Teilnehmer und empfangene Nachrichten zweifelsfrei identifizieren und zuweisen zu können. Hierbei spielen Signaturverfahren eine wichtige Rolle, da kein Geheimnis benötigt wird um einen Teilnehmer zu authentifizieren. Dabei können sich Teilnehmer durch

das Wissen oder den Besitz eines Geheimnisses (Passwort, Zertifikat, Schlüssel) authentifizieren. [Beutelspacher, Schwenk und Wolfenstetter 2015]

Nur wenn beide Eigenschaften gegeben sind ist eine Übertragung von Daten als sicher anzusehen. Falls die Geheimhaltung fehlt, kann der Inhalt durch Sniffing mitgelesen werden. Falls die Authentifikation der Teilnehmer fehlt, können sich Unbeteiligte als ëchte"Teilnehmer ausgeben und somit die Daten an ihrem Endpunkt entschlüsseln.

**Verschlüsselungsverfahren**

**Asymmetrische Verschlüsselung**

**Hybride Verfahren**

**Angriffe**

**Known Cipher Attack**

**Known Plaintext Attack**

**Chosen Plaintext Attack**

**Chosen Cipher Attack**

## 1.2 Mathematik

Mathematische Probleme stellen die Grundlage für moderne Kryptographie.

### 1.2.1 Diskreter Logarithmus

Bei der Bestimmung des Logarithmus wird der Exponent (hier: $x$) gesucht, welcher mit einer bekannten Zahl als Basis $z$, eine weitere bekannte Zahl $y$ ergibt.

$$z^x = y \tag{1.1}$$

Der diskrete Logarithmus bezieht hier auf die Berechnung des Logarithmus in ein Gruppe. Diese Gruppe bildet sich aus der Rechnung mit Restklassen (modulo). Dadurch entsteht folgendes Problem, bei der die Variable $x$ gesucht ist und alle anderen Variablen bekannt sind.

$$z^x \pmod n \equiv y \tag{1.2}$$

Hierbei ist in der Notation zu beachten, dass sich durch das Rechnen auf mit einer Gruppe, Äquivalenzklassen ($\equiv$) bilden. Diese entsprechen den Restklassen des Rechnen mit Modulo. $n$ ist die Mächtigkeit der Aquivalenzklassen.

Die Bestimmung von $x$ in 1.2 wird als Problem des diskreten Logarithmus bezeichnet. Mit der Komplexität wird sich in den Grundlagen der Komplexitätstheorie beschäftigt.

Dabei ist die Umkehrfunktion, des diskreten Logarithmus $f(x)$ 1.2, mathematisch einfach zu berechnen. Diese Umkehrfunktion entspricht der diskreten Exponentialfunktion:

$$f^{-1}(x) = z^x \pmod n \equiv y \tag{1.3}$$

Hierbei sind $z, x, n$ gegeben und $y$ gesucht.

### 1.2.2 Faktorisierung

### 1.2.3 Effiziente Berechnung der diskreten Exponentialfunktion

In der Kryptographie werden große Zahlen genutzt, um die Sicherheit der verwendeten Algorithmen zu gewährleisten. Hierfür wird als Beispiel angenommen, dass als Basis $z$ eine 256-bit Lange Zahl hoch einem 300-bit langem Exponenten $x$ genommen werden soll. Hierbei ist $n$ 1024-bit lang.

Wenn mann nun $z$ in Byte berechnet wäre dies eine 32 Byte lange Zahl.

$x$ entspricht einer ungefähr 90. stelligen Zahl.

$$z^{10^{90}} \pmod{n} \equiv y \tag{1.4}$$

Eine numerische Berechnung von $z^{10^{90}}$ ist aufgrund von begrenzten Ressourcen nicht möglich.

Jedoch kann man sich die diskrete Eigenschaft dieser Problems sich zu nutzte machen. Hierfür können Verfahren, wie Square-and-Multiply zusammen mit der Restklassenberechnung genutzt werden. Dadurch lassen sich auch großzahlige Exponenten berechnen. Hierfür soll ein einfaches Beispiel gegeben werden:

$$37^{52} \pmod{128} \equiv y \tag{1.5}$$

Bei Betrachtung der Äquivalenzgleichung fällt auf, dass $37^{52}$ eine große Zahl ergibt. Jedoch wird diese Zahl noch $x \pmod 1)28$ gerechnet. Dadurch liegt das Ergebnis in einem Zahlenraum von:

$$y \in \mathbb{N} \mid 0 \leq y < 128 \tag{1.6}$$

Auf Grundlage der Potenzgesetze wird $37^{52}$ nun zerlegt.

$$\begin{aligned} 52 &= 32 + 16 + 4 = 2^5 + 2^4 + 2^2 \\ 37^{52} \pmod{128} &\equiv 37^{2^5} * 37^{2^4} * 37^{2^2} \\ \equiv 37^{2^5} \pmod{128} * 37^{2^4} \pmod{128} &* 37^{2^2} \pmod{128} \end{aligned} \tag{1.7}$$

Die einzelnen Bestandteile werden dann iterativ berechnet und durch Multiplikation zusammengefasst (siehe 1.7). Dies wird als Square-and-Multiply-Verfahren bezeichnet.

$$\begin{aligned} 37^{2^2} \pmod{128} &\equiv (37^{2^1} \pmod{128})^2 \\ 37^{2^3} \pmod{128} &\equiv (37^{2^2} \pmod{128})^2 \\ 37^{2^4} \pmod{128} &\equiv (37^{2^3} \pmod{128})^2 \\ 37^{2^5} \pmod{128} &\equiv (37^{2^4} \pmod{128})^2 \end{aligned} \tag{1.8}$$

**Allgemein**

Gegeben mit gesucht $y$:

$$z^x \pmod{n} \equiv y \tag{1.9}$$

Zerlegung von $x$ eine Summe von Zweierpotenzen:

$$x = 2^0 + 2^1 + 2^2 + ... \tag{1.10}$$

Dabei bilden die binären Logarithmen der einzelnen Zweierpotenzen die Menge $\mathbb{K}$.

Berechnung der einzelnen Faktoren durch iteratives Square-and-Multiply-Verfahren. Dies wird bis $f(max(\mathbb{K}))$ berechnet. $max(\mathbb{K})$ steht hier für das Element von $\mathbb{K}$, mit dem größten Wert.

$$f(i+1) = f(i)^2 \pmod{n} \mid f(1) = z^1 \pmod{n} \tag{1.11}$$

Zuletzt wird das Produkt, aller Ergebnisse von $f(x)$ für die Elemente der Menge $\mathbb{K}$, gebildet. Dabei gilt:

$$\prod_{k \in \mathbb{K}} f(k) \equiv z^x \pmod{n} \equiv y \tag{1.12}$$

# Kapitel 2

# RSA

Rivest-Shamir-Adleman (RSA) ist ein Algorithmus, welcher zur Klasse der Public-Key-Algorithmen gehört. Der Algorithmus wurde von R. Rivest, A. Shamir und L. Adleman erfunde und trägt deshalb ein Anagram Ihrer Namen.

## 2.1 Sicherheit von RSA

Die Sicherheit des RSA-Algorithmus basiert auf zwei mathematischen Problemen, welche unter Aufwand endlicher Ressourcen, nicht gelöst werden können. Hierbei wird sich sowohl auf RSA-gestützte Verschlüsselungs- und Signaturverfahren bezogen. Diese zwei Probleme sind:

- Faktorisierung einer bekannten Zahl, welche das Produkt zweier großer Primzahlen ist. Im Kontext von RSA ist diese Zahl $n$.
- Bestimmung des diskreten Logarithmus. Bei RSA wäre dies die Bestimmung von

$$d \mid m^d \equiv c \pmod{n}. \tag{2.1}$$

Für die Sicherheit der Public-Key-Verschlüsselung von RSA, spielt Unberechenbarkeit der Faktorisierung die Hauptrolle. Falls mit RSA signiert werden soll, ist zusätzlich die Unberechenbarkeit des diskreten Logarithmus wichtig. Ansonsten könnte der private und geheime Schlüssel abgeleitet werden.

# Literatur

Beutelspacher, Albrecht, Jörg Schwenk und Klaus-Dieter Wolfenstetter [2015]. *Moderne Verfahren der Kryptographie*. springer [siehe S. 7, 8].