Sommersemester 2005

Hasso-Plattner-Institut, Universität Potsdam

Übung zur Vorlesung

Fachgebiet Internet-Technologien und -Systeme

Meinel / Kutzner

Aufgabenblatt 8
(NUR FÜR ULI-STUDENTEN)

(URL: http://www.hpi.uni-potsdam.de/index.php?id=411)

Abgabe: Mo, 13.06.2005, bis 12 Uhr MEZ (per E-Mail an mathias.kutzner@hpi.uni-potsdam.de)

Thema: Secret-Key Krypto-Systeme

Erreichbare Punkte: 10

Aufgabe 1: 10 Punkte

Machen Sie sich mit der Funktionsweise des Advanced Encryption Standard (AES) bekannt, insbesondere mit der Expansion des Schlüssels.

Gegeben ist der Schlüssel $k = 36\ 8a\ c0\ f4\ ed\ cf\ 76\ a6\ 08\ a3\ b6\ 78\ 31\ 31\ 27\ 6e$. Berechnen Sie die ersten fünf Words des expandierten Schlüssels. Geben Sie Ihren Rechenweg und alle Zwischenergebnisse an.

Hinweise:
In den folgenden Erklärungen werden hexadezimale Zahlen verwendet.

Der Algorithmus `KeyExpansion` macht aus dem Schlüssel `key`, der aus $4 \cdot Nk$ Bytes besteht, einen expandierten Schlüssel `w`, der aus $Nb \cdot (Nr+1)$ Words besteht. Je nach Schlüssellänge ist `Nk` = 4, 6 oder 8. `Nb` ist immer 4.
Zuerst werden die ersten `Nk` Words im expandierten Schlüssel `w` mit den Bytes des Schlüssels `key` gefüllt. Die Funktion `word()` schreibt die Bytes einfach hintereinander.
Wie die restlichen Words in `w` erzeugt werden, zeigt der folgenden Pseudocode.

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
      i = 0
      while (i < Nk)
            w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
            i = i+1
      end while
      i = Nk
      while (i < Nb * (Nr+1)]
            word temp = w[i-1]
            if (i mod Nk = 0)
                  temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
            else if (Nk > 6 and i mod Nk = 4)
                  temp = SubWord(temp)
            end if
            w[i] = w[i-Nk] xor temp
            i = i + 1
      end while
end
```

`Rcon[i]` repräsentiert das Word Array mit den Rundenkonstanten:

$Rcon[1] = 01000000$ $Rcon[2] = 02000000$ $Rcon[3] = 04000000$ $Rcon[4] = 08000000$
$Rcon[5] = 10000000$ $Rcon[6] = 20000000$ $Rcon[7] = 40000000$ $Rcon[8] = 80000000$
$Rcon[9] = 1b000000$ $Rcon[10] = 36000000$ $Rcon[11] = 6c000000$ $Rcon[12] = d8000000$
$Rcon[13] = ab000000$

Die Funktion `RotWord()` erhält als Eingabe ein Wort, das aus vier Bytes a_0, a_1, a_2, a_3 besteht und führt eine zyklische Permutation durch, so dass die Ausgabe a_1, a_2, a_3, a_0 ist.

Die Funktion `SubWord()` erhält als Eingabe ein Wort, das aus vier Bytes a_0, a_1, a_2, a_3 besteht. Auf jedes Byte wird die abgebildete S-Box angewendet. Ist zum Beispiel $a_0 = \{53\}$, dann ergibt sich das Ergebnis dieses Bytes aus Reihe 5 und Spalte 3 und ist somit $\{ed\}$.

		y															
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16