

- (20p)** Arbitrirani digitalni potpisi. Navedite protokol kada se radi asimetrična enkripcija, a arbitar ne vidi poruku kod arbitriranog digitalnog potpisivanja.
- (20p)** Objasnite uloge autentikacionog i ticket granting servera u Kerberos sistemu. Kako se postiže da lozinka ne putuje kroz mrežu? Kako se postiže jedinstvenost lozinke za sve servise pomoću Kerberos-a?
- (20p)** Stanje zadato na slici 1 propustiti kroz poslednju iteraciju AES algoritma prilikom dešifrovanja, prikazati stanje nakon svake operacije i stanje koje se dobija na kraju iteracije. Dati su: ključ poslednje iteracije (slika 2) i sadržaj inverse S-box tabele (slika 3).

25	DA	DA	5D
F8	2C	5F	60
F9	39	86	E9
A1	6B	B4	7D

Slika 1.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	CB
2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	B6	92
5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
A	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
B	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
E	A0	E0	3B	4D	AE	2A	F5	B0	C8	EB	BB	3C	83	53	99	61
F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

Slika 3.

AA	AA	AA	AA
BB	BB	BB	BB
CC	CC	CC	CC
DD	DD	DD	DD

Slika 2.

- (25p)** Nacrtati i objasniti postupak prilikom generisanja i prilikom prijema PGP (*Pretty Good Privacy*) poruke uz ostvarivanje tajnosti i autentikacije i uz korišćenje prstenova ključeva. Zanimariti kompresiju i konverziju. Koja je uloga prstenova ključeva kod PGP protokola? Koji mehanizam se koristi za upravljanje ključevima kod PGP protokola i na koji način se koriste prstenovi ključeva, kao podrška za taj mehanizam? Kako se izračunava legitimitet ključa?