1. (K)(**10p**) Šifrovati poruku “klima je postala nepredvidiva”, koristeći svaki od sledećih kriptografskih algoritama:
   a) *Playfair* algoritam sa ključnom reči: jun,
   b) *Vigenère* algoritam sa ključnom reči: jun,
   c) *Vigenère* algoritam sa *Autokey* poboljšanjem sa ključnom reči: jun,
   d) *Row Transposition* algoritam sa ključem: 42315

   Napomena: koristiti 26 slova engleske abecede.

2. (K)(**10p**) Objasniti ulogu, osobine i zahteve kodova za autentikaciju poruka (*MAC* kodovi). Kojim kriptografskim mehanizmima se realizuju i po čemu se razlikuju od *hash* funkcija?

3. (K)(**10p**) 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.

4. (K)(**10p**) Nacrtati i objasniti *CBC* i *CFB* modove funkcionisanja blok algoritama. Kada se koristi *CBC*, a kada *CFB*? Koja je razlika između ova dva moda? Stanje zadato na slici 1 propustiti kroz poslednju iteraciju *AES* algoritma prilikom šifrovanja, prikazati stanje nakon svake operacije i stanje koje se dobija na kraju iteracije. Dati su: ključ poslednje iteracije (slika 2) i sadržaj S-*box* tabele (slika 3).

1E	F7	54	CC
D3	38	97	60
57	72	2E	97
8E	04	BA	FA

Slika 1.

EB	76	F2	21
97	97	A1	0E
AF	C1	BC	BE
A2	E6	6B	78

Slika 2.

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

Slika 3.

5. (K)(**10p**) Objasniti *RSA* algoritam za šifrovanje pomoću javnog ključa. Opisati način formiranja privatnog i javnog ključa, kao i postupak prilikom šifrovanja, odnosno dešifrovanja ovim algoritmom. Šifrovati poruku M=10, koristeći javni ključ PU={17, 4307}. Za izračunavanje šifrovane vrednosti koristiti algoritam za brzu eksponentizaciju.

---

1. (I)(**10p**) Objasnite kako se u komunikaciji između *Kerberos realm*-ova obezbeđuje pristup klijenta iz jednog *realm*-a servisu iz drugog *realm*-a. Navedite svaki korak u autentikaciji i autorizaciji. Ako je u toku rada potrebno prići servisu iz nekog trećeg *realm*-a, da li je potrebno ponovo se ulogovati?

2. (I)(**10p**) Koje se sve poruke i kojim redosledom razmenjuju između klijenta i servera kod uspostavljanja *SSL* sesije (*SSL Handshake*). Pretpostavite da je potrebna samo autentikacija servera, a ne i klijenta.

3. (I)(**10p**) Koje funkcije se koriste u *S/MIME* za obezbeđivanje tajnosti, autentikacije (razmatrati obe varijante autentikacije) i tajnosti i autentikacije? Objasniti na koji način se vrši osiguravanje *MIME* entiteta u slučaju da želimo da postignemo tajnost. Objasniti na koji način se vrši osiguravanje *MIME* entiteta u slučaju da želimo da postignemo autentikaciju (razmatrati obe varijante autentikacije).

4. (I)(**10p**) Koji pristupi postoje kod detekcije upada? Opisati u kratkim crtama suštinu svakog od nabrojanih pristupa.

5. (I)(**10p**) Skicirati i objasniti direktni i reflektovani DDoS napad.

Napomena: Na ispitu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Potrebno je na svesci naznačiti ukoliko želite da Vam se poeni sa prvog kolokvijuma računaju umesto zadataka označenih sa K. Ispit traje 180 minuta.