

 $\underline{\text{Moja naslovnica}} \ / \ \text{Moji e-kolegiji} \ / \ \underline{\text{srs} \ \underline{\text{b}}} \ / \ \text{Opći dio} \ / \ \underline{\text{1. blic (osnove kriptografije i kriptoanalize)}}$

7anažata	notal: 19 ožvila 2022 20:01
	petak, 18. ožujka 2022., 20:01 Završeno
	petak, 18. ožujka 2022., 20:04
Proteklo vrijeme	
	2,00 od maksimalno 2,00 (100 %)
Pitanje 1	
Točno	
Broj bodova: 0,50 od 0,50	
Ako napadamo blo	k šifre AES128 i AES256 napadom grube sile, koliko će puta biti sporiji napad na AES256 od napada na AES128?
Odaberite jedan ili	više odgovora:
🔲 a. biti će jedna	ko brzi
☑ b. 2 ¹²⁸ puta sp	oriji √
c. 2 puta sporij	
☐ d. 128 puta sp	oriji
e. 2 ²⁵⁶ puta sp	oriji
f. ništa od nave	edenog jer napadi grubom silom na blok šifre nisu mogući
Your answer is corre	
Ispravan odgovor je 2 ¹²⁸ puta sporiji	
_ pata sporg.	
Pitanje 2 Točno	
Broj bodova: 0,50 od 0,50	
210) 200000. 0,30 00 0,30	
Što moramo poslar	i zajedno s blokovima skrivenog teksta kada koristimo CBC način kriptiranja?
Odaberite jedan ili	
	sažetak dijeljenog ključa
	pis skrivenog teksta
c. jednokratnu	
d. inicijalizacijs	
e. substitucijsk	
f. oznaku za in	regritet poruke
Va	
Your answer is corre	
	cijalizacijski vektor kako bi primatelj mogao dešifrirati skriveni tekst.
Ispravan odgovor je inicijalizacijski vekto	

Pitanje 3
Točno Broj bodova: 0,50 od 0,50
Ana šalje poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne netko drugi. Na koji način oni mogu biti osigurati željeno svojstvo?
Odaberite jedan ili više odgovora: a. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom.
□ b. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ.
🗆 c. Ana kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom.
☑ d. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. ✔
🗆 e. Prije slanja, Ana šifrira poruku svojim javnim ključem.
🗆 f. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom.
Your answer is correct.
Ispravan odgovor je:
Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom.
~ 4
Pitanje 4 Točno
Broj bodova: 0,50 od 0,50
Kriptosustav RSA je nesiguran ako:
Odaberite jedan ili više odgovora:
a. Napadač može za proizvoljno veliki broj odrediti je li prost ili složen.
□ b. Napadač može generirati proizvoljno veliki prosti broj.
C. Napadač može izračunati umnožak dva proizvoljno velika prosta broja.
d. Napadač može izračunati multiplikativni inverz modulo proizvoljno veliki prosti broj.
☑ e. Napadač može proizvoljni veliki broj rastaviti na proste faktore. ✔
Your answer is correct.
Ispravan odgovor je: Napadač može proizvoljni veliki broj rastaviti na proste faktore.
→ Obavijesti Drihaži
Prikaži \$

Moja naslovnica / M	oji e-kolegiji / <u>srs b</u> / Opći dio / <u>1. blic (osnove kriptografije i kriptoanalize)</u>	
	petak, 18. ožujka 2022., 20:00	
	Završeno	
Proteklo vrijeme	petak, 18. ožujka 2022., 20:04	
	1,50 od maksimalno 2,00 (75 %)	
•		
Pitanje 1 Točno Broj bodova: 0,50 od 0,50		
Kriptosustav RSA je	nesiguran ako:	
Odaberite jedan ili	više odgovora:	
•	vže za proizvoljno veliki broj odrediti je li prost ili složen.	
·	ože generirati proizvoljno veliki prosti broj.	
	c. Napadač može proizvoljni veliki broj rastaviti na proste faktore.✔	
d. Napadač mo	vže izračunati umnožak dva proizvoljno velika prosta broja.	
e. Napadač mo	že izračunati multiplikativni inverz modulo proizvoljno veliki prosti broj.	
Your answer is corre	ect.	
Ispravan odgovor je		
	izvoljni veliki broj rastaviti na proste faktore.	
Pitanje 2		
Točno		
Broj bodova: 0,50 od 0,50		
Ako napadamo blo	k šifre AES128 i AES256 napadom grube sile, koliko će puta biti sporiji napad na AES256 od napada na AES128?	
Odaberite jedan ili a. 2 ²⁵⁶ puta spe		
b. ništa od nav	edenog jer napadi grubom silom na blok šifre nisu mogući	
✓ c. 2 ¹²⁸ puta specificación.	oriji √	
d. biti će jedna	ko brzi	
e. 128 puta spo	priji	
f. 2 puta sporiji		
L pata sports		
Your answer is corre	ect.	
Ispravan odgovor je		
2 ¹²⁸ puta sporiji		

Your answer is correct.

Bez inicijalizacijskog vektora primatelj ne može dešifrirati skriveni tekst.

Ispravan odgovor je:

Kako bi primatelj mogao dešifrirati skriveni tekst.

→ Obavijesti

Moja naslovnica / M	Moja naslovnica / Moji e-kolegiji / srs_b / Opći dio / <u>1. blic (osnove kriptografije i kriptoanalize)</u>	
7¥	notal: 10. ožvilka 2022. 20:00	
	petak, 18. ožujka 2022., 20:00 Završeno	
	petak, 18. ožujka 2022., 20:04	
Proteklo vrijeme	·	
Ocjena	2,00 od maksimalno 2,00 (100 %)	
Pitanje 1 Točno Broj bodova: 0,50 od 0,50		
Kada koristimo CB	C način šifriranja, zašto zajedno s blokovima skrivenog teksta šaljemo i inicijalizacijski vektor?	
Odaberite jedan ili		
	jurali povjerljivost komunikacije. natelj mogao dešifrirati skriveni tekst.❤	
	obranili od napada čovjeka u sredini.	
	natelj mogao provjeriti digitalni potpis.	
	jurali integritet komunikacije.	
	ostavili zajednički tajni ključ.	
Ispravan odgovor je	g vektora primatelj ne može dešifrirati skriveni tekst.	
Pitanje 2		
Točno		
Broj bodova: 0,50 od 0,50		
Kod blok šifri (algoi	ritma kriptiranja bloka), uvijek su jednake veličine:	
Odaberite jedan ili	više odgovora:	
a. jasni tekst, s	skriveni tekst i ključ	
b. jasni tekst i	ključ	
c. skriveni teks	st i ključ	
d. jasni tekst i	skriveni tekst✓	
Your answer is corr	rect.	
Ispravan odgovor je	e:	

jasni tekst i skriveni tekst

Pitanje 3	
Točno	
Broj bodova: 0,	50 00 0,50
Ana šalje r	oruku Branku putem e-pošte. Ani i Braknu je bitno da sadržaj poruke ostane skriven. Na koji način oni mogu biti osigurati غز
svojstvo?	
Odaberite	jedan ili više odgovora:
a. Ana	u kriptira poruku Brankovim javnim ključem, Branko je dekriptira svojim privatnim ključem.✔
b. Ana	potpisuje poruku svojim privatnim ključem, Branko je dekriptira svojim privatnim ključem.
C. Ana	kriptira poruku svojim javnim ključem, Branko je dekriptira svojim privatnim ključem.
d. Ana	kriptira poruku Brankovim privatnim ključem, Branko je dekriptira svojim javim ključem.
e. Ana	kriptira poruku svojim privatnim ključem, Branko je dekriptira svojim javim ključem.
Your answ	er is correct.
Ispravan o	dgovor je:
Ana kriptira	a poruku Brankovim javnim ključem, Branko je dekriptira svojim privatnim ključem.
Pitanje 4	
r nanje 🕶	
Točno	
Točno	50 od 0,50
Točno Broj bodova: 0,! Ana šalje p	ooruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo?
Točno Broj bodova: 0,! Ana šalje p drugi. Na k	ooruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne
Točno Broj bodova: 0,4 Ana šalje podrugi. Na koodaberite	oruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo?
Točno Broj bodova: 0,4 Ana šalje podrugi. Na kon odaberite odaber	ooruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo? iedan ili više odgovora:
Ana šalje p drugi. Na k Odaberite a. Prijo	poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne soji način oni mogu biti osigurati željeno svojstvo? jedan ili više odgovora: e slanja, Ana šifrira poruku svojim javnim ključem.
Ana šalje podrugi. Na kodaberite a. Prijob. Ana	poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne soji način oni mogu biti osigurati željeno svojstvo? jedan ili više odgovora: e slanja, Ana šifrira poruku svojim javnim ključem. u kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom.
Ana šalje podrugi. Na ko Odaberite a. Prije b. Ana c. Ana	poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne poji način oni mogu biti osigurati željeno svojstvo? pjedan ili više odgovora: pe slanja, Ana šifrira poruku svojim javnim ključem. pa kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. pa izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom.
Ana šalje podrugi. Na ko Odaberite a. Prije b. Ana d. Ana d. Ana	poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo? jedan ili više odgovora: e slanja, Ana šifrira poruku svojim javnim ključem. t kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. t izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. t dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom.
Ana šalje podrugi. Na kodaberite a. Prije b. Ana d. Ana e. Prije f. Ana	oruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo? jedan ili više odgovora: e slanja, Ana šifrira poruku svojim javnim ključem. i kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. i izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. i dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. e slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. ✓
Ana šalje r drugi. Na k Odaberite a. Prije b. Ana c. Ana d. Ana e. Prije f. Ana	oruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo? jedan ili više odgovora: e slanja, Ana šifrira poruku svojim javnim ključem. l kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. l izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. l dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. e slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. lizračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. e slanja, Privatni ključ.
Ana šalje pdrugi. Na k Odaberite a. Prije b. Ana c. Ana d. Ana e. Prije f. Ana	oruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo? jedan ili više odgovora: e slanja, Ana šifrira poruku svojim javnim ključem. l kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. l izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. e slanja, Ana šifrira poruku koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. e slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. e slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ.
Ana šalje pdrugi. Na k Odaberite a. Prije b. Ana c. Ana d. Ana e. Prije f. Ana	oruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne oji način oni mogu biti osigurati željeno svojstvo? jedan ili više odgovora: e slanja, Ana šifrira poruku svojim javnim ključem. t kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. t izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. e slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. er is correct. dgovor je: na digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom.

Moja naslovnica / Moji e-kolegiji / srs b / Opći dio / 1. blic (osnove kriptografije i kriptoanalize)

Započeto	petak, 18. ožujka 2022., 20:00
Stanje	Završeno
Završeno	petak, 18. ožujka 2022., 20:04
Proteklo vrijeme	4 min 1 sek
Ocjena	1,50 od maksimalno 2,00 (75 %)

Pitanje **1**Točno
Broj bodova:

0,50 od 0,50

Odaberite jedan ili više odgovora:

Kada koristimo CBC način šifriranja, zašto zajedno s blokovima skrivenog teksta šaljemo i inicijalizacijski vektor?

a. Kako bi osiqurali povjerljivost komunikacije.

- ☐ b. Kako bi se obranili od napada čovjeka u sredini.
- c. Kako bi primatelj mogao provjeriti digitalni potpis.
- d. Kako bi uspostavili zajednički tajni ključ.
- e. Kako bi osigurali integritet komunikacije.
- ☑ f. Kako bi primatelj mogao dešifrirati skriveni tekst.
 ✓

Your answer is correct.

Bez inicijalizacijskog vektora primatelj ne može dešifrirati skriveni tekst.

Ispravan odgovor je:

Kako bi primatelj mogao dešifrirati skriveni tekst.

Pitanje **2**Točno
Broj bodova:
0,50 od 0,50

Ako napadamo blok šifre AES128 i AES256 napadom grube sile, koliko će puta biti sporiji napad na AES256 od napada na AES128?

Odaberite jedan ili više odgovora:

- a. 2²⁵⁶ puta sporiji
- ☑ b. 2¹²⁸ puta sporiji ✔
- c. 2 puta sporiji
- d. biti će jednako brzi
- e. 128 puta sporiji
- ☐ f. ništa od navedenog jer napadi grubom silom na blok šifre nisu mogući

Your answer is correct.

Ispravan odgovor je: 2¹²⁸ puta sporiji

Pitanje **3**Točno

Broj bodova: 0,50 od 0,50

Ana šalje poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne netko drugi. Na koji način oni mogu biti osigurati željeno svojstvo?

Odaberite jedan ili više odgovora:

- a. Ana kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom.
- □ b. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ.
- c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom.
- d. Prije slanja, Ana šifrira poruku svojim javnim ključem.
- ☑ e. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom.
 ✓
- f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom.

Your answer is correct.

Ispravan odgovor je:

Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom.

Pitanje 4 Kriptosustav RSA je **nesiguran** ako: Netočno Odaberite jedan ili više odgovora: Broj bodova: 0,00 od 0,50 a. Napadač može izračunati multiplikativni inverz modulo proizvoljno veliki prosti broj. ** □ b. Napadač može za proizvoljno veliki broj odrediti je li prost ili složen. c. Napadač može izračunati umnožak dva proizvoljno velika prosta broja. d. Napadač može generirati proizvoljno veliki prosti broj. ☑ e. Napadač može proizvoljni veliki broj rastaviti na proste faktore. Your answer is incorrect. Ispravan odgovor je: Napadač može proizvoljni veliki broj rastaviti na proste faktore. → Obavijesti Prikaži... **\$**

Moja naslovnica / Moji e-kolegiji / srs_b / Opći dio / 1. blic (osnove kriptografije i kriptoanalize)

Započeto	petak, 18. ožujka 2022., 20:01
Stanje	Završeno
Završeno	petak, 18. ožujka 2022., 20:05
Proteklo vrijeme	3 min 27 s
Ocjena	1,50 od maksimalno 2,00 (75 %)
Pitanje 1	
Točno	
Broj bodova: 0,50 od 0,50	
Kada koristimo CBC	C način šifriranja, zašto zajedno s blokovima skrivenog teksta šaljemo i inicijalizacijski vektor?
Odaberite jedan ili	više odgovora:
a. Kako bi prim	natelj mogao provjeriti digitalni potpis.
☐ b. Kako bi uspo	ostavili zajednički tajni ključ.
C. Kako bi osig	urali integritet komunikacije.
d. Kako bi se o	branili od napada čovjeka u sredini.
e. Kako bi prim	natelj mogao dešifrirati skriveni tekst.✔
🔲 f. Kako bi osigu	urali povjerljivost komunikacije.
Your answer is corre	ect.
Bez inicijalizacijskog	g vektora primatelj ne može dešifrirati skriveni tekst.
Ispravan odgovor je	
Kako bi primatelj m	ogao dešifrirati skriveni tekst.

Pitanje 2 Točno
Broj bodova: 0,50 od 0,50
Ana šalje poruku Branku putem e-pošte. Ani i Braknu je bitno da sadržaj poruke ostane skriven. Na koji način oni mogu biti osigurati željeno svojstvo?
Odaberite jedan ili više odgovora: a. Ana kriptira poruku svojim privatnim ključem, Branko je dekriptira svojim javim ključem.
□ b. Ana kriptira poruku svojim javnim ključem, Branko je dekriptira svojim privatnim ključem.
c. Ana kriptira poruku Brankovim privatnim ključem, Branko je dekriptira svojim javim ključem.
☑ d. Ana kriptira poruku Brankovim javnim ključem, Branko je dekriptira svojim privatnim ključem. ✔
□ e. Ana potpisuje poruku svojim privatnim ključem, Branko je dekriptira svojim privatnim ključem.
Your answer is correct. Ispravan odgovor je:
Ana kriptira poruku Brankovim javnim ključem, Branko je dekriptira svojim privatnim ključem.
Pitanje 3 Netočno
Broj bodova: 0,00 od 0,50
Kod blok šifri (algoritma kriptiranja bloka), uvijek su jednake veličine:
Odaberite jedan ili više odgovora:
☑ a. skriveni tekst i ključ ×
□ b. jasni tekst, skriveni tekst i ključ
□ c. jasni tekst i ključ
d. jasni tekst i skriveni tekst
Your answer is incorrect.
Ispravan odgovor je: jasni tekst i skriveni tekst

Točno Broj bodova: 0,50 od 0,50 Ana šalje poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne netko drugi. Na koji način oni mogu biti osigurati željeno svojstvo? Odaberite jedan ili više odgovora: a. Ana kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. b. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. d. Prije slanja, Ana šifrira poruku svojim javnim ključem. e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom.	Pitanje 4	
Ana šalje poruku Branku putem e-pošte. Branku je bitna autentičnost pošiljatelja — želi biti siguran da je poruku poslala baš Ana, a ne netko drugi. Na koji način oni mogu biti osigurati željeno svojstvo? Odaberite jedan ili više odgovora: a. Ana kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. b. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. d. Prije slanja, Ana šifrira poruku svojim javnim ključem. e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom.	ōčno	
netko drugi. Na koji način oni mogu biti osigurati željeno svojstvo? Odaberite jedan ili više odgovora: a. Ana kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. b. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. d. Prije slanja, Ana šifrira poruku svojim javnim ključem. e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.	Broj bodova: 0,50 od 0,50	
netko drugi. Na koji način oni mogu biti osigurati željeno svojstvo? Odaberite jedan ili više odgovora: a. Ana kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. b. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. d. Prije slanja, Ana šifrira poruku svojim javnim ključem. e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.		
 a. Ana kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom. ✓ b. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. ✓ c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. ✓ d. Prije slanja, Ana šifrira poruku svojim javnim ključem. ✓ e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. ✓ f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.		
 ☑ b. Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom. ☑ c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. ☑ d. Prije slanja, Ana šifrira poruku svojim javnim ključem. ☑ e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. ☑ f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.	Odaberite jedan ili više odgovora:	
 c. Ana dekriptira hash poruke koristeći dijeljeni javni ključ i pošalje ga zajedno s porukom. d. Prije slanja, Ana šifrira poruku svojim javnim ključem. e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.	🗆 a. Ana kriptira hash poruke koristeći Brankov priva	tni ključ i pošalje ga zajedno s porukom.
 d. Prije slanja, Ana šifrira poruku svojim javnim ključem. e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.	🛮 b. Ana izračuna digitalni potpis poruke koristeći sv	oj privatni ključ i pošalje ga zajedno s porukom. 🗸
 e. Prije slanja, Ana šifrira poruku šifrom AES u CTR načinu rada koristeći svoj privatni ključ. f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.	🗆 c. Ana dekriptira hash poruke koristeći dijeljeni jav	ni ključ i pošalje ga zajedno s porukom.
f. Ana izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom. Your answer is correct.	🗆 d. Prije slanja, Ana šifrira poruku svojim javnim klju	ıčem.
Your answer is correct.	🗆 e. Prije slanja, Ana šifrira poruku šifrom AES u CTR	načinu rada koristeći svoj privatni ključ.
	🗆 f. Ana izračuna digitalni potpis poruke koristeći Bra	ankov javni ključ i pošalje ga zajedno s porukom.
	Your answer is correct.	
	Isprayan odgovor je:	
Ana izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom.		atni ključ i pošalje ga zajedno s porukom.
	Ispravan odgovor je:	atni ključ i pošalje ga zajedno s porukom.
	■ Obavijesti	
■ Obavijesti	Prikaži	\$