1. Основні параметри шифру
а) складність апаратної або програмної реалізації;
б) стійкість;
в) довжина ключа;
г) складність перетворення;
д) всі відповіді вірні.

2. Встановлення автентичності сторін є:
а) аутентифікація;
б) ідентифікація;
в) шифрування;
г) атака

д) правильна відповідь відсутня

3. Чи вірний вислів «RSA - криптографічна система відкритого ключа, що забезпечує такі механізми захисту як шифрування і цифровий підпис»
а) так
б) немає

4. Криптографічний алгоритм, в якому ключ, який використовується для шифрування повідомлень, може бути отриманий з ключа дешифрування і навпаки, називають:
а) симетричним;
б) асиметричним;
в) синхронним;
г) асинхронним.
д) правильна відповідь відсутня

5.У більшості симетричних алгоритмів застосовують:
а) 1 ключ;
б) 2 ключа;
в) 3 ключа;
г) 4 ключа.

д) правильна відповідь відсутня

6.Надійність одноключового алгоритму визначається
а) статистичними властивостями ключа;
б) кількістю ключів;
в) обчислювальною складністю реалізації ключа.

г) формою ключа.

д) правильна відповідь відсутня

7.До симетричних схем шифрування відносяться:
а) схема Вернама;
б) RSA;
в) DSA;
г) шифр Ель-Гамаля.

д) правильна відповідь відсутня

8. Найкращими для використання в симетричних схемах шифрування є випадкові ключі, побудовані на основі:
а) шумоподібних послідовностей;
б) генераторів випадкових чисел;
в) перешкодостійких кодів;
г) ефективних кодів.
д) правильна відповідь відсутня

9. В сучасних комп'ютерних алгоритмах блокового шифрування зазвичай довжина блоку становить:
а) 64 біта;
б) 128 біт;
в) 256 біт
г) 512 біт.
д) правильна відповідь відсутня

10.Спроба викликати відхилення і зміни в системі захисту інформації називається::
а) злом;
б) несанкціонований доступ;
в) вторгнення.
г) атака;

д) правильна відповідь відсутня

11. Текст, який потрібно зашифрувати, називається:
а) відкритим;
б) закритим:
в) таємним;
г) секретним.
д) правильна відповідь відсутня

12. Сімейство зворотних перетворень відкритого тексту в шифротекст називається:
а) шифр;
б) ключ;
в) пароль;
г) код

д) правильна відповідь відсутня

13. Нормальне застосування криптографічного перетворення відкритого тексту, в результаті якого утворюється шифротекст, називається:
а) шифрування;
б) дешифрування;
в) кодування;
г) декодування.
д) правильна відповідь відсутня

14. Процес нормального застосування криптографічного алгоритму, підсумком якого буде перетворення шифротекста у відкритий текст, називається:
а) дешифрування;
б) декодування;
в) кодування;
г) шифрування.
д) правильна відповідь відсутня
15. Цілком таємної системою є
а) криптосистема Вернама;
б) криптосистема RSA;
в) криптосистема на еліптичній кривій:
г) блочна криптосистема.
д) правильна відповідь відсутня

16. Сучасна криптографія включає в себе основні напрямки: (перерахуйте їх)
а) Симетричні криптосистеми
б) Криптосистеми з відкритим ключем
в) Системи електронного підпису
г) Управління ключами

д) всі відповіді вірні

17. Криптология розділяється на два напрямки
а) криптографію
б) криптоаналіз
в) шифрування
г) дешифрування

д) а і б

18. Займається пошуком і дослідженням математичних методів перетворення інформації
а) криптографія
б) криптоаналіз
в) шифрування
г) дешифрування
д) правильна відповідь відсутня

19. Дослідження можливості розшифровки інформації без знання ключів
а) криптоаналіз
б) ріптографія
в) дешифрування

г) криптономікон

д) правильна відповідь відсутня

20. Кінцева множина використовуваних для кодування інформації знаків
а) Алфавіт
б) Латиниця
в) Символіка
г) Ні правильної відповіді
д) правильна відповідь відсутня

21. Упорядкований набір з елементів алфавіту
а) Текст
б) Шрифт
в) Стенограма
г) Експлікація
д) правильна відповідь відсутня

22. Інформация, необхідна для шифрування і дешифрування текстів
а) Ключ
б) Знак
в) Контроль
г) Секрет

д) всі відповіді вірні

23. Є кілька показників криптостійкості, серед яких:
а) кількість всіх можливих ключів
б) середній час, необхідний для криптоаналізу
в) кількість одного можливого ключа
г) максимальний час, необхідний для криптоаналізу

д) а і б

24. Існують кілька способів, відповідно до яких можуть класифікуватися криптографічні системи
а) криптосистеми обмеженого використання
б) криптосистеми загального використання
в) криптосистеми з секретним ключем
г) криптосистеми з відкритим ключем
д) всі відповіді вірні

25. Криптографічний система називається криптосистемою - \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, якщо її стійкість грунтується на збереженні в секреті самого характеру алгоритмів шифрування і дешифрування.
а) обмеженого використання
б) загального використання
в) криптосистемою з секретним ключем

г) стабільного

д) правильна відповідь відсутня

26. Прикладом криптографічної системи обмеженого використання можна вважати шифр
а) Юлія Цезаря
б) Октавіана Августа
в) Марка Антонія
г) Марка Цицерона

д) правильна відповідь відсутня

27. Криптографічний система називається криптосистемою \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ якщо її стійкість грунтується не на таємності алгоритмом мов шифрування і дешифрування, а на секретності її ключа
а) загального використання
б) обмеженого використання
в) криптосистемою з секретним ключем
г) стабільного

д) правильна відповідь відсутня

28.Однією з вимог забезпечення стійкості загальної криптографічного системи є
а) величезна кількість можливих ключів
б) невелика кількість можливих ключів
в) два можливих ключа
г) один можливий ключ
д) правильна відповідь відсутня

29. Велика кількість ключів \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ стійкості криптосистеми
а) не забезпечує
б) забезпечує
в) забезпечує, якщо правильно визначений шифр ключа

г) гарантує

д) правильна відповідь відсутня

30. Загальна криптографічний система називається \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ якщо в ній будь-які дві сторони, перед тим, як зв’язатися один з одним, повинні заздалегідь домовитися між собою про використання надалі деякої секретної частини інформації, яка і називається секретним ключем
а) криптосистемою з секретним ключем
б) загального використання
в) обмеженого використання
г) криптосистемою з уявним ключем

д) правильна відповідь відсутня

31. У 1976 році вони запропонували поняття криптографії з відкритим ключем
а) Уітфрід Диффи
б) Мартін Хеллман
в) Рональд Ривест
г) Еді Шамір

д) а і б

32. Перша практична реалізація криптографії з відкритим ключем запропонована
а) Рональдом Ривестом
б) Еді Шамір
в) Леонардом Адлеманом

г) Марком Хеммілом

д) а, б і в

33. Ці терміни відносяться до процесів системи обробки інформації, змістом яких є складання і розподіл ключів між користувачами
а) розподіл ключів
б) управління ключами
в) електронна (цифрова) підпис

г) а і б

д) правильна відповідь відсутня

 34. Система, в якій одному символу відповідають одна або декілька комбінацій двох і більше символів називають
а) багатолітерною системою шифрування
б) багатоцифровою системою шифрування
в) багатознаковою системою шифрування

г) тернарною системою шифрування

д) правильна відповідь відсутня

35. Це здатність протистояти спробам добре озброєного сучасною технікою і знаннями криптоаналітика дешифрувати перехоплений шифротекст, розкрити ключі шифру або порушити цілісність і автентичність відбитку інформації.
а) Стійкість
б) Сила
в) Міцність
г) Сталість
 д) правильна відповідь відсутня

36. Криптосистема шифрування даних RSA заснована на
а) труднощі розкладання великих чисел для генерації відкритого та закритого ключа;
б) труднощі рішення задачі дискретного логарифмування;
в) труднощі генерації великих простих чисел;
г) труднощі пошуку примітивного елемента в циклічній групі.
д) правильна відповідь відсутня

37. При алгоритмі шифрування Ель-Гамаля криптостійкість заснована на:
а) труднощі рішення задачі дискретного логарифмування;
б) труднощі розкладання великих чисел для генерації відкритого та закритого ключа;
в) труднощі генерації великих простих чисел;
г) труднощі пошуку примітивного елемента в циклічній групі.
д) правильна відповідь відсутня

36. Процес застосування зворотного перетворення шифру до відкритого тексту називається зашифрованістю, а результат цього перетворення
а) шіфротекста
б) криптограмою
в) розшифрування
г) дешифрованием
д) а і б

37. Процес зворотного перетворення шифротексту у відкритий текст називається
а) розшифрування
б) дешифрованием
в) кодообозначеніямі
г) археологією

д) правильна відповідь відсутня

38. Якщо генератор, залежить від секретного ключа то він
а) детермінований
б) випадковий
в) лінійний
г) незалежний
д) правильна відповідь відсутня

39. Якщо генератор є секретним ключем, дуже великої довжини, то він
а) випадковий
б) детермінований
в) з самосинхронізацією
г) синхронний
д) правильна відповідь відсутня

40. Вимірює невизначеність повідомлення в числі біт інформації, яка повинна бути відновлена, коли повідомлення було приховано від криптоаналитика в шіфротексті.
а) Ентропія
б) Розлад
в) Ендотропія

г) Оскюморон

д) правильна відповідь відсутня

41. Якщо криптоаналітик не може уточнювати розподіл ймовірностей можливих відкритих текстів за наявним у нього шифротекстом, навіть якщо він володіє всіма необхідними для цього засобами, то криптосистема називається -
а) теоретично стійкою
б) практично стійкою
в) середньостійкі
г) непохитної
д) правильна відповідь відсутня

42. Поле, що складається з кінцевого числа елементів це
а) Кінцеве поле
б) Поле Галуа
в) Нескінченне поле

г) а і б
д) правильна відповідь відсутня

43. Так називається комутативне кільце з одиничним елементом щодо множення в якому кожен не нульовий елемент має зворотний елемент по множенню.
а) Полем
б) Кільцем
в) Кодом
г) Масою
д) правильна відповідь відсутня

44. Функція, яка стискає рядок чисел довільного розміру в рядок чисел фіксованого розміру це
а) хеш-функція
б) хаш-функція
в) зіп-функція

г) нокс-функція
д) правильна відповідь відсутня

45. Шифри заміни ділять на групи:
а) шифри простої заміни
б) шифри складної заміни
в) багатоалфавітної заміни

г) а + б + в
д) правильна відповідь відсутня

46. Потенційна небезпека порушення одного або кількох властивостей системи криптографічного протоколу

а) загроза
б) намір
в) шантаж

г) булінг
д) правильна відповідь відсутня

47. Описує процес шифрування і здійснює залежне від ключа відображення послідовностей блоків тексту (повідомлення) відкритого в послідовності блоків тексту (повідомлення) шифрованого
а) Функція шифрування
б) Функція криптографічна
в) Функція одностороння
г) нокс-функція
д) правильна відповідь відсутня

48. Функція, що описує процес розшифрування і здійснює відображення, зворотне до функції шифрування. Визначається на множині всіх шифрованих текстів (повідомлень) і реалізується алгоритмом розшифрування.
а) Функція розшифрування
б) Функція равновероятности
в) Функція з секретом
г) нокс-функція
д) правильна відповідь відсутня

49. Функція, яка використовується для збільшення аналітичної складності проміжних послідовностей, наприклад, в генераторах фільтруючих і генераторах комбінує шифросистем поточних або реалізована s-блоками в шифросистемах блокових
а) Функція ускладнення
б) Функція фільтруюча
в) Функція равновероятности
 г) Хеш-функція
д) правильна відповідь відсутня

50. Функція-сервіс безпеки, що забезпечує можливість перевірки того, що отримані дані дійсно створені конкретним джерелом. Ця функція не забезпечує захисту від повторного нав'язування або модифікації даних.
а) Функція-сервіс аутентифікації джерела даних
б) Функція-сервіс аутентифікації сторін
в) Функція-сервіс безпеки

г) Хеш-функція
д) правильна відповідь відсутня