1. Poruku „kolokvijum master“ šifrovati *Vigenère* algoritmom sa *autokey* poboljšanjem i ključem: „zastita“. Objasniti zašto je uvedeno *autokey* poboljšanje. Napomena: koristiti 26 slova engleske abecede.
2. Navedite sve korake *Needham-Schroeder* protokola. Navedite detaljno zbog čega je moralo da se uvodi poboljšanje protokola. Objasnite poboljšanje koje je uveo *Neumann*. Zašto neko, ko se u prvom koraku lažno predstavi (npr. učesnik C se predstavi kao učesnik A), ne može da se lažno autentikuje u slučaju poboljšanja koje je uveo *Neumann*?
3. 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).

4E	7A	86	87
40	36	9F	A6
2A	37	4E	93
E8	11	A6	5C

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.

4. Čemu služe modovi funkcionisanja blok algoritama? Nacrtati i objasniti *CBC* i *CFB* modove funkcionisanja blok algoritama. Kada se koristi *CBC*, a kada *CFB*? Koja je razlika između ova dva moda?
5. Kod *Diffie-Hellman* algoritma objasniti po kom pravilu se biraju globalni javni elementi, a zatim za dva učesnika u komunikaciji objasniti na koji način svaki od njih formira par ključeva i kako dobijaju zajedničku tajnu vrednost. Dokazati da učesnici u komunikaciji dobijaju istu vrednost iako koriste različite proračune da do nje dođu.

Napomene: Na kolokvijumu nisu dozvoljena nikakva pomoćna sredstva, ni kalkulatori ni literatura. Kolokvijum traje 120 minuta.