ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
Departement Informatik

Open Class – Sieben Wunder der Informatik

Prof. Dr. Juraj Hromkovič

Übungsaufgaben – Blatt 6

Zürich, 7. Dezember 2005

Zusammenfassung und Aufgaben

Eine Zusammenfassung des Vortrages und eine Einleitung in die Kryptographie finden Sie in dem Buch

> Juraj Hromkovič: *Theoretische Informatik.*
> Teubner-Verlag (Februar 2004), ISBN 3-519-10332-X,
> Seiten 299–316.

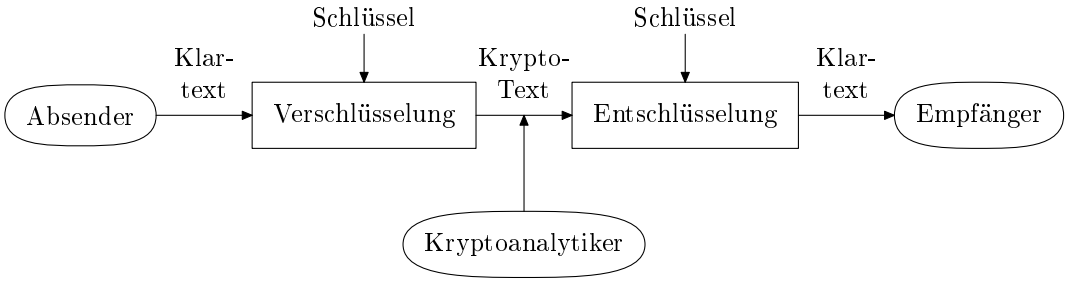
Deshalb präsentieren wir hier nur eine kurze Zusammenfassung.

Definitionen

Kryptologie bezeichnete ursprünglich die Lehre von den Geheimsprachen.

Kryptographie ist die Wissenschaft von der Entwicklung von Kryptosystemen.

Kryptoanalyse ist die Kunst, Kryptosysteme zu brechen.



Klartext heisst der normale Text, den ein *Absender* an einen *Empfänger* schicken möchte.

Verschlüsselung (Chiffrierung) bezeichnet den Prozess der Umwandlung des Klartextes in einen in einer geheimen Sprache formulierten *Krypto-Text.*

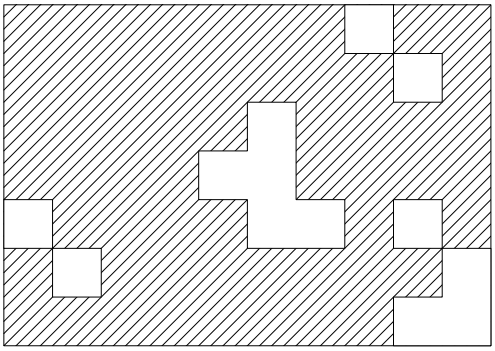
Schlüssel ist die Bezeichnung für ein gemeinsames Geheimnis des Senders und des Empfängers; er wird verwendet, um die Verschlüsselung und auch die Entschlüsselung durchzuführen.

Der Krypto-Text wird über einen unsicheren Kanal an den Empfänger geschickt. Der Empfänger benutzt den Schlüssel, um zu *entschlüsseln* (zu *dechiffrieren*), d. h. um aus dem Krypto-Text den ursprünglichen Klartext wiederherzustellen.

Beispiele von Krypto-Systemen

Caesar Verschiebung der Buchstaben in einem Alphabet

Richelieu



I		L	O	V	E		Y	O	U
I		H	A	V	E		Y	O	U
D	E	E	P		U	N	D	E	R
M	Y		S	K	I	N		M	Y
L	O	V	E		L	A	S	T	S
F	O	R	E	V	E	R		I	N
H	Y	P	E	R	S	P	A	C	E

Aufgabe 17

Entwerfen Sie ein Krypto-System, in dem die Anzahl der möglichen Schlüssel mindestens 10^{77} ist (also grösser als die Anzahl der Protonen im Universum). Dabei soll die Länge der Schlüssel höchstens einige hundert Symbole betragen. **10 Punkte**

Auf dem Weg vom Experimentieren zu einer Wissenschaft

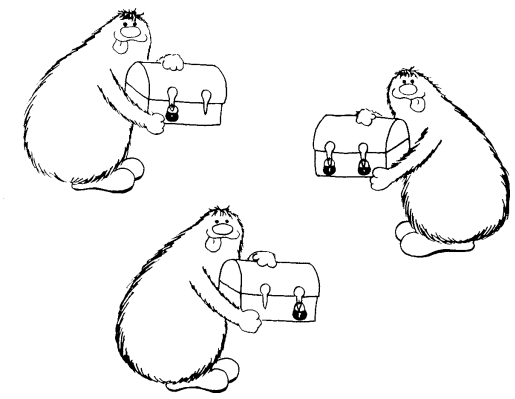
Forderungen:

1. Chiffrierung und Dechiffrierung müssen effizient durchführbar sein.
2. Das System soll *sicher* sein, d. h. ohne den geheimen Schlüssel schwer zu knacken.

Probleme:

a) Was bedeutet sicher? Viele mögliche Schlüssel, zum Beispiel mehr als Protonen im Universum?

b) Zuerst muss der geheime Schlüssel ausgetauscht werden. Wie kann man dies sicher durchführen?



Dies können wir auch algorithmisch umsetzen: Wir definieren die XOR-Funktion $\oplus$ (exclusive OR) durch

$$0 \oplus 0 = 0 \quad , \qquad 0 \oplus 1 = 1 \quad ,$$
$$1 \oplus 0 = 1 \qquad \text{und} \qquad 1 \oplus 1 = 0 \quad .$$

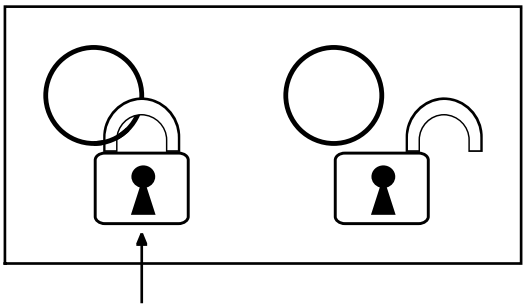
Sei der Klartext dargestellt als eine Folge von Bits, z. B. 101011. Dann verwenden wir als Schlüssel auch eine Folge von Bits, z. B. 011011 und führen die Verschlüsselung wie folgt durch:

	Klartext	101011
$\oplus$	Schlüssel	011011
	Krypto-Text	110000

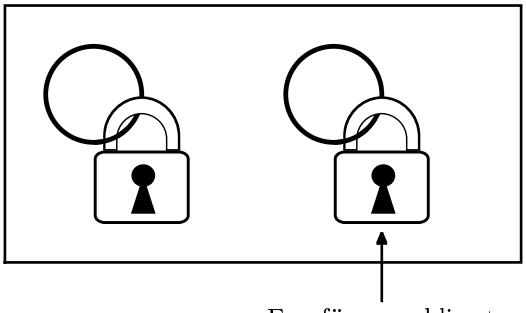
Eine 1 im Schlüssel bedeutet, das Bit in sein Komplement umzudrehen (also 1 auf 0 abzubilden und 0 auf 1), und eine 0 im Schlüssel bedeutet, das Bit unverändert zu lassen.
Man kann nun den Klartext aus dem Krypto-Text folgendermassen zurückgewinnen:

	Krypto-Text	110000
$\oplus$	Schlüssel	011011
	Klartext	101011

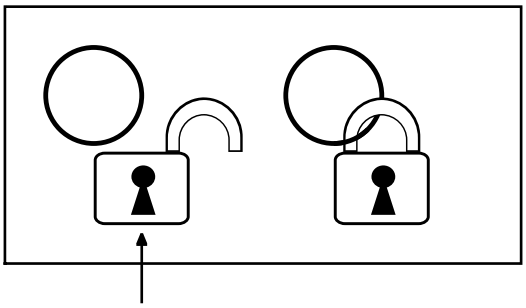
Dies funktioniert, weil $a \oplus b = b \oplus a$ und $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ gelten. Man kann also die Argumente der $\oplus$-Operation beliebig vertauschen. Weiter gilt $a \oplus a = 0$ und $a \oplus 0 = a$. Damit entspricht das Ergebnis zweimaligen Anwendens eines Schlüssels auf einen Text wieder dem Text, auf den überhaupt kein Schlüssel angewendet wurde.



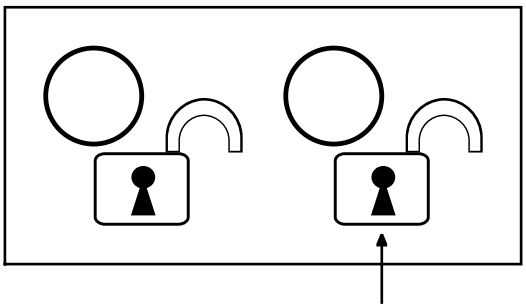
	Klartext	101011
$\oplus$	Absender-Schlüssel	011011
	Erster Krypto-Text	110000



	Erster Krypto-Text	110000
$\oplus$	Empfänger-Schlüssel	101010
	Zweiter Krypto-Text	011010



	Zweiter Krypto-Text	011010
$\oplus$	Absender-Schlüssel	011011
	Dritter Krypto-Text	000001



	Dritter Krypto-Text	000001
$\oplus$	Empfänger-Schlüssel	101010
	Klartext	101011

Aufgabe 18

Ein Absender will einen Klartext an zwei Empfänger schicken. Dies soll so realisiert werden, dass der gesendete Krypto-Text nur dann dechiffrierbar ist, wenn sich beide Empfänger

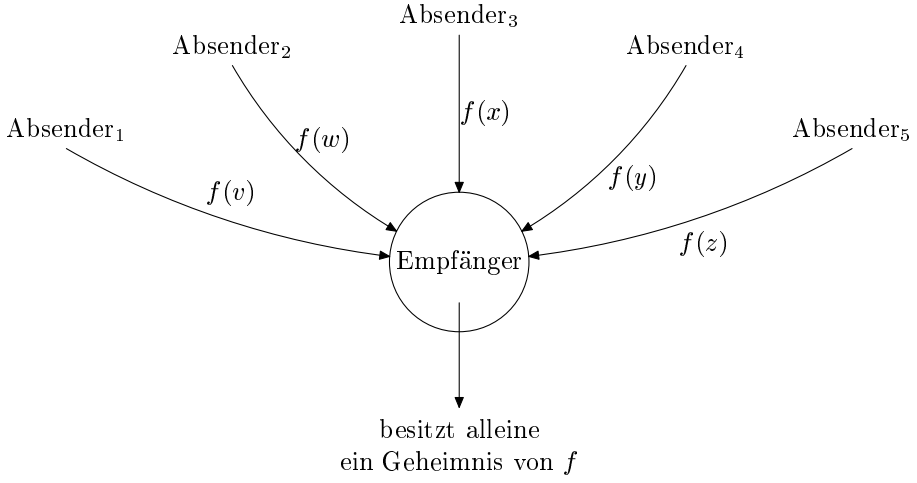
zusammentun. Die Aufgabe des Absenders ist es, den Schlüssel so auf beide Empfänger zu verteilen, dass keiner von ihnen ohne die Hilfe des anderen auch nur einen Bruchteil des Textes dechiffrieren kann. Wie kann der Absender dies erreichen?
Hinweis: Beachten Sie, dass dieses Ziel nicht erreicht wird, wenn der Absender die erste Hälfte des Schlüssels dem ersten Empfänger und die zweite Hälfte dem anderen Empfänger gibt. **10 Punkte**

Das oben genannte Verfahren war bei seiner Vorstellung verblüffend, jedoch funktioniert es nicht, um sich gegen einen aktiven Gegner zu schützen, der sich als (rechtmässiger) Empfänger ausgeben kann, wobei er jedoch seinen eigenen Schlüssel ins Protokoll einsetzt.
Die Informatik hat der Kryptologie eine wissenschaftliche Basis gegeben, anhand der der Begriff der *Sicherheit* eines Krypto-Systems definiert wird: Ein Krypto-System ist *sicher,* wenn es keinen effizienten randomisierten Algorithmus gibt, der aus einem Krypto-Text den Klartext berechnen kann.
Auf der Komplexitätstheorie basieren wesentliche Entwicklungen in der Kryptographie im Zusammenhang mit dem Problem des sicheren Austauschs eines Schlüssels.

Einweg-Funktionen

Als *Einweg-Funktion* bezeichnen wir eine Funktion f mit diesen Eigenschaften:

1. f ist effizient berechenbar und kann zur Verschlüsselung verwendet werden.
2. Die inverse Funktion f^{-1} ist nicht effizient berechenbar; es gibt also keinen effizienten Algorithmus, der aus einem Wert $f(x)$ das Argument x berechnen kann. Damit ist $f(x)$ als Krypto-Text sicher.
3. Wenn man ein Geheimnis kennt, kann man aus $f(x)$ das Argument x, also den Klartext, effizient berechnen.



Ein Kandidat für eine Einweg-Funktion Es sei $n = p \cdot q$ für zwei grosse Primzahlen p und q. Einen Klartext x chiffrieren wir vermöge

$$f_n(x) := x^2 \bmod n \quad .$$

Es ist kein effizienter Algorithmus bekannt, der für eine gegebene Zahl m ein x findet, so dass $x^2 \bmod n = m$, es sei denn, man kennt die Zerlegung $n = p \cdot q$. Man wird also p und q geheim halten, denn kennt man p oder q, so kann man aus m ein passendes x effizient bestimmen.
Jeder Teilnehmer A kann nun seine Einweg-Funktion f_{n_A} in ein öffentliches Verzeichnis (wie in ein Telefonbuch) aufnehmen lassen, so dass ein jeder f_{n_A} benutzen darf, um Teilnehmer A geheime Nachrichten zuzuschicken. Denn nur A kann f_n^{-1} effizient berechnen. Deswegen nennt man solche Systeme *Public-Key-Krypto-Systeme* (Krypto-Systeme mit öffentlichen Schlüsseln).

Bonus-Aufgabe 6

Betrachten Sie ein System, in dem jeder Teilnehmer eine eigene Einweg-Funktion bestimmt hat und in dem diese Funktionen öffentlich verzeichnet sind. Ein Teilnehmer A möchte sein Einverständnis mit einem Text T unmissverständlich kundtun. Ihm ist erlaubt, an alle Teilnehmer Nachrichten zu versenden. Wie kann er dabei folgende Dinge garantieren?

(i) Jeder Teilnehmer des Systems kann sich effizient davon überzeugen, dass A wirklich ihr/sein Einverständnis abgegeben hat.

(ii) Kein Teilnehmer (ausser A selbst) kann sich als A ausgeben, d. h. wenn A nicht einverstanden mit einem Text ist, so kann dies auch kein Teilnehmer behaupten (oder niemand würde es glauben).

10 Bonus-Punkte

Ihre Lösungen zu den Aufgaben können Sie entweder persönlich bei der Open-Class-Veranstaltung am 14. Dezember 2005 abgeben oder bis zum 14. Dezember per E-Mail (möglichst als PDF-Datei) an `hjb@inf.ethz.ch` oder per Post an folgende Adresse schicken:

Dr. Hans-Joachim Böckenhauer
Informationstechnologie und Ausbildung
ETH Zentrum CAB F 11.1
Universitätsstrasse 6
8092 Zürich

Bitte vergessen Sie nicht, Ihre Lösung mit Ihrem Namen und Ihrer E-Mail-Adresse zu versehen.
Falls Ihre Lösung uns bis zum 12. Dezember 2005 erreicht, können Sie die korrigierte Lösung bereits in der Veranstaltung am 14. Dezember abholen (sonst bei der nächsten Veranstaltung).