Započeto	petak, 18. ožujka 2022., 20:01
Stanje	Završeno
Završeno	petak, 18. ožujka 2022., 20:04
Proteklo vrijeme	2 min 40 s
Ocjena	**2,00** od maksimalno 2,00 (**100**%)

Pitanje **1**

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. biti će jednako brzi
- [x] b. 2^{128} puta sporiji ✔
- [ ] c. 2 puta sporiji
- [ ] d. 128 puta sporiji
- [ ] e. 2^{256} puta sporiji
- [ ] f. ništa od navedenog jer napadi grubom silom na blok šifre nisu mogući

Your answer is correct.

Ispravan odgovor je:
2^{128} puta sporiji

Pitanje **2**

Točno

Broj bodova: 0,50 od 0,50

Što **moramo** poslati zajedno s blokovima skrivenog teksta kada koristimo CBC način kriptiranja?

Odaberite jedan ili više odgovora:

- [ ] a. kriptografski sažetak dijeljenog ključa
- [ ] b. digitalni potpis skrivenog teksta
- [ ] c. jednokratnu bilježnicu
- [x] d. inicijalizacijski vektor ✔
- [ ] e. substitucijsku tablicu
- [ ] f. oznaku za integritet poruke

Your answer is correct.

Moramo poslati inicijalizacijski vektor kako bi primatelj mogao dešifrirati skriveni tekst.

Ispravan odgovor je:
inicijalizacijski vektor

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.
- [x] 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.

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.
- [x] 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

Prikaži...

Započeto	petak, 18. ožujka 2022., 20:00
Stanje	Završeno
Završeno	petak, 18. ožujka 2022., 20:04
Proteklo vrijeme	3 min 56 s
Ocjena	**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:

- [ ] a. Napadač može za proizvoljno veliki broj odrediti je li prost ili složen.
- [ ] b. Napadač može generirati proizvoljno veliki prosti broj.
- [x] c. Napadač može proizvoljni veliki broj rastaviti na proste faktore. ✔
- [ ] d. Napadač može izračunati umnožak dva proizvoljno velika prosta broja.
- [ ] e. Napadač može izračunati multiplikativni inverz modulo proizvoljno veliki prosti broj.

Your answer is correct.

Ispravan odgovor je:
Napadač može proizvoljni veliki broj rastaviti na proste faktore.

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. 2^{256} puta sporiji
- [ ] b. ništa od navedenog jer napadi grubom silom na blok šifre nisu mogući
- [x] c. 2^{128} puta sporiji ✔
- [ ] d. biti će jednako brzi
- [ ] e. 128 puta sporiji
- [ ] f. 2 puta sporiji

Your answer is correct.

Ispravan odgovor je:
2^{128} puta sporiji

Pitanje **3**

Netočno

Broj bodova: 0,00 od 0,50

Ana šalje poruku Branku putem e-pošte. Ani je bitan integritet poruke — želi da je Branko dobije u točno onom obliku u kojem je Ana šalje, odnosno da Branko otkrije ako je poruka promijenjena u transportu. Ana može osigurati željeno svojstvo tako da:

Odaberite jedan ili više odgovora:

- [x] a. Izračuna kod za integritet poruke koristeći dijeljeni tajni ključ i pošalje ga zajedno s porukom. ✔
- [ ] b. Prije slanja, šifrira poruku šifrom AES u CTR načinu rada koristeći dijeljeni tajni ključ.
- [ ] c. Dekriptira hash poruke koristeći svoj javni ključ i pošalje ga zajedno s porukom.
- [ ] d. Kriptira hash poruke koristeći Brankov privatni ključ i pošalje ga zajedno s porukom.
- [ ] e. Izračuna digitalni potpis poruke koristeći Brankov javni ključ i pošalje ga zajedno s porukom.
- [ ] f. Izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom.

Your answer is incorrect.

Ispravni odgovori su:
Izračuna digitalni potpis poruke koristeći svoj privatni ključ i pošalje ga zajedno s porukom.,

Izračuna kod za integritet poruke koristeći dijeljeni tajni ključ i pošalje ga zajedno s porukom.

Pitanje **4**

Točno

Broj bodova: 0,50 od 0,50

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

Odaberite jedan ili više odgovora:

- [ ] a. Kako bi uspostavili zajednički tajni ključ.
- [ ] b. Kako bi primatelj mogao provjeriti digitalni potpis.
- [ ] c. Kako bi osigurali povjerljivost komunikacije.
- [ ] d. Kako bi se obranili od napada čovjeka u sredini.
- [x] e. Kako bi primatelj mogao dešifrirati skriveni tekst. ✔
- [ ] f. Kako bi osigurali integritet komunikacije.

Your answer is correct.

Bez inicijalizacijskog vektora primatelj ne može dešifrirati skriveni tekst.

Ispravan odgovor je:
Kako bi primatelj mogao dešifrirati skriveni tekst.

◄ Obavijesti

Prikaži...

Započeto	petak, 18. ožujka 2022., 20:00
Stanje	Završeno
Završeno	petak, 18. ožujka 2022., 20:04
Proteklo vrijeme	4 min 1 sek
Ocjena	**2,00** od maksimalno 2,00 (**100**%)

Pitanje **1**

Točno

Broj bodova: 0,50 od 0,50

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

Odaberite jedan ili više odgovora:

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

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

Kod blok šifri (algoritma kriptiranja bloka), uvijek su jednake veličine:

Odaberite jedan ili više odgovora:

- a. jasni tekst, skriveni tekst i ključ
- b. jasni tekst i ključ
- c. skriveni tekst i ključ
- d. jasni tekst i skriveni tekst ✔

Your answer is correct.

Ispravan odgovor je:
jasni tekst i skriveni tekst

Pitanje **3**

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:

- [x] a. Ana 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 answer is correct.

Ispravan odgovor je:
Ana kriptira poruku Brankovim javnim ključem, Branko je dekriptira svojim privatnim ključem.

Pitanje **4**

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

◄ Obavijesti

Prikaži...

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

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

Odaberite jedan ili više odgovora:

- [ ] a. Kako bi osigurali 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.
- [x] 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. 2^{256} puta sporiji
- [x] b. 2^{128} 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:
2^{128} 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.
- [x] 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**

Netočno

Broj bodova:
0,00 od 0,50

Kriptosustav RSA je **nesiguran** ako:

Odaberite jedan ili više odgovora:

- [x] 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.
- [x] 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...

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

Odaberite jedan ili više odgovora:

- [ ] a. Kako bi primatelj mogao provjeriti digitalni potpis.
- [ ] b. Kako bi uspostavili zajednički tajni ključ.
- [ ] c. Kako bi osigurali integritet komunikacije.
- [ ] d. Kako bi se obranili od napada čovjeka u sredini.
- [x] e. Kako bi primatelj mogao dešifrirati skriveni tekst. ✔
- [ ] f. Kako bi osigurali povjerljivost komunikacije.

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

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.
- [x] 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:

- [x] 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

Pitanje **4**

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.
- [x] 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.

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

◄ Obavijesti

Prikaži...