Anita želi poslati Bojanu torbo s skrivno vsebino, npr. z novim tajnim receptom (recimo za najboljši sladoled, čeprav se šele pri Coca-coli zavedamo prave vrednosti recepta). To stori tako, da jo zaklene s svojo ključavnico (t.i. žabico), katere ključ ima le ona, in jo pošlje Bojanu.

Bojan prepozna Anitino ključavnico in torbo, a ker nima ključa, je ne more odpreti. Zato doda še svojo ključavnico in dvakrat zaklenjeno torbo vrne po pošti Aniti.

Tudi Anita prepozna svojo torbo in svojo ključavnico, opazi pa tudi Bojanovo ključavnico, zato odklene svojo ključavnico in jo pošlje nazaj k Bojanu.

Slednji samo še odklene svojo ključavnico in že lahko pride do vsebine torbe, tj. tajnega recepta.



Nihče drug razen Anite in Bojana ne more priti do vsebine torbe, saj je le-ta ves čas, ko je na poti zaklenjena. Zato sta Anita in Bojan prepričana, da je recept ostal tajen. Vendar temu ni nujno tako.

VPRAŠANJA:

1. Pojasni:
	1. kako bi lahko v primeru zgornjega kriptografskega protokola izvedli napad srednjega moža \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (3 točke)
	2. in v čem je v bistvu problem.
	\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (1 točka)
2. V digitalnem svetu bo vsebina torbe (recept) v resnici digitalno zaporedje bitov, zaklepanje pa dosežemo/izvedemo z uporabo funkcije, ki je še vedno odvisna od skrbno izbranih ključev s strani Anite in Bojana. Kakšne lastnosti naj ima ta funkcija, da bo pošiljanje tajnega recepta varno?
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (2 točki)
3. Predlagaj vsaj en predlog za funkcijo iz točke (b) z utemeljitvijo, zakaj res deluje.
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (2 točki)

REŠITEV.

1. Napadalec Oskar pri prvi izmenjavi prestreže torbo, kupi še eno povsem enako torbo in enako ključavnico, kot je Anitina, pa čeprav njo zaklepa in odklepa povsem drugačen ključ kot Anitin. Nato da v novo torbo nek stari recept, ki ni prav nič posebnega in jo zaklene s svojo novo ključavnico ter jo pošlje Bojanu. Ker le-ta ne odkrije nobene razlike med Anitino ključavnico in Oskarjevo kopijo, dodatno zaklene, nič hudega sluteč, napačno torbo s svojo ključavnico in jo pošlje nazaj. Oskar prestreže tudi to pošiljko in vidi tako ugotovi, kako izgleda Bojanova ključavnica. Kupi na zunaj popolnoma enako ključavnico, vendar ima tudi ta povsem drugačen ključ od Bojanovega. S kopijo Bojanove ključavnice dodatno zaklene originalno torbo in jo pošlje nazaj Aniti. Slednja ne odkrije nobene razlike med Bojanovo ključavnico in Oskarjevo kopijo (saj sta praktično identični, le da ju odpirata drugačna ključa), zato nič hudega sluteč odstrani svojo ključavnico in jo pošlje nazaj. Oskar tudi tokrat prestreže pošiljko in ker ima ključ od Bojanove kopije ključavnice, sedaj brez težav pride do tajnega recepta.

(2 točki)

Če se Oskar na tem mestu ustavi, potem bo Bojan lahko posumil, da je nekaj narobe (saj še vedno pričakuje torbo z receptom), zato še pri kopiji torbe odstrani kopijo Anitine ključavnice, za katero tudi ima ključ in kopijo torbe (s starim receptom, ki ni prav nič posebnega). Kopija torbe je sedaj zaklenjena le še z Bojanovo ključavnico in Oskar jo pošlje nazaj Bojanu, ki vloži veliko denarja v novo slaščičarno, a se mu slabo piše, saj njegov sladoled z Oskarjevim podtaknjenim receptom ne bo prav nič posebnega (če ne gre celo za pravi strup).

(1 točka)

Problem je torej v prepoznavanju Anitine in Bojanove ključavnice ter torbe. Če Oskarju uspe kupiti na videz popolne kopije, ga prav nič ne moti, če imajo drugačne ključe.

(1 točka)

1. Naj bosta $A$ in $B$ zaporedoma Anitin in Bojanov ključ. Za ključ $K\in \left\{A,\right.\left.B\right\}$ naj bo $f\_{K}$ izbrana funkcija za zaklepanje, $g\_{K}$ pa njen inverz, ki ga uporabljamo za odklepanje.

Potem je $f\_{A}(\left\{tajno sporočilo\right\})$ prva pošiljka, $f\_{B}\left(f\_{A}\left\{tajno sporočilo\right\}\right)$ pa druga. Tretja je potem $g\_{A}\left(f\_{B}\left(f\_{A}\left(\left\{tajno sporočilo\right\}\right)\right)\right)$ , a brez pravila o zamenjavi (tj. $g\_{A}°f\_{B}=f\_{B}°g\_{A}$ ) težko pridemo do $f\_{B}\left(\left\{tajno sporočilo\right\}\right)$ , ki jo Bojan po prejetju brez težav odklene:

$g\_{B}\left(f\_{B}\left\{tajno sporočilo\right\}\right)= \left\{tajno sporočilo\right\}$ .

 (2 točki)

1. Naj bo $α$ generator neke ciklične grupe, $x$ pa tajno sporočilo.

**Prvi predlog** je $y=f\_{K}\left(x\right)=xα^{K}$ , tj. ElGamalovo šifriranje.
V tem primeru je $g\_{K}\left(y\right)=yα^{-K}=\left(xα^{K}\right)α^{-K}$ .

Prepričajmo se še, da v tem primeru velja pravilo o zamenjavi:

$$g\_{A}\left(f\_{B}(x)\right)=\left(xα^{B}\right)α^{-A}=xα^{B-A}=\left(xα^{-A}\right)α^{B}=f\_{B}\left(g\_{A}(x)\right)$$

ki je posledica pravila o zamenjavi pri seštevanju: $B+\left(-A\right)=\left(-A\right)+B$ (glej eksponente).

(2 točki)

**Drugi predlog** sestavi na osnovi RSA šifriranja, ki je posledica pravila o zamenjavi pri množenju: $B\*A=A\*B$ (zopet glej eksponente).

(2 točki)