1. (**10п**) Дешифровати поруку CLJPCDOMKLLJABFDVZVCQIVJWOZOG која је шифрована *Vigenere* алгоритмом са autokey побољшањем и коришћењем кључа KLJUC. У алгоритму се користи енглески алфабет.

   Прва два реда *Vigenere* таблице изгледају овако:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A

2. (**10п**) Скицирати протокол који се користи за дистрибуцију јавних кључева код асиметричних криптографских алгоритама коришћењем технике сертификата за јавне кључеве. Која је разлика у односу на коришћење технике ауторитета за јавне кључеве?

3. (**10п**) *Double DES и Triple DES.*

   а) Квантитативно изразити сигурност *Double DES* алгоритма у односу на *brute force* напад. Укратко образложити.

   б) Квантитативно изразити сигурност *Triple DES* алгоритма у односу на *brute force* напад. Укратко образложити. Приказати и укратко објаснити различите могуће конфигурације алгоритма за шифровање (процесе енкрипције и декрипције и кључеве који се користе).

4. (**15п**) За оригиналну поруку 1234h и кључ 25ABh приказати поступак и дати вредност шифроване поруке ако се користи поједностављени *AES* алгоритам (*S-AES*). Константе итерације које се користе у функцији експанзије кључа су: *Rcon*(1) = 80h, *Rcon*(2) = 30h. Код операције мешања колона користи се аритметика у пољу $GF(2^4)$ по модулу x^4+x+1.

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

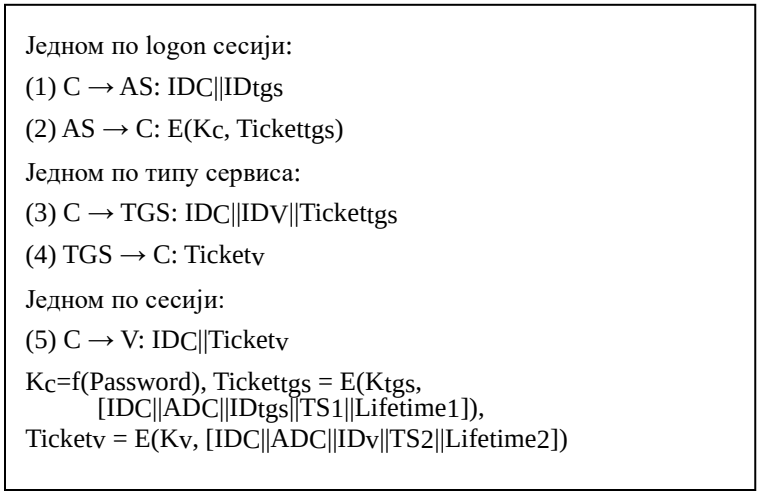
Слика 1. *S-box* конфигурација.

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

Слика 2. Коефицијенти за операцију мешања колона.

Напомена: *На колоквијуму нису дозвољена никаква помоћна средства, ни калкулатори ни литература. Колоквијум траје 70 минута.*

1. (**15/10п**) На слици је дата наивна шема за аутентикацију корисника у систему који опслужује већи број сервиса. Објаснити на који начин и зашто је могуће извршити напад понављањем поруке (*Replay*). Објаснити шта је све додато на ове поруке у оквиру Kerberos v4 како би се напади спречили.



2. (**15/10п**) Шта се све мора урадити ако је компромитован приватни кључ издаваоца X.509 сертификата да би се поново успоставио систем сигурности заснован на X.509?
3. (**15/10п**) Скицирати структуру *PGP* поруке и укратко објаснити компоненте из које се састоји. Означити делове поруке који су опциони. Означити делове поруке који су енкриптовани уз навођење кључа који је искоришћен за сваку од енкрипција.
4. (**10/5п**) *DDoS напад*.

   а) **(2/1п)** Укратко објаснити намену *DoS и DDoS напада.*

   б) **(4/2п)** Укратко објаснити заузимање интерних ресурса у DDoS нападу затрпавањем SYN пакетима.

   в) **(4/2п)** Скицирати и укратко објаснити рефлектовани DDoS напад.

Напомена: *На испиту нису дозвољена никаква помоћна средства, ни калкулатори ни литература. Испит траје 70 минута.*