Prvi kolokvijum iz Zaštite podataka (SI4ZP, IR4ZP) *28.03.2015.*

1. Kako se može uspostaviti međusobna komunikacija učesnika u kojoj se postiže tajnost bez prethodne razmene tajnih ključeva, a zahvaljujući postojanju javnih ključeva. Na kojim osobinama sistema sa javnim ključem je zasnovano postizanje tajnosti.
2. Koje parametre treba uzeti u obzir prilikom dizajna *Feistel* algoritma i na koji način promena svakog od parametara utiče na algoritam? Detaljno objasniti kako ovi parametri izgledaju u *DES* algoritmu.
3. Za originalnu poruku A10Ch i ključ 1F29h dati međurezultat svake operacije, kao i vrednost šifrovane poruke ako se koristi pojednostavljeni *AES* algoritam (*S-AES*). Nacrtati strukturu pojednostavljenog *AES* algoritma. Koristiti opis modifikacija u odnosu na *AES* algoritam dat u prilogu.

Napomene: Na kolokvijumu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Kolokvijum traje 90 minuta.

Prilog. Modifikacije *AES* algoritma potrebne da bi se dobio *S-AES*

Pojednostavljeni *AES* algoritam ima veličinu bloka 16 bita, veličinu ključa 16 bita i 2 iteracije. Struktura algoritma odgovara strukturi *AES128* bez iteracija od 2 do 9. Stanje je matrica veličine dva puta dva, pri čemu svako polje matrice ima veličinu 4 bita (Slika 1a). Sve operacije u algoritmu su modifikovane da rade na nivou 4-bitnih vrednosti. *S-box* tabela koja se koristi za operaciju zamene data je na slici 1b. Konstantna matrica koja se koristi kod operacije mešanja kolona data je na slici 1c.

S0,0	S0,1
S1,0	S1,1

a)

	00b	01b	10b	11b
00b	9h	4h	Ah	Bh
01b	Dh	1h	8h	5h
10b	6h	2h	0h	3h
11b	Ch	Eh	Fh	7h

b)

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$$

c)

Slika 1. Prikaz stanja (a), *S-box* tabele (b) i koeficijenata matrice za operaciju mešanja kolona (c) kod *S-AES* algoritma

Kod operacije mešanja kolona koristi se aritmetika u polju GF(2^4) po modulu x^4+x+1. U tabeli 1 prikazani su rezultati sabiranja, a u tabeli 2 rezultati množenja kod ovakve aritmetike (vrednosti su heksadecimalne).

Tabela 1. Sabiranje u polju GF(2^4) po modulu x^4+x+1

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

Tabela 2. Množenje u polju GF(2^4) po modulu x^4+x+1

·	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

Kod ekspanzije ključa konstante iteracije koje se koriste u funkciji g su: Rcon(1)=80h i Rcon(2)=30h.