

Question 1

Not answered

Marked out of 1.00

Opišite sunčev sistem.

Question 2

Not answered

Marked out of 1.00

Отворени текст ЦЕЗАР шифрован је са пет различитих кључева. Уколико је се у отвореном тексту и приликом шифровања користе само велика слова српске азбуке, спојити кључ са шифратом.

10 Choose... ▾

3 Choose... ▾

29 Choose... ▾

20 Choose... ▾

14 Choose... ▾

The correct answer is: 10 – ЕЊПЈШ, 3 – ШИКГЋ, 29 – ХЂЖШП, 20 – ЊЦЏСИ,
14 – ЈСЋМГ

Question 3

Not answered

Marked out of 1.00

Алиса и Боб размењују заједничку тајну користећи Дифи Хелманов алгоритам. Алиса шаље Бобу вредност $g^a \pmod{p}$, а Боб Алиси $g^b \pmod{p}$. У тој комуникацији шта је јавно а шта тајно?

a Choose... ▾

 g^b Choose... ▾

g Choose... ▾

p Choose... ▾

b Choose... ▾

 g^a Choose... ▾

The correct answer is: a – тајно, g^b – јавно, g – јавно, p – јавно, b – тајно, g^a – јавно

Question 4

Not answered

Marked out of 1.00

Код класичних крипtosистема одредити шта је јавно а шта тајно:

шифрат Choose... ▾

комуникација Choose... ▾

отворени текст Choose... ▾

кључ Choose... ▾

The correct answer is: шифрат – јавно, комуникација – јавно, отворени текст – тајно, кључ – тајно

Question 5

Not answered

Marked out of 1.00

Одредити редослед корака код избора тајног и јавног кључа RSA алгоритмом:

1. Choose... ▾
5. Choose... ▾
4. Choose... ▾
2. Choose... ▾
3. Choose... ▾

The correct answer is: 1. – бирају се два велика приста броја p и q , 5. – проглашавају се јавни и тајни кључ, 4. – налази се d такво да је $e \cdot d = 1 \pmod{r}$,
2. – формирају се производи $N = p \cdot q$ и $f(N) = r = (p-1) \cdot (q-1)$, 3. – бира се број e мањи од r и узајамно прост са r

Question 6

Not answered

Marked out of 1.00

Отворени текст VISER шифрован је три пута и добијена су три различита шифрата: QQKII, QDNZM и XGLBZO. Без познавања кључева одредити који је шифрат добијен шифровањем Цезаровом, који шифровањем Вижнеровом а који шифровањем Плејферовом шифром:

- QQKII Choose... ▾
- QDNZM Choose... ▾
- XGLBZO Choose... ▾

The correct answer is: QQKII – Вижнерова шифра, QDNZM – Цезарова шифра, XGLBZO – Плејферова шифра

Question 7

Not answered

Marked out of 1.00

Код DES алгоритма:

величина блока је Choose... ▾

дужина подкључа је Choose... ▾

дужина кључа је Choose... ▾

The correct answer is: величина блока је – 64 бита, дужина подкључа је – 48 бита, дужина кључа је – 56 бита

Question 8

Not answered

Marked out of 1.00

Спојити одговарајућу шифру и њену карактеристику:

Проста супституција Choose... ▾

Вижнерова Choose... ▾

Хилова Choose... ▾

Вернамова Choose... ▾

Афина Choose... ▾

Плејферова Choose... ▾

Цезарова Choose... ▾

The correct answer is: Проста супституција – моноалфабетска, Вижнерова – полиалфабетска, Хилова – полиалфабетска, Вернамова – полиалфабетска, Афина – моноалфабетска, Плејферова – полиалфабетска, Цезарова – моноалфабетска

Question 9

Not answered

Marked out of 1.00

Које су од наведених шифри полиграмске:

Проста супституција Choose... ▾

Афина Choose... ▾

Хилова Choose... ▾

Вернамова Choose... ▾

Плејферова Choose... ▾

Цезарова Choose... ▾

The correct answer is: Проста супституција – не, Афина – не, Хилова – да, Вернамова – не, Плејферова – да, Цезарова – не

Question 10

Not answered

Marked out of 1.00

U modelu sgurnosti sa više nivoa odrediti stepen tajnosti (1 najviši, 4 najniži)

1 Choose... ▾

3 Choose... ▾

2 Choose... ▾

4 Choose... ▾

The correct answer is: 1 – državna tajna, 3 – poverljivo, 2 – strogo poverljivo, 4 – bez stepena tajnosti (javno)

Question 11

Not answered

Marked out of 1.00

Спојити појам и одговарајући опис појма

стеганографски
канал

Choose... ▾

тајна порука

Choose... ▾

стего кључ

Choose... ▾

носилац поруке

Choose... ▾

стеганографске
функције

Choose... ▾

стеганографски
медијум

Choose... ▾

The correct answer is: стеганографски канал – канал преко кога се шаље стеганографски медијум, тајна порука – порука која се уграђује, стего кључ – тајна вредност помоћу које се једна порука уграђује у другу, носилац поруке – било која порука преко које се преноси скривена порука, стеганографске функције – функције уградњивања тајне поруке и издвајања тајне поруке, стеганографски медијум – порука која у себи садржи уграђену другу поруку

Question 12

Not answered

Marked out of 1.00

Алиса и Боб размењују заједничку тајну користећи Дифи Хелманов алгоритам. Договорили су се да уређени пар (p,g) буде $(13,7)$. Алиса је замислила број 4 а Боб број 5.

Алиса шаље Бобу

Choose... ▾

Заједничка тајна је

Choose... ▾

Боб шаље Алиси

Choose... ▾

The correct answer is: Алиса шаље Бобу – 9, Заједничка тајна је – 3, Боб шаље Алиси – 11

Question 13

Not answered

Marked out of 1.00

PGP koristi

Select one:

- a. ne znam
- b. asimetrične algoritme
- c. i simetrične i asimetrične algoritme
- d. simetrične algoritme
- e. simetrične algoritme, asimetrične algoritme i kompresiju

The correct answer is: simetrične algoritme, asimetrične algoritme i kompresiju

Question 14

Not answered

Marked out of 1.00

Koliko sestrića ima Paja Patak?

Select one:

- a. 2
- b. 4
- c. 3

The correct answer is: 3

Question 15

Not answered

Marked out of 1.00

Izabratи tačan iskaz:

Select one:

- a. ni ACL lista ni C lista nisu izvedene iz Lampsonove kontrolne matrice
- b. i ACL lista i C lista su izvedene iz Lampsonove kontrolne matrice
- c. ACL lista jeste a C lista nije izvedena iz Lampsonove kontrolne matrice
- d. ne znam
- e. C lista jeste a ACL lista nije izvedena iz Lampsonove kontrolne matrice

The correct answer is: i ACL lista i C lista su izvedene iz Lampsonove kontrolne matrice

Question 16

Not answered

Marked out of 1.00

Koliko osnovnih tipova mrežnih barijera postoji:

Select one:

- a. ne znam
- b. 4
- c. 2
- d. 3
- e. 1

The correct answer is: 3

Question 17

Not answered

Marked out of 1.00

Sistemi koji treba da registruju napade u toku njihovog dešavanja ili naknadno, analizom podataka nazivaju se:

Select one:

- a. modeli sigurnosti sa više nivoa
- b. ne znam
- c. mrežne barijere
- d. anti virus programi
- e. sistemi za detekciju upada

The correct answer is: sistemi za detekciju upada

Question 18

Not answered

Marked out of 1.00

Autentifikacija (samo) smart karticom je odluka na osnovu nečega

Select one:

- a. što korisnik zna
- b. što korisnik ima
- c. što korisnik jeste
- d. što korisnik zna da ima
- e. ne znam

The correct answer is: što korisnik ima

Question 19

Not answered

Marked out of 1.00

U protokolima za autentifikaciju mogu se koristiti:

Select one:

- a. simetrični i asimetrični kriptografski algoritmi i heš funkcije
- b. samo simetrični kriptografski algoritmi
- c. samo simetrični i asimetrični kriptografski algoritmi
- d. samo heš funkcije
- e. ne znam

The correct answer is: simetrični i asimetrični kriptografski algoritmi i heš funkcije

Question 20

Not answered

Marked out of 1.00

U praksi, u kodovima se pojavljuje bar jedna greška na svakih:

Select one:

- a. 2000 linija koda
- b. 1500 linija koda
- c. ne znam
- d. 2500 linija koda
- e. 1000 linija koda

The correct answer is: 2000 linija koda

Question 21

Not answered

Marked out of 1.00

Ukoliko se poseduje samo exe fajl a postoji namera (potreba) da se analizira i izmeni kod neophodan alat je:

Select one:

- a. samo disasembler i hex editor
- b. samo dibager i hex editor
- c. samo disasembler
- d. i disasembler i dibager
- e. ne znam

The correct answer is: i disasembler i dibager

Question 22

Not answered

Marked out of 1.00

Nedostatak fizičke podelje resursa je to što:

Select one:

- a. traži pažljivo planiranje, implementaciju i kontrolu u toku rada
- b. ne znam
- c. ne rešava problem sukoba između procesa/korisnika
- d. je skupo i nepraktično
- e. može lako da dođe do zloupotrebe podataka

The correct answer is: je skupo i nepraktično

Question 23

Not answered

Marked out of 1.00

Сигурност крипtosистема почива на

Select one:

- a. безбедности канала за комуникацију
- b. не знам
- c. тајности кључа за шифровање
- d. тајности кључа за дешифровање
- e. тајности алгоритма за шифровање

The correct answer is: тајности кључа за дешифровање

Question 24

Not answered

Marked out of 1.00

Тајност комуникација је:

Select one:

- a. не знам
- b. пожељно право
- c. загарантовано право
- d. подразумевано право
- e. етичко право

The correct answer is: загарантовано право

Question 25

Not answered

Marked out of 1.00

Дифи Хелманов алгоритам се користи за:

Select one:

- a. не знам
- b. размену симетричних кључева
- c. шифровање симетричног кључа
- d. генерисање паре кључева (тајни-јавни)
- e. генерисање тајног кључа на основу одабраног јавног

The correct answer is: размену симетричних кључева

Question 26

Not answered

Marked out of 1.00

У пракси, биометријску аутентификацију је најбоље вршити помоћу:

Select one:

- a. карактеристика ириса, длана или отиска прста без разлике
- b. геометрије длана
- c. ne znam
- d. отиска прста
- e. карактеристика ириса

The correct answer is: отиска прста

Question 27

Not answered

Marked out of 1.00

Детекција аномалија као метода за откривање злонамерних програма се заснива на:

Select one:

- a. ne znam
- b. registrovanju neuobičajenog понаšања
- c. траžењу сличности са већ познатим злонамерним програмима
- d. reverzном инженерингу
- e. праћењу промена у фајловима

The correct answer is: registrovanju neuobičajenog понаšања

Question 28

Not answered

Marked out of 1.00

TCB (*Trusted Computing Base*) je:

Select one:

- a. deo operativnog sistema zadužen za beleženje podataka o aktivnostima
- b. deo sigurnog jezgra koji je zadužen za kontrolu pristupa
- c. ne znam
- d. deo jezgra zadužen za sigurnosno kritične operacije
- e. skup zaštitnih mehanizama implementiranih u operativnom sistemu za koje se veruje da obezbeđuju zahteve sigurnosti

The correct answer is: skup zaštitnih mehanizama implementiranih u operativnom sistemu za koje se veruje da obezbeđuju zahteve sigurnosti

Question 29

Not answered

Marked out of 1.00

Код OTP шифре, дужина кључа

Select one:

- a. зависи од алгоритма који се користи за генерисање кључа
- b. је исте или веће дужине али се одређеним алгоритмом скраћује на потребну дужину
- c. је исте дужине као отворени текст
- d. је фиксне дужине за дати алгоритам, па се из њега генерише кључ потребне величине
- e. не знам

The correct answer is: је исте дужине као отворени текст

Question 30

Not answered

Marked out of 1.00

Алиса жели да пошаље Бобу поруку шифровану RSA алгоритмом. Она поруку шифрује

Select one:

- a. не знам
- b. својим приватним кључем
- c. Бобовим приватним кључем
- d. Бобовим јавним кључем
- e. својим јавним кључем

The correct answer is: Бобовим јавним кључем

Question 31

Not answered

Marked out of 1.00

Колика треба да је дужина хеш функције да би се постигла иста сигурност као код симетричног система коме је кључ дужине n :

Select one:

- a. 2^*n
- b. 2^n
- c. $n/2$
- d. не знам
- e. n

The correct answer is: 2^*n

Question 32

Not answered

Marked out of 1.00

Koji program ovde ne pripada:

Select one:

- a. *Code red*
- b. ne znam
- c. *Morris Worm*
- d. *Brain*
- e. *SQL Slammer*

The correct answer is: *Brain*

Question 33

Not answered

Marked out of 1.00

Šta **ne** spada u osnovne zadatke NGSCB (*Next Generation Secure Computing Base*):

Select one:

- a. jaka izolacija procesa
- b. ne znam
- c. atest
- d. DRM
- e. bezbedno skladištenej podataka i siguran prenos podataka

The correct answer is: DRM

Question 34

Not answered

Marked out of 1.00

U biometrijskim sistemima prilikom autentifikacije (verifikacije) :

Select one:

- a. ne znam
- b. postoje 3 faze
- c. postoje 4 faze
- d. broj faza zavisi od tipa biometrije
- e. postoje 2 faze

The correct answer is: postoje 2 faze

Question 35

Not answered

Marked out of 1.00

Које се операције користе код OTP шифре ?

Select one:

- a. само XOR
- b. не знам
- c. XOR и супституције
- d. само транспозиције
- e. само супституције

The correct answer is: само XOR

Question 36

Not answered

Marked out of 1.00

Алиса је послала поруку Бобу шифровану RSA алгоритмом. Боб поруку десифрује

Select one:

- a. не знам
- b. Алисиним јавним кључем
- c. Алисиним приватним кључем
- d. својим јавним кључем
- e. својим приватним кључем

The correct answer is: својим приватним кључем

Question 37

Not answered

Marked out of 1.00

Нека је дужина хеш функције 128 бита. Колико различитих хеш вредности функција може да генерише:

Select one:

- a. 2^{129}
- b. 2^{128}
- c. $2^{128} + 1$
- d. $2^{128} - 1$
- e. не знам

The correct answer is: 2^{128}

Question 38

Not answered

Marked out of 1.00

Faza prepoznavanja je faza kod:

Select one:

- a. ne znam
- b. autentifikacije koja se zasniva na nečemu što jeste
- c. autentifikacije koja se zasniva na nečemu što imate
- d. autentifikacije koja se zasniva na nečemu što znate
- e. dvo-faktorske autentifikacije

The correct answer is: autentifikacije koja se zasniva na nečemu što jeste

Question 39

Not answered

Marked out of 1.00

Prednosti metode za detekciju zlonamernih programa koja se zasniva na praćenju promena je to što:

Select one:

- a. ne znam
- b. ne traži ažuriranje baze kontrolnih vrednosti
- c. je brza metoda
- d. može da detektuje i do tada nepoznate zlonamerne programe
- e. što ne traži angažovanje korisnika

The correct answer is: može da detektuje i do tada nepoznate zlonamerne programe

Question 40

Not answered

Marked out of 1.00

Код OTP шифре

Select one:

- a. дужина кључа је небитна јер се скраћује/продужава на потребну дужину и употребљава се само два пута
- b. не знам
- c. дужина кључа мора бити једнака дужини поруке и употребљава се само једном
- d. дужина кључа је једнака дужини поруке и може да се употребљава неколико пута
- e. дужина кључа је небитна јер се скраћује/продужава на потребну дужину и употребљава се само једном

The correct answer is: дужина кључа мора бити једнака дужини поруке и употребљава се само једном

Question 41

Not answered

Marked out of 1.00

Који алгоритам не припада наведеној групи:

Select one:

- a. MD5
- b. SHA-3
- c. SHA-0
- d. AES
- e. не знам

The correct answer is: AES

Question 42

Not answered

Marked out of 1.00

Metamorfični zlonamerni program:

Select one:

- a. menja svoj oblik i delimično funkcionalnost u već zaraženom sistemu
- b. ne znam
- c. menja svoj oblik ali zadržava funkcionalnost u već zaraženom sistemu
- d. menja svoj oblik i funkcionalnost pre nego što inficira novi sistem
- e. menja svoj oblik ali zadržava funkcionalnost pre nego što inficira novi sistem

The correct answer is: menja svoj oblik ali zadržava funkcionalnost pre nego što inficira novi sistem

Question 43

Not answered

Marked out of 1.00

Недостатак OTP шифре је то

Select one:

- a. је основни захтев да кључ буде потпуно случајан низ битова што је технички неизводљиво.
- b. што је технологија преноса низа битова (кључа) велике дужине подложна грешкама приликом преноса па је дешифровање поруке отежано
- c. што је процес генерисања велике количине бинарних низова који имају особине случајности по правилу спор а употребљава се само једном.
- d. кључ мора бити случајан низ битова и не сме да се преноси несигурним каналом што значи да друга страна за дешифровање мора да генерише исти такав случајан низ битова, што је немогуће.
- e. не знам

The correct answer is: што је процес генерисања велике количине бинарних низова који имају особине случајности по правилу спор а употребљава се само једном.

Question 44

Not answered

Marked out of 1.00

Прислушкивање је напад на:

Select one:

- a. расположивост
- b. интегритет
- c. не знам
- d. аутентификацију
- e. поверљивост

The correct answer is: поверљивост

Question 45

Not answered

Marked out of 1.00

Симетрични крипtosистеми су они:

Select one:

- a. који користе исти кључ и исти алгоритам и за шифровање и за дешифровање
- b. код којих је исти алгоритам за шифровање и дешифровање
- c. код којих се користи исти кључ за шифровање и дешифровање
- d. код којих су кључ за шифровање и кључ за дешифровање симетрични
- e. не знам

The correct answer is: код којих се користи исти кључ за шифровање и дешифровање

Question 46

Not answered

Marked out of 1.00

Дигитални потпис је сервис који треба да обезбеди

Select one:

- a. расположивост
- b. не знам
- c. аутентификацију и ауторизацију
- d. повериљивост
- e. интегритет и непорецивост

The correct answer is: интегритет и непорецивост

Question 47

Not answered

Marked out of 1.00

Дужина отиска (хеш вредности) MD5 алгоритма је:

Select one:

- a. 128 бита
- b. 160 бита
- c. не знам
- d. 256 бита
- e. 512 бита

The correct answer is: 128 бита

Question 48

Not answered

Marked out of 1.00

Dvo faktorska autentifikacija захтева:

Select one:

- a. tačno 2 od 3 stavke - нешто што знаете и имате
- b. било које 2 од 3 stavke (нешто што знаете/имате/јесте)
- c. tačno 2 od 3 stavke - нешто што јесте и имате
- d. tačno 2 od 3 stavke - нешто што знаете и јесте
- e. ne znam

The correct answer is: било које 2 од 3 stavke (нешто што знаете/имате/јесте)

Question 49

Not answered

Marked out of 1.00

Šifrovanje злонамерних програма се користи да би се онемогућило његово откривање методом:

Select one:

- a. ne znam
- b. детекције neuobičajenog понаšања
- c. детекције промена
- d. linearizације
- e. детекције потписа

The correct answer is: детекције потписа

Question 50

Not answered

Marked out of 1.00

DoS (Denial of Service) напад је напад на:

Select one:

- a. поверљивост
- b. расположивост
- c. аутентификацију
- d. интегритет
- e. не знам

The correct answer is: расположивост

Question 51

Not answered

Marked out of 1.00

Дужина отиска (хеш вредност) SHA-2 алгоритма је:

Select one:

- a. 512 бита
- b. 256 бита
- c. у зависности од варијанте, могу бити све наведене вредности
- d. 384 бита
- e. не знам

The correct answer is: у зависности од варијанте, могу бити све наведене вредности

Question 52

Not answered

Marked out of 1.00

Single sign on je postupak kojim se obezbeđuje:

Select one:

- a. zaštita sistema takva da korisnik ima samo jedan pokušaj za prijavu sistemu
- b. da sistemu može da se pristupa samo preko jedinstvene lozinke/biometrije/uređaja...
- c. ne znam
- d. da sistemu može da pristupa samo jedna određena osoba
- e. da se korisnik prijavljuje samo jedanput a sve ostale naknadne prijave se obavljaju automatski

The correct answer is: da se korisnik prijavljuje samo jedanput a sve ostale naknadne prijave se obavljaju automatski

Question 53

Not answered

Marked out of 1.00

Salami Attack predstavlja:

Select one:

- a. kod koji se integriše u više različitih delova računara
- b. serija malih beznačajnih napada koji se mnogo puta ponavljaju
- c. napad koji otvara zadnja vrata (*backdoor*) na računaru za druge zlonamerne programe
- d. ne znam
- e. napad koji dugo ostaje neotkriven

The correct answer is: serija malih beznačajnih napada koji se mnogo puta ponavljaju

Question 54

Not answered

Marked out of 1.00

Код секвенцијалних алгоритама (који теже да превазиђу недостатке OTP шифре) шифрат се добија тако што се вредност отвореног текста сабира по модулу 2 (XOR) са

Select one:

- a. потпуно случајним кључем који је дужине отвореног текста
- b. не знам
- c. псеудо случајним бинарним низом који се добија од кратког случајног кључа
- d. са поновљеним кратким случајним кључем
- e. са кључем који се добија од кратког случајног кључа и отвореног текста

The correct answer is: псеудо случајним бинарним низом који се добија од кратког случајног кључа

Question 55

Not answered

Marked out of 1.00

Непорецивост је сервис који пријемној страни пружа необорив доказ да

Select one:

- a. не знам
- b. је поруку примио од тачно одређене особе
- c. током преноса поруке није дошло до нарушавања поверљивости
- d. је порука проверена од стране одговарајућег сертификационог тела
- e. је порука стигла непромењена

The correct answer is: је поруку примио од тачно одређене особе

Question 56

Not answered

Marked out of 1.00

Алиса шаље Бобу отворену поруку M и хеш те поруке $h(M)=h_1$. Боб по пријему поруке такође рачуна хеш $h(M)=h_2$. Упоређивањем h_1 и h_2 Боб проверава:

Select one:

- a. да ли је канал за комуникацију пресечен
- b. да ли је било прислушкивања током преноса
- c. не знам
- d. да ли је порука M промењена током преноса
- e. да ли је поруку послала Алиса

The correct answer is: да ли је порука M промењена током преноса

Question 57

Not answered

Marked out of 1.00

Нека је Z скуп знакова над којим се дефинише кључ. Уколико је кључ дужине 5 и

$Z=\{1,2,3,4,\dots,9,a,b,c,\dots,x,y,z,A,B,C,\dots,X,Y,Z,*,#,$\}$, тада је величина простора кључева уколико слова у кључу могу да се понављају:

Select one:

- a. 5^{64}
- b. $5^{64}-1$
- c. 64^5
- d. не знам
- e. 64^5-1

The correct answer is: 64^5

Question 58

Not answered

Marked out of 1.00

Jedno od mogućih rešenja za *single sign on* je:

Select one:

- a. keyboard logger
- b. ne znam
- c. smart kartica
- d. generator lozinki
- e. rečnik lozinki

The correct answer is: smart kartica

Question 59

Not answered

Marked out of 1.00

Za prikupljanje naizgled nebitnih podataka sa više različitih izvora koji objedinjeni daju konkretnu informaciju koristi se:

Select one:

- a. ne znam
- b. vremenske bombe
- c. napad linearizacijom
- d. *salami attack*
- e. trojanski konj

The correct answer is: *salami attack*

Question 60

Not answered

Marked out of 1.00

Jedna od nepожељних особина генератора псеудо случајних бројева је

Select one:

- a. то што не могу да се користе за OTP шифру
- b. не знам
- c. то што му је за рад потребна почетна вредност
- d. то што се у њиховом раду користе компликоване математичке функције
- e. периодичност

The correct answer is: периодичност

Question 61

Not answered

Marked out of 1.00

Нека је јавни кључ (N, e) приватни d . Поступак дигиталног потписивања поруке M је дефинисан са:

Select one:

- a. не знам
- b. $S = M^d \pmod{N}$
- c. $S = (M^d \pmod{N})^e$
- d. $S = (M^e \pmod{N})^d$
- e. $S = M^e \pmod{N}$

The correct answer is: $S = M^d \pmod{N}$

Question 62

Not answered

Marked out of 1.00

Шифровањем хеш вредности симетричним/асиметричним алгоритмом може истовремено да се врши:

Select one:

- a. провера интегритета и аутентификација
- b. не знам
- c. аутентификација и поверљивост
- d. провера интегритета и поверљивости
- e. провера интегритета, поверљивост и аутентификација

The correct answer is: провера интегритета и аутентификација

Question 63

Not answered

Marked out of 1.00

Autentifikacija pomoću smart kartice gde se dodatno zahteva i ukucavanje PIN koda je autentifikacija na osnovu nečega što:

Select one:

- a. korisnik ima, zna i jeste
- b. ne znam
- c. korisnik ima i zna
- d. korisnik ima i jeste
- e. korisnik zna i jeste

The correct answer is: korisnik ima i zna

Question 64

Not answered

Marked out of 1.00

Koji je od sledećih формата најпогоднији за LSB супституцију:

Select one:

- a. png
- b. tif
- c. bmp
- d. не знам
- e. jpeg

The correct answer is: bmp

Question 65

Not answered

Marked out of 1.00

Да би се успешно дешифраовао шифрат шифрован секвенцијалним шифарским системом неопходно је да се поседује

Select one:

- a. комплетан радни кључ
- b. случајни кључ и генератор псеудослучајних бројева
- c. не знам
- d. само случајан кључ
- e. само генератор псеудо случајних бројева

The correct answer is: случајни кључ и генератор псеудослучајних бројева

Question 66

Not answered

Marked out of 1.00

За шифровање и дигитално потписивање

Select one:

- a. не знам
- b. користи се исти или различити пар кључева, у зависности од договора страна у комуникацији
- c. користи се исти или различити пар кључева, у зависности од услова комуникације
- d. користи се различити пар кључева
- e. користи се исти пар кључева

The correct answer is: користи се различити пар кључева

Question 67

Not answered

Marked out of 1.00

Предност шифровања хеш вредности (приликом аутентификације и провере интегритета) асиметричним алгоритмом у односу на шифровање симетричним алгоритмом је то што:

Select one:

- a. нема потребе за "интерним" поверењем
- b. не знам
- c. што је поступак аутентификације бржи
- d. може да се провери и поверљивост
- e. нема потребе за употребом лиценцираног софтвера

The correct answer is: нема потребе за "интерним" поверењем

Question 68

Not answered

Marked out of 1.00

Линеарни померачки регистри

Select one:

- a. представљају коначно решење за генерирање радног кључа
- b. представљају напуштено решење за генераторе псевудослучајног низа бројева
- c. користе се за генерирање случајног кључа који се користи за формирање радног кључа
- d. користе се као градивни елементи сложенијих генератора
- e. не знам

The correct answer is: користе се као градивни елементи сложенијих генератора

Question 69

Not answered

Marked out of 1.00

Валидност јавних кључева

Select one:

- a. се утврђује помоћу дигиталног потписа
- b. не знам
- c. потврђује трећа страна од поверења
- d. је ствар поверења између страна у комуникацији
- e. се подразумева

The correct answer is: потврђује трећа страна од поверења

Question 70

Not answered

Marked out of 1.00

Приликом дигиталног потписивања (шифровања приватним кључем)

Select one:

- a. шифрује се хеш поруке
- b. не знам
- c. шифрује се цела порука
- d. шифрује се првих 64 бита поруке
- e. шифрује се унапред договорени део поруке

The correct answer is: шифрује се хеш поруке

Question 71

Not answered

Marked out of 1.00

За отворени тест и за шифровање користе се слова српске азбуке. Слова од А до Ш су редом нумерисана бројевима од 1 до 30 док су бројеви од од 31 до 36 додељени редом словима А,Е,Н,О,Р,Т. Шифрује се реч РЕНТА. Који од следећих шифрата **није** добијен коришћењем наведене шифре.

Select one:

- a. 20 32 16 22 31
- b. не знам
- c. 35 7 33 36 1
- d. 20 7 16 36 1
- e. 35 32 33 22 31
- f. 35 7 32 22 31

The correct answer is: 35 7 32 22 31

Question 72

Not answered

Marked out of 1.00

у конфигурационој датотеци aide.conf значи:

Select one:

- a. да се нaredba posle nje proverava
- b. да се naredba posle nje ne proverava
- c. ништа од наведеног
- d. не знам
- e. коментар

The correct answer is: коментар

Question 73

Not answered

Marked out of 1.00

! u konfiguracijskoj datoteci aide.conf znači:

Select one:

- a. da se naredba posle nje ne proverava
- b. ne znam
- c. da se naredba posle nje proverava
- d. komentar
- e. ništa od navedenog

The correct answer is: da se naredba posle nje ne proverava

Question 74

Not answered

Marked out of 1.00

Ako je u konfiguracijskoj datoteci aide.conf zadato pravilo: low=s+shal+c i ako je primijenjeno na datoteku primer, i ako istoj datoteci promenimo prava

Select one:

- a. AIDE će registrirati promenu bez navođenja i informacije mtime
- b. AIDE će registrirati promenu navođenjem i informacije mtime
- c. ne znam
- d. ništa od navedenog
- e. AIDE neće registrirati promenu

The correct answer is: AIDE će registrirati promenu bez navođenja i informacije mtime

Question 75

Not answered

Marked out of 1.00

AIDE naredba provere sistema je:

Select one:

- a. ništa od navedenog
- b. \$aide -c /etc/aide/aide.conf.autogenerated -C
- c. ne znam
- d. \$cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
- e. \$aide -c /etc/aide/aide.conf.autogenerated -i

The correct answer is: \$aide -c /etc/aide/aide.conf.autogenerated -C

Question 76

Not answered

Marked out of 1.00

AIDE naredba inicijalizacije sistema je:

Select one:

- a. ništa od navedenog
- b. \$cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
- c. \$aide -c /etc/aide/aide.conf.autogenerated -i
- d. ne znam
- e. \$aide -c /etc/aide/aide.conf.autogenerated -C

The correct answer is: \$aide -c /etc/aide/aide.conf.autogenerated -i

Question 77

Not answered

Marked out of 1.00

Informacije o promeni sistema AIDE skladišti:

Select one:

- a. prvo u bazu aide.db.new ali se potom mora ručno iskopirati u aide.db
- b. direktno u bazu aide.db
- c. ništa od navedenog
- d. ne znam
- e. u bazu aide.db.new ali se automatski kopira u aide.db

The correct answer is: prvo u bazu aide.db.new ali se potom mora ručno iskopirati u aide.db

Question 78

Not answered

Marked out of 1.00

Nakon izvršenja koda: @echo off :a ping localhost>>a.txt goto :a dešava se

Select one:

- a. napad prekoračenja bafera
- b. ne znam
- c. SQL injection napad
- d. DOS napad
- e. XSS napad

The correct answer is: DOS napad

Question 79

Not answered

Marked out of 1.00

Pravo x nad direktorijumom u Linux OS znači:

Select one:

- a. čitanje sadržaja direktorijuma
- b. izmena sadržaja direktorijuma
- c. pozicioniranje, prikazivanje dugog listinga i pretraživanje
- d. ne znam
- e. samo pozicioniranje

The correct answer is: pozicioniranje, prikazivanje dugog listinga i pretraživanje

Question 80

Not answered

Marked out of 1.00

U Linux OS pravo 654 odgovara:

Select one:

- a. rw---wxr-x
- b. r-x-wxrw-
- c. rw-r-xr--
- d. r-xrw-r--
- e. ne znam

The correct answer is: rw-r-xr--

Question 81

Not answered

Marked out of 1.00

Nakon izvršenja koda: @echo off :a dir>>a.txt goto :a

Select one:

- a. a.txt ne menja veličinu
- b. a.txt se neprekidno uvećava
- c. ne znam
- d. uvek se nanovo prepisuje isti sadržaj u a.txt
- e. matični direktorijum se puni novim datotekama

The correct answer is: a.txt se neprekidno uvećava

Question 82

Not answered

Marked out of 1.00

Prilikom slanja podataka iz html forme, može se reći da:

Select one:

- a. zavisi koji je podrazumevani metod
- b. metod GET otkriva podatke
- c. zavisi od web čitača
- d. metod POST otkriva podatke
- e. ne znam

The correct answer is: metod GET otkriva podatke

Question 83

Not answered

Marked out of 1.00

Kod velikih sistema direktna primena Lampsonove matrice je:

Select one:

- a. nemoguća
- b. složena i spora za izvršenje
- c. ne znam
- d. preporučljiva
- e. obavezna

The correct answer is: složena i spora za izvršenje

Question 84

Not answered

Marked out of 1.00

Mrežna barijera tipa *packet filter*

Select one:

- a. ne znam
- b. analizira kompletan paket ali ne prati stanje konekcije
- c. analizira samo zaglavljiva paketa ali ne prati stanje konekcije
- d. analizira zaglavljiva paketa i prati stanje konekcije
- e. analizira kompletan paket i pamti stanje konekcije

The correct answer is: analizira samo zaglavljiva paketa ali ne prati stanje konekcije

Question 85

Not answered

Marked out of 1.00

Bitno svojstvo IDS-a zasnovanog na potpisu je:

Select one:

- a. otkrivanje i nepoznatih napada
- b. brzo i jednostavno otkrivanje već poznatih napada
- c. mogućnost otkrivanja anomalija u sistemu
- d. to što ne moraju da se ažuriraju
- e. ne znam

The correct answer is: brzo i jednostavno otkrivanje već poznatih napada

Question 86

Not answered

Marked out of 1.00

Autentifikacija pomoću otiska prsta je odluka na osnovu nečega

Select one:

- a. što korisnik jeste
- b. ne znam
- c. što korisnik zna
- d. što korisnik ima
- e. što korisnik zna da ima

The correct answer is: što korisnik jeste

Question 87

Not answered

Marked out of 1.00

Kod *challenge-response* autentifikacije, ukoliko Boban želi da autentikuje Anu on joj šalje:

Select one:

- a. slučajnu vrednost
- b. ne znam
- c. heš vrednost svoje lozinke
- d. svoju lozinku kojoj je dopisana slučajna vrednost
- e. heš slučajne vrednosti

The correct answer is: slučajnu vrednost

Question 88

Not answered

Marked out of 1.00

Primenom disasemblera od binarnog koda dobija se:

Select one:

- a. precizan izvorni kod višeg programskog jezika iz koga je binarni fajl kompajliran
- b. neprecizna asemblerski kod
- c. precizan asemblerski kod
- d. neprecizan izvorni kod višeg programskog jezika iz koga je binarni fajl kompajliran
- e. ne znam

The correct answer is: neprecizna asemblerski kod

Question 89

Not answered

Marked out of 1.00

Granične adrese koje koristi jedan korisnik/proces kod istoimene metode mogu da budu:

Select one:

- a. samo obe dinamičke
- b. obe istovremeno statičke ili obe istovremeno dinamičke
- c. ne znam
- d. početna statička a krajnja dinamička
- e. samo obe statičke

The correct answer is: obe istovremeno statičke ili obe istovremeno dinamičke

Question 90

Not answered

Marked out of 1.00

Uobičajeno, zlonamerni programi se dele na osnovu:

Select one:

- a. štete koju čine u sistemu
- b. težine detektovanja
- c. ne znam
- d. principa širenja i delovanja
- e. načina neutralisanja

The correct answer is: principa širenja i delovanja

Question 91

Not answered

Marked out of 1.00

Тајност комуникација се односи на:

Select one:

- a. спречавање неовлашћених лица да дођу до садржаја поруке или података који се преносе тајним комуникационим путевима
- b. не знам
- c. спречавање неовлашћених лица да дођу до садржаја поруке или података током преноса и чувања
- d. спречавање неовлашћених лица да дођу до садржаја поруке или података који се преносе јавним комуникационим путевима
- e. омогућавање овлашћеним лицима да дођу до садржаја поруке или података који се преносе јавним комуникационим путевима

The correct answer is: спречавање неовлашћених лица да дођу до садржаја поруке или података који се преносе јавним комуникационим путевима

Question 92

Not answered

Marked out of 1.00

Шифрарски систем је сигуран ако

Select one:

- a. је најефикаснији познати напад потпуна претрага простора кључева који треба да је довољно велики.
- b. ако из шифрата могу да се добију само минималне информације о алгоритму и отвореном тексту.
- c. не знам
- d. ако се у алгоритму шифровања користи што више различитих операција
- e. ако је простор кључева већи од 2^{100}

The correct answer is: је најефикаснији познати напад потпуна претрага простора кључева који треба да је довољно велики.

Question 93

Not answered

Marked out of 1.00

Задатак савремених алгоритама шифровања је да

Select one:

- a. трансформише низове битова који носе информацију из отвореног текста у нови бинарни низ на такав начин да неовлашћене стране анализом шифрата не могу да дођу до информација које постоје у отвореном тексту.
- b. да кодује отворени текст у бинарни низ на такав начин да неовлашћене стране анализом шифрата не могу да дођу до информације који је систем кодовања коришћен и тиме не могу да дођу до информације које постоје у отвореном тексту.
- c. да прво кодује а отворени текст а затим одређеним операцијама трансформише тај низ битова у облик тако да се од неовлашћене стране скрије чињеница да се информација преноси.
- d. не знам
- e. интегрише низ битова који носе информацију у отворени текст на такав начин да неовлашћена страна анализом шифрата не може да дође до информације која постоји у отвореном тексту.

The correct answer is: трансформише низове битова који носе информацију из отвореног текста у нови бинарни низ на такав начин да неовлашћене стране анализом шифрата не могу да дођу до информација које постоје у отвореном тексту.

Question 94

Not answered

Marked out of 1.00

Хеш функција је

Select one:

- a. једносмерна функција која за улаз произвољне коначне величине даје излаз исте дужине као што је улаз
- b. инвертибилна функција која за улаз произвољне коачне величине даје излаз исте дужине као што је улаз
- c. једносмерна функција која за улаз произвољне коачне величине даје излаз фиксне дужине
- d. не знам
- e. инвертибилна функција која за улаз произвољне коачне величине даје излаз фиксне дужине

The correct answer is: једносмерна функција која за улаз произвољне коачне величине даје излаз фиксне дужине

Question 95

Not answered

Marked out of 1.00

Статистичка детекција је метода која се користи

Select one:

- a. не знам
- b. за аутентификацију
- c. за постојање скривених порука у стеганоанализи
- d. за постојање скривених порука у криптоанализи
- e. за проверу интегритета података

The correct answer is: за постојање скривених порука у стеганоанализи

Question 96

Not answered

Marked out of 1.00

Који од наведених алгоритама је секвенцијални?

Select one:

- a. DES
- b. не знам
- c. Twofish
- d. AES
- e. A5/1

The correct answer is: A5/1

Question 97

Not answered

Marked out of 1.00

Серификационо тело (CA) потврђује валидност јавних кључева сертификатом који

Select one:

- a. CA потписује својим јавним кључем
- b. не знам
- c. се не потписује јер су се учесници у комуникацији договорили да је CA страна од поверења
- d. CA потписује својим тајним кључем
- e. потписује власник сертификата својим тајним кључем

The correct answer is: CA потписује својим тајним кључем

Question 98

Not answered

Marked out of 1.00

MAC (*Mesage Authentification Code*) се добија тако што се

Select one:

- a. порука се шифрује секвенцијално а затим се узима унапред договорени део шифрата
- b. блоковским алгоритмом се шифрује само први блок поруке
- c. порука се шифрује секвенцијално а затим се узима само последњих 64 бита шифрата
- d. порука шифрује блоковским алгоритмом а затим се памти само последњи блок шифрата
- e. не знам

The correct answer is: порука шифрује блоковским алгоритмом а затим се памти само последњи блок шифрата

Question 99

Not answered

Marked out of 1.00

Када се информација крије унутар видео фајла углавном се користи:

Select one:

- a. DCT метода
- b. не знам
- c. Водени печат
- d. Imagedowngrading
- e. LSB метода

The correct answer is: DCT метода

Question 100

Not answered

Marked out of 1.00

Нека је Z скуп знакова над којим се дефинише кључ. Уколико је кључ дужине 5 и

$Z = \{0, 1, 2, 3, 4, \dots, 9, a, b, c, \dots, x, y, z, A, B, C, \dots, X, Y, Z\}$, тада је величина простора кључева, уколико слова у кључу не могу да се понављају:

Select one:

- a. $62!^5$
- b. $(62*61*60*59*58)^5$
- c. $62*61*60*59*58$
- d. не знам
- e. $62!/5!$

The correct answer is: $62*61*60*59*58$

Question 101

Not answered

Marked out of 1.00

Секвенцијални алгоритми

Select one:

- a. се користе тамо где је битно да шифрат буде пренет без грешака
- b. не знам
- c. се користе тамо где је битна брзина и рад у реалном времену
- d. се више не користе
- e. се користе као део већих шифарских система

The correct answer is: се користе тамо где је битна брзина и рад у реалном времену

Question 102

Not answered

Marked out of 1.00

MAC (*Message Authentication Code*) може да се користи у процесу:

Select one:

- a. провере интегритета
- b. не знам
- c. провере поверљивости
- d. ауторизације
- e. аутентификације

The correct answer is: аутентификације

Question 103

Not answered

Marked out of 1.00

Када се порука скривена методом `imagedowngradin` враћа назад, тако добијена слика је

Select one:

- a. већа од скривене
- b. мања од скривене
- c. идентична скривеној
- d. апроксимирана је у односу на скривену
- e. не знам

The correct answer is: апроксимирана је у односу на скривену

Question 104

Not answered

Marked out of 1.00

Шифарски систем ако не може да буде "разбијен" ни уз примену неограничених ресурса, људства и времена је

Select one:

- a. безусловно сигуран
- b. делимично сигуран
- c. рачунски сигуран
- d. несигуран
- e. не знам

The correct answer is: безусловно сигуран

Question 105

Not answered

Marked out of 1.00

Секвенцијалнио алгоритми

Select one:

- a. се реализују искључиво софтверски
- b. се реализују искључиво хардверски
- c. не знам
- d. представљају само идејни концепт
- e. могу да се реализују и хардверски и софтверски

The correct answer is: могу да се реализују и хардверски и софтверски

Question 106

Not answered

Marked out of 1.00

Који модел PKI (Public Key Infrastructure) се користи код савремених Интернет претраживача:

Select one:

- a. претраживачи у свом раду немају потребу да користе PKI
- b. олигархијски модел
- c. не знам
- d. монополски модел
- e. зависи од претраживача

The correct answer is: олигархијски модел

Question 107

Not answered

Marked out of 1.00

Дужина кључа који је потребан за израчунавање HMAC (*Hash Mesage Authentication Code*) вредности је:

Select one:

- a. бар 128 бита
- b. не знам
- c. дужине поруке
- d. већи од 64 бита
- e. мањи од 64 бита

The correct answer is: мањи од 64 бита

Question 108

Not answered

Marked out of 1.00

Када се порука сакривена LSB методом враћа назад, тако добијена слика је

Select one:

- a. мања од сакривене
- b. идентична сакривеној
- c. не знам
- d. већа од сакривене
- e. апроксимирана је у односу на сакривену

The correct answer is: идентична сакривеној

Question 109

Not answered

Marked out of 1.00

Безусловно сигурна шифра:

Select one:

- a. не знам
- b. је кодна књига
- c. је ECB
- d. не постоји
- e. је OTP шифра

The correct answer is: је OTP шифра

Question 110

Not answered

Marked out of 1.00

Изабрати тачно тврђење:

Select one:

- a. не знам
- b. однос брзина асиметричних и симетричних алгоритама зависе од конкретних алгоритама
- c. брзине извршења асиметричних и симетричних алгоритама су приближно исте
- d. асиметрични алгоритми су бржи од симетричних
- e. асиметрични алгоритми су спорији од симетричних

The correct answer is: асиметрични алгоритми су спорији од симетричних

Question 111

Not answered

Marked out of 1.00

Колико параметара има функција HMAC (*Hash Mesage Authentification Code*):

Select one:

- a. не знам
- b. 3 - (M,K,h(M))
- c. 1 - (M)
- d. 2 - (M,K)
- e. 4 - (M,K,h(M),h(K))

The correct answer is: 2 - (M,K)

Question 112

Not answered

Marked out of 1.00

OTP је безусловно сигурна шифра:

Select one:

- a. безусловно сигурне шифре нема
- b. уз одређене услове
- c. не знам
- d. претпостављано
- e. доказано

The correct answer is: доказано

Question 113

Not answered

Marked out of 1.00

Блоковски алгоритми

Select one:

- a. се реализују равноправно и софтверски и хардверски
- b. се најчешће реализују хардверски
- c. се најчешће реализују софтверски
- d. не знам
- e. представљају само идејно решење

The correct answer is: се најчешће реализују софтверски

Question 114

Not answered

Marked out of 1.00

Асиметрични криптографски алгоритми се често користе

Select one:

- a. за размену симетричног кључа којим се затим шифрује порука
- b. за шифровање великих датотека
- c. за шифровање порука када је битна брзина
- d. не знам
- e. за шифровање веома поверљивих података

The correct answer is: за размену симетричног кључа којим се затим шифрује порука

Question 115

Not answered

Marked out of 1.00

Фиксне вредности ipad (0x360x36...0x36) и opad (0x560x56...0x56), свака дужине по 64 бита, се користе за израчунавање:

Select one:

- a. HMAC вредности
- b. MAC вредности
- c. хеш функције у MD5 алгоритму
- d. хеш функције у SHA-x алгоритмима
- e. не знам

The correct answer is: HMAC вредности

Question 116

Not answered

Marked out of 1.00

Техника којом се у дигитални садржај утискују додатне информације као што су подаци о аутору, власништву, лиценцама и слично назива се:

Select one:

- a. LSB супституција
- b. водени печат
- c. не знам
- d. imagedowngrading
- e. DCT метода

The correct answer is: водени печат

Question 117

Not answered

Marked out of 1.00

OTP шифра може да се користи

Select one:

- a. нема правила везаног за број коришћења
- b. само два пута
- c. не знам
- d. највише пет пута
- e. само једном

The correct answer is: само једном

Question 118

Not answered

Marked out of 1.00

За дигитално потписивање користе се

Select one:

- a. хибридни криптографски системи
- b. симетрични криптографски системи
- c. не знам
- d. криптографски системи које је одредило изабрано сертификационо тело
- e. асиметрични криптографски системи

The correct answer is: асиметрични криптографски системи

Question 119

Not answered

Marked out of 1.00

Уградњом података о времену слања поруке у саму поруку,

Select one:

- a. може да се открије поновно слање исте поруке
- b. може да се изврши ауторизација
- c. може да се открије неовлашћена измена података
- d. може да се изврши аутентификација
- e. не знам

The correct answer is: може да се открије поновно слање исте поруке

Question 120

Not answered

Marked out of 1.00

Код LSB супституције колико битова максимално може да се промени а да то остане непримећено ?

Select one:

- a. до 40%
- b. до 50%
- c. не знам
- d. до 20%
- e. до 30%

The correct answer is: до 50%

Question 121

Not answered

Marked out of 1.00

У класификацији стеганографских техника компјутерска стеганографија спада у:

Select one:

- a. безшифарне технике
- b. техничку стеганографију
- c. не знам
- d. семаграме
- e. решеткасти код

The correct answer is: безшифарне технике

Question 122

Not answered

Marked out of 1.00

Отворени текст ПЕРА шифрује се Вижнеровом шифром са кључем ПЕРА. Алфабет који се користи је српска азбука и слова су нумерисана редом бројевима од 1 до 30. Шифрат који се добија на тај начин је:

Select one:

- a. ЖЉИБ
- b. отворени текст и кључ не смеју да буду исти
- c. БИЛО
- d. ОЛИБ
- e. не знам

The correct answer is: ЖЉИБ

Question 123

Not answered

Marked out of 1.00

Аутентификација која се реализује шифровањем хеш вредности симетричним алгоритмом подразумева

Select one:

- a. постојање "интерног" поверења
- b. тајну комуникацију
- c. не знам
- d. претходну проверу поверљивости
- e. употребу MAC-а

The correct answer is: постојање "интерног" поверења

Question 124

Not answered

Marked out of 1.00

Ако је

 $X=01011001$ и $Y=11001100$

тада је

 $((X \text{ xor } X) \text{ xor } Y) \text{ xor } Y$

једнако

Select one:

- a. X
- b. не знам
- c. $X \text{ xor } Y$
- d. Y
- e. 0

The correct answer is: X **Question 125**

Not answered

Marked out of 1.00

Нека је дат јавни кључ $(N,e)=(299,31)$. За генерирање тајног кључа користи се RSA алгоритам. Који од следећих бројева може бити тајни кључ:Напомена: $N=13*23$

Select one:

- a. сва три понуђена
- b. 247
- c. 775
- d. не знам
- e. 511

The correct answer is: сва три понуђена

Question 126

Not answered

Marked out of 1.00

Случајна измена садржаја поруке током преноса

Select one:

- a. не знам
- b. се детектује другачијим механизмима у односу на механизме детекције намерне измене
- c. се спречава уградњом механизма за опоравак података
- d. се игнорише
- e. спада у нарушување интегритета поруке

The correct answer is: спада у нарушување интегритета поруке

Question 127

Not answered

Marked out of 1.00

Шта се код стеганографије крије ?

Select one:

- a. комуникација
- b. чињеница да се преноси порука
- c. стеганографски медијум
- d. не знам
- e. стеганографски канал

The correct answer is: чињеница да се преноси порука

Question 128

Not answered

Marked out of 1.00

Нека се реч CAKE шифрује Плејферовом шифром са кључем TEST. Алфабет који се користи су велика слова енглеске абецеде где се поистовећују слова I и J. Шифрат добијен на тај начин је:

Select one:

- a. не знам
- b. GTPD
- c. TGPD
- d. TGDP
- e. не знам
- f. GTDP

The correct answer is: GTPD

Question 129

Not answered

Marked out of 1.00

Фејстелова шифра (мрежа) представља

Select one:

- a. посебан секвенцијалан алгоритам
- b. посебан блоковски алгоритам
- c. не знам
- d. идејно решење секвенцијалне шифре
- e. једно идејно решење блоковске шифре

The correct answer is: једно идејно решење блоковске шифре

Question 130

Not answered

Marked out of 1.00

Предност шифровања хеш вредности асиметричним алгоритмом у односу на шифровање симетричним алгоритмом је у томе што

Select one:

- a. не знам
- b. нема потребе за "интерним" поверењем
- c. може да се провери и поверљивост
- d. нема потребе за употребом лиценцираног софтвера
- e. је поступак аутентификације бржи

The correct answer is: нема потребе за "интерним" поверењем

Question 131

Not answered

Marked out of 1.00

Modeli sigurnosti:

Select one:

- a. детаљно прописују додатна ограничења и одређују начин њихове реализације
- b. уводе јасно дефинисана ограничења на додатне мере
- c. дaju стриктна упутства о реализацији додатних мера
- d. ne znam
- e. само дaju препоруке за додатна ограничења

The correct answer is: само дaju препоруке за додатна ограничења

Question 132

Not answered

Marked out of 1.00

Мрежна баријера типа *stateful packet filter*

Select one:

- a. анализира само заглавља пакета али не прати стање конекције
- b. анализира комплетан пакет али не прати стање конекције
- c. анализира заглавља пакета и прати стање конекције
- d. анализира комплетан пакет и памти стање конекције
- e. ne znam

The correct answer is: анализира заглавља пакета и прати стање конекције

Question 133

Not answered

Marked out of 1.00

Stalno ažuriranje IDS-a zasnovanog na potpisu je:

Select one:

- a. nepreporučljivo
- b. preporučljivo
- c. nebitno za rad sistema
- d. neophodno
- e. ne znam

The correct answer is: neophodno

Question 134

Not answered

Marked out of 1.00

Rečnik često korišćenih lozinki:

Select one:

- a. ne postoji
- b. ne znam
- c. postoji
- d. u izradi je
- e. postoji ideja da se napravi

The correct answer is: postoji

Question 135

Not answered

Marked out of 1.00

Cilj savršene sigurnosti unazad (PFC) je:

Select one:

- a. ne znam
- b. da se spreči da neovlašćeno lice sazna sesijski ključ
- c. da se spreči da neovlašćeno lice dešifruje poruke koje su ranije razmenjene čak i ako naknadno sazna tajni ključ
- d. da se spreči ponovljeno slanje poruke od strane neovlašćenog lica
- e. da se sazna da li je u nekoj prethodnoj komunikaciji učestvovalo neovlašćeno lice

The correct answer is: da se spreči da neovlašćeno lice dešifruje poruke koje su ranije razmenjene čak i ako naknadno sazna tajni ključ

Question 136

Not answered

Marked out of 1.00

Samo-modifikujući kod:

Select one:

- a. otporan je na pokušaj izmene "spolja"
- b. sam se prilagođava okruženju
- c. ima sposobnost da menja svoj izvorni kod nakon izvesnog vremena
- d. ima sposobnost da menja svoju izvršnu verziju nakon svakog izvršavanja
- e. ne znam

The correct answer is: ima sposobnost da menja svoju izvršnu verziju nakon svakog izvršavanja

Question 137

Not answered

Marked out of 1.00

Jedna od prednosti segmentacije memorije kao metode zaštite je:

Select one:

- a. moguće je ostvariti različite nivoje zaštite kod različitih segmenata
- b. ne treba da prati promene u veličini segmenata
- c. ne zahteva veliko angažovanje operativnog sistema
- d. ne znam
- e. ne treba da se parti promena lokacije segmenta

The correct answer is: moguće je ostvariti različite nivoje zaštite kod različitih segmenata

Question 138

Not answered

Marked out of 1.00

Стеганографија је:

Select one:

- a. процес уграђивања тајне поруке у другу тајну поруку при чему треба да се прикрије чињеница да се комуницира
- b. процес уграђивања поруке која треба да је тајна у поруку која такође треба да је тајна
- c. не знам
- d. процес прикривања чињенице да се преноси тајна порука
- e. процес уграђивања поруке која треба да је тајна у поруку која није тајна

The correct answer is: процес уграђивања поруке која треба да је тајна у поруку која није тајна

Question 139

Not answered

Marked out of 1.00

Реч ГОРА је шифрована различитим шифрама. Који од понуђених шифрата је добијен коришћењем шифре транспозиције:

Select one:

- a. не знам
- b. АГРО
- c. РАГА
- d. ГАРИ
- e. РОДА

The correct answer is: АГРО

Question 140

Not answered

Marked out of 1.00

Крипtosистеми који користе исти кључ за шифровање и дешифровање називају се:

Select one:

- a. симетрични крипто системи
- b. не знам
- c. блоковски крипто системи
- d. секвенцијални крипто системи
- e. тајни крипто системи

The correct answer is: симетрични крипто системи

Question 141

Not answered

Marked out of 1.00

Да ли хеш функција треба да поседује својство лавинског ефекта?

Select one:

- a. нема става
- b. да
- c. пожељно је
- d. не знам
- e. не

The correct answer is: да

Question 142

Not answered

Marked out of 1.00

Кључ код Хилове шифре је матрица која

Select one:

- a. не мора да буде инвертибилна уколико се користи само једном
- b. не мора да буде инвертибилна
- c. мора бити инвертибилна
- d. не мора бити инвертибилна али све подматрице морају
- e. не знам

The correct answer is: мора бити инвертибилна

Question 143

Not answered

Marked out of 1.00

Хеш функције се не користе за шифровање порука јер је

Select one:

- a. тада тешко утврдити да ли је дошло до нарушавања интегритета поруке
- b. не знам
- c. немогуће извршити дешифровање
- d. шифровање веома споро
- e. несигурно јер хеш функције не користе кључ

The correct answer is: немогуће извршити дешифровање

Question 144

Not answered

Marked out of 1.00

Šta od sledećeg ne prati stanje konekcije?

Select one:

- a. stateless paket filter
- b. proxy server
- c. ne znam
- d. NAT
- e. statefull paket filter

The correct answer is: stateless paket filter

Question 145

Not answered

Marked out of 1.00

Лавински ефекат је такво својство алгоритма (функције) да

Select one:

- a. мале промене улаза изазивају мале промене излаза
- b. мале промене улаза изазивају велике промене излаза
- c. да промене улаза прате промене излаза
- d. да промене на улазу немају никакав утицај на излаз
- e. не знам

The correct answer is: мале промене улаза изазивају велике промене излаза

Question 146

Not answered

Marked out of 1.00

Нека је дат јавни кључ $(N,e)=(77,13)$. За генерирање тајног кључа користи се RSA алгоритам. Који од следећих бројева може бити тајни кључ:

Nапомена: $N=7*11$

Select one:

- a. 33
- b. 35
- c. не знам
- d. 39
- e. 37

The correct answer is: 37

Question 147

Not answered

Marked out of 1.00

За шифровање Афином шифром користе се само велика слова енглеске абецеде нумерисана од 0 до 25. Ако је кључ уређени пар $(3,17)$, како гласи формула за дешифровање?

Select one:

- a. $d(y)=3(y-23)(\text{mod } 26)$
- b. $d(y)=9(y-23)(\text{mod } 26)$
- c. не знам
- d. $d(y)=9(y-17) \ (\text{mod } 26)$
- e. $d(y)=3(y-17)(\text{mod } 26)$

The correct answer is: $d(y)=9(y-17) \ (\text{mod } 26)$

Question 148

Not answered

Marked out of 1.00

DES алгоритам је:

Select one:

- a. не знам
- b. је само идејно решење
- c. блоковски алгоритам Фејстеловог типа
- d. секвенцијални алгоритам
- e. итеративни блоковски алгоритам

The correct answer is: блоковски алгоритам Фејстеловог типа

Question 149

Not answered

Marked out of 1.00

Čemu služi komanda? iptables -A FORWARD -d 172.16.32.2 --dport http -j DROP

Select one:

- a. pušta sve HTTP saobraćajna web server
- b. odbija pakete sa adrese 172.16.32.2 na port 80
- c. ne znam
- d. blokira se prolaz paketa sa adrese 172.16.32.2 na port 80 na server kome su namenjeni
- e. pušta sve pakete sa adrese 172.16.32.2 na port 80 na lokalni računar

The correct answer is: blokira se prolaz paketa sa adrese 172.16.32.2 na port 80 na server kome su namenjeni

Question 150

Not answered

Marked out of 1.00

Koju vrstu napada sprečavamo komandom?

```
iptables -A FORWARD -p tcp --tcp-flags SYN,ACK,FIN,RST -i public_interface -m limit --limit 1/s -j ACCEPT
```

Select one:

- a. DOS
- b. SYN flood
- c. ne znam
- d. Port scan
- e. Ping of death

The correct answer is: Port scan

Question 151

Not answered

Marked out of 1.00

Ukoliko je neprivilegovani korisnik Windows sistema George kome je dato pravo upisa u direktorijum C:\1 član grupe CannibalCorpse kojoj je dato pravo Read and Execute za taj direktorijum, da li korisnik može da upiše fajl u taj direktorijum?

Select one:

- a. ne može se odrediti na osnovu navedenog
- b. zavisi od članstva u ostalim grupama
- c. može
- d. ne znam
- e. ne može

The correct answer is: ne može

Question 152

Not answered

Marked out of 1.00

Сигурност DES алгоритма почива на

Select one:

- a. броју рунди
- b. величини кључа
- c. генерисању подкључка
- d. не знам
- e. S-боксовима

The correct answer is: S-боксовима

Question 153

Not answered

Marked out of 1.00

Čemu služi komanda chattr -i /etc/passwd?

Select one:

- a. komanda nema nikakav uticaj na datoteku /etc/passwd
- b. ne znam
- c. dozvoljava izmenu sadržaja datoteke /etc/passwd korisnicima koji imaju prava izmene sadržaja te datoteke
- d. zabranjuje izmenu sadržaja datoteke /etc/passwd
- e. zabranjuje iščitavanje datoteke od strane običnih korisnika

The correct answer is: dozvoljava izmenu sadržaja datoteke /etc/passwd korisnicima koji imaju prava izmene sadržaja te datoteke

Question 154

Not answered

Marked out of 1.00

Čemu služi komanda sudo -u wcoyote jed /home

Select one:

- a. ne znam
- b. korisnik koji pokreće komandu izvršava jed /home kao korisnik root
- c. svim korisnicima daje pravo da odrede jed /home kao root korisnici
- d. korisnik koji pokreće komandu izvršava jed /home kao korisnik wcoyote
- e. korisniku wcoyote daje pravo da odradi komandu jed /home kao root

The correct answer is: korisnik koji pokreće komandu izvršava jed /home kao korisnik wcoyote

Question 155

Not answered

Marked out of 1.00

AES алгоритам је:

Select one:

- a. итеративни блоковски алгоритам
- b. секвенцијални алгоритам
- c. алгоритам који се не користи за шифровање
- d. не знам
- e. блоковски алгоритам Фејстеловог типа

The correct answer is: итеративни блоковски алгоритам

Question 156

Not answered

Marked out of 1.00

Koja distribucija Linuxa nema root nalog?

Select one:

- a. ne znam
- b. openSUSE
- c. Ubuntu
- d. sve distribucije imaju root nalog
- e. Red Hat

The correct answer is: sve distribucije imaju root nalog

Question 157

Not answered

Marked out of 1.00

Model sigurnosti sa više nivoa je pojam koji se odnosi na uvođenje:

Select one:

- a. ne znam
- b. kontrole u više različitih tačaka sistema
- c. različitih stepena tajnosti resursa
- d. različitih nivoa restrikcija u sistemu
- e. kontrole sistema spolja

The correct answer is: različitih stepena tajnosti resursa

Question 158

Not answered

Marked out of 1.00

Mrežna barijera tipa *application proxy*

Select one:

- a. analizira kompletan paket i pamti stanje konekcije
- b. analizira kompletan paket ali ne prati stanje konekcije
- c. ne znam
- d. analizira zaglavlja paketa i prati stanje konekcije
- e. analizira samo zaglavlja paketa ali ne prati stanje konekcije

The correct answer is: analizira kompletan paket i pamti stanje konekcije

Question 159

Not answered

Marked out of 1.00

Prednost IDS zasnovanog na anomalijama je to što:

Select one:

- a. brzo i jednostavno otkrivaju već poznate napade
- b. mogu da otkriju nepoznate napade
- c. ne moraju da se ažuriraju
- d. lako i jednostavno se implementiraju
- e. ne znam

The correct answer is: mogu da otkriju nepoznate napade

Question 160

Not answered

Marked out of 1.00

U praksi, kao najprihvatljivije rešenje za izbor lozinki pokazao se izbor:

Select one:

- a. ne znam
- b. zasnovan na bilo kojem od ostala tri ponuđena principa (svi su se pokazali podjednako dobri/loši)
- c. zasnovan na potpuno slučajnom izboru znakova
- d. zasnovan na ličnim podacima
- e. zasnovan na frazama

The correct answer is: zasnovan na frazama

Question 161

Not answered

Marked out of 1.00

Timestamp:

Select one:

- a. ne znam
- b. je simetrični ključ koji se koristi za šifrovanje poruka u datom trenutku
- c. je podatak o vremenu kada je izvršena autentifikacija radi dokumentovanja komunikacije
- d. je podatak o trenutnom vremenu koji se koristi u bezbednosnim protokolima
- e. je sesijski ključ koji se koristi u bezbednosnim protokolima

The correct answer is: je podatak o trenutnom vremenu koji se koristi u bezbednosnim protokolima

Question 162

Not answered

Marked out of 1.00

Zlonamerni programi koji se šire tako što navedu korisnike da pokrenu (najčešće) besplatne aplikacije za koje se kasnije pokaže da imaju funkciju različitu od očekivane nazivaju se:

Select one:

- a. trojanski konj
- b. *backdoor* (zadnja vrata)
- c. ne znam
- d. *rabbit*
- e. logička bomba

The correct answer is: trojanski konj

Question 163

Not answered

Marked out of 1.00

Hardware-based debugging (HardICE):

Select one:

- a. je program koji otkriva i blokira rad dibagera
- b. je dibager čije se aktivnosti teško detektuju
- c. je program koji otkriva prisustvo dibagera
- d. ne znam
- e. paket funkcija operativnog sistema Windows za utvrđivanje da li je program pokrenut pomoću dibagera

The correct answer is: je dibager čije se aktivnosti teško detektuju

Question 164

Not answered

Marked out of 1.00

Segmentacija i straničenje su metode koje se koriste za zaštitu:

Select one:

- a. baze računarskog sistema
- b. ne znam
- c. memorije
- d. procesa
- e. operativnog sistema

The correct answer is: memorije

Question 165

Not answered

Marked out of 1.00

Крипто системи са јавним и тајним кључем

Select one:

- a. користи јавни кључ за шифровање а тајни за десифровање
- b. користи прво јавни а затим тајни за шифровање а тајни па јавни за десифровање
- c. користи прво тајни а затим јавни за шифровање а јавни па тајни за десифровање
- d. користи тајни кључ за шифровање и јавни за десифровање
- e. не знам

The correct answer is: користи јавни кључ за шифровање а тајни за десифровање

Question 166

Not answered

Marked out of 1.00

Једносмерне функције:

Select one:

- a. не знам
- b. доказано не постоје
- c. за сваку функцију појединачно се доказује да је/није једносмерна
- d. није доказано ни да постоје ни да не постоје
- e. доказано постоје

The correct answer is: није доказано ни да постоје ни да не постоје

Question 167

Not answered

Marked out of 1.00

Основна примена хеш функција је

Select one:

- a. у поступку провере поверљивости
- b. у поступку аутентификације
- c. не знам
- d. за шифровање великих фајлова
- e. за шифровање фајлова када је битна брзина

The correct answer is: у поступку аутентификације

Question 168

Not answered

Marked out of 1.00

ECB (Electronic Codebook Mode)

Select one:

- a. за шифровање текућег блока користи кључ К и шифрат претходног блока
- b. за шифровање блока отвореног текста користи подкључ генерисан из подкључа претходног блока и претходни блок отвореног текста
- c. не знам
- d. шифрује блок отвореног текста тако што обави операцију XOR тог блока и шифрата претходног блока
- e. шифрује блок по блок са истим кључем К

The correct answer is: шифрује блок по блок са истим кључем К

Question 169

Not answered

Marked out of 1.00

CBC (Cipher Block Chaining)

Select one:

- a. шифрује блок отвореног текста тако што обави операцију XOR тог блока и шифрата претходног блока
- b. не знам
- c. за шифровање блока отвореног текста користи подкључ генерисан из подкључа претходног блока и претходни блок отвореног текста
- d. шифрује блок по блок са истим кључем К
- e. за шифровање текућег блока користи кључ К и шифрат претходног блока

The correct answer is: за шифровање текућег блока користи кључ К и шифрат претходног блока

Question 170

Not answered

Marked out of 1.00

Недостатак ECB режима рада је то што

Select one:

- a. не знам
- b. спори су
- c. не задовољава својство дифузије
- d. не задовољава својство конфузије
- e. истим блоковима одговарају исти шифрати

The correct answer is: истим блоковима одговарају исти шифрати

Question 171

Not answered

Marked out of 1.00

Код CBC режима рада блоковских алгоритама, евентуална намерна или случајна промена блока се аутоматски исправља након

Select one:

- a. не знам
- b. 16 блокова
- c. 4 блока
- d. 8 блокова
- e. 2 блока

The correct answer is: 2 блока

Question 172

Not answered

Marked out of 1.00

ByteSub, ShiftRow, MaxColumn, AddRoundKey су операције које се везују за

Select one:

- a. троструки DES алгоритам
- b. A5/1 алгоритам
- c. не знам
- d. AES алгоритам
- e. DES алгоритам

The correct answer is: AES алгоритам

Question 173

Not answered

Marked out of 1.00

Који је исказ тачан:

Select one:

- а. не знам
- б. интегритет представља скуп поступака који треба да открију да ли је дошло до неовлашћене измене података и обезбеди механизме за њихов опоравак
- с. интегритет представља скуп поступака који треба да спрече (или открију) неовлашћену измену података без обзира да ли су подаци јавни или шифровани
- д. интегритет представља скуп поступака који треба да спрече или открију неовлашћену измену података током преноса поверљивих података
- е. интегритет је скуп поступака који треба да обезбеди да не дође до било какве измене поверљивих података

The correct answer is: интегритет представља скуп поступака који треба да спрече (или открију) неовлашћену измену података без обзира да ли су подаци јавни или шифровани

Question 174

Not answered

Marked out of 1.00

MAC (*Mesage Authentication Code*) је:

Select one:

- а. кратка шифрована порука
- б. сервис (услуга)
- с. режим рада алгоритма
- д. криптографски алгоритам
- е. не знам

The correct answer is: кратка шифрована порука

Question 175

Not answered

Marked out of 1.00

Mrežna barijera koja može da spreči širenje zlonamernog softvera

Select one:

- a. je tipa *packet filter*
- b. je tipa *application proxy*
- c. ne postoji
- d. je tipa *stateful packet filter*
- e. ne znam

The correct answer is: je tipa *application proxy*

Question 176

Not answered

Marked out of 1.00

Timestamp je podatak koji se koristi u bezbednosnim protokolima:

Select one:

- a. da bi se sprečilo gubljenje paketa tokom slanja poruke
- b. da bi se sprečilo napad ponovljenog slanja poruke
- c. da bi se sprečio napad "čovek u sredini"
- d. ne znam
- e. da bi se sprečilo naknadno dešifrovanje poruka od strane neovlašćenog lica

The correct answer is: da bi se sprečilo napad ponovljenog slanja poruke

Question 177

Not answered

Marked out of 1.00

Zlonamerni programi koji omogućavaju neautorizovan pristup sistemu nazivaju se:

Select one:

- a. crv
- b. *trapdoor (backdoor)*
- c. *rabbit*
- d. ne znam
- e. trojanski konj

The correct answer is: *trapdoor (backdoor)*

Question 178

Not answered

Marked out of 1.00

Maskiranje koda je tehnika koja se koristi da:

Select one:

- a. se sakrije prisustvo koda u računaru
- b. bi se kod učinio teško razumljivim
- c. onemogući bilo kakva izmena koda
- d. bi se sakrila fizička lokacija koda
- e. ne znam

The correct answer is: bi se kod učinio teško razumljivim

Question 179

Not answered

Marked out of 1.00

Izabratи tačan iskaz:

Select one:

- a. straničenje deli memoriju na segmente promenljive veličine a segmentacija na segmente fiksne veličine
- b. i segmentacija i straničenje deli memoriju na segmente promenljive veličine
- c. ne znam
- d. straničenje deli memoriju na segmente fiksne veličine a segmentacija na segmente promenljive veličine
- e. i segmentacija i straničenje deli memoriju na segmente fiksne veličine

The correct answer is: straničenje deli memoriju na segmente fiksne veličine a segmentacija na segmente promenljive veličine

Question 180

Not answered

Marked out of 1.00

Salt je:

Select one:

- a. oblik u kome se lozinka čuva u računaru
- b. šifrovana lozinka
- c. oblik u koji se lozinka konvertuje pre nego što se računa njen heš
- d. slučajna vrednost koja se dodaje na lozinku
- e. ne znam

The correct answer is: slučajna vrednost koja se dodaje na lozinku

Question 181

Not answered

Marked out of 1.00

У Дифи Хелмановом протоколу, број r који се користи за степеновање по модулу p током израчунавања

Select one:

- a. треба да буде велики прост број
- b. може да буде било који велики број
- c. може да буде било који прост број
- d. не знам
- e. треба да буде производ два велика праста броја

The correct answer is: треба да буде велики прост број

Question 182

Not answered

Marked out of 1.00

За хеш функције је важно да

Select one:

- a. буду ефикасне
- b. да имају што ширу примену
- c. не знам
- d. да буду инвертибилне
- e. да им отисак (дужина) буде што дужи

The correct answer is: буду ефикасне

Question 183

Not answered

Marked out of 1.00

U modelu sigurnosti sa više nivoa:

Select one:

- a. svi objekti istog tipa dobijaju isti stepen tajnosti
- b. samo fajlovima se dodeljuje stepen tajnosti
- c. samo odabranim objektima se dodeljuje stepen tajnosti
- d. ne znam
- e. svakom objektu se dodeljuje stepen tajnosti

The correct answer is: svakom objektu se dodeljuje stepen tajnosti

Question 184

Not answered

Marked out of 1.00

Prednost mrežne barijere tipa *packet filter* je:

Select one:

- a. ne usporava saobraćaj (efikasnost)
- b. mogućnost odbacivanja paketa
- c. mogućnost praćenja stanja konekcije
- d. ne znam
- e. mogućnost analiziranja celog paketa

The correct answer is: ne usporava saobraćaj (efikasnost)

Question 185

Not answered

Marked out of 1.00

Da bi se postavio IDS zasnovan na anomalijama neophodno je:

Select one:

- a. prvo definisati "normalno" ponašanje sistema koji se štiti
- b. definisati prioritete zaštite
- c. prvo definisati bazu već poznatih napada
- d. same anomalije sistema koji se štiti svesti na minimum
- e. ne znam

The correct answer is: prvo definisati "normalno" ponašanje sistema koji se štiti

Question 186

Not answered

Marked out of 1.00

U fajlu lozinki za svakog korisnika, između ostalog, čuva se vrednost koja se dobija tako što se računa:

Select one:

- a. heš(lozinka)+heš(slučajna vrednost)
- b. heš(lozinka+slučajna vrednost)
- c. heš(lozinka)+slučajna vrednost
- d. ne znam
- e. heš(heš(lozinka)+slučajna vrednost)

The correct answer is: heš(lozinka+slučajna vrednost)

Question 187

Not answered

Marked out of 1.00

Kod autentifikacije koja koristi javni ključ **nije** bezbedno:

Select one:

- a. potpiši pa šifruj uz upotrebu slučajne vrednosti
- b. ne znam
- c. šifruj pa potpiši uz upotrebu slučajne vrednosti
- d. potpiši pa šifruj uz upotrebu podatka o vremenu
- e. šifruj pa potpiši uz upotrebu podatka o vremenu

The correct answer is: šifruj pa potpiši uz upotrebu podatka o vremenu

Question 188

Not answered

Marked out of 1.00

Zlonamerni softver koji nemenski troši sistemske resurse naziva se:

Select one:

- a. *trapdoor*
- b. ne znam
- c. trojanski konj
- d. *rabbit*
- e. crv

The correct answer is: *rabbit*

Question 189

Not answered

Marked out of 1.00

Da bi se otežao BOBE ("*break once, break everywhere*") napad koristi se:

Select one:

- a. ne znam
- b. HardICE
- c. maskirani softver
- d. šifrovani softver
- e. metamorfični softver

The correct answer is: metamorfični softver

Question 190

Not answered

Marked out of 1.00

Page table koristi operativni sistem da bi:

Select one:

- a. pratio promene veličine stranice
- b. lakše izvršio kontrolu pristupa određenim stranicama
- c. povezao stranice u koje je upisan neki podatak ili program
- d. povezao adresu stranice i njeno ime
- e. ne znam

The correct answer is: povezao stranice u koje je upisan neki podatak ili program

Question 191

Not answered

Marked out of 1.00

Шифром транспозиције колона шифрован је текст: DOG IS MAN'S BEST FRIEND. Димензија изабране матрице је 5x4 а кључна реч је HUSKY. Шифрат је:

Select one:

- a. DOGITBRISBESSMANENDX
- b. не знам
- c. DMEIISFDGNTNOASESBRX
- d. DSSTEOMBBNGAERDINSIX
- e. ISFDGNTNOASEDMEISBRX

The correct answer is: DMEIISFDGNTNOASESBRX

Question 192

Not answered

Marked out of 1.00

Алгоритми који у једном тренутку шифрују један бит (бајт) називају се:

Select one:

- a. секвенцијални алгоритми
- b. асиметрични алгоритми
- c. симетрични алгоритми
- d. блоковски алгоритми
- e. не знам

The correct answer is: секвенцијални алгоритми

Question 193

Not answered

Marked out of 1.00

Колизија код хеш функција означава појаву да

Select one:

- a. не знам
- b. иста порука може да да две различите хеш вредности
- c. две различите поруке дају исту хеш вредност
- d. да ако је дужина хеш вредности N, постоји низ дужине N који није хеш вредност ни једне поруке
- e. да постоји порука за коју не може да се израчуна хеш вредност

The correct answer is: две различите поруке дају исту хеш вредност

Question 194

Not answered

Marked out of 1.00

Jedan (od nekoliko) предуслова за постојање тајног канала је да:

Select one:

- a. пријемник и предајник на тајном каналу буду истог нивоа (имају иста права)
- b. су пријемник и предајник истовремено prisutni на тајном каналу
- c. нико други сем пријемника и предајника не сме да зна за постојање тајног канала
- d. пријемник и предајник деле неке zajedничке ресурсе
- e. ne znam

The correct answer is: пријемник и предајник деле неке zajedничке ресурсе

Question 195

Not answered

Marked out of 1.00

Slučajna vrednost koja se dodaje lozinkama služi:

Select one:

- a. da bi lozinka bila duža
- b. da se oteža napad rečnikom
- c. da se oteža napad grubom silom
- d. ne znam
- e. da bi heš lozinke bio duži

The correct answer is: da se oteža napad rečnikom

Question 196

Not answered

Marked out of 1.00

TCP protokol ne bi trebao da se koristi za autentifikaciju jer:

Select one:

- a. jer ne može da se koristi *timestamp*
- b. jer se TCP protokol koristi na transportnom nivou
- c. upotreba IP adrese za autentifikaciju ima ozbiljne sigurnosne nedostatke
- d. upotreba IP adrese za autentifikaciju je teška za realizaciju
- e. ne znam

The correct answer is: upotreba IP adrese za autentifikaciju ima ozbiljne sigurnosne nedostatke

Question 197

Not answered

Marked out of 1.00

Detekcija potpisa kao metoda za otkrivanje zlonamernih programa se zasniva na:

Select one:

- a. ne znam
- b. traženju sličnosti sa već poznatim zlonamernim programima
- c. praćenju promena u fajlovima
- d. registrovanju neuobičajenog ponašanja
- e. reverznom inženjeringu

The correct answer is: traženju sličnosti sa već poznatim zlonamernim programima

Question 198

Not answered

Marked out of 1.00

Nedostatak metamorfičnog softvera je:

Select one:

- a. da bi se efektivno sprečio napad treba primeniti više vrsta metamorfizma
- b. što se teško realizuje
- c. ne znam
- d. što nema uticaja na reverzni inženjering
- e. što se teško prate i ispravljaju eventualne greške

The correct answer is: što se teško prate i ispravljaju eventualne greške

Question 199

Not answered

Marked out of 1.00

Višestruko prepisivanje sadržaja diska različitim podacima se primenjuje:

Select one:

- a. ne znam
- b. da bi podaci bili razumljivi samo vlasniku ukoliko više korisnika istovremeno koristi isti memorijski prostor
- c. da bi se sprečilo kreiranje tajnog kanala
- d. radi zaštite podataka kada više korisnika koristi isti memorijski prostor
- e. radi zaštite podataka da ne bi više korisnika koristilo isti memorijski prostor

The correct answer is: radi zaštite podataka kada više korisnika koristi isti memorijski prostor

Question 200

Not answered

Marked out of 1.00

Дати су параметри $p=17$ и $q=5$. Алиса и Боб размењују кључеве уз помоћ Дифи Хелмановог алгоритма. Алиса је замислила број 3 а Боб 7. Алиса шаље Бобу:

Select one:

- a. $3^5 \pmod{17} = 5$
- b. $7^5 \pmod{17} = 11$
- c. не знам
- d. $5^3 \pmod{17} = 6$
- e. $5^7 \pmod{17} = 10$

The correct answer is: $5^3 \pmod{17} = 6$

Question 201

Not answered

Marked out of 1.00

Slučajna vrednost (salt) koja se pridružuje lozinkama je:

Select one:

- a. javna ili tajna u zavisnosti od broja korisnika
- b. javna za male sisteme a tajna za velike
- c. tajna
- d. javna
- e. ne znam

The correct answer is: javna

Question 202

Not answered

Marked out of 1.00

IKE (*Internet Key Exchange*) i ESP/AH (*Encapsulating Security Payload/Authentication Header*) su dve celine:

Select one:

- a. ne znam
- b. https protokola
- c. Kerberos protokola
- d. IPsec protokola
- e. SSL protokola

The correct answer is: IPsec protokola

Question 203

Not answered

Marked out of 1.00

Kod obavezne kontrole pristupa ko određuje prava pristupa objektu?

Select one:

- a. operativni sistem
- b. administrator sistema
- c. ne znam
- d. vlasnik objekta
- e. zavisi od operativnog sistema

The correct answer is: administrator sistema

Question 204

Not answered

Marked out of 1.00

Блоковски алгоритам у једном тренутку:

Select one:

- a. делују на један бајт отвореног текста
- b. не знам
- c. делују на један бајт унутар блока
- d. делују на све битове текућег блока и претходног блока
- e. делују на све битове унутар блока

The correct answer is: делују на све битове унутар блока

Question 205

Not answered

Marked out of 1.00

Дати су параметри $p=17$ и $q=11$. Алиса и Боб размењују кључеве уз помоћ Дифи Хелмановог алгоритма. Алиса је замислила број 7 а Боб 9. Боб шаље Алиси:

Select one:

- a. $7^{11} \pmod{17}=14$
- b. $9^{11} \pmod{17}=15$
- c. $11^7 \pmod{17}=3$
- d. не знам
- e. $11^9 \pmod{17}=6$

The correct answer is: $11^9 \pmod{17}=6$

Question 206

Not answered

Marked out of 1.00

Teoretski, biometrisku autentifikaciju je najbolje vršiti pomoću:

Select one:

- a. karakteristika irisa
- b. otiska prsta
- c. geometrije dlana
- d. ne znam
- e. karakteristika irisa, dlana ili otiska prsta bez razlike

The correct answer is: karakteristika irisa

Question 207

Not answered

Marked out of 1.00

Koje od sledećih svojstava **nije** poželjno za sigurnosni protokol:

Select one:

- a. ne znam
- b. da bude što komplikovaniji i računski složen
- c. da radi i kada se menjaju uslovi prenosa
- d. treba da radi i u slučaju kada napadač pokuša da ga "razbije"
- e. da bude robustan

The correct answer is: da bude što komplikovaniji i računski složen

Question 208

Not answered

Marked out of 1.00

Detekcija promena kao metoda za otkrivanje zlonamernih programa se zasniva na:

Select one:

- a. traženju sličnosti sa već poznatim zlonamernim programima
- b. ne znam
- c. praćenju promena u fajlovima
- d. reverznom inženjeringu
- e. registrovanju neuobičajenog ponašanja

The correct answer is: praćenju promena u fajlovima

Question 209

Not answered

Marked out of 1.00

Monitor referenci je:

Select one:

- a. ne znam
- b. deo sigurnog jezgra koji je zadužen za kontrolu pristupa
- c. deo operativnog sistema zadužen za beleženje podataka o aktivnostima
- d. skup zaštitnih mehanizama implementiranih u operativnom sistemu za koje se veruje da obezbeđuju zahteve sigurnosti
- e. deo jezgra zadužen za sigurnosno kritične operacije

The correct answer is: deo sigurnog jezgra koji je zadužen za kontrolu pristupa

Question 210

Not answered

Marked out of 1.00

Код блоковског алгоритма, по правилу

Select one:

- a. однос дужина блока отвореног текста и блока шифрата зависи од алгоритма
- b. блок шифрата је исте дужине као блок отвореног текста
- c. блок шифрата је мање дужине од блока отвореног текста
- d. не знам
- e. блок шифрата је веће дужине од блока отвореног текста

The correct answer is: блок шифрата је исте дужине као блок отвореног текста

Question 211

Not answered

Marked out of 1.00

Једносмерна хеш функција генерише отисак дужине 160 бита. Колико различитих порука генерише хеш облика 0000....0001 :

Select one:

- a. не знам
- b. 160
- c. бесконачно много
- d. само једна
- e. две

The correct answer is: бесконачно много

Question 212

Not answered

Marked out of 1.00

Шта сме да се уради са 24-битном BMP сликом уколико треба да се сачува порука која је стеганографски утиснута у њу:

Select one:

- a. не знам
- b. са се претвори у 8-битну BMP слику
- c. да се изврши компресија
- d. ништа од наведеног
- e. да се конвертује у JPEG формат

The correct answer is: ништа од наведеног

Question 213

Not answered

Marked out of 1.00

Техником image downgrading-a

Select one:

- a. не знам
- b. могуће је BMP сакрити у JPEG
- c. могуће је JPEG сакрити у JPEG
- d. могуће је JPEG сакрити у BMP
- e. могуће је BMP сакрити у BMP

The correct answer is: могуће је BMP сакрити у BMP

Question 214

Not answered

Marked out of 1.00

Колико у просеку треба покушаја грубом силом да би се разбила шифра помераја у азбуци од 30 слова:

Select one:

- a. 15
- b. 2^{15}
- c. не знам
- d. 2^{30}
- e. 2^{14}

The correct answer is: 15

Question 215

Not answered

Marked out of 1.00

Симетрични алгоритми:

Select one:

- a. имају проблем размене кључева
- b. користе краћи кључ од асиметричних алгоритама
- c. спорији су од асиметричних
- d. користе се искључиво за дигитално потписивање
- e. не знам

The correct answer is: имају проблем размене кључева

Question 216

Not answered

Marked out of 1.00

Za ECB i CBC režime rada važi:

Select one:

- a. i u CBC i u ECB režimu isti blok šifrovan istim ključem uvek daje isti šifrat
- b. u CBC režimu isti blok šifrovan istim ključem uvek daje isti šifrat, dok u ECB režimu to ne mora da bude slučaj
- c. u ECB režimu isti blok šifrovan istim ključem uvek daje isti šifrat, dok u CBC režimu to ne mora da bude slučaj
- d. ne znam
- e. i u CBC i u ECB režimu isti blok šifrovan istim ključem uvek daje različit šifrat

The correct answer is: u ECB režimu isti blok šifrovan istim ključem uvek daje isti šifrat, dok u CBC režimu to ne mora da bude slučaj

Question 217

Not answered

Marked out of 1.00

Alisa želi da pošalje Bobu poruku m šifrovanu RSA algoritmom. Alisa šifruje poruku:

Select one:

- a. svojim javnim ključem
- b. ne znam
- c. svojim privatnim ključem
- d. Bobovim javnim ključem
- e. Bobovim privatnim ključem

The correct answer is: Bobovim javnim ključem

Question 218

Not answered

Marked out of 1.00

Sigurnost RSA algoritma leži u:

Select one:

- a. složenosti računanja logaritama u konačnim poljima
- b. složenosti pronalaženja prostih faktora velikih brojeva
- c. ne znam
- d. složenosti množenja dva velika prosta broja
- e. činjenici da se koristi samo jedan ključ

The correct answer is: složenosti pronalaženja prostih faktora velikih brojeva

Question 219

Not answered

Marked out of 1.00

Koji od sledećih algoritama može se koristiti za digitalno potpisivanje:

Select one:

- a. AES
- b. Diffie-Hellman
- c. RSA
- d. ne znam
- e. DES

The correct answer is: RSA

Question 220

Not answered

Marked out of 1.00

Ako pošiljalac šifruje poruku sa javnim ključem primaoca i takav šifrat pošalje primaocu, šta je nedostatak takve komunikacije:

Select one:

- a. ne znam
- b. autentifikacija
- c. autorizacija
- d. integritet poruke
- e. poverljivost

The correct answer is: autentifikacija

Question 221

Not answered

Marked out of 1.00

Sertifikat služi:

Select one:

- a. za potvrdu vlasništva nad privatnim ključem
- b. za autorizaciju
- c. ne znam
- d. za potvrdu vlasništva nad javnim ključem
- e. za autentifikaciju

The correct answer is: za potvrdu vlasništva nad javnim ključem

Question 222

Not answered

Marked out of 1.00

Vrhovni CA je potpisani od strane

Select one:

- a. samog sebe
- b. njemu ravnopravnog CA
- c. ničeg od navedenog
- d. države
- e. ne znam

The correct answer is: samog sebe

Question 223

Not answered

Marked out of 1.00

Šta se smešta na disk prilikom kreiranja korisničkih naloga?

Select one:

- a. ne znam
- b. par korisničko ime - heš lozinke
- c. par heš korisničkog imena - heš lozinke
- d. par korisničko ime - lozinka
- e. par korisničko ime - šifrat lozinke

The correct answer is: par korisničko ime - heš lozinke

Question 224

Not answered

Marked out of 1.00

Da bi se smanjila dužina digitalnog potpisa poruke, računa se:

Select one:

- a. digitalni potpis, a zatim njegov heš
- b. heš poruke koji se digitalni potpisuje
- c. ne znam
- d. heš šifrata koji se zatim digitalno potpisuje
- e. ni jedno od navedenih

The correct answer is: heš poruke koji se digitalni potpisuje

Question 225

Not answered

Marked out of 1.00

Aktivan napad koji onemogućava funkcionisanje sistema ili pružanje neke usluge je napad na:

Select one:

- a. ne znam
- b. integritet
- c. raspoloživost
- d. poverljivost
- e. autentičnost

The correct answer is: raspoloživost

Question 226

Not answered

Marked out of 1.00

Pasivan napad koji se realizuje kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta i uvid u osetljive informacije je napad na:

Select one:

- a. autentičnost
- b. ne znam
- c. raspoloživost
- d. poverljivost
- e. integritet

The correct answer is: poverljivost

Question 227

Not answered

Marked out of 1.00

Aktivan napad kojim se neovlašćeno menjaju podaci, pristupna prava ili način funkcionisanja sistema je napad na:

Select one:

- a. poverljivost
- b. integritet
- c. raspoloživost
- d. ne znam
- e. autentičnost

The correct answer is: integritet

Question 228

Not answered

Marked out of 1.00

Aktivan napad koji se realizuje tako što se generišu lažni podaci ili lažni saobraćaj je napad na:

Select one:

- a. ne znam
- b. raspoloživost
- c. integritet
- d. autentičnost
- e. poverljivost

The correct answer is: autentičnost

Question 229

Not answered

Marked out of 1.00

Šta je rezultat operacije ((a XOR b) XOR a) XOR (a XOR b) ?

Select one:

- a. b
- b. 0
- c. ne znam
- d. a
- e. 1

The correct answer is: a

Question 230

Not answered

Marked out of 1.00

Šifrovanjem teksta PERA Viženerovom šifrom sa ključem PERA u engleskom alfabetu gde je A=0 dobija se sledeći šifrat:

Select one:

- a. ne znam
- b. SHUD
- c. EIIA
- d. PERA
- e. Nije dozvoljeno da se poklope otvoren tekst i ključ

The correct answer is: EIIA

Question 231

Not answered

Marked out of 1.00

Šifrovanjem teksta MARKO Viženerovom šifrom sa ključem MARKO u engleskom alfabetu gde je A=0 dobija se sledeći šifrat:

Select one:

- a. YAIUC
- b. AYUIC
- c. MARKO
- d. Nije dozvoljeno da se poklope otvoren tekst i ključ
- e. ne znam

The correct answer is: YAIUC

Question 232

Not answered

Marked out of 1.00

Šifrovanjem teksta MARKO Viženerovom šifrom sa ključem PERA u engleskom alfabetu gde je A=0 dobija se sledeći šifrat:

Select one:

- a. ne može da se odredi jer nedostaju informacije
- b. ne znam
- c. BEIKD
- d. BEIKO
- e. BEIK

The correct answer is: BEIKD

Question 233

Not answered

Marked out of 1.00

Šifrat otvorenog teksta JOHN dobijen Cezarovom šifrom (koristi se engleski alfabet) je:

Select one:

- a. NSKQ
- b. NSLP
- c. ne znam
- d. MRKQ
- e. MRLP

The correct answer is: MRKQ

Question 234

Not answered

Marked out of 1.00

Otvoreni tekst x se šifruje Afinom šifrom $y = E_k(x) = 6x + 3 \pmod{26}$. Šifrat se dešifruje sledećim izrazom:

Select one:

- a. $x = 15(y - 3) \pmod{15}$
- b. $x = 6(y-3) \pmod{26}$
- c. ne znam
- d. ni jednim od navedenih
- e. $x = 6y - 3 \pmod{26}$

The correct answer is: ni jednim od navedenih

Question 235

Not answered

Marked out of 1.00

Ako je $x=01101$, $y=01010$ i $z=00111$, koliko je ($x \text{ XOR } x \text{ XOR } x \text{ XOR } y \text{ XOR } y \text{ XOR } z \text{ XOR } z \text{ XOR } x \text{ XOR } x \text{ XOR } y \text{ XOR } z$):

Select one:

- a. 00001
- b. 00000
- c. ne znam
- d. 00100
- e. 00010

The correct answer is: 00000

Question 236

Not answered

Marked out of 1.00

Ako je korišćenjem šifre pomeraja od poruke HAL dobijen šifrat IBM, tada ključ iznosi (koristi se engleski alfabet):

Select one:

- a. 4
- b. 2
- c. 3
- d. ne znam
- e. 1

The correct answer is: 1

Question 237

Not answered

Marked out of 1.00

Ako je korišćenjem Afine šifre sa parametrima $(a,b)=(3,5)$ (po modulu 26) dobijen šifrat $y=11$, poruka x je:

Select one:

- a. 4
- b. ne znam
- c. 2
- d. 1
- e. 3

The correct answer is: 2

Question 238

Not answered

Marked out of 1.00

Šta je rezultat operacije ((a XOR b) XOR b) XOR (a XOR b) XOR 0 ?

Select one:

- a. a
- b. 1
- c. ne znam
- d. b
- e. 0

The correct answer is: b

Question 239

Not answered

Marked out of 1.00

Otvoreni tekst x šifruje se Afinom šifrom $y = E_k(x) = 17x + 6 \pmod{26}$. Šifrat se dešifruje sledećim izrazom:

Select one:

- a. ni jednim od navedenih
- b. $x = 23(y - 6) \pmod{26}$
- c. ne znam
- d. $x = 26(y - 6) \pmod{26}$
- e. $x = 23(y + 6) \pmod{26}$

The correct answer is: $x = 23(y - 6) \pmod{26}$

Question 240

Not answered

Marked out of 1.00

Ako je korišćenjem šifre pomeraja od poruke CEZAR dobijen šifrat GIDEV, tada ključ iznosi (koristi se engleski alfabet):

Select one:

- a. 4
- b. 1
- c. ne znam
- d. 3
- e. 2

The correct answer is: 4

Question 241

Not answered

Marked out of 1.00

DES algoritam ima:

Select one:

- a. 4 rundi
- b. 16 rundi
- c. ne znam
- d. 8 rundi
- e. 12 rundi

The correct answer is: 16 rundi

Question 242

Not answered

Marked out of 1.00

Trostruki DES:

Select one:

- a. ne znam
- b. prvo dešifruje sa prvim ključem, pa šifruje sa drugim, pa dešifruje sa prvim
- c. prvo šifruje sa prvim ključem, pa šifruje sa drugim, pa šifruje sa trećim
- d. prvo šifruje sa prvim ključem, pa šifruje sa drugim, pa dešifruje sa trećim
- e. prvo šifruje sa prvim ključem, pa dešifruje sa drugim, pa šifruje sa prvim

The correct answer is: prvo šifruje sa prvim ključem, pa dešifruje sa drugim, pa šifruje sa prvim

Question 243

Not answered

Marked out of 1.00

AES može da ima

Select one:

- a. ne znam
- b. 14, 16 ili 48 rundi
- c. 12, 14 ili 16 rundi
- d. 8,10 ili 12 rundi
- e. 10, 12 ili 14 rundi

The correct answer is: 10, 12 ili 14 rundi

Question 244

Not answered

Marked out of 1.00

Algoritam DES3 ima:

Select one:

- a. 10 rundi
- b. ne znam
- c. 12 rundi
- d. 16 rundi
- e. 48 rundi

The correct answer is: 48 rundi

Question 245

Not answered

Marked out of 1.00

Odrediti red veličine broja operacija šifrovanja i dešifrovanja za napad na trostruki DES metodom susret u sredini:

Select one:

- a. 2^{168}
- b. 2^{56}
- c. 2^{112}
- d. ne znam
- e. 2^{64}

The correct answer is: 2^{112}

Question 246

Not answered

Marked out of 1.00

Dužina ključa kod AES algoritma može da bude:

Select one:

- a. 64, 128, 192 ili 256 bita
- b. proizvoljne dužine
- c. ne znam
- d. 128, 192 ili 256 bita
- e. 64, 128 ili 192 bita

The correct answer is: 128, 192 ili 256 bita

Question 247

Not answered

Marked out of 1.00

Dužina bloka kod AES algoritma može da bude:

Select one:

- a. 64, 128 ili 192
- b. ne znam
- c. 128, 192 ili 256 bita
- d. 64, 128, 192 ili 256 bita
- e. proizvoljne dužine

The correct answer is: 128, 192 ili 256 bita

Question 248

Not answered

Marked out of 1.00

Ključ je dužine 64 bita. Koliki je prostor ključeva?

Select one:

- a. 2^{32}
- b. $2^{64} - 2$
- c. 2^{128}
- d. 2^{64}
- e. ne znam

The correct answer is: 2^{64} **Question 249**

Not answered

Marked out of 1.00

Neka je $Z = \{A, B, C, \dots, X, Y, Z, 0, 1, \dots, 9\}$ skup nad kojim se definiše ključ. Ukoliko je ključ dužine 8 i znaci u ključu mogu da se ponavljaju, koliki je prostor ključeva:

Select one:

- a. $(26 + 10)^8$
- b. $(26 \times 10)^8$
- c. $8^{(26 + 10)}$
- d. ne znam
- e. $26 \times 10 \times 8$

The correct answer is: $(26 + 10)^8$ **Question 250**

Not answered

Marked out of 1.00

Ključ je dužine 16 bita. Koliki je prostor ključeva?

Select one:

- a. ne znam
- b. 2^{32}
- c. 2^{16}
- d. 2^8
- e. $2^{16} - 2$

The correct answer is: 2^8

Question 251

Not answered

Marked out of 1.00

Neka je $Z=\{A,B,C,\dots,X,Y,Z,0,1,\dots,9,+,-,* , /, =, ?, !, \$, \#, @, \&, _ \}$ skup nad kojim se definiše ključ. Ukoliko je ključ dužine 6 i znaci u ključu mogu da se ponavljaju, koliki je prostor ključeva:

Select one:

- a. ne znam
- b. $(26 \times 10 \times 12)^6$
- c. $26 \times 10 \times 12 \times 6$
- d. $6^{(26 + 10 + 12)}$
- e. $(26 + 10 + 12)^6$

The correct answer is: $(26 + 10 + 12)^6$

Question 252

Not answered

Marked out of 1.00

Neka je $Z=\{A,B,C,\dots,X,Y,Z,0,1,\dots,9,+,-,* , /, =, ?, !, \$, \#, @, \&, _ \}$ skup nad kojim se definiše ključ. Ukoliko je ključ dužine 8 i znaci u ključu mogu da se ponavljaju, koliki je prostor ključeva:

Select one:

- a. $8^{(26 + 10 + 12)}$
- b. $(26 + 10 + 12)^8$
- c. $26 \times 10 \times 12 \times 8$
- d. ne znam
- e. $(26 \times 10 \times 12)^8$

The correct answer is: $(26 + 10 + 12)^8$

Question 253

Not answered

Marked out of 1.00

Neka je $Z = \{A, B, C, \dots, X, Y, Z, 0, 1, \dots, 9, +, -, *, /, =, ?, !, \$, \#, @, \&, _\}$ skup nad kojim se definiše ključ. Ukoliko je ključ dužine 24 i znaci u ključu mogu da se ponavljaju, koliki je prostor ključeva:

Select one:

- a. $(26 \times 10 \times 12)^{24}$
- b. $2^{(26 + 10 + 12)}$
- c. $(26 + 10 + 12)^{24}$
- d. $26 \times 10 \times 12 \times 24$
- e. ne znam

The correct answer is: $(26 + 10 + 12)^{24}$

Question 254

Not answered

Marked out of 1.00

Ključ je dužine 128 bita. Koliki je prostor ključeva?

Select one:

- a. 2^{256}
- b. 2^{64}
- c. 2^{128}
- d. ne znam
- e. $2^{128} - 2$

The correct answer is: 2^{128}

Question 255

Not answered

Marked out of 1.00

Ključ je dužine 256 bita. Koliki je prostor ključeva?

Select one:

- a. 2^{128}
- b. 2^{256}
- c. ne znam
- d. 2^{512}
- e. $2^{256} - 2$

The correct answer is: 2^{256} **Question 256**

Not answered

Marked out of 1.00

Ključ je dužine 56 bita. Koliki je prostor ključeva?

Select one:

- a. 2^{56}
- b. $2^{56} - 2$
- c. 2^{112}
- d. ne znam
- e. 2^{28}

The correct answer is: 2^{56} **Question 257**

Not answered

Marked out of 1.00

Ukoliko se koriste velika slova engleskog alfabeta za ključ dužine 4, koliki je prostor ključeva ukoliko slova u ključu mogu da se ponavljaju:

Select one:

- a. 4^{26}
- b. 26^4
- c. ne znam
- d. 26×4
- e. $26 \times 25 \times 24 \times 23$

The correct answer is: 26^4

Question 258

Not answered

Marked out of 1.00

Ukoliko se koriste velika slova engleskog alfabetu za ključ dužine 26, koliki je prostor klučeva ukoliko znaci u ključu mogu da se ponavljaju:

Select one:

- a. 26^{26}
- b. $26!$
- c. ne znam
- d. 2^{26}
- e. 26×26

The correct answer is: 26^{26}

Question 259

Not answered

Marked out of 1.00

Ukoliko se koriste velika slova engleskog alfabetu za ključ dužine 6, koliki je prostor klučeva ukoliko slova u ključu mogu da se ponavljaju:

Select one:

- a. 26^6
- b. ne znam
- c. 26×6
- d. 6^{26}
- e. $26 \times 25 \times 24 \times 23 \times 22 \times 21$

The correct answer is: 26^6

Question 260

Not answered

Marked out of 1.00

Neka je $Z=\{A,B,C,\dots,X,Y,Z,0,1,\dots,9\}$ skup nad kojim se definiše ključ. Ukoliko je ključ dužine 6 i znaci u ključu mogu da se ponavljaju, koliki je prostor ključeva:

Select one:

- a. ne znam
- b. $26 \times 10 \times 6$
- c. $6^{(26 + 10)}$
- d. $(26 + 10)^6$
- e. $(26 \times 10)^6$

The correct answer is: $(26 + 10)^6$

Question 261

Not answered

Marked out of 1.00

Neka je $Z=\{A,B,C,\dots,X,Y,Z,0,1,\dots,9\}$ skup nad kojim se definiše ključ. Ukoliko je ključ dužine 18 i znaci u ključu mogu da se ponavljaju, koliki je prostor ključeva:

Select one:

- a. ne znam
- b. $(26 \times 10)^{18}$
- c. $26 \times 10 \times 18$
- d. $18^{(26 + 10)}$
- e. $(26 + 10)^{18}$

The correct answer is: $(26 + 10)^{18}$

Question 262

Not answered

Marked out of 1.00

Dat je prost broj $p=19$ i generator $g=2$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=5$ i $b=8$:

Select one:

- a. $k = 9$
- b. ne znam
- c. $k = 16$
- d. $k = 13$
- e. $k = 2$

The correct answer is: $k = 16$

Question 263

Not answered

Marked out of 1.00

Dat je prost broj $p=7$ i generator $g=5$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=3$ i $b=5$:

Select one:

- a. ne znam
- b. $k = 2$
- c. $k = 6$
- d. $k = 1$
- e. $k = 4$

The correct answer is: $k = 6$

Question 264

Not answered

Marked out of 1.00

Dat je prost broj $p=7$ i generator $g=3$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=3$ i $b=6$:

Select one:

- a. $k = 2$
- b. $k = 6$
- c. $k = 1$
- d. ne znam
- e. $k = 4$

The correct answer is: $k = 1$

Question 265

Not answered

Marked out of 1.00

Dat je prost broj $p=7$ i generator $g=3$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=2$ i $b=5$:

Select one:

- a. $k = 2$
- b. $k = 1$
- c. $k = 4$
- d. ne znam
- e. $k = 6$

The correct answer is: $k = 4$

Question 266

Not answered

Marked out of 1.00

U Diffie-Hellmanovom protokolu sa parametrima $(p,g)=(13,2)$ Alisa je zamislila broj 5, Boban je zamislio broj 7. Poruke koje razmenjuju su:

Select one:

- a. Alisa šalje Bobanu 6 a Boban šalje Alisi 11
- b. Alisa šalje Bobanu 8 a Boban šalje Alisi 3
- c. ne znam
- d. Alisa šalje Bobanu 9 a Boban šalje Alisi 10
- e. Alisa šalje Bobanu 12 a Boban šalje Alisi 5

The correct answer is: Alisa šalje Bobanu 6 a Boban šalje Alisi 11

Question 267

Not answered

Marked out of 1.00

U Diffie-Hellmanovom protokolu sa parametrima $(g,p)=(13,2)$ Alisa je zamislila broj 6, Boban je zamislio broj 9. Poruke koje razmenjuju Alisa i Bob su:

Select one:

- a. Alisa šalje Bobanu 12 a Boban Alisi 5
- b. ne znam
- c. Alisa šalje Bobanu 9 a Boban Alisi 10
- d. Alisa šalje Bobanu 6 a Boban Alisi 11
- e. Alisa šalje Bobanu 8 a Boban Alisi 3

The correct answer is: Alisa šalje Bobanu 12 a Boban Alisi 5

Question 268

Not answered

Marked out of 1.00

U Diffie-Hellmanovom protokolu sa parametrima $(g,p)=(13,2)$ Alisa je zamislila broj 3, Boban je zamislio broj 4. Poruke koje razmenjuju Alisa i Bob su:

Select one:

- a. Alisa šalje Bobanu 12 a Boban Alisi 5
- b. Alisa šalje Bobanu 9 a Boban Alisi 10
- c. Alisa šalje Bobanu 8 a Boban Alisi 3
- d. ne znam
- e. Alisa šalje Bobanu 6 a Boban Alisi 11

The correct answer is: Alisa šalje Bobanu 8 a Boban Alisi 3

Question 269

Not answered

Marked out of 1.00

U Diffie-Hellmanovom protokolu sa parametrima $(p,g)=(13,2)$ Alisa je zamislila broj 8, Boban je zamislio broj 10. Poruke koje razmenjuju Alisa i Bob su:

Select one:

- a. Alisa šalje Bobanu 12 a Boban Alisi 5
- b. Alisa šalje Bobanu 6 a Boban Alisi 11
- c. Alisa šalje Bobanu 9 a Boban Alisi 10
- d. Alisa šalje Bobanu 8 a Boban Alisi 3
- e. ne znam

The correct answer is: Alisa šalje Bobanu 9 a Boban Alisi 10

Question 270

Not answered

Marked out of 1.00

Dati su generator $g=2$ i moduo $p=5$. Alisa je zamislila broj $a=7$, a Bob broj $b=8$. Korišćenjem Diffie-Hellmannovog protokola odredite deljenu tajnu:

Select one:

- a. $k=5$
- b. ne znam
- c. $k=1$
- d. $k=7$
- e. $k=3$

The correct answer is: $k=1$

Question 271

Not answered

Marked out of 1.00

U Diffie-Hellmanovom protokolu sa parametrima $(g,p)=(2,5)$ Alisa je zamislila broj 2 a Boban je zamislio broj 7. Zajednička tajna je:

Select one:

- a. ne znam
- b. 1
- c. 3
- d. 2
- e. 4

The correct answer is: 4

Question 272

Not answered

Marked out of 1.00

U Diffie-Hellmanovom protokolu sa parametrima $(g,p)=(2,5)$ Alisa je zamislila broj 2, Boban je zamislio broj 11. Zajednička tajna je:

Select one:

- a. 1
- b. 4
- c. 2
- d. 3
- e. ne znam

The correct answer is: 4

Question 273

Not answered

Marked out of 1.00

Dat je prost broj $p=11$ i generator $g=6$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=3$ i $b=6$:

Select one:

- a. $k = 4$
- b. ne znam
- c. $k = 6$
- d. $k = 3$
- e. $k = 9$

The correct answer is: $k = 4$

Question 274

Not answered

Marked out of 1.00

Dat je prost broj $p=11$ i generator $g=6$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=3$ i $b=7$:

Select one:

- a. ne znam
- b. $k = 6$
- c. $k = 4$
- d. $k = 3$
- e. $k = 9$

The correct answer is: $k = 6$

Question 275

Not answered

Marked out of 1.00

Dat je prost broj $p=11$ i generator $g=7$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=3$ i $b=6$:

Select one:

- a. $k = 4$
- b. ne znam
- c. $k = 3$
- d. $k = 9$
- e. $k = 6$

The correct answer is: $k = 9$

Question 276

Not answered

Marked out of 1.00

Dat je prost broj $p=11$ i generator $g=7$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=2$ i $b=7$:

Select one:

- a. $k = 6$
- b. ne znam
- c. $k = 9$
- d. $k = 3$
- e. $k = 4$

The correct answer is: $k = 3$

Question 277

Not answered

Marked out of 1.00

Dat je prost broj $p=7$ i generator $g=5$. Koristeći Diffie-Hellmanov protokol odredite tajni ključ ako su zamišljene vrednosti $a=5$ i $b=2$:

Select one:

- a. $k = 2$
- b. $k = 1$
- c. ne znam
- d. $k = 4$
- e. $k = 6$

The correct answer is: $k = 2$

Question 278

Not answered

Marked out of 1.00

Javni ključ u RSA algoritmu je $(n, e) = (403, 103)$. Digitalni potpis poruke $m=4$ je:

Select one:

- a. sig $(m) = 256$
- b. sig $(m) = 172$
- c. ne znam
- d. sig $(m) = 346$
- e. sig $(m) = 264$

The correct answer is: sig $(m) = 264$

Question 279

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(247,31)$ digitalni potpis poruke $m=4$ iznosi:

Select one:

- a. ne znam
- b. 211
- c. 45
- d. 82
- e. 73

The correct answer is: 82

Question 280

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(247,31)$ digitalni potpis poruke $m=5$ iznosi:

Select one:

- a. 73
- b. 82
- c. ne znam
- d. 45
- e. 211

The correct answer is: 73

Question 281

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(247,31)$ digitalni potpis poruke $m=7$ iznosi:

Select one:

- a. 82
- b. 73
- c. 45
- d. 211
- e. ne znam

The correct answer is: 45

Question 282

Not answered

Marked out of 1.00

Koristeći RSA kriptosistemu sa javnim ključem $(n,e)=(55,27)$ dobijena je šifrovana poruka $s(m)=18$. Originalna poruka je:

Select one:

- a. 3
- b. 2
- c. 4
- d. ne znam
- e. 5

The correct answer is: 2

Question 283

Not answered

Marked out of 1.00

Koristeći RSA kriptosistemu sa javnim ključem $(n,e)=(55,27)$ dobijena je šifrovana poruka $s(m)=42$. Originalna poruka je:

Select one:

- a. ne znam
- b. 5
- c. 4
- d. 2
- e. 3

The correct answer is: 3

Question 284

Not answered

Marked out of 1.00

Koristeći RSA kriptosistemu sa javnim ključem $(n,e)=(55,27)$ dobijena je šifrovana poruka $s(m)=49$. Originalna poruka je:

Select one:

- a. 5
- b. 2
- c. ne znam
- d. 4
- e. 3

The correct answer is: 4

Question 285

Not answered

Marked out of 1.00

Koristeći RSA kriptosistemu sa javnim ključem $(n,e)=(55,27)$ dobijena je šifrovana poruka $s(m)=25$. Originalna poruka je:

Select one:

- a. 3
- b. ne znam
- c. 5
- d. 2
- e. 4

The correct answer is: 5

Question 286

Not answered

Marked out of 1.00

Javni ključ u RSA algoritmu je $(n,e) = (403,103)$. Privatni ključ je:

Select one:

- a. $d = 3$
- b. $d = 17$
- c. ne znam
- d. $d = 7$
- e. $d = 13$

The correct answer is: $d = 7$

Question 287

Not answered

Marked out of 1.00

U RSA algoritmu dati su parametri: $(n,e)=(323,17)$. Privatni ključ d jednak je:

Select one:

- a. 19
- b. ne znam
- c. 15
- d. 17
- e. 13

The correct answer is: 17

Question 288

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(247,31)$ razlika javnog i privatnog ključa iznosi:

Select one:

- a. 15
- b. ne znam
- c. 11
- d. 9
- e. 24

The correct answer is: 24

Question 289

Not answered

Marked out of 1.00

Javni ključ u RSA algoritmu je $(n, e) = (403, 103)$. Digitalni potpis poruke $m=3$ je:

Select one:

- a. $\text{sig}(m) = 346$
- b. $\text{sig}(m) = 256$
- c. $\text{sig}(m) = 172$
- d. $\text{sig}(m) = 264$
- e. ne znam

The correct answer is: $\text{sig}(m) = 172$

Question 290

Not answered

Marked out of 1.00

Javni ključ u RSA algoritmu je $(n, e) = (403, 103)$. Digitalni potpis poruke $m=5$ je:

Select one:

- a. $\text{sig}(m) = 264$
- b. $\text{sig}(m) = 346$
- c. ne znam
- d. $\text{sig}(m) = 172$
- e. $\text{sig}(m) = 256$

The correct answer is: $\text{sig}(m) = 346$

Question 291

Not answered

Marked out of 1.00

Javni ključ u RSA algoritmu je $(n, e) = (403, 103)$. Digitalni potpis poruke $m=6$ je:

Select one:

- a. $\text{sig}(m) = 346$
- b. $\text{sig}(m) = 172$
- c. $\text{sig}(m) = 254$
- d. $\text{sig}(m) = 264$
- e. ne znam

The correct answer is: $\text{sig}(m) = 254$

Question 292

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(187,23)$ digitalni potpis poruke $m=3$ iznosi:

Select one:

- a. 128
- b. 115
- c. 97
- d. ne znam
- e. 130

The correct answer is: 130

Question 293

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(187,23)$ digitalni potpis poruke $m=2$ iznosi:

Select one:

- a. 130
- b. 128
- c. 97
- d. ne znam
- e. 115

The correct answer is: 128

Question 294

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(187,23)$ digitalni potpis poruke $m=4$ iznosi:

Select one:

- a. 128
- b. 97
- c. ne znam
- d. 115
- e. 130

The correct answer is: 115

Question 295

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(187,23)$ digitalni potpis poruke $m=5$ iznosi:

Select one:

- a. 146
- b. ne znam
- c. 128
- d. 130
- e. 115

The correct answer is: 146

Question 296

Not answered

Marked out of 1.00

U RSA algoritmu sa parametrima $(n,e)=(247,31)$ digitalni potpis poruke $m=3$ iznosi:

Select one:

- a. 73
- b. 45
- c. 211
- d. 82
- e. ne znam

The correct answer is: 211

Question 297

Not answered

Marked out of 1.00

Koja dva algoritma su po načinu funkcionisanja slična:

Select one:

- a. One Time Pad i Cezarova šifra
- b. Jednostavni XOR i One Time Pad
- c. Afina šifra i jednostavni XOR
- d. Afina šifra i Vigenereo- ova šifra
- e. ne znam

The correct answer is: Jednostavni XOR i One Time Pad

Question 298

Not answered

Marked out of 1.00

Frekvencijska analiza nema efekta na

Select one:

- a. Hilovu šifru
- b. Viženerovu šifru
- c. Plejferovu šifru
- d. ne znam
- e. OTP

The correct answer is: OTP

Question 299

Not answered

Marked out of 1.00

Šifarski sistem OTP može da se koristi:

Select one:

- a. ne znam
- b. dok se ne posumnja u sigurnost ključa
- c. samo jednom
- d. više od dva puta
- e. najviše dva puta

The correct answer is: samo jednom

Question 300

Not answered

Marked out of 1.00

Bezuslovno sigurni šifarski sistem:

Select one:

- a. ne postoji
- b. ne znam
- c. ima dužinu ključa 512 bitova
- d. ima dužinu ključa 1024 bitova
- e. ima istu dužinu i ključa i poruke

The correct answer is: ima istu dužinu i ključa i poruke

Question 301

Not answered

Marked out of 1.00

Šifra OTP je:

Select one:

- a. ne znam
- b. asimetrična blokovska
- c. simetrična blokovska
- d. asimetrična sekvencijalna
- e. simetrična sekvencijalna

The correct answer is: simetrična sekvencijalna

Question 302

Not answered

Marked out of 1.00

Ako je heš dužine 50 bitova koliko je potrebno napraviti poruka da bismo sigurno došli do kolizije:

Select one:

- a. 2^{50}
- b. $2^{50} + 1$
- c. ne znam
- d. $2^{25} + 1$
- e. 2^{25}

The correct answer is: $2^{50} + 1$

Question 303

Not answered

Marked out of 1.00

Ako je heš dužine 224 bitova koliko je potrebno napraviti poruka da bismo sigurno došli do kolizije:

Select one:

- a. $2^{224} + 1$
- b. 2^{224}
- c. $2^{112} + 1$
- d. 2^{225}
- e. ne znam

The correct answer is: $2^{224} + 1$

Question 304

Not answered

Marked out of 1.00

Ako je heš dužine 100 bitova koliko treba napraviti poruka da bismo sigurno došlo do kolizije?

Select one:

- a. ne znam
- b. 2^{50}
- c. $2^{100} + 1$
- d. 2^{99}
- e. $2^{99} + 1$

The correct answer is: $2^{100} + 1$

Question 305

Not answered

Marked out of 1.00

Ako je heš dužine 128 bitova koliko je potrebno napraviti poruka da bismo sigurno došli do kolizije:

Select one:

- a. 2^{128}
- b. $2^{128} + 1$
- c. ne znam
- d. 2^{129}
- e. $2^{64} + 1$

The correct answer is: $2^{128} + 1$

Question 306

Not answered

Marked out of 1.00

Jednosmerna heš funkcija generiše otisak dužine 160 bitova. Koliko mogućih ulaznih poruka generiše heš vrednost 1?

Select one:

- a. beskonačno mnogo poruka
- b. samo jedna
- c. $2^{160} + 1$
- d. ne znam
- e. 2^{160}

The correct answer is: beskonačno mnogo poruka

Question 307

Not answered

Marked out of 1.00

Ako je heš dužine 256 bitova koliko je potrebno napraviti poruka da bismo sigurno došli do kolizije:

Select one:

- a. $2^{256} + 1$
- b. ne znam
- c. 2^{256}
- d. 2^{128}
- e. 2^{256+1}

The correct answer is: $2^{256} + 1$

Question 308

Not answered

Marked out of 1.00

Ako je heš dužine 384 bitova koliko je potrebno napraviti poruka da bismo sigurno došli do kolizije:

Select one:

- a. 2^{385}
- b. $2^{384} + 1$
- c. 2^{384}
- d. ne znam
- e. $2^{192} + 1$

The correct answer is: $2^{384} + 1$

Question 309

Not answered

Marked out of 1.00

Ako je heš dužine 512 bitova koliko je potrebno napraviti poruka da bismo sigurno došli do kolizije:

Select one:

- a. $2^{256} + 1$
- b. 2^{512+1}
- c. $2^{512} + 1$
- d. ne znam
- e. 2^{512}

The correct answer is: $2^{512} + 1$

Question 310

Not answered

Marked out of 1.00

Kada se matrica kontrole pristupa podeli na kolone

Select one:

- a. dobijaju se liste kontrole pristupa (ACL)
- b. dobijaju se liste deljenih prava (CL)
- c. dobija se Lampsonova matrica
- d. definišu se stepeni tajnosti
- e. ne znam

The correct answer is: dobijaju se liste kontrole pristupa (ACL)

Question 311

Not answered

Marked out of 1.00

Kada se matrica kontrole pristupa podeli na vrste

Select one:

- a. definišu se stepeni tajnosti
- b. dobijaju se liste deljenih prava (CL)
- c. dobija se Lampsonova matrica
- d. ne znam
- e. dobijaju se liste kontrole pristupa (ACL)

The correct answer is: dobijaju se liste deljenih prava (CL)

Question 312

Not answered

Marked out of 1.00

Autorizacija je proces kojim se ispituje:

Select one:

- a. poverljivost i raspoloživost
- b. ne znam
- c. da li sistemu pristupa čovek ili računar
- d. prava korisnika koji pristupa sistemu
- e. identitet korisnika koji pristupa sistemu

The correct answer is: prava korisnika koji pristupa sistemu

Question 313

Not answered

Marked out of 1.00

Odabratи tačan (jedan) iskaz:

za ACL važi

Select one:

- a. ne znam
- b. zaštita je orijentisana prema podacima
- c. lako se dodaju/brišu korisnici
- d. lako se menjaju prava u odnosu na korisnike
- e. teže su za implementaciju od C lista

The correct answer is: zaštita je orijentisana prema podacima

Question 314

Not answered

Marked out of 1.00

Odabratи tačan (jedan) iskaz:

za C liste važi

Select one:

- a. lako se menjaju prava u odnosu na resurse
- b. lako se menjaju prava u odnosu na korisnike
- c. zaštita je orijentisana prema podacima
- d. lakše su za implementaciju od ACL
- e. ne znam

The correct answer is: lako se menjaju prava u odnosu na korisnike

Question 315

Not answered

Marked out of 1.00

CAPTCHA je:

Select one:

- a. metoda kontrole pristupa koju većina ljudi ne može da prođe
- b. ne znam
- c. zlonamerni softver
- d. protokol za autentifikaciju
- e. test za restrikciju pristupa za automatizovane sisteme

The correct answer is: test za restrikciju pristupa za automatizovane sisteme

Question 316

Not answered

Marked out of 1.00

Autentifikacija lozinkom je odluka na osnovu nečega

Select one:

- a. ne znam
- b. što korisnik zna
- c. što korisnik zna da ima
- d. što korisnik jeste
- e. što korisnik ima

The correct answer is: što korisnik zna

Question 317

Not answered

Marked out of 1.00

Kontrola pristupa se sastoji od:

Select one:

- a. autentifikacije i raspoloživosti
- b. autentifikacije i autorizacije
- c. autorizacije i poverljivosti
- d. poverljivosti i raspoloživosti
- e. ne znam

The correct answer is: autentifikacije i autorizacije

Question 318

Not answered

Marked out of 1.00

Keylogger je:

Select one:

- a. uređaj za siguran prenos od tastature do PC-a
- b. ne znam
- c. hakerska komponenta za presretanje lozinki
- d. uređaj za autorizaciju
- e. komponenta za autentifikaciju

The correct answer is: hakerska komponenta za presretanje lozinki

Question 319

Not answered

Marked out of 1.00

Idealna biometrija **ne** podrazumeva:

Select one:

- a. univerzalnost
- b. razlikovanje
- c. ne znam
- d. stalnost
- e. obavezno korišćenje lozinki

The correct answer is: obavezno korišćenje lozinki

Question 320

Not answered

Marked out of 1.00

Kada je reč o autentifikaciji s javnim ključem nije bezbedno:

Select one:

- a. ne znam
- b. potpiši pa šifruj upotrebom slučajne vrednosti
- c. potpiši pa šifruj upotrebom timestampa
- d. šifruj pa potpiši upotrebom slučajne vrednosti
- e. šifruj pa potpiši upotrebom timestampa

The correct answer is: šifruj pa potpiši upotrebom timestampa

Question 321

Not answered

Marked out of 1.00

Kod protokola za autentifikaciju zasnovanih na kriptografiji sa javnim ključem treba koristiti:

Select one:

- a. sesijski ključ
- b. različit par ključeva za šifrovanje i digitalno potpisivanje
- c. heš vrednosti sesijskog ključa
- d. ne znam
- e. isti par ključeva za šifrovanje i digitalno potpisivanje

The correct answer is: različit par ključeva za šifrovanje i digitalno potpisivanje

Question 322

Not answered

Marked out of 1.00

Izbaciti uljeza:

Select one:

- a. TCP
- b. Kerberos
- c. SSL
- d. ne znam
- e. IPSec

The correct answer is: TCP

Question 323

Not answered

Marked out of 1.00

Izabratи tačan iskaz:

Select one:

- a. SSL postoji na socket nivou (deo je korisničkog prostora)
- b. SSL postoji na mrežnom nivou (deo je operativnog sistema)
- c. IPSec je u odnosu na SSL jednostavniji
- d. SSL postoji na transportnom nivou
- e. ne znam

The correct answer is: SSL postoji na socket nivou (deo je korisničkog prostora)

Question 324

Not answered

Marked out of 1.00

Izabratи tačan iskaz:

Select one:

- a. SSL nudi šifrovanje, integritet ali ne i autentifikaciju
- b. SSL nudi šifrovanje i autentifikaciju ali ne i integritet
- c. SSL nudi šifrovanje, integritet i autentifikaciju
- d. ne znam
- e. SSL nudi integritet i autentifikaciju ali ne i šifrovanje

The correct answer is: SSL nudi šifrovanje, integritet i autentifikaciju

Question 325

Not answered

Marked out of 1.00

Kod protokola Kerberos tačno je:

Select one:

- a. Ne zahteva poverenje u treću stranu
- b. Zahteva da se koristi PKI
- c. ne znam
- d. Kerberos je zasnovan na asimetričnom kripto sistemu
- e. Kerberos je zasnovan na simetričnom kripto sistemu

The correct answer is: Kerberos je zasnovan na simetričnom kripto sistemu

Question 326

Not answered

Marked out of 1.00

Challenge-Response je:

Select one:

- a. kriptografski protokol
- b. softver koji prima ili odbija dolazeće veze ka računaru
- c. protokol za autentifikaciju
- d. ne znam
- e. softver koji obezbeđuje korisnicima da koriste algoritme koje žele da bi obezbedili sigurnu komunikaciju

The correct answer is: protokol za autentifikaciju

Question 327

Not answered

Marked out of 1.00

Sesijski ključ je

Select one:

- a. simetrični ključ koji ima vremenski ograničeno trajanje
- b. ne znam
- c. simetrični ključ za najviše dve komunikacije
- d. simetrični ključ samo za jednu komunikaciju
- e. simetrični ključ koji se kloristi uvek u komunikaciji za dva tačno određena učesnika

The correct answer is: simetrični ključ samo za jednu komunikaciju

Question 328

Not answered

Marked out of 1.00

Sigurnosni protokol koji je zasnovan na poverenju u treću stranu je:

Select one:

- a. ne znam
- b. SSL
- c. Kerberos
- d. https
- e. IPSec

The correct answer is: Kerberos

Question 329

Not answered

Marked out of 1.00

Ticket Granting Ticket (TGT) je pojam vezan za sledeći protokol:

Select one:

- a. TCP
- b. IPSec
- c. Kerberos
- d. ne znam
- e. SSL

The correct answer is: Kerberos

Question 330

Not answered

Marked out of 1.00

Izabratи tačan iskaz:

Select one:

- a. ne znam
- b. IPSec postoji na mrežnom nivou (deo je operativnog sistema)
- c. IPSec postoji na transportnom sloju
- d. IPSec postoji na socket nivou (deo je korisničkog prostora)
- e. IPSec je u odnosu na SSL jednostavniji

The correct answer is: IPSec postoji na mrežnom nivou (deo je operativnog sistema)

Question 331

Not answered

Marked out of 1.00

Izabratи tačan iskaz:

Select one:

- a. ne znam
- b. IPSec nudi šifrovanje, integritet ali ne i autentifikaciju
- c. IPSec nudi integritet i autentifikaciju ali ne i šifrovanje
- d. IPSec nudi šifrovanje, integritet i autentifikaciju
- e. IPSec nudi integritet i autentifikaciju ali ne i šifrovanje

The correct answer is: IPSec nudi šifrovanje, integritet i autentifikaciju

Question 332

Not answered

Marked out of 1.00

Sigurnost operativnog sistema opšte namene se najefikasnije realizuje kroz:

Select one:

- a. ne znam
- b. sigurnost fizičkog pristupa sistemu
- c. sigurnost na nivou korisničkih aplikacija
- d. sigurnost mrežnog pristupa sistemu
- e. sigurno jezgro (kernel)

The correct answer is: sigurno jezgro (kernel)

Question 333

Not answered

Marked out of 1.00

Na sigurnost operativnog sistema opšte namene broj linija programskog koda kernela utiče na sledeći način:

Select one:

- a. ne znam
- b. manji broj linija koda smanjuje mogućnost grešaka i olakšava rešavanje problema i propusta
- c. veći broj linija koda ukazuje na kompleksnije i kvalitetnije realizovano sigurno jezgro
- d. broj linija koda kernela nema nikakav uticaj na potencijalnu sigurnost jezgra operativnog sistema
- e. standardom se određuje preko kojeg broj linija koda se jezgro smatra "hesigurnim"

The correct answer is: manji broj linija koda smanjuje mogućnost grešaka i olakšava rešavanje problema i propusta

Question 334

Not answered

Marked out of 1.00

NGSCB je deo operativnog sistema koji:

Select one:

- a. ne znam
- b. je implementiran u *Linux* OS
- c. podržava hardversku tehnologiju članova grupe TCG
- d. koristi simetričnu kriptografiju
- e. je namenjen samo za zatvorene sisteme

The correct answer is: podržava hardversku tehnologiju članova grupe TCG

Question 335

Not answered

Marked out of 1.00

Kod operativnih sistema opšte namene preporučljivo je da aktivnosti i mehanizmi od značaja za sigurnost budu implementirani na:

Select one:

- a. ne znam
- b. jednom sloju kako bi analiza i ispravka bila jednostavnija i brža
- c. nivou fajl sistema kako bi korisnički i sistemski fajlovi bili zaštićeni
- d. korisničkom nivou kako bi mehanizmi bili što dalji od jezgra
- e. što više različitih nivoa kako bi napadaču bilo teže da prati i analizira mehanizme

The correct answer is: jednom sloju kako bi analiza i ispravka bila jednostavnija i brža

Question 336

Not answered

Marked out of 1.00

Operativni sistem od poverenja **ne** mora da obezbedi:

Select one:

- a. DAC kontrolu pristupa
- b. autentifikaciju/autorizaciju
- c. MAC kontrolu pristupa
- d. ne znam
- e. grafičko okruženje

The correct answer is: grafičko okruženje

Question 337

Not answered

Marked out of 1.00

Model granične adrese je model koji se koristi za

Select one:

- a. zaštitu memorije
- b. zaštitu operativnog sistema
- c. zaštitu korisničkih fajlova
- d. ograničavanja lokacija sa kojih stižu podaci
- e. ne znam

The correct answer is: zaštitu memorije

Question 338

Not answered

Marked out of 1.00

Ako su istovremeno primjenjeni MAC (*Mandatory Access Control*) i DAC (*Discretionary Access Control*):

Select one:

- a. onda je MAC "stariji" od DAC
- b. operativni sistem određuje šta će biti "starije"
- c. onda je DAC "stariji" od MAC
- d. administrator određuje šta će biti "starije"
- e. ne znam

The correct answer is: onda je MAC "stariji" od DAC

Question 339

Not answered

Marked out of 1.00

Kod diskrecione kontrole pristupa ko određuje prava pristupa objektu?

Select one:

- a. operativni sistem
- b. administrator sistema
- c. vlasnik objekta
- d. ne znam
- e. zavisi od operativnog sistema

The correct answer is: vlasnik objekta

Question 340

Not answered

Marked out of 1.00

Jedan od nedostataka segmentacije memorije kao metode zaštite je to što:

Select one:

- a. ne znam
- b. nije moguće primeniti različite nivoje zaštite
- c. može da dovede do fragmentacije memorije
- d. jednom segmentu može da pristupi samo jedan korisnik
- e. segmenti ne mogu da menjaju lokaciju u memoriji

The correct answer is: može da dovede do fragmentacije memorije

Question 341

Not answered

Marked out of 1.00

Zbog načina na koji mrežna barijera pregleda stavke iz liste za kontrolu pristupa preporučljivo je praviti listu na sledeći način:

Select one:

- a. Pravila se ređaju od opštijih ka preciznijim
- b. Pravila se ređaju proizvoljnim rasporedom jer je "deny" uvek jači od "allow"
- c. ne znam
- d. Prvo se unose "deny" pravila pa onda "allow"
- e. Pravila se ređaju od preciznijih ka opštijim.

The correct answer is: Pravila se ređaju od preciznijih ka opštijim.

Question 342

Not answered

Marked out of 1.00

Kod loših softverskih rešenja i softvera sa propustima, ako postoji jaka kriptografska zaštita u pozadini

Select one:

- a. loše softversko rešenje će otežati razumevanje i analizu od strane napadača, što će sa dobrom kriptografijom povećati sigurnost
- b. ne znam
- c. jaka kriptografija ne može da obezbedi sigurnost podataka korisnika kod lošeg sofvera
- d. kriptografija će nezavisno od softverskih rešenja obezbititi sigurnost podataka korisnika
- e. loši efekti propusta u softveru imaju zanemarljiv uticaj na sigurnost podataka ako je kriptografska zaštita adekvatna

The correct answer is: jaka kriptografija ne može da obezbedi sigurnost podataka korisnika kod lošeg sofvera

Question 343

Not answered

Marked out of 1.00

Korisnički softver se često plasira na tržište po sledećem principu:

Select one:

- a. razvija se tako što se dugo i opsežno proverava pre distribuiranja korisnicima, da bi kompanije smanjile troškove ulaganja u naknadne ispravke grešaka
- b. razvija se brzo da bi se što pre predstavio kupcima, a propusti i greške se naknadno ispravljaju
- c. softver otvorenog koda se razvija polako i opsežno testira, a softver zatvorenog koda se izbacuje brzo i naknadno ispravlja.
- d. razvija se da bi ima što manje sigurnosnih propusta, ako je potrebno i smanjivanjem broja funkcija i mogućnosti
- e. ne znam

The correct answer is: razvija se brzo da bi se što pre predstavio kupcima, a propusti i greške se naknadno ispravljaju

Question 344

Not answered

Marked out of 1.00

Ispravke, zakrpe i nove verzije softvera:

Select one:

- a. predstavljaju nepotrebno opterećivanje sistema zato što proizvođači ubacuju suvišne opcije da bi korisnicima prodali nove verzije programa
- b. ispravljaju poznate probleme, ali mogu da donesu neke nove propuste
- c. obezbeđuju da softver na kraju bude potpuno bez propusta, ako je proizvođač ažuran i izbacuje redovno dopune
- d. ne znam
- e. omogućavaju da proizvođač bude korak ispred napadača i da oni nemaju vremena za analizu da iskoriste mane

The correct answer is: ispravljaju poznate probleme, ali mogu da donesu neke nove propuste

Question 345

Not answered

Marked out of 1.00

Buffer overflow može da se zloupotrebi (između ostalog):

Select one:

- a. samo na Windows operativnim sistemima
- b. samo na UNIX/Linux operativnim sistemima
- c. ne znam
- d. samo ako je dostupan izvorni kod softvera
- e. ubacivanjem zlonamernog koda

The correct answer is: ubacivanjem zlonamernog koda

Question 346

Not answered

Marked out of 1.00

Prednosti anti-virusa koji detektuje zlonamerne programe na osnovu potpisa su:

Select one:

- a. jednostavno i lako detektuje poznat zlonamerni kod uz minimalno angažovanje korisnika
- b. osetljiv je na sumnjive akcije programa i logički, na osnovu skupa pravila, otkriva zlonamerni softver
- c. zahteva vrlo malu bazu potpisa koja pokriva ogroman broj zlonamernog koda, što ga čini brzim
- d. lako otkriva varijacije zlonamernog koda i nove verzije na osnovu poznatog potpisa
- e. ne znam

The correct answer is: jednostavno i lako detektuje poznat zlonamerni kod uz minimalno angažovanje korisnika

Question 347

Not answered

Marked out of 1.00

Mane anti-virusa koji detektuje zlonamerne programe na osnovu potpisa su:

Select one:

- a. procesorski je zahtevan - znatno usporava funkcionisanje i odziv operativnog sistema
- b. ne može da zaštitи korisnika od crva - zlonamernih programa koji se kriju u nosiocu
- c. ne znam
- d. ne može da otkrije nove i promenljive zlonamerne programe, baza potpisa može da postane velika, što usporava rad.
- e. može da protumači legitimne akcije programa kao zlonamerne - lažni alarmi, potrebno je često podešavanje osetljivosti

The correct answer is: ne može da otkrije nove i promenljive zlonamerne programe, baza potpisa može da postane velika, što usporava rad.

Question 348

Not answered

Marked out of 1.00

Reverzni inženjering je proces u kome se:

Select one:

- a. kompajlira asemblerski kod u izvršni binarni kod
- b. ne znam
- c. rekonstruišu asemblerske instrukcije na osnovu binarne datoteke
- d. koristi slabost programskih jezika za ubacivanje zlonamernog koda u memoriju
- e. vraća kod višeg programskog jezika na osnovu asemblerskog koda

The correct answer is: rekonstruišu asemblerske instrukcije na osnovu binarne datoteke

Question 349

Not answered

Marked out of 1.00

Debugger je alat koji:

Select one:

- a. omogućava praćenje izvršenja programa i analizu resursa koje koristi
- b. ne znam
- c. omogućava automatizovano ispravljanje grešaka (*bug-ova*) programa koji se izvršava
- d. omogućava napadaču da namerno implementira greške (*bug-ove*) u binarne datoteke
- e. omogućava dinamičko praćenje izvornog koda programa za koji imamo binarni fajl

The correct answer is: omogućava praćenje izvršenja programa i analizu resursa koje koristi

Question 350

Not answered

Marked out of 1.00

Reverzni inženjering je tehnika koja se koristi za:

Select one:

- a. dobijanje omplete slike ulaza i izlaza koju program ima pri izvršavanju
- b. analizu exe fajlova
- c. ne znam
- d. konvertovanje exe fajlova u drugi oblik
- e. dobijanje izvornog koda od exe koda

The correct answer is: analizu exe fajlova

Question 351

Not answered

Marked out of 1.00

Koji programski jezik je osjetljiv na prekoračenje bafera?

Select one:

- a. ne znam
- b. C#
- c. C/C++
- d. Java
- e. ni jedan od navedenih

The correct answer is: C/C++

Question 352

Not answered

Marked out of 1.00

Open source code u odnosu na softver zatvorenog koda u pogledu ukupne sigurnosti:

Select one:

- a. predstavljaju podjednaka rešenja
- b. predstavlja neuporedivo lošije rešenje
- c. ne znam
- d. predstavlja neuporedivo bolje rešenje
- e. nisu uporedivi

The correct answer is: predstavljaju podjednaka rešenja

Question 353

Not answered

Marked out of 1.00

Izbaciti uljeza:

Select one:

- a. *OllyDbg*
- b. ne znam
- c. *IDA Pro*
- d. *Komodo*
- e. *Soft ICE*

The correct answer is: *Komodo***Question 354**

Not answered

Marked out of 1.00

Koja se od navedenih tehnika je **najmanje** efikasna za sprečavanje reverznog inženjeringa?

Select one:

- a. *anti-disassembly* tehnika
- b. *anti-debugging* tehnika
- c. šifrovanje izvornog koda
- d. maskiranje koda
- e. ne znam

The correct answer is: šifrovanje izvornog koda

Question 355

Not answered

Marked out of 1.00

DRM:

Select one:

- a. koristi samo kriptografske mere zaštite
- b. može se koristiti samo za zaštitu audio zapisa od neovlašćenog umnožavanja
- c. u nekim slučajevima koristi neetičke rootkit alate
- d. može se koristiti samo za zaštitu video zapisa od neovlašćenog umnožavanja
- e. ne znam

The correct answer is: u nekim slučajevima koristi neetičke rootkit alate

Question 356

Not answered

Marked out of 1.00

Mrežna barijera koja ima filter paketa sa uspostavljanjem stanja (statefull firewall):

Select one:

- a. analizira kompletan sadržaj paketa (i zaglavlje i sadržaj)
- b. pamti odbačene pakete
- c. ne znam
- d. vraća odbačene pakete pošiljaocu
- e. pamti zahteve za uspostavljanjem veze tokom sesije

The correct answer is: pamti zahteve za uspostavljanjem veze tokom sesije

Question 357

Not answered

Marked out of 1.00

Koju od dole navedenih usluga ne pruža mrežna barijera ?

Select one:

- a. Proxy servisi
- b. Prevođenje mrežnih adresa
- c. sprečavanje prekoračenja bafera
- d. ne znam
- e. filtriranje paketa

The correct answer is: sprečavanje prekoračenja bafera

Question 358

Not answered

Marked out of 1.00

Mrežna barijera se realizuje:

Select one:

- a. ne znam
- b. isključivo kao hardver
- c. može biti i softver i hardver
- d. kao deo operativnog sistema
- e. isključivo kao softver

The correct answer is: može biti i softver i hardver

Question 359

Not answered

Marked out of 1.00

Koji se zlonamerni program ne zahteva nosioca?

Select one:

- a. ne znam
- b. virus
- c. trojanski konj
- d. logička bomba
- e. crv

The correct answer is: crv

Question 360

Not answered

Marked out of 1.00

Zlonamerni program koji se ugrađuje u neki koristan program i aktivira se kada se ispunе odgovarajući uslovi naziva se:

Select one:

- a. malware
- b. virus
- c. ne znam
- d. logička bomba
- e. crv

The correct answer is: logička bomba

Question 361

Not answered

Marked out of 1.00

Windows Defender je:

Select one:

- a. ne znam
- b. program koji omogućava pravljenje zaštićenih particija na disku
- c. antivirus program
- d. program koji obezbeđuje uslugu autentifikacije
- e. drugi naziv za Windows-ovu zaštitnu barijeru (*firewall*)

The correct answer is: antivirus program

Question 362

Not answered

Marked out of 1.00

Logičke bombe su posebna vrsta:

Select one:

- a. virusa
- b. crva
- c. ne znam
- d. trojanskog konja
- e. špijunskog programa

The correct answer is: trojanskog konja

Question 363

Not answered

Marked out of 1.00

Napad zlonamernim programima koji koriste ljudske slabosti naziva se:

Select one:

- a. ne znam
- b. društveni inženjerинг
- c. ubacivanje logičke bombe
- d. odbijanje usluge
- e. društvena mreža

The correct answer is: društveni inženjerинг

Question 364

Not answered

Marked out of 1.00

Najbolja preventivna zaštita od zlonamernog koda je:

Select one:

- a. zaštita u realnom vremenu (real time protection)
- b. skeniranje računara na zahtev (on demand scan)
- c. redovna defragmentacija diska
- d. blokiranje Internet veze
- e. ne znam

The correct answer is: zaštita u realnom vremenu (real time protection)

Question 365

Not answered

Marked out of 1.00

Prilikom instaliranja antivirus programa preporuka je da se instalira:

Select one:

- a. ne znam
- b. dva do četiri anti virus programa
- c. što više antivirus programa kako bi se pokrila što veća baza virusa
- d. najmanje dva antivirus programa
- e. samo jedan pouzdan antivirus program

The correct answer is: samo jedan pouzdan antivirus program

Question 366

Not answered

Marked out of 1.00

Nedostatak IDS-a za detekciju anomalija je to što

Select one:

- a. ne otkriva nove upade već detektuje samo već poznate
- b. se algoritam za detekciju sporo izvršava
- c. to što je zahtevan po pitanju resursa
- d. može da generiše previše lažnih alarma
- e. ne znam

The correct answer is: može da generiše previše lažnih alarma

Question 367

Not answered

Marked out of 1.00

Metode za zaštitu od kompromitujućeg el-mg zračenja (KEMZ) obuhvataju:

Select one:

- a. ne znam
- b. oklapanje uređaja slabo vodljivim materijalima
- c. filtriranje visoko frekv. komponenti napajanja
- d. izradu linija za masu sa minimalnom površinom
- e. filtriranje nisko frekv. komponenti napajanja

The correct answer is: filtriranje visoko frekv. komponenti napajanja

Question 368

Not answered

Marked out of 1.00

Smart kartica obezbeđuje:

Select one:

- a. ne znam
- b. četvorostruku autentifikaciju
- c. trostruku autentifikaciju
- d. dvostruku autentifikaciju
- e. jednostruku autentifikaciju

The correct answer is: trostruku autentifikaciju

Question 369

Not answered

Marked out of 1.00

Sigurnost podataka koji se nalaze na Smart karticama se postiže:

Select one:

- a. samo pomoću PIN-a
- b. ne znam
- c. skremblovanjem
- d. primenom heš vrednosti
- e. šifrovanjem

The correct answer is: šifrovanjem

Question 370

Not answered

Marked out of 1.00

Očitavanje SMART kartice je moguće prisluškivati:

Select one:

- a. ne znam
- b. Postavljanjem prisluškivača elektromagnetskog zračenja u blizini uređaja za očitavanje
- c. Postavljanjem prisluškivača zvučnih zapisa
- d. Samo neposrednim kontaktom ili modifikacijom uređaja za očitavanje
- e. Postavljanjem skrivene video kamere

The correct answer is: Postavljanjem prisluškivača elektromagnetskog zračenja u blizini uređaja za očitavanje

Question 371

Not answered

Marked out of 1.00

Šta se dešava sa RAM memorijom po isključenju računara?

Select one:

- a. U RAM memoriju se ne upisuju osetljivi podaci, tako da po gašenju računara nema smisla rekonstruisati sadržaj.
- b. U RAM memoriji ne ostaju nikakvi podaci pošto je za njen rad potrebno napajanje
- c. RAM memorija služi za čuvanje podatka po isključivanju računara, da bi računar imao brz pristup prethodnim sesijama prilikom ponovnog uključivanja.
- d. ne znam
- e. U kratkom vremenskom periodu od gašenja računara u RAM memoriji postoje zaostala nanelektrisanja na osnovu kojih se može očitati osetljiv sadržaj.

The correct answer is: U kratkom vremenskom periodu od gašenja računara u RAM memoriji postoje zaostala nanelektrisanja na osnovu kojih se može očitati osetljiv sadržaj.

Question 372

Not answered

Marked out of 1.00

Sadržaj SMART kartice je moguće očitati

Select one:

- a. Pomoću optičkog skenera
- b. ne znam
- c. Očitavanjem namagnetisanja
- d. Samo povezivanjem čitača na kontakte kartice
- e. Direktnim kontaktom ili putem radio talasa

The correct answer is: Direktnim kontaktom ili putem radio talasa

Question 373

Not answered

Marked out of 1.00

Visokofrekventno elektromagnetsko zračenje računara:

Select one:

- a. Predstavlja "beli šum" i ne nosi korisne informacije
- b. Može da nosi dovoljno informacija za kompromitovanje sistema
- c. Lokalnog je karaktera i ne smatra se sigurnosnom rupom
- d. Može da se kontroliše pažljivim projektovanjem softvera
- e. ne znam

The correct answer is: Može da nosi dovoljno informacija za kompromitovanje sistema

Question 374

Not answered

Marked out of 1.00

Za prislушкиvanje naponskih nivoa provodnika:

Select one:

- a. Naponski nivoi se mogu rekonstruisati preciznim merenjem vibracija u okolini kabla
- b. Naponski nivoi se mogu rekonstruisati bez kontakta sa kablom merenjem elektromagnetskog zračenja
- c. Neophodno je neopaženo prevezati kabl na opremu za prislушкиvanje
- d. ne znam
- e. Ne postoje metode bez pristupa aktivnoj opremi koja emituje signal

The correct answer is: Naponski nivoi se mogu rekonstruisati bez kontakta sa kablom merenjem elektromagnetskog zračenja

Question 375

Not answered

Marked out of 1.00

Ukoliko paket ne zadovoljava ni jedno od pravila u iptables lancu, šta se dešava sa paketom?

Select one:

- a. paket čeka u redu na izmenu pravila u lancu
- b. paket se odbija
- c. ne znam
- d. paket se prihvata
- e. primenjuje se podrazumevana polisa

The correct answer is: primenjuje se podrazumevana polisa

Question 376

Not answered

Marked out of 1.00

U koliko u listi za kontrolu pristupa ne postoji ni jedno pravilo koje odgovara pristiglom paketu:

Select one:

- a. Paket će biti prosleđen
- b. ne znam
- c. Paket će biti poslat administratoru
- d. Paket će biti odbačen
- e. Od izvorišta će biti zatražena dodatna informacija

The correct answer is: Paket će biti odbačen

Question 377

Not answered

Marked out of 1.00

Mrežna barijera (firewall) posle filtriranja paketa, paket koji ne zadovoljava ni jedno od definisanih pravila za kontrolu pristupa:

Select one:

- a. vraća pošiljaocu
- b. odbacuje
- c. ne znam
- d. čuva u posebno za to definisanoj memoriji
- e. oporavlja a zatim propušta

The correct answer is: odbacuje

Question 378

Not answered

Marked out of 1.00

Pri analizi paketa pristiglog na mrežnu barijeru dolazi do poklapanja sa jednim od pravila liste za kontrolu pristupa. Koje su dalje akcije mrežne barijere?

Select one:

- a. Mrežna barijera uvek prosleđuje paket ako dođe do poklapanja sa pravilom iz liste
- b. Mrežna barijera uvek odbacuje paket ako dođe do poklapanja sa pravilom iz liste
- c. ne znam
- d. Mrežna barijera pretražuje ostatak liste i izvršava restriktivniju akciju koja odgovara paketu, u koliko postoji.
- e. Mrežna barijera izvršava akciju vezanu za pravilo sa kojim se paket poklapa i zanemaruje ostatak liste.

The correct answer is: Mrežna barijera izvršava akciju vezanu za pravilo sa kojim se paket poklapa i zanemaruje ostatak liste.

Question 379

Not answered

Marked out of 1.00

U listama za kontrolu pristupa mrežne barijere paketi mogu da se filtriraju na osnovu:

Select one:

- a. Izvořišne i odredišne IP adrese i porta
- b. Izvořišne i odredišne MAC adrese i domena
- c. Izvořišnih i odredišnih web adresa i domena
- d. Izvořišnog protokola fizičkog sloja
- e. ne znam

The correct answer is: Izvořišne i odredišne IP adrese i porta

Question 380

Not answered

Marked out of 1.00

Na kraju svih pravila liste za kontrolu pristupa postoji implicitna (nevidljiva) stavka:

Select one:

- a. Deny all (odbaci sve)
- b. Ignore all (zanemari sve)
- c. ne znam
- d. Allow all (prosledi sve)
- e. Stavka koju administrator podešava

The correct answer is: Deny all (odbaci sve)

Question 381

Not answered

Marked out of 1.00

Liste za kontrolu pristupa mrežne barijere se koriste za filtriranje paketa tako što se:

Select one:

- a. Redom proveravaju pravila i traži prvo podudaranje sa parametrima paketa, posle čega se ostatak liste zanemaruje.
- b. Proveravaju sva pravila od početka do kraja i u koliko ima više podudaranja, restriktivnije (deny) pravilo odlučuje.
- c. ne znam
- d. Sva pravila se redom proveravaju i prvo se primenjuju ona koja definišu portove transportnog sloja, a zatim ona koja definišu IP adrese u koliko paket nije odbačen
- e. Prolaskom kroz celu listu se dinamički kreira "meta" pravilo koje je zbir svih odgovarajućih parametara koji se poklapaju sa pristiglim paketom i zatim se primenjuje zbirna odluka.

The correct answer is: Redom proveravaju pravila i traži prvo podudaranje sa parametrima paketa, posle čega se ostatak liste zanemaruje.

Question 382

Not answered

Marked out of 1.00

Ako administrator mrežne barijere želi da dopusti web servis klijentima, standardno treba da napravi pravilo:

Select one:

- a. Koje propušta sav odredišni UDP protokol
- b. Koje propušta odredišni port web servisa - 80
- c. Koje propušta izvorišni port web servisa - 80
- d. ne znam
- e. Koje propušta sve odredišne IP adrese web servera

The correct answer is: Koje propušta odredišni port web servisa - 80

Question 383

Not answered

Marked out of 1.00

Ako je IDS detektovao napad koji se desio taj događaj se označava kao:

Select one:

- a. TP (True Positive)
- b. FP (False Positive)
- c. FN (False Negative)
- d. TN (True Negative)
- e. ne znam

The correct answer is: TP (True Positive)

Question 384

Not answered

Marked out of 1.00

Kada IDS tekuću legitimnu aktivnost prepozna kao napad, taj događaj se označava kao:

Select one:

- a. TN (True Negative)
- b. FN (False Negative)
- c. FP (False Positive)
- d. ne znam
- e. TP (True Positive)

The correct answer is: FP (False Positive)

Question 385

Not answered

Marked out of 1.00

Ako je IDS propusti da detektuje napad koji se desio taj događaj se označava kao:

Select one:

- a. FP (False Positive)
- b. FN (False Negative)
- c. TP (True Positive)
- d. ne znam
- e. TN (True Negative)

The correct answer is: FN (False Negative)

Question 386

Not answered

Marked out of 1.00

Ako je IDS korektno registruje legitimnu aktivnost taj događaj se označava kao:

Select one:

- a. TN (True Negative)
- b. TP (True Positive)
- c. ne znam
- d. FP (False Positive)
- e. FN (False Negative)

The correct answer is: TN (True Negative)

Question 387

Not answered

Marked out of 1.00

Količnik broja stvarnih upada koje je IDS detektovao i zbiru pravih alarma i propuštenih alarma ($TP / (TP + FN)$) označava se kao:

Select one:

- a. osetljivost
- b. taj odnos nema statistički značaj
- c. određenost
- d. tačnost
- e. ne znam

The correct answer is: osetljivost

Question 388

Not answered

Marked out of 1.00

Količnik ispravno detektovanih legitimnih aktivnosti upada i zbra stvarno negativnih i lažnih alarma ($TN / (TN + FP)$) koje detektuje IDS označava se kao:

Select one:

- a. osetljivost
- b. ne znam
- c. tačnost
- d. određenost
- e. taj odnos nema statistički značaj

The correct answer is: određenost

Question 389

Not answered

Marked out of 1.00

Količnik broja stvarnih upada koje je IDS detektovao i zbra pravih alarma i lažnih alarma ($TP / (TP + FP)$) označava se kao:

Select one:

- a. određenost
- b. ne znam
- c. tačnost
- d. taj odnos nema statistički značaj
- e. osetljivost

The correct answer is: tačnost

Question 390

Not answered

Marked out of 1.00

Količnik ispravno detektovanih legitimnih aktivnosti upada i zbira stvarno negativnih i propuštenih alarma ($TN / (TN + FN)$) koje detektuje IDS označava se kao:

Select one:

- a. ne znam
- b. osetljivost
- c. određenost
- d. taj odnos nema statistički značaj
- e. tačnost

The correct answer is: taj odnos nema statistički značaj

Question 391

Not answered

Marked out of 1.00

Dat je primer liste za kontrolu pristupa u pseudo kodu:

10 deny from 192.168.1.0 /24

20 allow from 192.168.1.10

30 deny all

Šta će se desiti sa paketom sa sledeće adrese?

192.168.1.10

Select one:

- a. Biće odbačen zbog pravila 10
- b. Data lista nije dovoljna da bi se odredila sudbina paketa
- c. Biće prosleđen zbog pravila 20
- d. Biće odbačen zbog pravila 30
- e. ne znam

The correct answer is: Biće odbačen zbog pravila 10

Question 392

Not answered

Marked out of 1.00

Dat je primer liste za kontrolu pristupa u pseudo kodu:

10 allow from 10.0.0.0 /8
20 allow from 192.168.1.0 /24
30 deny all

Šta će se desiti sa paketom sa sledeće adrese?

192.168.1.12

Select one:

- a. Biće prosleđen zbog pravila 10
- b. Biće prosleđen zbog pravila 20
- c. Data lista nije dovoljna da bi se odredila soubina paketa
- d. ne znam
- e. Biće odbačen zbog pravila 30

The correct answer is: Biće prosleđen zbog pravila 20

Question 393

Not answered

Marked out of 1.00

Dat je primer liste za kontrolu pristupa u pseudo kodu:

10 allow from 192.168.1.10
20 deny from 192.168.1.0 /24
30 deny all

Šta će se desiti sa paketom sa sledeće adrese?

192.168.1.10

Select one:

- a. Biće odbačen zbog pravila 30
- b. Biće prosleđen zbog pravila 10
- c. Biće odbačen zbog pravila 20
- d. Data lista nije dovoljna da bi se odredila soubina paketa
- e. ne znam

The correct answer is: Biće prosleđen zbog pravila 10

Question 394

Not answered

Marked out of 1.00

Dat je primer liste za kontrolu pristupa u pseudo kodu:

10 deny from 192.168.0.0 /24
20 allow from 192.168.0.10
30 deny all

Šta će se desiti sa paketom sa sledeće adrese?

192.168.0.10

Select one:

- a. Biće prosleđen zbog pravila 20
- b. Biće odbačen zbog pravila 30
- c. Biće odbačen zbog pravila 10
- d. Data lista nije dovoljna da bi se odredila subbina paketa
- e. ne znam

The correct answer is: Biće odbačen zbog pravila 10

Question 395

Not answered

Marked out of 1.00

Dat je primer liste za kontrolu pristupa u pseudo kodu:

10 allow from 192.168.1.0 /24
20 deny from 192.168.2.10
30 deny all

Šta će se desiti sa paketom sa sledeće adrese?

192.168.2.20

Select one:

- a. Biće odbačen zbog pravila 30
- b. Biće prosleđen zbog pravila 10
- c. Data lista nije dovoljna da bi se odredila subbina paketa
- d. Biće odbačen zbog pravila 20
- e. ne znam

The correct answer is: Biće odbačen zbog pravila 30

Question 396

Not answered

Marked out of 1.00

Dat je primer liste za kontrolu pristupa u pseudo kodu:

10 allow from 192.168.1.0 /24
20 deny from 192.168.1.100
30 deny all

Šta će se desiti sa paketom sa sledeće adrese?

192.168.2.10

Select one:

- a. Biće odbačen zbog pravila 30
- b. Biće prosleđen zbog pravila 10
- c. Biće odbačen zbog pravila 20
- d. Data lista nije dovoljna da bi se odredila slobodna paketa
- e. ne znam

The correct answer is: Biće odbačen zbog pravila 30

Question 397

Not answered

Marked out of 1.00

Jedan od osnovnih problema koje operativni sistem treba da reši je efikasna podjela resursa računara.

Podjela kod koje se različitim korisnicima/procesima dodeljuju različiti resursi naziva se:

Answer: X

The correct answer is: fizička

Question 398

Not answered

Marked out of 1.00

Postupak kojim se otvoreni tekst записује у облику бинарног низа назива се:

Answer: X

The correct answer is: кодовање

Question 399

Not answered

Marked out of 1.00

Способност система да овлашћеном кориснику пружи услугу кад год је потребна назива се:

Answer: 

The correct answer is: расположивост

Question 400

Not answered

Marked out of 1.00

Супституција код које се један знак замењује увек истим знаком назива се:

Answer: 

The correct answer is: проста

Question 401

Not answered

Marked out of 1.00

Скуп активности које треба да спрече или детектују неовлашћену измену или брисање података било да се подаци чувају или преносе означава се као:

Answer: 

The correct answer is: интегритет података

Question 402

Not answered

Marked out of 1.00

Супституција код које се током шифровања један знак не замењује увек истим знаком већ неким из дозвољеног скupa знакова назива се:

Answer: 

The correct answer is: полиалфабетска

Question 403

Not answered

Marked out of 1.00

Супституција код које је основни елемент вршења супституције група знакова назива се:

Answer: 

The correct answer is: полиграмска

Question 404

Not answered

Marked out of 1.00

Autentifikација која захтева све три ставке (нешто што се зна, има и јесте) назива се

Answer: 

The correct answer is: трофакторска

Question 405

Not answered

Marked out of 1.00

Алгоритми који који елементе отвореног текста обрађују један по један називају се:

Answer: 

The correct answer is: проточни

Question 406

Not answered

Marked out of 1.00

Генератор псеудослучајних вредности, на основу кратког (случајног) кључа генерише

Answer: 

The correct answer is: радни кључ

Question 407

Not answered

Marked out of 1.00

Сервис који обезбеђује проверу идентитета назива се:

Answer: 

The correct answer is: аутентификација

Question 408

Not answered

Marked out of 1.00

Алгоритми који приликом шифровања обрађују блокове отвореног текста називају се:

Answer: 

The correct answer is: блоковски

Question 409

Not answered

Marked out of 1.00

Додела права аутентификованим кориснику назива се:

Answer: 

The correct answer is: ауторизација

Question 410

Not answered

Marked out of 1.00

Шифарски систем код кога је време потребно за "разбијање" шифрата дуже од времена у ком информација треба да буде тајна, назива се:

Answer: 

The correct answer is: рачунски сигуран

Question 411

Not answered

Marked out of 1.00

Imagedowngrading је техника којом се у слици скрива

(Напомена: одговор садржи једну реч)

Answer:



The correct answer is: слика

Question 412

Not answered

Marked out of 1.00

За детекцију постојања скривених порука у стеганоанализи користи се
(довољно је да се наведе само једна метода у облику: *** детекција):

Answer:



The correct answer is: визуелна детекција

Question 413

Not answered

Marked out of 1.00

Jedan od основних проблема које оперативни систем треба да реши је ефикасна подела ресурса рачунара.

Подела код које само један корисник/процес у једном тренутку може да користи ресурс назива се:

Answer:



The correct answer is: привремена

Question 414

Not answered

Marked out of 1.00

Шифарски систем, код кога је цена "разбијања" шифрата превазилази вредност шифроване информације назива се:

Answer:



The correct answer is: рачунски сигуран

Question 415

Not answered

Marked out of 1.00

Код блоковских алгоритама, блок шифрата се добија вишеструком применом одређене функције на блок отвореног текста и међурезултате. Једна примена функција назива се:

Answer: 

The correct answer is: рунда

Question 416

Not answered

Marked out of 1.00

Криптографски систем који користећи систем са јавним кључем за размену симетричног кључа а потом прелази на симетричну криптографију назива се:

Answer: 

The correct answer is: хибридни

Question 417

Not answered

Marked out of 1.00

Својство блоковских алгоритама такво, да иако се познаје неки пар блокова отвореног текста P_i и њему припадајућег шифрата C_i није могуће да се одреди блок отвореног текста P_j иако се зна шифрат C_j назива се својство

Answer: 

The correct answer is: дифузије

Question 418

Not answered

Marked out of 1.00

Својство шифарских алгоритама такво, да су код напада потпуном претрагом кључева сви кључеви подједнако вероватни, назива се својство

Answer: 

The correct answer is: конфузије

Question 419

Not answered

Marked out of 1.00

Својство шифарских алгоритама такво, да је сваки бит шифрата у функцији сваког бита кључа, назива се

Answer:



The correct answer is: комплетност

Question 420

Not answered

Marked out of 1.00

Нека је дат јавни кључ $(N,e)=(55,7)$ и приватни кључ 23 генерисани RSA алгоритмом. Шифрује се порука $M=12$. Резултат је (уписати број):

Answer:



The correct answer is: 23

Question 421

Not answered

Marked out of 1.00

Zlonamerni рачунарски код који може да се интегрише на постојећи програм или фајл и да се на тај начин преноси са рачунара на рачунар назива се:

Answer:



The correct answer is: virus

Question 422

Not answered

Marked out of 1.00

Jедан од основних проблема које оперативни систем треба да реши је ефикасна подела ресурса рачунара.

Подела код које се различитим корисnicima/procesima додељују одређени делови ресурса назива се:

Answer:



The correct answer is: логичка

Question 423

Not answered

Marked out of 1.00

Функције које релативно лако могу да се израчунају али њихова инверзна вредност може да се одреди само изузетно сложеним поступком називају се

Answer:



The correct answer is: једносмерне

Question 424

Not answered

Marked out of 1.00

Нека је дат јавни кључ $(N,e)=(33,7)$ и приватни кључ 3 генерисани RSA алгоритмом. Шифрат је $C=27$. Порука је је (уписати број):

Answer:



The correct answer is: 15

Question 425

Not answered

Marked out of 1.00

Отворени текст је шифрован Афином шифром. Кључ је уређени пар $(7,15)$ а за шифровање се користе искључиво велика слова енглеске абецеде нумерисана редом, од 0 до 25. Ако је добијени шифрат OPHJAR како гласи отворени текст?

Answer:



The correct answer is: ЛАКО ЈЕ

Question 426

Not answered

Marked out of 1.00

Jedan od основних проблема које оперативни систем треба да реши је ефикасна подела ресурса рачунара.

Подела код које сви корисници/процеси могу да користе све ресурсе али су подаци разумљиви само власнику док су за остale неразумљиви назива се:

Answer:



The correct answer is: криптографска

Question 427

Not answered

Marked out of 1.00

Komunikacioni kanal koji nije projektovan od strane dizajnera sistema i nije pod kontrolom ali može da posluži za protok informacija naziva se:

Answer: 

The correct answer is: tajni

Question 428

Not answered

Marked out of 1.00

Шифром двоструке транспозиције шифрована је реч PLEASURE. Одабрана димензија матрице је 3x3, правило за пермутацију колона је (3,1,2) а правило за пермутацију врста је (2,3,1). Добијени шифрат је:

Answer: 

The correct answer is: ELSXEURPA

Question 429

Not answered

Marked out of 1.00

Potpuno automatizovan javni Tjuringov test за razlikovanje čoveka od računara tj. test koji čovek može da prođe sa lakoćom dok računar ne može da ga prođe sa verovatnoćom većom od one koja bi se postigla nasumičnim pogadanjem naziva se

Answer: 

The correct answer is: CAPTCHA

Question 430

Not answered

Marked out of 1.00

Zlonamerni program koji ima osobinu da može da se širi kroz mrežu bez potrebe za asistencijom korisnika naziva se:

Answer: 

The correct answer is: crv

Question 431

Not answered

Marked out of 1.00

Skup metoda za ograničavanje korišćenja digitalnih sadržaja u cilju zaštite autorskih prava skraćeno se zapisuje:

Answer: 

The correct answer is: DRM

Question 432

Not answered

Marked out of 1.00

Скуп активности које треба да обезбеде да неовлашћена страна у комуникацији не дође до поверљивих информација назива се:

Answer: 

The correct answer is: поверљивост

Question 433

Not answered

Marked out of 1.00

Супституција код које се већина знакова мења истим седмима најфреkvентијих који могу да се мењају на више начина назива се

Answer: 

The correct answer is: хомофони

Question 434

Not answered

Marked out of 1.00

Дати су параметри $p=13$ и $q=11$. Алиса и Боб размењују кључеве уз помоћ Дифи Хелмановог алгоритма. Алиса је замислила број 3 а Боб 4. Заједничка тајна је:

Answer: 

The correct answer is: 1