Розпочато	Wednesday 24 May 2023 13:40 PM
Стан	Завершено
Завершено	Wednesday 24 May 2023 14:05 PM
Витрачено часу	25 хв 10 сек
Балів	43/45
Оцінка	**29** з можливих 30 (**97**%)

Питання **1**

Завершено

Балів 1,00 з 1,00

Яке основне використання HMAC?

a) Шифрування повідомлень
b) Перевірка цілісності даних
c) Безпечної передачі даних

Виберіть одну відповідь:

- 1. b
- 2. a
- 3. c

Питання **2**

Завершено

Балів 1,00 з 1,00

Які основні вимоги накладаються на алгоритм MAC?

a) Важкооборотність
b) Стійкість до колізій
c) Алгоритмічна складність
d) Ніяких вимог не накладається

Виберіть одну або декілька відповідей:

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

Питання **3**

Завершено

Балів 1,00 з 1,00

Нехай $p = 17, g = 3$ відкриті параметри криптосистеми Ель-Гамала, спільні для декількох користувачів, $a = 7$ секретний ключ одного з них. Завершіть формування його відкритих ключів

a)$h = 10$; b)$h = 11$; c)$h = 12$; d)$h = 3$; e)$h = 4$; f)$h = 5$;

Виберіть одну відповідь:

1. c
2. a
3. b
4. f
5. d
6. e

Питання **4**

Завершено

Балів 1,00 з 1,00

Чому в протоколі Діффі-Гелмана доцільно передбачати аунтентифікацію абонентів?

a) Без автентифікації можливо зламати задачу дискретного логарифмування

b) Без автентифікації можливо зламати задачу факторизації великих чисел

c) Без автентифікації супротивник може замінити своїм ключем відкритий ключ, який той надсилає законному користувачу

d) Завдяки автентифікації неможливо провести атаку на основі «парадоксу днів народжень» абонентів

Виберіть одну відповідь:

1. c
2. a
3. b
4. d

Питання **5**

Завершено

Балів 1,00 з 1,00

У чому полягає ідея лінійного шифру?

a) кожна літера в алфавіті замінюється на свій числовий еквівалент, шифрується за допомогою певної мат. функції та перетворюється назад у букву

b) у тому, що спочатку множимо порядковий номер літери, а потім виконуємо додаткову заміну Цезаря

c) кожен символ у відкритому тексті замінюється на символ, що знаходиться на деякому постійному числі позицій ліворуч або праворуч від нього в алфавіті

d) утворення закодованих слів шляхом множинного поділу

Виберіть одну відповідь:

1. a
2. b
3. d
4. c

Питання **6**

Завершено

Балів 1,00 з 1,00

Як називається ідентифікація людини за унікальними, властивими тільки їй, біологічними ознаками?

a) Апаратна

b) Парольна

c) Біометрична

d) Багатофакторна

Виберіть одну відповідь:

1. a
2. b
3. d
4. c

Питання **7**

Завершено

Балів 1,00 з 1,00

Що є результатом ділення кілець лишків?

a) Теорема Ейлера
b) Китайська теорема про лишки
c) Мала теорема Ферма
d) Велика теорема Ферма

Виберіть одну відповідь:

1. c
2. b
3. d
4. a

Питання **8**

Завершено

Балів 1,00 з 1,00

Що забезпечує стійкість ECC?

a) Він не є безпечним
b) Складність оберненої операції є неполіноміальною
c) Функція є необоротною

Виберіть одну відповідь:

1. b
2. a
3. c

Питання **9**

Завершено

Балів 1,00 з 1,00

Коли автентифікація є однобічною?

a) Коли клієнт системи для доступу до інформації доводить свою автентичність;

b) Коли, крім клієнта, свою автентичність

повинна підтверджувати і система (наприклад, банк);

c) Коли використовується так звана нотаріальна служба автентифікації для підтвердження достовірності кожного з партнерів в обміні інформацією.

d) Коли система підтверджує свою автентичність

Виберіть одну відповідь:

1. c
2. b
3. d
4. a

Питання **10**

Завершено

Балів 1,00 з 1,00

Визначення криптографічної хеш-функції:

a) Функція, яка перетворює довільну стрічку в число
b) Функція, яка перетворює довільну стрічку в масив бітів певного розміру
c) Функція, яка перетворює фіксовану стрічку в число.

Виберіть одну відповідь:

1. a
2. c
3. b

Питання **11**

Завершено

Балів 1,00 з 1,00

Нехай маємо два простих різних числа **p=3557** і **q=2579** та відкриту експоненту **e=3** , тоді значення відкритого ключа буде:

a) **{e,n}={3,9173503}**

b) **{e,n}={46,9173503}**

c) **{e,n}={6111579,9173503}**

d) **{e,n}={9173503,3}**

Виберіть одну відповідь:

1. b
2. c
3. d
4. a

Питання **12**

Завершено

Балів 1,00 з 1,00

У чому полягає надійність криптосистеми RSA?

a) Складність отримання приватного ключа з публічного
b) Неможливість отримати ключ шифрування
c) Дана система не є надійною

Виберіть одну відповідь:

1. c
2. b
3. a

Питання **13**

Завершено

Балів 1,00 з 1,00

У чому полягає функція конфіденційності криптографічного протоколу?

a) специфічний набір даних не стане доступним або розкритим для неавторизованих суб'єктів або процесів, а залишиться невідомим противнику.

b) у забезпеченні аутентифікації джерела даних і цілісності переданого повідомлення.

c) у захисті ідентифікаторів від прослуховування.

d) один з учасників отримує підтвердження того, що ніякий інший учасник крім заздалегідь визначеного другого учасника не може отримати доступ до жодного секретного ключа.

Виберіть одну відповідь:

1. d
2. a
3. c
4. b

Питання **14**

Завершено

Балів 1,00 з 1,00

Оберіть стійкі типи шифрів:

a) Шифр Цезаря
b) Шифр Ель-Гамаля
c) Шифр Вернама
d) Шифр множення

Виберіть одну або декілька відповідей:

1. c
2. b
3. a
4. d

Питання **15**

Завершено

Балів 1,00 з 1,00

Як використовується RSA у алгоритмах MASH?

a) Ітераційна функція для одного блоку хешу

b) Один з кроків алгоритму — шифрування повідомлення з допомогою RSA

c) Не використовується

Виберіть одну відповідь:

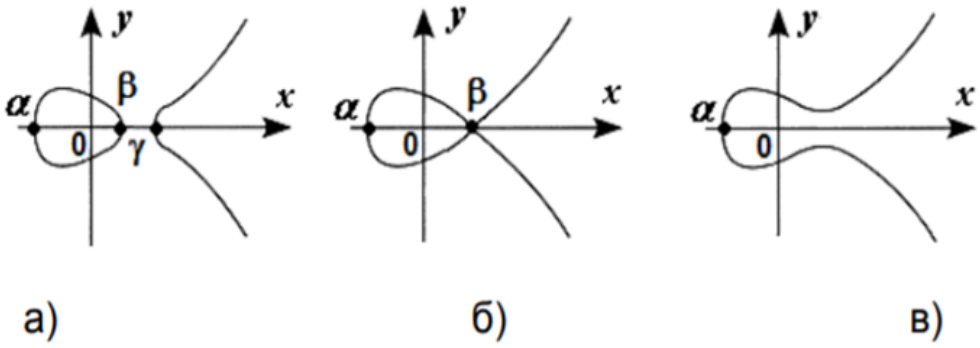
1. c
2. a
3. b

Питання **16**

Завершено

Не оцінено

Яка з еліптичних кривих, поданих на рисунку є сингулярною?



Виберіть одну відповідь:

1. б
2. a
3. в

Питання **17**

Завершено

Балів 1,00 з 1,00

1.

Якщо цілі числа p і q близькі одне до одного, то їх можна знайти методом:

a) Ферма

b) Лагранжа

c) Мерсонна

d) Лемана

Виберіть одну відповідь:

1. a
2. c
3. b
4. d

Питання **18**

Завершено

Балів 1,00 з 1,00

Якщо E_p (a,b) – еліптична крива над полем GF(p), характеристика якого то рівнянням Вейєрштрасса цієї кривої є

а) $y^2 + y \equiv x^3 + ax + b(\mathrm{mod}\ p)$ б) $y^2 + xy \equiv x^3 + ax + b(\mathrm{mod}\ p)$

в) $y^2 \equiv x^3 + ax + b(\mathrm{mod}\ p)$ г) $y^2 \equiv x^3 + ax^2 + bx + c(\mathrm{mod}\ p)$

Виберіть одну відповідь:

1. а
2. б
3. г
4. в

Питання **19**

Завершено

Балів 1,00 з 1,00

Порядок скінченної групи - це :

a) кількість попарно-впорядкованих елементів групи

b) кількість елементів групи, в якій всі степені елемента групи утворюють у ній підгрупу, порядок якої не дорівнює порядку елемента

c) кількість елементів групи, в якій всі степені елемента групи утворюють у ній підгрупу, порядок якої дорівнює порядку елемента

d) кількість нейтральних елементів групи

Виберіть одну відповідь:

1. b
2. c
3. d
4. a

Питання **20**

Завершено

Балів 1,00 з 1,00

Криптографічна стійкість алгоритму Ель-Гамаля базується на складності

а) Обчислення дискретного логарифма

б) Операції піднесення до степення за модулем

в) Факторизації великих чисел

г) Обчислення символу Легжандра

Виберіть одну відповідь:

1. а
2. б
3. в
4. г

Питання **21**

Завершено

Балів 1,00 з 1,00

Що таке атака відображенням?

a) спроба підмінити одного користувача іншим.

b) атака на систему шляхом запису і подальшого відтворення раніше надісланих коректних повідомлень або їх частин.

c) повторне використання раніше переданого в поточному або попередньому сеансі повідомлення або будь-якої його частини в поточному сеансі протоколу.

d) підміна або інший метод обману, який використовує комбінацію даних з раніше виконаних протоколів, в тому числі протоколів, раніше нав'язаних супротивником.

Виберіть одну відповідь:

1. c
2. a
3. d
4. b

Питання **22**

Завершено

Балів 1,00 з 1,00

Яка математична проблема забезпечує стійкість криптосистем, побудованих на еліптичних кривих?

а) Визначення точок на кривій, координати яких були б надзвичайно великими числами

б) Пошук на еліптичній кривій точок P(x, y), в яких x > y

в) Дискретне логарифмування на еліптичній кривій

г) Пошук двох точок кривої, які мали б однакові абсциси, а їх ординати відрізнялись знаками

Виберіть одну відповідь:

1. а
2. б
3. в
4. г

Питання **23**

Завершено

Балів 1,00 з 1,00

Оберіть ВСІ елементи, якими формально можна задати криптосистему чи шифр.

a) алфавіт для запису повідомлень, алфавіт для запису криптосистем
b) простір ключів, апаратна установка
c) твірний простір
d) шифруюче відображення, дешифруюче відображення

Виберіть одну або декілька відповідей:

- [ ] 1. b
- [x] 2. d
- [x] 3. a
- [ ] 4. c

Питання **24**

Завершено

Балів 1,00 з 1,00

Для будь-якого елемента існує?

a) 2^n обернених відображень
b) $k(x-1)$ обернених відображень
c) не для кожного елемента можна знайти обернене відображення
d) лише одне обернене відображення

Виберіть одну відповідь:

- ( ) 1. c
- (•) 2. d
- ( ) 3. a
- ( ) 4. b

Питання **25**

Завершено

Балів 1,00 з 1,00

Які з методів відносяться до методів розв'язання задачі дискретного логарифмування?

a) метод Ітерацій

b) метод Лагранжа

c) метод Шенкса

d) метод перебору

Виберіть одну або декілька відповідей:

- [ ] 1. a
- [x] 2. c
- [ ] 3. b
- [x] 4. d

Питання **26**

Завершено

Балів 1,00 з 1,00

Для яких бінарних операцій кілець справджуються дистрибутивні закони?

a) множення матриць
b) додавання
c) об'єднання та перетин множин
d) множення

Виберіть одну або декілька відповідей:

- [ ] 1. c
- [x] 2. d
- [x] 3. b
- [ ] 4. a

Питання **27**

Завершено

Балів 0,50 з 0,50

Що називається порядком групи точок еліптичної кривої над полем GF(p)?

а) Кількість точок кривої

б) Число $D=4a^3+27b^2 \bmod p$

в) Найменше натуральне число n, при якому скалярний добуток nG=G, де G - генератор групи

г) Сума a+b

Виберіть одну відповідь:

1. а
2. г
3. б
4. в

Питання **28**

Завершено

Балів 1,00 з 1,00

За протоколом Діффі-Гелмана розподілу ключів

a) Виробляється ключ симетричного шифру

b) Виробляється ключ асиметричного шифру

c) Використовується електронний цифровий підпис

d) Виробляється рандомізатор

Виберіть одну відповідь:

1. a
2. d
3. b
4. c

Питання **29**

Завершено

Балів 1,00 з 1,00

Що таке RSA?

a) алгоритм шифрування, який утворений поєднанням операції xor з ключем, довжина якого не менша довжини переданого повідомлення

b) алгоритм шифрування з відкритим ключем, який базується на факторизації простих чисел

c) алгоритм шифрування, в якому кожна буква відкритого тексту замінюється на ту, що віддалена від неї в алфавіті на сталу кількість позицій

d) алгоритм шифрування, який як ключ використовує слово

Виберіть одну відповідь:

1. d
2. a
3. c
4. b

Питання **30**

Завершено

Балів 1,00 з 1,00

Проміжні результати $g^x \bmod p$ і $g^y \bmod p$ за протоколом Діффі-Гелмана використовуються для

a) Захисту від атаки «людина посередині»

b) Захисту від атаки відтворення

c) Для забезпечення аутентифікації учасників протоколу

d) Для передачі один одному

Виберіть одну відповідь:

1. b
2. d
3. a
4. c

Питання **31**

Завершено

Балів 1,00 з 1,00

(p, g, h) – відкритий ключ, a – секретний ключ криптосистеми Ель-Гамала,

(C_1, C_2) – отриманий шифротекст, у результаті зашифрування відкритого повідомлення M.

Як провести розшифрування?

a) $M = C_2(C_1^a)^{-1} \bmod p$
b) $M = (C_2 C_1^a)^{-1} \bmod p$
c) $M = C_1^a C_2 h \bmod p$
d) $M = C_1(C_1^a)^{-1} \bmod p$
e) $M = (C_1 C_2^a)^{-1} \bmod p$
f) $M = C_1 C_2^{a\square} h \bmod p$

Виберіть одну відповідь:

1. d
2. a
3. c
4. e
5. b
6. f

Питання **32**

Завершено

Балів 1,00 з 1,00

Згідно з теоремою про обернене відображення f: X -> Y - відображення НЕ буває:

a) Об'єктивним
b) Ін'єктивним
c) Сюр'єктивним
d) Бієктивним

Виберіть одну відповідь:

1. b
2. d
3. c
4. a

Питання **33**

Завершено

Балів 1,00 з 1,00

Яка з перелічених властивостей не притаманна кільцям?

a) існування протилежного числа

b) біполярність

c) асоціативність

d) комутативність

Виберіть одну відповідь:

1. d
2. a
3. c
4. b

Питання **34**

Завершено

Балів 1,00 з 1,00

Яка різниця між MAC і HMAC при передачі інформації?

a) Ніякої

b) MAC відправляється з повідомленням, HMAC — окремо

c) HMAC відправляється з повідомленням, MAC — окремо

Виберіть одну відповідь:

1. a
2. b
3. c

Питання **35**

Завершено

Балів 1,00 з 1,00

Яка основна відмінність між афінним шифром та шифром Цезаря?

a) Використання НСД
b) фіксований ключ
c) кількість відображень для елемента множини
d) використання великої теореми Ферма

Виберіть одну відповідь:

1. b
2. d
3. c
4. a

Питання **36**

Завершено

Балів 1,00 з 1,00

Що використовується для підтвердження достовірності отриманої інформації в вебі?

a) SSL-сертифікати
b) Паролі
c) Перевірка третьої сторони

Виберіть одну відповідь:

1. a
2. c
3. b

Питання **37**

Завершено

Балів 0,00 з 1,00

Оберіть основні недоліки афінного шифру.

a) Вузька сфера застосування
b) Складність реалізації
c) Відносно невелика кількість тривіальних та нетривіальних шифрів
d) Шифр нестійкий до зовнішніх атак

Виберіть одну відповідь:

1. b
2. a
3. d
4. c

Питання **38**

Завершено

Балів 1,00 з 1,00

Нехай ***m*** текст для шифрування алгоритмом RSA і ***e*** відкритий ключ,тоді зашифрований текст ***c*** обчислюється з допомогою рівняння:

a) $c = m^{2e} \bmod n$

b) $c = 2m^{e} \bmod n$

c) $c = \sqrt[e]{m} \bmod n$

d) $c = m^{e} \bmod n$

Виберіть одну відповідь:

1. b
2. a
3. c
4. d

Питання **39**

Завершено

Балів 0,50 з 1,00

Яка операція властива кільцям?

a) множення

b) ділення

c) додавання

d) віднімання

Виберіть одну або декілька відповідей:

1. d
2. c
3. a
4. b

Питання **40**

Завершено

Балів 1,00 з 1,00

Що гарантує так званий “ефект лавини”?

a) значення хеш-функції не може давати ніякої інформації про окремі біти інформації,
а лише про повідомлення в цілому.

b) неможливо утворити повідомлення, для якого буде повернено визначене хеш-значення.

c) неможливо знайти два повідомлення для яких буде повернено однакове хеш-значення;

d) можливо створити повідомлення, для якого буде повернено визначене хеш-значення.

Виберіть одну відповідь:

1. c
2. b
3. d
4. a

Питання **41**

Завершено

Балів 1,00 з 1,00

Натуральне число ***l*** називають дискретним логарифмом елемента ***a*** з основою ***b***, якщо

a) $a^l = b$

b) $\sqrt[l]{b} = a$

c) $b^l = a$

d) $b^l = 2$

Виберіть одну відповідь:

1. c
2. b
3. a
4. d

Питання **42**

Завершено

Балів 1,00 з 1,00

Які вимоги накладаються на криптографічну хеш-функцію?

a) Стійкість до обороту
b) Детермінованість
c) Стійкість до колізій
d) Стійкість до підбору аргументу
e) Всі вищезгадані пункти

Виберіть одну відповідь:

1. b
2. c
3. a
4. e
5. d

Питання **43**

Завершено

Балів 1,00 з 1,00

Для чого використовується MAC?

a) Перевірка цілісності повідомлення
b) Автентифікація джерела інформації
c) Адресація вузлів мережі

Виберіть одну або декілька відповідей:

1. b
2. c
3. a

Питання **44**

Завершено

Балів 1,00 з 1,00

Який суттєвий недолік присутній алгоритмам MASH?

a) Слабка стійкість
b) Низька швидкодія і велика кількість використаної пам’яті
c) Складний для імплементації

Виберіть одну відповідь:

1. a
2. b
3. c

Питання **45**

Завершено

Балів 1,00 з 1,00

Яка функція ***f*** називається важкооборотною (односторонньою)?

a) функція, в якій різним значенням аргумента відповідають різні результати, тобто, для двох елементів ***x, y*** з ***Y*** виконується: ***f(x) = f(y)*** тоді й тільки тоді, якщо ***x = y***.

b) ***f*** обчислюється за поліноміальний час.

c) кожен поліноміальний ймовірнісний алгоритм на вході ***y=f(x)*** для випадкового ***x ∈ {0,1}^{n}*** знаходить якийсь із прообразів значення ***y*** із ймовірністю, яка для досить великих ***n*** не перевищує $\frac{1}{n}$

d) ***f*** обчислюється за сталий час.

Виберіть одну або декілька відповідей:

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

Питання **46**

Завершено

Балів 1,00 з 1,00

Алгоритм Діффі-Гелмана забезпечує:

a) Безумовно безпечний обмін повідомленням між абонентами мережі

b) Безпечний обмін повідомленнями між абонентами мережі за умови аутентифікації сторін

c) Електронний цифровий підпис повідомлення

d) Надійне зашифрування повідомленнь

Виберіть одну відповідь:

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

◄ test

Перейти до...