

2. naloga
a)DNS protokol
b)MX oziroma **MaileXchange**[?](http://ucilnica.fri.uni-lj.si/mod/wiki/view.php?id=10148&page=MaileXchange)
c)ns.fri.uni-lj.si
d)Vsebuje IP naslov(e) strežnika za pošto. Brez tega dela odgovora se ne bi mogli povezati na ns.fri.uni-lj.si, saj nam je DNS strežnik odgovoril z imenom namesto z IPjem strežnika.

3. naloga
a)POP3
b)Uporablja se za elektronsko pošto. POP3 strežnik shranjuje naše prihodna sporočila dokler jih uporabnik ne prebere(prenese na lokalni računalnik). Strežnika posluša na vratih 110.
c)Podatki potujejo od uporabnika do strežnika kot golo besedilo, vključno z geslom.
d)Z enkripcijo prometa.

5. naloga
a)TCP
b)TCP
c)TCP
d)UDP
e)UDP
f)TCP
g)TCP

7. naloga


Predstavitvena plast zagotavlja različne načine kodiranja in sisteme pretvorb za aplikacijsko plast. Pretvarja podatke, poslane po omrežju, iz ene v drugo obliko, določa sintakso, transformacijo in formiranje podatkov. Naloge predstavitvene plasti pri modelu TCP/IP sodijo v aplikacjisko plast.

8. naloga
a)MIME ali Multipurpose Internet Mail Extensions se uporablja pri e-pošti, kot razširitev, ki omogoča večpredstavna sporočila in dodatne znake, kot so č,š,ž in podobni.
b)Uporablja se na aplikacijski plasti
c)Quoted-printable, Base 64, Binary.
d)
e)

9. naloga

**Zloraba piškotkov:**

**Cookie hijacking – "ugrabitev" piškotkov**

Če je še kdo na istem omrežju kot jaz in strežnik in ima dovoljeno branje iz omrežja, lahko ukrade piškotke. Zaradi tega, ker piškotki vsebujejo osebne podatke (uporabniška imena, gesla, ipd.), njihova vsebina ne sme biti dostopna do ostalih računalnikov.

**Cookie poisoning – "zastrupljanje" piškotkov**

Medtem, ko naj bi se piškotki samo hranili na računalniku in pošiljali strežniku nazaj nespremenjeni, lahko napadalec spremeni njihove vrednosti preden jih naprej posreduje strežniku. Na primer: piškotek vsebuje ceno nekega plačila, ki ga mora uporabnik plačati. Če spremenimo to vrednost, lahko plačamo manj ali več.

10.naloga

**INTEGRITETA SPOROČILA**

* Ali je bilo sporočilo med prenosom spremenjeno?
* Uporabimo digitalni izvleček, ga podpišemo in pošljemo skupaj s sporočilom
* Zgoščevalne funkcije
	+ Prstni odtis (hash) sporočila m: f = h(m)
	+ m poljubno dolgo sporočilo; f je kratek, omejene dolžine
	+ kolizija: različna sporočila imajo enak prstni odtis
	+ pri vseh možnih vhodih je frekvenca (hash) rezultatov enaka
	+ mala sprememba vhoda povzroči veliko spremembo podpisa
	+ težko najti drugačno vhodno vrednost za isti podpis
	+ bitne operacije brez ključa
	+ MD5 (osnova za sha1, uporaba v bazah za shranjevanje gesel)
	+ SHA-1 (najpomembnejši 160 bitov)
	+ SHA 256 – 256 bitov