Computational Logic

Einführung in die Theoretische Informatik

Woche 13

Harald Zankl

Institut für Informatik @ UIBK
Wintersemester 2014/2015

Inhalte der Lehrveranstaltung

Einführung in die Logik

Syntax & Semantik der Aussagenlogik, Formales Beweisen, Konjunktive und Disjunktive Normalformen

Einführung in die Algebra

Boolesche Algebra, Universelle Algebra, Logische Schaltkreise

Einführung in die Theorie der Formalen Sprachen

Grammatiken und Formale Sprachen, Reguläre Sprachen, Kontextfreie Sprachen

Einführung in die Berechenbarkeitstheorie

Algorithmisch unlösbare Probleme, Turing Maschinen, Registermaschinen

Einführung in die Programmverifikation

Prinzipien der Analyse von Programmen, Verifikation nach Hoare, Verschlüsselung und Sicherheit

Zusammenfassung der letzten LV

Definition

Die Regeln des Hoare-Kalkül sind wie folgt definiert:

$$\frac{}{\{Q\{x \mapsto t\}\}\ x := t\ \{Q\}}\ [z] \qquad \frac{\{Q'\}\ P\ \{R'\}}{\{Q\}\ P\ \{R\}}\ [a], Q \models Q', R' \models R$$

$$\frac{\{Q\}\ P_1\ \{R\} \quad \{R\}\ P_2\ \{S\}}{\{Q\}\ P_1; P_2\ \{S\}}\ [s] \qquad \frac{\{I \wedge B\}\ P\ \{I\}}{\{I\}\ \text{while } B \text{ do } P \text{ end } \{I \wedge \neg B\}}\ [w]$$

Lemma

Ist ein Hoare-Tripel in diesem Kalkül ableitbar, dann ist es wahr.

Pressestimmen ①

> *Präsident Barack Obama hat am Wochenende klargestellt: Die US-Geheimdienste werden weiterhin Daten in aller Welt sammeln, auch in Deutschland. Seiner Ansicht nach benötigen die USA die digitalen Ausspähungen zur „Wahrung der nationalen Sicherheit". [...] Die „NSA-Affäre" is die schwerste Krise im deutsch-amerikanischen Verhältnis seit dem Konflikt zwischen Bundeskanzler Gerhard Schröder und Präsident George W. Bush über die deutsche Rolle im Irak-Krieg 2003.*

Pressestimmen ②

> *Die amerikanischen Internet-Unternehmen, die den Weltmarkt dominieren sind Teil des Problems: Sie dienen nicht ihren eigenen wirtschaftlichen Interessen, sondern offenbar auch nachrichtendienstlichen und militärischen*

Dieter Heumann, SZ, 23.1.2014

Pressestimmen ③

Unabhängige US-Kommission hält NSA-Spähaktionen für illegal
Nutzlos im Kampf gegen den Terrorismus und eine Bedrohung für die Bürgerrechte: Eine Kommission, die die US-Regierung berät, übt ungewöhnlich heftige Kritik an der Vorratsdatenspeicherung durch die NSA. Sie fordert, die Abhöraktionen vollständig zu stoppen.

SZ online, 23.1. 2014

Definition

Wer oder was ist die NSA? NSA steht für National Security Agency, dem größten Auslandsgeheimdienst der USA, dessen Aufgabe die Entschlüsselung und Auswertung elektronischer Kommunikation ist.

Verschlüsselung und Entschlüsselung

Kryptographie

- Nachrichten werden seit sehr, sehr langer Zeit verschlüsselt. Beschreibung erster Geheimschriften durch Herodot (400 v. Chr.)
- Kryptographie bezeichnet die Verschlüsselung und Entschlüsselung von Nachrichten, im Gegensatz zur Steganographie
- Zwei Arten der Kryptographie
  1. Transposition
     Die Buchstaben einer Nachricht werden vertauscht.
  2. Substitution
     Die Buchstaben einer Nachricht werden ersetzt.

Beispiel

Ein antikes Beispiel für Transposition ist die von Sparta verwendete *scytale* (500 n. Chr.); die *scytale* ist ein Holzstab um den ein Lederband gewickelt wird.

Beispiel

Substitutionsschlüssel wurden von Julius Cäsar in den Gallischen Kriegen beschrieben: Römische Buchstaben wurden durch griechische Buchstaben ersetzt.

Definition

- Die orginale Nachricht wird Klartext, die verschlüsselt Nachricht wird Geheimtext genannt.
- Ein Verschiebechiffre ersetzt jeden Buchstaben des Klartexts im Geheimtext mit einem um n Buchstaben verschobenen Buchstaben.
- Ein Verschiebechiffre ist eine Operation auf einen Restklassenring.

Beispiel (Verschiebechiffre)

I	N	F	O	R	M	A	T	I	K	$(n = 0)$
K	P	H	Q	T	O	C	V	K	M	$(n = 2)$
A	F	X	G	J	E	S	L	A	C	$(n = 18)$

Algorithmus und Schlüssel

Die Verallgemeinerung des Verschiebechiffre verwendet eine beliebige Permutation der Klarbuchstaben anhand eines Schlüssels

Beispiel (Verschiebechiffre mit Schlüssel)

Klartext:	I	N	F	O	R	M	A	T	I	K
Schlüssel:	C	O	D	E	C	O	D	E	C	O
Geheimtext:	L	C	J	T	U	B	E	Y	L	Z

Kryptoanalyse

Definition

- Als Kryptoanalyse bezeichnet man Techniken zur Entschlüsselung des Geheimtexts ohne Wissen des Schlüssels.
- Die Kryptoanalyse basiert auf mathematischen, statistischen und linguistischen Methoden.
- Die Frequenzanalyse verwendet die Häufigkeit von Buchstaben in einem Alphabet.

Beispiel

Häufige Buchstaben in Englisch

a	8.2
b	1.5
c	2.8
d	4.3

e	12.7
f	2.2
g	2.0
...	

Le Chiffre Indéchiffrable

Definition

Die bis jetzt betrachteten Verschlüsselungen sind monoalphabetische Substitutionsschlüssel, die bis in die Renaissance verwendet wurden, allerdings (fast) machtlos gegen die Angriffe der Frequenzanalyse waren.

Beispiel

König Philip II von Spanien verlangte, dass der französische Kryptoanalyst Francois Viète aufgrund eines angeblichen Paktes mit dem Teufel verurteilt werden sollte, da Viète problemlos die spanischen Nachrichten lesen konnte ...

Definition

Die Vigenère Verschlüsselung verwendet statt einem Alphabet für die Verschlüsselung soviele Geheimalphabete wie Buchstaben.

Vigenère Verschlüsselung

- Für einen deutschen Klartext werden 30 Geheimalphabete verwendet
- Jeder Buchstabe wird in einem anderen Alphabet verschlüsselt
- Schlüsselwort wird verwendet, um zu bestimmen wie welcher Buchstabe verschlüsselt wird
- Frequenzanalyse ist machtlos, da die gleiche Verschlüsselung verschiedene Buchstaben bedeuten kann

Babbage gegen Vigenère

- Charles Babbage (1791 - 1871, UK) bekannt für die „Analytical Machine“
- Wiederholungen im Geheimtext lassen auf die Länge des Schlüsselwortes schließen
- Dadurch kann eine Vigenère Verschlüsselung nach mehreren Schritten auf eine monoalphabetische Verschlüsselung zurückgeführt werden

Eine wirklich sichere Verschlüsselung

Definition

- Das Einmalschlüssel-Verfahren basiert auf der Verwendung von randomisierten Schlüsseln.
- Ein Schlüssel wird nur einmal verwendet.
- Ein Schlüssel muss also mindestens so lang wie die Nachricht sein.
- Der Schlüssel ist Sender sowie Empfänger bekannt.
- Jede Nachricht wird mit der Vigenère Verschlüsselung kodiert.

Absolut sicher (und absolut nutzlos?)

- Um die Methode von Babbage anzuwenden braucht es Wiederholungen, die in diesem Fall nicht gegeben sind.
- Andererseits müssen die Schlüssel irgendwie generiert und ausgetauscht werden.

Mechanisierung der Verschlüsselung und Entschlüsselung

Enigma

- Mechanisierung der Verschlüsselung als Antwort auf die Entschlüsselung des Vigenère Codes
- Die Entschlüsselung des Vigenère Codes ist zeitintensiv und hängt von der Länge des Schlüssels ab
- mechanische bzw. elektrische Kodiermaschinen erlauben lange Schlüssel
- Enigma wurde von Arthur Scherbius entwickelt und schlußendlich an das deutsche Militär verkauft
- Hauptakteure der Entschlüssung: Rejewski & Turing

Alice und Bob: der Anfang

Austausch von Schlüsseln

- Wie sollen Alice und Bob sicher miteinander kommunizieren ohne gemeinsamen Schlüssel?
- Wie können sie einen Schlüssel austauschen, ohne sich zu treffen?
- Das „key-distribution problem“ galt lange Zeit als unlösbar.

Neuere Methoden

Methode	vorgestellt	geknackt
DES	1975	1998 (56h, Schlüssellänge 56Bit)
		1999 (22h, Schlüssellänge 56Bit)
RSA	1977 (1983 Patent)	?
BB84	1984 (2004 realisiert)	beweisbar sicher

Eine unendliche Geschichte?

- *code maker* vs. *code breaker*
- Quantum Verschlüsselung ist die erste praktische Realisierung des Einmalschlüssel-Verfahrens
- Mehrheit der Erfindungen in der Kryptographie und Kryptoanalyse sind geheim
  - die Existenz von Einwegfunktionen wurde von Ronald Rivest, Adi Shamir und Leonard Adleman nachgewiesen (RSA Verschlüsselung)
  - allerdings wurde ihre Erfindung von Clifford Cocks und James Ellis vom Goverment Communication Center (UK) vorweggenommen

Klausuren

Erste Klausur

- Bitte registrieren Sie sich online für die Klausur
- 2. Feber 2015, 12:15-14:00, HS B
- Prüfungsstoff ist (fast) alles

Zweite Klausur

- 27. Feber 2015, 12:00-13:45, HSB 2
- Prüfungsstoff ist (fast) alles

Dritte Klausur

- Oktober 2015
- Prüfungsstoff ist (fast) alles

Vielen Dank

für Ihre Aufmerksamkeit!