technische universität
dortmund

Sicherheit: Fragen und Lösungsansätze
Übung 6

Thomas Ruhroth | Dortmund
13.Nov 2012

Übung 5

- ~~Hinweise~~
- Evaluation
- Gruppenübung
- Besprechung der Abgaben

- Ziele:
  - Verschiedene Wissensblöcke in Prüfungen
  - Wissen für den Block 2
  - Aufgaben vom Typ: Anwenden

Hinweise zu Ihren Abgaben

- Stellen Sie die Lösung **präzise** und kurz dar
  - *Kurz* heißt nicht schluderig!
- Keine Email-Abgabe!
- Schreiben Sie nicht mehr Infos als nötig in die Lösungen
- Seien Sie eindeutig
- Fragen: Gerne
  - Bitte ins InPUD
- Jeder nur ein Kreuz.
- Wer seinen Zettel nicht zurückbekommen hat, sollte einen Termin mit mir machen :-)

Hinweise zu Ihren Abgaben

- ✓ Richtig (kleinere Probleme werden ignoriert)
- ~ Überwiegend Richtig
  - Ungenauigkeit
  - Unrichtigkeiten
  - Achten sie auf Unterstreichungen
- ¬ K „nicht knakig“
- NL nicht lesbar
- LB:
  - 10 … 0 (lesbar bis unleserlich)
  - Schlechter als 5: Ich musste Raten! Gefahr von Punktverlust!

HA 1.1

Key				Round 1				Round 2			
f4	5d	51	18	b3	ee	bf	a7	f7	19	a6	01
b4	9e	f4	98	6a	f4	00	98	E5	11	11	89
58	cd	5e	9c	7c	b1	ef	73	38	89	66	15
ea	a8	cf	a6	47	ef	20	86	1b	f4	d4	52

HA1.2(Key: Schlüssel)

Zustandsmatrix 1			
c1	dc	73	73
d2	e8	4f	e6
f7	9b	60	fc
d4	f8	7e	ee

Zustandsmatrix 2			
78	86	8f	8f
b5	9b	84	8e
68	14	d0	b0
48	41	f3	28

Zustandsmatrix 3			
78	86	8f	8f
9b	84	8e	b5
d0	b0	68	14
28	48	41	F3

Zustandsmatrix 4			
be	78	a5	26
16	16	71	31
20	a1	12	1c
93	35	ee	d6

Mal und Plus mal anders

$$68_{16} \circ 3_{16} = 01101000_2 \circ 0000011_2$$

$$(x^6+x^5+x^3)*(x+1)\ mod\ (x^8+x^4+x^3+x+1)$$

$$(x^7+x^6+x^4+x^6+x^5+x^3)\ mod\ (x^8+x^4+x^3+x+1)$$

$$(x^7+x^4+x^5+x^3)\ mod\ (x^8+x^4+x^3+x+1)$$

$$(x^7+x^4+x^5+x^3)$$

$$10111000_2 = B8_{16}$$

Achtung: + ist XOR!

$$x^2+x^2=0 \qquad x^2+x^2+x^2=x^2$$

Beispiel

$$8\mathrm{F} \circ 01 + 8\,E \circ 02 + 68 \circ 03 + 41 \circ 01$$

$$8\mathrm{F} + 07 + B8 + 41 = 71$$

HA 1.6 und 1.7

Zustandsmatrix 5 (Key: Round 1)			
0d	96	1a	81
7c	e2	71	a9
5c	10	fd	6f
d4	da	ce	50

Zustandsmatrix 6 (Key: Round 2)			
20	89	04	0d
7d	b2	c2	99
6c	21	2c	df
48	bc	83	da