Vorlesungsmodul Sicherheit in der Informationstechnik
- VorlMod SichInf -

Matthias Ansorg

13. Oktober 2004 bis 26. März 2005

Studentische Mitschrift zur Vorlesung Sicherheit in der Informationstechnik bei Prof. Dr. Wolfgang Schmitt (Wintersemester 2004/2005) im Studiengang Informatik an der Fachhochschule Gießen-Friedberg. Die Veranstaltung besteht aus 2 SWS Vorlesung und 2 SWS Übungen .

- **Bezugsquelle:** Die vorliegende studentische Mitschrift steht im Internet zum Download bereit. Quelle: Persönliche Homepage Matthias Ansorg http://matthias.ansorgs.de/.
- **Lizenz:** Diese studentische Mitschrift ist public domain, darf also ohne Einschränkungen oder Quellenangabe für jeden beliebigen Zweck benutzt werden, kommerziell und nichtkommerziell; jedoch enthält sie keinerlei Garantien für Richtigkeit oder Eignung oder sonst irgendetwas, weder explizit noch implizit. Das Risiko der Nutzung dieser studentischen Mitschrift liegt allein beim Nutzer selbst. Einschränkend sind außerdem die Urheberrechte der angegebenen Quellen zu beachten.
- **Korrekturen und Feedback:** Fehler zur Verbesserung in zukünftigen Versionen, sonstige Verbesserungsvorschläge und Wünsche bitte dem Autor per e-mail mitteilen: Matthias Ansorg <mailto:matthias@ansorgs.de>.
- **Format:** Die vorliegende studentische Mitschrift wurde mit dem Programm LyX (graphisches Frontend zu LaTeX) unter Linux geschrieben und mit pdfLaTeXals pdf-Datei erstellt. Grafiken wurden mit dem Programm xfig unter Linux erstellt und als pdf-Dateien exportiert.
- **Dozent:** Prof. Dr. Wolfgang Schmitt.
- **Verwendete Quellen:** .
- **Klausur:**
  - Es gibt eine Klausur am Ende des Semesters. Ein Student hält auch ein Referat (Ausnahme) in 2005-01 zum Thema »Sicherheit im WLAN«.
  - Die Klausur richtet sich nach den beiden Klausuren, die Prof. Dr. Schmitt in [2] zur Verfügung stellt. Zusätzlich kommt jedoch das Thema »Firewall« hinzu.
  - Man kann auch Sitzscheine erhalten: 40% der Punkte in der Klausur oder Anwesenheit mit Anwesenheitsliste.

Inhaltsverzeichnis

1 Übersicht 5

I Symmetrische Chiffren - Theorie und Anwendung 7

2 Mathematische Grundlagen 9
2.1 Grundlagen . . . 9
2.2 Modulare Arithmetik . . . 9

3 Monoalphabetische Chiffren und Grundbegriffe 11
3.1 Übungsaufgaben . . . 11
3.1.1 Aufgabe 1 . . . 11
3.1.2 Aufgabe 2 . . . 11

4 Polyalphabetische Chiffren 15

5 Komposition von Verfahrensklassen 17

6 Beispiele aus der Praxis 19

II Grundlegende Verfahren und Protokolle 21

7 Mathematische Grundlagen und Begriffe 23

8 Chipkarten 25

9 Verschlüsselung mit öffentlichen Schlüsseln 27

10 Schlüsseltausch und Schlüsselvereinbarung 29

11 Integrität und Authentizität 31

12 Beispiele aus der Praxis 33

III Zugriffskontrolle 35

13 Benutzer- und Systembestimmte Zugriffskontrolle 37

14 Rollenbasierte Zugriffskontrolle **39**

15 Firewalls **41**

16 Beispiele aus der Praxis **43**

Kapitel 1

Übersicht

Während die Veranstaltung »Datenschutz und Datensicherheit« organisatorische und technische Sicherheitsdienste beinhaltete, geht es hier um die Sicherheitsmechanismen mit denen diese Dienste implementiert werden. Dabei werden jedoch nur die algorithmischen Prinzipien behandelt, nicht die Details ihrer Implementierung. Inhaltsübersicht:

- Symmetrische Chiffren - Theorie und Anwendung
  Dieses Semester nicht mehr derart ausführlich wie in der Vergangenheit.
  - Mathematische Grundlagen
  - Monoalphabetische Chiffren und Grundbegriffe
  - Polyalphabetische Chiffren
  - Komposition von Verfahrensklassen
  - Beispiele aus der Praxis
- Grundlegende Verfahren und Protokolle
  - Mathematische Grundlagen und Begriffe
  - Chipkarten
  - Verschlüsselung mit öffentlichen Schlüsseln
  - Schlüsseltausch und Schlüsselvereinbarung
  - Integrität und Authentizität
  - Beispiele aus der Praxis (AES; Sicherheitsprotokolle (sofern Zeit bleibt; diese Protokolle, z.B. ssh, sind dann Anwendungen der bisher behandelten Mechanismen.)
- Zugriffskontrolle
  Evtl. bleibt keine Zeit für diesen Teil.
  - Grundbegriffe
  - Benutzer- und Systembestimmte Zugriffskontrolle
  - Rollenbasierte Zugriffskontrolle
  - Firewalls
  - Beispiele aus der Praxis (Mechnismen der Zugriffskontrolle auf Dateien; Sicherheit im WLAN)

Teil I

Symmetrische Chiffren - Theorie und Anwendung

Kapitel 2

Mathematische Grundlagen

2.1 Grundlagen

Symmetrische Verfahren zeichnen sich dadurch aus, dass für Verschlüsselungslgorithmus e (»encryption«) und Entschlüsselungsalgorithmus d (»decryption«) derselbe Parameter k (»key«) verwendet wird. Wenn m (»message«) der Klartext ist, gilt dann:

$$d_k\left(e_k\left(m\right)\right) = m$$

Der Geheimtext $c = e_k\left(m\right)$ (»chiffre«) wird auch als Chiffre bezeichnet. Bei symmetrischen Verfahren benötigt man einen sicheren Nachrichtenkanal zur Schlüsselverteilung. Das ist oft problematisch: denn wenn schon ein sicherer Kanal zur Verfügung steht, warum übermittelt man nicht direkt den Klartext darüber? Meist deshalb, weil es einfacher ist, symmetrische Schlüssel darüber zu übermitteln: sie sind kurz und können auf Vorrat übermittelt werden, wie im diplomatischen Dienst angewandt.

Im weiteren Verlauf dieses Dokumentes wird Klartext stets in Kleinbuchstaben, Geheimtext in Großbuchstaben geschrieben. Diese Konvention besteht auch in der Literatur.

2.2 Modulare Arithmetik

Zwei Zahlen a, b sind kongruent zueinander, wenn sie bei Division $mod\, n$ den gleichen Rest ergeben:

$$\begin{aligned} a &\equiv b\,(mod\, n) \\ \Leftrightarrow a\, mod\, n &= b\, mod\, n \\ \Leftrightarrow & \end{aligned}$$

Kapitel 3

Monoalphabetische Chiffren und Grundbegriffe

Monoalphabetische Chiffren haben nur eine Regel, um ein Zeichen der Nachricht m auf ein Zeichen des Geheimtextes c abzubilden.

3.1 Übungsaufgaben

3.1.1 Aufgabe 1

Von welchem Typ ist der Verschlüsselungsalgorithmus? Transpositionschiffre. Denn die Buchstaben bleiben was sie sind, aber nicht wo sie sind: sie sind alle noch im Geheimtext zu finden, nur in anderer Reihenfolge.

Kann man durch statistische Untersuchungen eine Transpositions- von einer Substitutionschiffre unterscheiden? Ja. Bei einer Transpositionschiffre bleiben die sprachspezifischen Häufigkeiten der Einzelzeichen erhalten (Häufigkeiten sind positionsunabhängig), bei einer Substitutionschiffre erhält man durch Abbildung auf andere Einzelzeichen Häufigkeiten, die nicht mehr den sprachspezifischen Häufigkeiten entsprechen. Die Kontur des Histogramms (des »Häufigkeitsgebirges«) ändert sich nur bei Substitutionschiffren.

3.1.2 Aufgabe 2

Gesamtzahl der weißen Felder durch zeilenweise Abzählung der weißen Felder:

$$320 = 16+15+16+15+17+12+17+16+15+14+15+14+15+15+17+12+17+15+16+15+16$$

Gesamtzahl der weißen Felder durch Subtraktion der schwarzen Felder von der Gesamtzahl der Felder des Rechtecks. Die schwarzen Felder in den ersten 10 und letzten 10 Zeilen sind dabei nahezu gleich viele, da diese Bereiche bis auf eine Zeile (Unterschied: 1 schwarzes Feld) zueinander punktsymmetrisch sind. Die Zeile zwischen diesen beiden Bereichen fügt noch einmal 4 schwarze Felder hinzu.

$$320 = 19 \cdot 21 - (2 \cdot (3+4+3+4+2+7+2+3+4+5)+1+4) = 19 \cdot 21 - 79 = 399 - 79$$

Anzahlen und Häufigkeiten von Feldern mit einzelnen Zahlen:

Zahl	Anzahl	Häufigkeit	Buchstabe
1			r
2			
3			
4			
5			
6			i
7			
8			
9			
10			
11			m
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			p
23			
24			
25			
26			

Man zeichne sich ein Histogramm aus diesen Daten und vergleiche die Häufigkeiten mit denen der Zeichen der deutschen Sprache. Die Häufigkeiten werden nur ungefähr übereinstimmen: Abweichungen sind teils zufällig (ein Zahlenrätsel ist kein besonders langer Text . . .) und liegen teils daran, dass die enthaltenen Wörter willkürlich und entsprechend den Anforderungen kreuzweiser Anordnung gewählt wurden, sich also von den Wörtern unterscheiden, die in natürlicher Sprache vorkommen. So zum Beispiel werden keine Bindewörter wie »und«, »als« usw. vorkommen. Analyse:

- gegeben ist:

$$\begin{aligned} 1 &= r \\ 6 &= i \\ 11 &= m \\ 22 &= p \end{aligned}$$

- Zahen 5 und 10 haben fast gleiche Häufigkeit, d.h. es gibt keinen ausgeprägten e-Gipfel, keinen ausgeprägten n-Gipfel.

- Untersuchung von Bigrammen

– Die folgenden Vorkommen sprechen für $5 = e$:

$$\begin{aligned} \text{viermal: } 5\,6 &= 5\,i \\ \text{dreimal: } 6\,5 &= i\,5 \\ \text{siebenmal: } 5\,1 &= 5\,r \\ \text{fünfmal: } 1\,5 &= r\,5 \end{aligned}$$

– Die folgenden sehr geringen Vorkommen sprechen für $10 \neq n$:

$$\begin{aligned} \text{einmal: } 5\,10 &\neq e\,n \\ \text{zweimal: } 6\,10 &\neq i\,n \end{aligned}$$

ebenso das Auftreten von $1\,10 \neq rn$ - dasBigramm rn ist in Texten aber sehr selten.

- Vermutung: $10 = a$ oder $10 = t$. $10 = t$ scheidet aus, das z.B. eit kein eigenständiges Wort ist, jedoch eia und air. Also ist $10 = a$.
- Vermutung: $n \in \{1, 2, 4, 7\}$. $2 \neq n$, da sonst eine Folge $anaa$ im Text auftreten würde. Jedoch ist $3 = n$, da $5\,3 = en$ vierzehnmal auftritt.
- Die restlichen Buchstaben kann man analog zu obigem Verfahren oder aber durch Vermuten ganzer Wörter ermitteln.

Kapitel 4

Polyalphabetische Chiffren

Kapitel 5

Komposition von Verfahrensklassen

Kapitel 6

Beispiele aus der Praxis

Teil II

Grundlegende Verfahren und Protokolle

Kapitel 7

Mathematische Grundlagen und Begriffe

Kapitel 8

Chipkarten

Kapitel 9

Verschlüsselung mit öffentlichen Schlüsseln

Kapitel 10

Schlüsseltausch und Schlüsselvereinbarung

Kapitel 11

Integrität und Authentizität

Kapitel 12

Beispiele aus der Praxis

Teil III

Zugriffskontrolle

Kapitel 13

Benutzer- und Systembestimmte Zugriffskontrolle

Kapitel 14

Rollenbasierte Zugriffskontrolle

Kapitel 15

Firewalls

Kapitel 16

Beispiele aus der Praxis

Literaturverzeichnis

[1] Prof. Dr. Wolfgang Schmitt: Skript zur Veranstaltung Sicherheit in der Informationstechnik. Enthält den weitaus meisten Teil des Stoffes dieser Veranstaltung. Es fehlt nur der Teil zu »Zugriffskontrolle und Firewalls« - er wird entweder im Internet veröffentlicht wahrscheinlich aber an der Tafel vorgestellt. Man konnte sich in eine Liste eintragen, um dieses Skript zu erhalten. Es wird etwa 5 EUR kosten (bei 0,07 EUR pro Doppelseite).

[2] Prof. Dr. Wolfgang Schmitt: Unterlagen zur Veranstaltung Sicherheit in der Informationstechnik. Enthält eine Inhaltsübersicht dieser Veranstaltung und zwei alte Klausuren.