



1. Übungsblatt

Ziel dieser Übung ist die Wiederholung der wichtigsten Begriffe und Algorithmen aus Trusted Systems. Besonders für Studenten die Trusted Systems nicht gehört haben, werden in der 1. Übungswoche zusätzliche Sprechstunden angeboten, die sie auf

http://www.cdc.informatik.tu-darmstadt.de/lehre/WS08_09/vorlesung/Kryptographie_I.html

finden. Die Vorlesungsunterlagen zu Trusted Systems finden sie auf

<http://www.informatik.tu-darmstadt.de/trustedsystems/>.

Anmeldeschluss für die Übungen ist Freitag (17.10.2009) um 23:59.

GRUPPENÜBUNGEN

G1 (Erweiterter Euklidischer Algorithmus).

Lies aufmerksam das Kochrezept für den Erweiterten Euklidischen Algorithmus auf der Rückseite und verstehe es.

- Berechne den $\gcd(123, 121)$ im Kopf. Benutze hierfür, daß $\gcd(a, b) = \gcd(b, a \bmod b)$ ist.
- Stelle den $\gcd(123, 121)$ als Linearkombination seiner beiden Argumente dar. Finde also $x, y \in \mathbb{Z}$, so daß die Gleichung $123x + 121y = \gcd(123, 121)$ erfüllt ist.
- Berechne nun den $\gcd(15, 10, 6)$ im Kopf.
- Stelle auch hier den $\gcd(15, 10, 6)$ als Linearkombination seiner *drei* Argumente dar. Finde also $x, y, z \in \mathbb{Z}$, so daß die Gleichung $15x + 10y + 6z = \gcd(15, 10, 6)$ erfüllt ist.
- Zu guter Letzt. Stelle den $\gcd(90, 78, 56, 34, 2)$ als Linearkombination seiner Argumente dar. Und zwar wieder im Kopf.

G2 (Verschlüsselungsmodi).

Verschlüsseln Sie den String $S = 101010101010$ in den Modi:

- ECB (Electronic Code Book Mode)
- CBC (Cipher Block Chaining Mode)
- CFB (Cipher Feedback Mode)
- OFB (Output Feedback Mode)

Eine Beschreibung der Modi finden sie in dem Trusted Systems Unterlagen (buchmann3.pdf), sowie im Buch *Einführung in die Kryptographie*.

Verwenden Sie die Permutationschiffre mit Blocklänge 3 und Schlüssel $k = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Der Initialisierungsvektor ist 000. Im OFB- und CFB-Mode verwenden Sie $r = 2$.

Wie wirken sich Bitfehler in den Chiffretextblöcken bei den einzelnen Verfahren auf die dann entschlüsselten Klartextblöcke aus?

G3 (Verschlüsselungsverfahren).

Es wird vorgeschlagen, zum verschlüsseln eines n Bit langen Strings (über dem Alphabet $\Sigma = \{0, 1\}$) mit einem n Bit langen Schlüssel K , beide als die Binärdarstellung einer natürlichen Zahl zu interpretieren, beide Zahlen $\text{mod } 2^n$ zu addieren, und dann das Ergebnis wieder als n Bit langen String darzustellen.

Bestimmen sie für dieses Verfahren:

- Den Klartextraum \mathcal{P}
- Den Chiffretextraum \mathcal{C}
- Den Schlüsselraum \mathcal{K}
- Die Menge aller Verschlüsselungsfunktionen \mathcal{E}
- Die Menge aller Entschlüsselungsfunktionen \mathcal{D}

Welche sind gleich?

G4 (Permutationschiffre).

In Trusted Systems wurde die Permutationschiffren vorgestellt.

- Zur Verbesserung der Sicherheit wird vorgeschlagen, Klartexte immer doppelt mit 2 unabhängigen Schlüsseln K_1 und K_2 zu verschlüsseln. Bewerten die diese Idee.
- Ein Nachteil der Permutationschiffre ist, dass gleiche Buchstaben im Klartext immer auf gleiche Buchstaben im Chiffretext abgebildet werden. Als Gegenmaßnahme wird vorgeschlagen, im Chiffretext immer 2 benachbarte Zeichen zu vertauschen. Hat der Chiffretext eine ungerade Anzahl von Zeichen, wird das letzte Zeichen zum Abschluss noch mit dem 1. getauscht.

In wie weit erschwert das einen Angriff auf das Verfahren?

KOCHREZEPT

Erweiterter Euklidischer Algorithmus. Der hier beschriebene Algorithmus löst Probleme der Form: Gegeben $a = 12, b = 7$ stelle den $\text{gcd}(a, b)$ als Linearkombination seiner Argumente dar. Man geht dabei wie folgt vor. Stelle diese Tabelle auf:

Iterationen:	k	0	1	2	\dots	k
Reste:	r_k	a	b	$r_2 = r_0 \bmod r_1$	\dots	$r_k = r_{k-2} \bmod r_{k-1}$
Quotienten:	q_k		$q_1 = \frac{r_0 - r_2}{r_1}$	\dots		$q_k = \frac{r_{k-1} - r_{k+1}}{r_k}$
Koeffizienten:	x_k	1	0	$x_2 = x_1 q_1 + x_0$	\dots	$x_k = x_{k-1} q_{k-1} + x_{k-2}$
	y_k	0	1	$y_2 = y_1 q_1 + y_0$	\dots	$y_k = y_{k-1} q_{k-1} + y_{k-2}$

Tabelle 1: Erweiterter Euklidischer Algorithmus — Theorie

Man wendet den Erweiterten Euklidischen Algorithmus durch das Ausfüllen der Tabelle nach den obigen Vorschriften an.

k	0	1	2	3	4	5	k	0	1	2	3	4	5
r_k	12	7	5	2	1	0	r_k	12	7	5	2	1	0
q_k		1	1	2	2		q_k		1	1	2	2	
x_k	1	0	1	1	3	7	$(-1)^k x_k$	1	-0	1	-1	3	-7
y_k	0	1	1	2	5	12	$(-1)^{k+1} y_k$	-0	1	-1	2	-5	12

Ohne Vorzeichen bei den Koeffizienten

Mit Vorzeichen bei den Koeffizienten

Der $\text{gcd}(12, 7)$ ist der letzte Rest ungleich 0, welcher $r_4 = 1$ ist. Man kann folgendes beobachten: In jeder Spalte k gilt: $r_k = (-1)^k x_k a + (-1)^{k+1} y_k b$. Der Vorfaktor (-1) folgt in den letzten beiden Zeilen einer Art Welle.

Man baut sich also erst die linke Tabelle ohne die Vorzeichen bei den Koeffizienten, und fügt dann die ‘Welle’ an (-1) sen hinzu (siehe rechts). Dann kann man die Linearkombination ablesen. Es ergibt sich für den gcd die Linearkombination $1 = 3 \cdot 12 - 5 \cdot 7$.