ЗАШТИТА ПОДАТАКА

Симетрични алгоритми заштите

AES

Zadatak

- AES(*Advanced Encryption Standard*). Stanje zadato na Sl. 1 propustiti kroz poslednju iteraciju AES algoritma prilikom šifrovanja (nema *MixColumns* operacije), prikazati stanje nakon svake od tri operacije i stanje koje se dobija na kraju iteracije. Dati su: skraćeni sadržaj *S-box* tabele (slika 2) i ključ poslednje iteracije (*round key* – Sl. 3).

Zadatak

2A	39	45	56
BC	C4	D5	FE
25	87	64	6D
8F	F5	E6	A3

Slika 1 – stanje na ulazu poslednje AES iteracije

Zadatak

	y											
x		3	4	5	6	7	9	A	C	D	E	F
	2	26	36	3F	F7	CC	A5	E5	71	D8	31	15
	3	C3	18	96	05	9A	12	80	EB	27	B2	75
	4	1A	1B	6E	5A	A0	3B	D6	29	E3	2F	84
	5	ED	20	FC	B1	5B	CB	BE	4A	4C	58	CF
	6	FB	43	4D	33	85	F9	02	50	3C	9F	A8
	8	EC	5F	97	44	17	A7	7E	64	59	19	73
	A	0A	49	06	24	5C	D3	AC	91	95	E4	79
	B	6D	8D	D5	4E	A9	56	F4	65	7A	AE	08
	C	2E	1C	A6	B4	C6	DD	74	4B	BD	8B	8A
	D	66	48	03	F6	0E	35	57	86	C1	1D	9E
	E	11	69	D9	8E	94	1E	87	CE	55	28	DF
	F	0D	BF	E6	42	68	99	2D	B0	54	BB	16

Slika 2 – skraćeni sadržaj S-box tabele

Zadatak

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

Slika 3 – ključ poslednje iteracije

Rešenje

E5	**12**	**6E**	**B1**
65	**1C**	**03**	**BB**
3F	**17**	**43**	**3C**
73	**E6**	**8E**	**0A**

Rešenje

E5	**12**	**6E**	**B1**
1C	**03**	**BB**	**65**
43	**3C**	**3F**	**17**
0A	**73**	**E6**	**8E**

Rešenje

E5	12	6E	B1
1C	03	BB	65
43	3C	3F	17
0A	73	E6	8E

$\oplus$

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A

=

49	0B	46	E6
6B	F9	6A	39
25	E0	16	17
F9	52	A7	E4