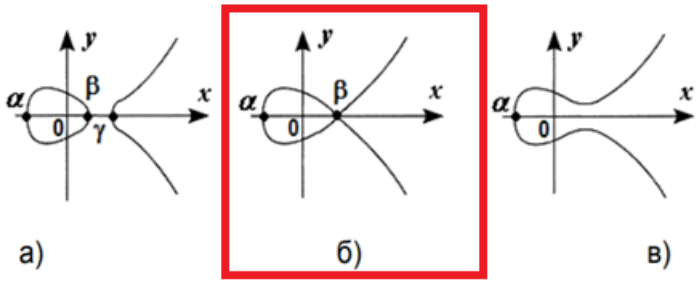
Зміст

Тема 14

1. Яка з еліптичних кривих, поданих на рисунку є сингулярною?



2.Якщо $E_p(a, b)$ – еліптична крива над полем GF(p), характеристика якого $p \neq 2; 3$, то рівнянням Вейєрштрасса цієї кривої є

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

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

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

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

3. У групі точок еліптичної кривої $E_p(a, b)$ над скінченним полем GF(p) груповою операцією є

a) додавання точок

b) інверсія точок

c) множення точок

d) з'єднання точок

4.Що називається порядком групи точок еліптичної кривої $E_p(a, b)$ над полем GF(p)?

a) Кількість точок кривої

b) Число $D = 4a^3 + 27b^2 \mathrm{mod}\ p$

c) Найменше натуральне число n, при якому скалярний добуток $nG = G$, де G – генератор групи

d) Сума a+b

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

a) Визначення точок на кривій, координати яких були б надзвичайно великими числами
b) Пошук на еліптичній кривій точок P(x, y), в яких x > y
c) Дискретне логарифмування на еліптичній кривій
d) Пошук двох точок кривої, які мали б однакові абсциси, а їх ординати відрізнялись знаками

Тема 13

1.Чому криптосистему Ель-Гамаля можна віднести до схеми ймовірнісного шифрування?

a) Через подвоєння довжини шифротексту порівняно з довжиною відкритого тексту
b) Через використання відкритих і секретних ключів
c) Через уведення у процес шифрування рандомізатора
d) Через складність задачі дискретного логарифмування, покладеної в основу криптосистеми

2.Криптографічна стійкість алгоритму Ель-Гамаля базується на складності

a) Обчислення дискретного логарифма
b) Операції піднесення до степення за модулем
c) Факторизації великих чисел
d) Обчислення символу Легжандра

3. (p, g, h) – відкритий ключ, a – секретний ключ криптосистеми Ель-Гамаля, r – рандомізатор, вибраний для зашифруваннявідкритого повідомлення M. Як знайти шифротекст?

a) $(h^r \bmod p, Mg^r \bmod p)$

b) $\boldsymbol{(g^r \bmod p, Mh^r \bmod p)}$

c) $(Mg^r \bmod p, Mh^r \bmod p)$

d) $(g^r \bmod p, M+h^r \bmod p)$

e) $(Mg^{-r} \bmod p, h^r \bmod p)$

f) $(g^a \bmod p, Mh^a \bmod p)$

4. (p, g, h) – відкритий ключ, a – секретний ключ криптосистеми Ель-Гамаля, (C_1, C_2) – отриманий шифротекст, у результаті зашифрування відкритого повідомлення M. Як провести розшифрування?

a) $\boldsymbol{M = C_2 (C_1^a)^{-1} \bmod p}$

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) $M = C_1 C_2^a \ h \bmod p$

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

a) $h = 10$;

b) $\boldsymbol{h = 11}$;

c) $h = 12$;

d) $h = 3$

e) $h = 4$

f) $h = 5$;

Тема 11

1.Криптографічна стійкість алгоритму Діффі-Халлмана базується на складності

a) Обчислення дискретного логарифма

b) Операції піднесення до степення за модулем

c) Факторизації великих чисел

d) Обчислення символу Легпожандра

2. Алгоритм Діффі-Хеллмана 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

3.За протоколом Діффі-Хеллмана розподілу ключів

a) Виробляється ключ симетричного шифру

b) Виробляється ключ асиметричного шифру

c) Використовується електронний цифровий підпис

d) Виробляється рандомізатор

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

a) Захисту від атаки «людина посередині»

b) Захисту від атаки відтворення

c) Для забезпечення аутентифікації учасників протоколу

d) Для передачі один одному

5. Навіщо в протоколі Діффі-Хелмана доцільно передбачати аунтентифікацію абонентів?

a) Без аунтентифікації можливо зламати задачу дискретного логарифмування
b) Без аунтеентифікації можливо зламати задачу факторизації великих чисел
c) Без аунтеентифікації супротивник може замінити своїм ключем відкритий ключ, який той надсилає законному користувачу
d) Завдяки аунтентифікації неможливо провести атаку на основі «парадоксу днів народжень» абонентів

5. 2 Запитанння до теми "Формальне задання криптосистеми.Властивості шифруючих відображень."

1. Згідно з теоремою про обернене відображення f: $X \to Y$ - відображення НЕ буває:

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

2. 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

3. Алгоритм вважається "коректним", якщо:

a) компоненти криптосистеми не породжують похідних систем
b) різним криптосистемам відповідають різні відкриті тексти
c) умова є рівнозначною до принципової можливості дешифрування
d) кожен компонент криптосистеми є нейтральним елементом

4. 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

5. 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

6.2 Запитання до теми "Алгоритм Евкліда. Групи та кільця. Арифметика лишків. Конгруенції."

1. Яка абстрактна операція властива кільцям?

a) множення
b) ділення
c) додавання
d) віднімання

2. Для яких бінарних операцій кілець справджуються дистрибутивні закони?

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

3. Яка з перелічених властивостей не притаманна кільцям?

a) існування протилежного числа

b) біполярність

c) асоціативність

d) комутативність

4. Яка основна відмінність між Афінним шрифтом та шрифтом Цезаря?

a) Використання НСД

b) фіксований ключ

c) кількість відображень для елемента множини

d) використання великої теореми Ферма

5. Яку арифметичну операцію не можна використовувати за розшифрування афінного шрифту, коли числа не є взаємно простими?

a) додавання за модулем

b) віднімання

c) ділення

d) множення

7.2 Запитання до теми “Кільце лишків. Функція Ейлера. Шифр зсуву та лінійний шифр. Афінні шифри.”

1. 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

2. Оберіть основні недоліки афінного шрифту.

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

3. Оберіть захищені типи шифрів.

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

4. Якщо заданий ключ шифрування к=2 і фраза “Падає сніг”, яким буде результат шифрування фрази шрифтом Цезаря?

a) “свєвз упйд”
b) “гінс єадап”
c) “дапєа нсгі”
d) “уамга ісзо”

5. Що є результатом ділення кілець лишків?

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

5. 1 Запитанння до теми “Формальне задання криптосистеми. Властивості шифруючих відображень.”

1. Які коди відносяться до двійкових?
   - **a) МТК - 2**
   - **b) ASCII**
   - **c) код Брайля**
   - **d) код Хаффмана**
2. Ізоморфні групи мають такі властивості:
   - **a) тотожні алгебраїчні**
   - b) тотожні бінарні
   - c) сумарні алгебраїчні
   - d) протилежні алгебраїчні
3. 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**

6.1 Запитання до теми “Алгоритм Евкліда. Групи та кільця. Арифметика лишків. Конгруенції.”

1. Найбільший спільний дільник чисел a = 1634 та b = 252.
   - a) 4
   - b) 8
   - c) 1
   - **d) 2**

2. Доведення коректності шифрування за допомогою алгоритму RSA основане на

a) теоремі Ейлера;

b) теоремі про існування первісних коренів за модулем великого числа;

c) властивостях символу Лежандра;

d) розширеному алгоритмі Евкліда.

3. НСК чисел a = 45 та b = 60

a) 180

b) 60

c) 255

d) 45

4. НСД чисел a = 45 та b = 60 c=5

a) 180

b) 45

c) 5

d) 60

5. 2*3=?

a) 2mod(3)

b) 1mod(7)

c) 1mod(4)

d) 1mod(2)

7. 1 Запитання до теми “Кільце лишків. Функція Ейлера. Шифр зсуву та лінійний шифр. Афінні шифри.”

1. Чому дорівнює значення phi (10)? phi - функція Ейлера

a) 3

b) 4

c) 5

d) 6

2. Скільки розв’язків має конгруенція 26x 49mod 169

a) Один
b) 13
c) Жодного
d) 19

3. Що таке дифузія?

a) Вплив одного знака відкритого ключа на значну кількість знаків шифротекста.
b) Вплив одного знака закритого ключа на значну кількість знаків шифротекста
c) Вплив одного знака відкритого тексту на значну кількість знаків шифротекста.
d) Вплив алгоритму захисту інформації на значну кількість знаків шифротекста.

4. Які з наступних алгоритмів НЕ є симетричними?

a) DES
b) RSA
c) IDEA
d) RC4

5. Результат шифрування слова Test за шифром Цезаря з кроком 5

a) Pitux
b) Yjxy
c) 4545
d) Docd

5 Запитання до теми “Формальне задання криптосистеми. Властивості шифруючих відображень.”

1. Алгоритм вважається “коректним”, якщо:

a) компоненти криптосистеми не породжують похідних систем
b) різним криптосистемам відповідають різні відкриті тексти
c) умова є рівнозначною до принципової можливості дешифрування
d) кожен компонент криптосистеми є нейтральним елементом

2. Групою називається непорожня множина G наділена ..

a) бінарною операцією *

b) бінарною операцією +

c) бінарною операцією /

d) бінарною операцією ^

3. Гомоморфізм, який є бієктивним відображенням, називається:

a) поліморфізмом

b) ізоморфізмом

c) циклічним

d) гомоморфізмом

4. Методом ітерацій суперник може скористатися, коли є :

a) доступ до шифруючого відображення із фіксованим ключем (без знання ключа К "зашитого" в алгоритмі).

b) якщо родина {EK} K ∈ K є підгрупою

c) підслуханий криптотекст C = EK(M).

d) якщо родина {EK} K ∈ K не є підгрупою

5. Ізоморфні групи мають такі властивості:

a) тотожні алгебраїчні

b) тотожні бінарні

c) сумарні алгебраїчні

d) протилежні алгебраїчні

6 Запитання до теми “Алгоритм Евкліда. Групи та кільця. Арифметика лишків. Конгруенції.”

1. Яка основна відмінність між Афінним шрифтом та шрифтом Цезаря?

a) Використання НСД

b) фіксований ключ

c) кількість відображень для елемента множини

2. бінарна операція множення • асоціативна на множині K ,тобто для довільних $a, b, c \in K$ виконується рівність

a) (a*b)*c = a*b*c

b) (a*b)*c = a*(b*c)

c) (a*b)*c =(b*c)/a

d) відповіді А та Б

3. 2*4=?

a) 2 mod 4

b) 2 mod 3

c) 1 mod 8

d) 1 mod 7

4. Непорожня множина K, на якій визначено операції додавання і множення, називається кільцем, якщо виконуються такі умови:

a) Операція множення деасоціативна

b) Операція множення асоціативна.

c) Операція множення дистрибутивна відносно операції додавання.

d) Операція множення дистрибутивна відносно операції віднямма.

НСД(16, 20, 28)=?

a) 2

b) 4

c) 9

d) 3

7 Запитання до теми “Кільце лишків. Функція Ейлера. Шифр зсуву та лінійний шифр. Афінні шифри.”

1. Результатом ділення кілець лишків є?
   a) Теорема Ейлера
   b) Китайська теорема про лишки
   c) Теорема Лагранжа
   d) Перша теорема Коші

2. Якщо a ∈ Z∗n та a і n взаємно прості, то aφ(n) ≡ 1 (mod n), де φ(n) це функція:
   a) Ейлера
   b) Коші
   c) Больцано-Вейєрштрасса
   d) Ферма

3. Ідея лінійного шифру?
   a) утворення закодованих слів шляхом множинного поділу
   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) кожна літера в алфавіті замінюється на свій числовий еквівалент, шифрується за допомогою певної мат. функції та перетворюється назад у букву

4. Ідея шифру зсуву(Шифру Цезаря)

a) в якому кожен символ у відкритому тексті замінюється символом, що знаходяться на деякому постійному числі позицій ліворуч або праворуч нього в алфавіті.

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

c) утворення закодованих слів шляхом множинного поділу

d) Змінюється у довільному порядку зберігаючи послідовність в хеш таблиці

5. Яким буде результат шифрування слова КУТ шифром Цезаря з ключем 2?

a) ЛФУ

b) НФХ

c) МХФ;

d) ХМФ.

8 Важко оборотні функції. Дискретний логарифм

1. Яка функція f називається важко оборотною (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 $x \in \{0,1\}^n$ знаходить якийсь із прообразів значення y із ймовірністю, яка для досить великих n не перевищує $\frac{1}{n}$.

d) f обчислюється за сталий час.

2. Які функції відносяться до односторонніх функцій з секретом?

a) функція Ребіна

b) Множення і факторизація

c) Модульне експоненціювання та дискретне логарифмування

d) криптосистема RSA

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

a) $a^l = b$

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

c) $\boldsymbol{b^l = a}$

d) $b^l = 2$

4. Які методи відносяться до методів розв'язання задачі дискретного логарифмування?

a) Метод Ітерацій

b) Метод Лагранжа

c) Метод Шенкса

d) Метод перебору

5. 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.

9 Поняття криптосистеми з відкритим ключем.RSA: опис, коректність та надійність

1. 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

2. Система шифрування на основі RSA вважається надійною, починаючи з розміру?

a) 256 біт

b) 512 біт

c) 1024 біти

d) 2048 біт

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

a) Ферма

b) Лагранжа

c) Мерсонна

d) Лемана

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

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

b) $c = 2m^e \ mod \ n$

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

d) $c = m^e \ mod \ n$

5. 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}

10 Криптографічні протоколи (обмін ключем, цифровий підпис, аутентифікація,ідентифікація, підкидання монети по телефону).

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

a) Апаратна

b) Парольна

c) Біометрична

d) Багатофакторна

2. 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

3. У якому році компанія Adobe додала можливість вбудовувати цифрові підписи в PDF?

a) 1976

b) 1988

c) 1999

d) 2008

4. 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;

5. 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) в забезпеченні аутентифікації джерела даних і цілісності переданого повідомлення.

c) в 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;

11. Протокол Діффі-Хеллмана

1)Протокол Діффі-Хелмана це

a) Метод обміну криптографічними ключами. Прикладів узгодження ключа, що дозволяє двом або більше учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку.

b) Криптосистема з відкритим ключем, яку засновано на складності обчислення дискретних логарифмів у скінченному полі.

c) Криптосистема з відкритим ключем, яка дозволяє лише двом учасникам, отримати спільний секретний ключ до обчислення дискретних логарифмів у скінченному полі

2) Криптографічна стійкість алгоритму Діффі–Хеллмана заснована на

a) Додатковому шифруванні ключа

b) Складності перехоплення повідомлення

c) Складності вирішення проблеми дискретного логарифмування

3)Який тип атаки з’являється при використанні простого(класичного) алгоритму Діффі–Хеллмана в лінії зв’язку не захищеній від модифікації?

a) Грубої сили

b) Людина по середині

c) На основі підібраного шифротексту

4) Будь-яка кількість учасників може узяти участь в узгоджені ключа в протоколі Діффі-Хеллмана через

a) Атаку на основі підібраного шифротексту

b) Ітеративне виконання протоколу узгодження і обмін проміжними даними

c) Обчислення хеш функції

5) Керол – криптоаналітик. Вона читає листування Боба і Аліси котрі використовують протокол Діффі-Хеллмана, але не може змінити вмісту повідомлень. Якщо Керол знає відкриті прості числа g = 29, p = 47, та відкриті ключі Боба 6 та Аліси 17 чи може Керол знайти секретний ключ s. Якщо так то який він?

a) Так, 16
b) Так, 34
c) Так, 12
d) Ні

6) Для розширення алгоритму Діффі- Хеллмана на більші групи, треба дотримуватись засад:

a) Починаючи з простого ключа секрет утворюється піднесенням поточного значення до приватного показника один раз, в будь-якому порядку
b) Починаючи з простого ключа рсекрет утворюється піднесенням поточного значення до приватного показника двічі, в строго визначеному порядку
c) Будь-яке проміжне значення можна показувати, але кінцеве значення містить спільний секрет і не може бути оприлюднене.
d) Будь-яке проміжне значення не може бути оприлюднине, а кінцеве значення може.

12. Цифровий підпис. Використання криптосистем з відкритим ключем для цифрового підпису.

1)Які криптосистем з відкритим ключем використовуються для цифрового підпису?

a) RSA
b) DSA
c) Ель-Гамаля
d) Всі відповіді вірні

2)Що таке електронний цифровий підпис?

a) Вид підпису отриманий випадковим перетворенням набору електронних даних
b) Вид підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача.
c) Криптосистема з відкритим ключем, яку засновано на складності обчислення дискретних логарифмів у скінченному полі.

3)Для чого використовують електронний цифровий підпис?

a) Для аутентифікації підписувача
b) Для спотвореня перехоплених даних
c) Для підтвердження цілісності даних в електронній формі
d) Для перехоплення даних

4)Як генерується цифровий підпис з використанням RSA без збереження змісту документа в таємниці?

a) Відправник хешує повідомлення, щоб створити дайджест, який шифрує своїм секретним ключем отримуючи цифровий підпис.
b) Одержувач розшифровує підпис відкритим ключем відправника, який попередньо захешований, отримуючи цифровий підпис..
c) Відправник хешує повідомлення, щоб створити дайджест, додає його до повідомлення яке потім шифрує відкритим ключем отримувача.

5) Для того, щоб використання цифрового підпису мало сенс, необхідно виконання умов:

a) Верифікація підпису повинна проводитися відкритим ключем, що відповідним саме тому закритому ключу, який використовувався під час підписання.

b) Без володіння відкритим ключем має бути легко створити законний цифровий підпис.

c) Без володіння закритим ключем має бути обчислювально складно створити законний цифровий підпис.

d) Жодної з перелічених

13. Схема Ель-Гамаля

1) Сем Ель-Гамаля це

a) Метод обміну криптографічними ключами. Прикладів узгодження ключа, що дозволяє двом або більше учасникам, що не мають жодних попередніх даних один про одного, отримати спільний секретний ключ із використанням незахищеного каналу зв'язку.

b) Криптосистема з відкритим ключем, яку засновано на складності обчислення дискретних логарифмів у скінченному полі.

c) Криптосистема з відкритим ключем, яка дозволяє двом та лише двом учасникам, отримати спільний секретний ключ до обчислення дискретних логарифмів у скінченному полі

2)Що включає в себе схема Ель-Гамаля?

a) Алгоритм шифрування

b) Алгоритм цифрового підпису

c) Зашифрований канал передачі

d) Алгоритм Евкліда

3) Криптографічна стійкість схеми Ель-Гамаля базується на

a) Додатковому шифруванні ключа

b) Складності перехоплення повідомлення

c) Складності вирішення проблеми дискретного логарифмування у скінченному полі

4)Як виглядає відкритий ключ в схемі Ель-Гамаля, що працює в режимі шифрування

a) Випадкове просте число, g довжиною p

b) Трійка чисел $(\mathbf{p}, \mathbf{g}, \mathbf{y})$ де $\mathbf{p}$ випадкове просте число, $\mathbf{g}$ примітивний елемент поля $\mathbb{Z}_{\mathbf{p}}$, а $\mathbf{y} = \mathbf{g}^{\mathbf{x}} \bmod \mathbf{p}$, де x випадкове ціле число $\mathbf{1} < \mathbf{x} < \mathbf{p} - \mathbf{1}$

c) Пара чисел (p, g) де p випадкове просте число, а $g = p^x \bmod p$, де x випадкове просте число $1 < x < p - 1$

5) Як виглядає цифровий підпис в схемі Ель-Гамаля, що працює в режимі підпису

a) Випадкове просте число, g довжиною p

b) Трійка чисел (p, g, y) де p випадкове просте число, g примітивний елемент поля $\mathbb{Z}_p$, а $y = g^x \bmod p$, де x випадкове ціле число $1 < x < p - 1$

c) Пара чисел $(\mathbf{r}, \mathbf{s})$ де $\mathbf{s} \equiv (\mathbf{m} - \mathbf{xr})\mathbf{k}^{-\mathbf{1}} \mathbf{mod}\ (\mathbf{p} - \mathbf{1})$, та $\mathbf{r} = \mathbf{g}^{\mathbf{k}} \bmod \mathbf{p}$, де $\mathbf{1} < \mathbf{k} < \mathbf{p} - \mathbf{1}$ та взаємно прості з $\mathbf{p} - \mathbf{1}$, $\mathbf{m} = \mathbf{h}(\mathbf{M})$ – хеш-сума.

14 Поняття криптографічної хеш-функції. Побудова хеш-функції на основі RSA

1. 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.

2. Для чого використовуються хеш-функції при роботі з файловою системою?

a) Стиснення інформації

b) Порівняння даних

c) Перевірка цілісності

3. 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

4. У чому полягає надійність криптосистеми RSA?

a) Складність отримання приватного ключа з публічного

b) Неможливість отримати ключ шифрування

c) Дана система не є надійною

5. 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

6. Який суттєвий недолік присутній алгоритмам MASH?

a) Слабка стійкість

b) Низька швидкодія і велика кількість використаної пам’яті

c) Складний для імплементації

15 Криптографічні алгоритми на основі еліптичних кривих (ECC)

1.У чому полягає основна перевага ECC над RSA?

a) **ECC дозволяє користуватись ключами меншого розміру для отримання необхідного рівня безпеки**
b) ECC алгоритми складніші для розуміння і реалізації
c) ECC не має переваг над RSA

2. Чи є проблемою ріст квантових обчислень для ECC?

a) **Так**
b) Ні

3. Як вирішується проблема генерації всіх точок області кривої?

a) Це не є проблемою
b) Тільки один учасник спілкування генерує всі точки
c) **Користуються заготованими кривими**

4.За рахунок чого забезпечується безпека ECC?

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

16 Проблема достовірності інформації. Контроль незмінності даних з допомоги MAC та MDC. Порівняльний аналіз

1. Що використовується для підтвердження достовірності отриманої інформації в вебі?

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

2. Яке основне використання HMAC?

a) Шифрування повідомлень

b) Перевірка цілісності даних

c) Безпечної передачі даних

3.В чому є основна перевага використання HMAC над MAC?

a) Ніяких, HMAC —попередня версія MAC

b) HMAC обчислюється швидше

c) MAC і HMAC мають різні цілі

4. Які основні вимоги накладаються на алгоритм MAC?

a) Важкооборотність

b) Стійкість до колізій

c) Алгоритмічна складність

d) Ніяких вимог не накладається

5. 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

6. Для чого використовується MAC?

a) Перевірка цілісності повідомлення

b) Автентифікація джерела інформації

c) Адресація вузлів мережі