**ОСНОВИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

**Модуль 1: Симетричні криптосистеми**

***І. Модель симетричної криптосистеми***

1. **Яка головна характеристика симетричного шифрування?**

A) Використання двох різних ключів

B) Використання одного секретного ключа ✅

C) Відсутність шифрування

D) Використання відкритих ключів

1. **Який з наведених алгоритмів є симетричним?**

A) RSA

B) ECC

C) AES ✅

D) ElGamal

1. **Що є основним недоліком симетричних шифрів?**

A) Використання надто складних алгоритмів

B) Проблема розповсюдження ключів ✅

C) Низька швидкість шифрування

D) Висока складність реалізації

1. **Що є головною перевагою симетричних шифрів?**

A) Захист від квантових атак

B) Висока швидкість ✅

C) Відсутність необхідності ключів

D) Невеликий розмір ключа

1. **Яка особливість симетричної криптосистеми?**

A) Використання одного ключа ✅

B) Використання відкритого та закритого ключа

C) Шифрування тільки файлів

D) Використання цифрового підпису

1. **Який з наведених алгоритмів не є симетричним?**

A) AES

B) DES

C) RSA ✅

D) Twofish

1. **Чому симетричне шифрування швидше за асиметричне?**

A) Використовує коротші ключі

B) Використовує один ключ ✅

C) Використовує хеш-функції

D) Використовує квантові алгоритми

1. **Яка довжина ключа в AES-128?**

A) 64 біти

B) 128 біт ✅

C) 256 біт

D) 512 біт

1. **Як передається ключ у симетричних системах?**

A) Через відкритий канал

B) Через захищений канал ✅

C) Використовуючи цифровий підпис

D) Використовуючи квантову телепортацію

1. **Який із наведених алгоритмів є блочним шифром?**

A) RC4

B) AES ✅

C) OTP

D) MD5

1. **Яке основне призначення симетричних криптосистем?**

A) Підпис документів

B) Захист конфіденційності ✅

C) Аутентифікація користувачів

D) Генерація випадкових чисел

1. **Яка основна проблема симетричних ключів у масштабованих системах?**

A) Складність розподілу ключів ✅

B) Велика швидкість шифрування

C) Відсутність математичних операцій

D) Захист від атак квантових комп’ютерів

1. **Чи можна використовувати один і той самий ключ багаторазово в симетричних шифрах?**

A) Так, це безпечно

B) Ні, це небезпечно ✅

C) Так, але тільки в AES

D) Так, якщо використовувати хешування

1. **Чи захищені симетричні шифри від атак на ключ?**

A) Так, завжди

B) Ні, при витоку ключа ✅

C) Тільки у випадку довгого ключа

D) Так, якщо використовувати цифровий підпис

1. **Що потрібно для шифрування та розшифрування в симетричних шифрах?**

A) Два різних ключі

B) Один і той самий ключ ✅

C) Цифровий сертифікат

D) Квантова передача

1. **Яка основна різниця між симетричним і асиметричним шифруванням?**

A) Використання одного або двох ключів ✅

B) Використання цифрових сертифікатів

C) Використання блокового шифрування

D) Відсутність криптографічних операцій

1. **Як називається процес перетворення відкритого тексту в зашифрований?**

A) Дешифрування

B) Кодування

C) Шифрування ✅

D) Компресія

1. **Що відбувається при зміні одного біта у відкритому тексті при блочному шифруванні?**

A) Весь шифртекст змінюється ✅

B) Шифртекст залишається незмінним

C) Змінюється тільки один біт шифртексту

D) Алгоритм видає помилку

1. **Чому довший ключ у симетричному шифруванні вважається більш безпечним?**

A) Збільшує швидкість обчислень

B) Ускладнює атаку перебором ✅

C) Робить шифр непередбачуваним

D) Зменшує розмір шифртексту

1. **Що таке ініціалізаційний вектор (IV) у симетричних алгоритмах?**

A) Додатковий параметр для уникнення повторів у шифртексті ✅

B) Довжина ключа

C) Метод розподілу ключів

D) Тип асиметричного шифру

1. **Яка головна функція симетричних криптосистем у захисті даних?**

A) Забезпечення конфіденційності ✅

B) Генерація цифрових підписів

C) Захист від підробки даних

D) Доступ до секретних файлів

1. **Який з наведених алгоритмів не є симетричним?**

A) AES

B) DES

C) RSA ✅

D) Twofish

1. **Що таке стійкість симетричного алгоритму?**

A) Неможливість розшифрування без ключа ✅

B) Неможливість швидкого шифрування

C) Використання квантових механізмів

D) Унікальна довжина ключа

1. **Яка операція найчастіше використовується в симетричних шифрах?**

A) XOR ✅

B) Додавання за модулем 10

C) Перетворення в ASCII

D) Ділення на прості числа

1. **Яка основна функція ключа у симетричних системах?**

A) Визначення порядку бітів у шифртексті

B) Визначення зміни кожного біта вихідного тексту ✅

C) Компресія даних

D) Зниження складності алгоритму

1. **Який метод атаки є небезпечним для симетричних шифрів?**

A) Атака відкритого тексту ✅

B) Використання квантових комп’ютерів

C) Використання цифрового підпису

D) Використання випадкових чисел

1. **Чому симетричні шифри не використовуються для цифрового підпису?**

A) Вони не можуть забезпечити перевірку автентичності ✅

B) Вони повільні

C) Вони використовують відкритий ключ

D) Вони мають надто короткий ключ

1. **Який вид криптографічної атаки може розкрити симетричний ключ?**

A) Атака грубою силою ✅

B) Використання великих простих чисел

C) Використання цифрового сертифіката

D) Використання цифрового підпису

1. **Як зберігаються ключі у симетричних системах?**

A) У відкритому доступі

B) У зашифрованому вигляді ✅

C) У відкритому тексті

D) Без будь-якого захисту

***ІІ. Класичні методи шифрування (Шифр Цезаря, Вернама. Квадрат Полібія. Шифр гамування)***

1. **Яка головна слабкість шифру Цезаря?**

A) Великий розмір ключа

B) Простота розшифрування ✅

C) Використання блочного шифрування

D) Використання асиметричних ключів

1. **У чому особливість шифру Вернама?**

A) Він є абсолютно стійким ✅

B) Використовує відкритий ключ

C) Використовує змінний ключ

D) Використовує багаторазові ключі

1. **Який принцип використовує квадрат Полібія?**

A) Використання матриці 4x4

B) Використання координатної системи ✅

C) Використання випадкових перестановок

D) Використання хеш-функцій

1. **Що є головною характеристикою шифру гамування?**

A) Використання блочного шифрування

B) Додавання випадкової послідовності до тексту ✅

C) Компресія даних

D) Використання різних ключів для кожного блоку

1. **Як можна зламати шифр Цезаря?**

A) Використовуючи атаку грубою силою ✅

B) Використовуючи квантові комп’ютери

C) Використовуючи цифровий підпис

D) Використовуючи випадкові числа

1. **Який основний недолік шифру Вернама?**

A) Не забезпечує повну безпеку

B) Потребує використання ключа такої ж довжини, як і повідомлення ✅

C) Використовує один ключ для всіх повідомлень

D) Легко зламується атакою частотного аналізу

1. **Як квадрат Полібія використовує координати для шифрування?**

A) Використовує один набір координат

B) Використовує координати рядка та стовпця ✅

C) Використовує два незалежні шифри

D) Використовує довільну перестановку літер

1. **Яка головна характеристика шифру гамування?**

A) Симетричне блочне шифрування

B) Використання псевдовипадкової послідовності ✅

C) Використання публічного ключа

D) Шифрування на основі перестановки

1. **Який з цих методів є найменш захищеним?**

A) Шифр Вернама

B) Квадрат Полібія

C) Шифр гамування

D) Шифр Цезаря ✅

1. **Чому шифр Вернама не використовується у практиці?**

A) Він недостатньо надійний

B) Потребує довгих ключів, рівних за розміром повідомленню ✅

C) Використовує занадто складні алгоритми

D) Його легко зламати за допомогою комп’ютерних обчислень

1. **Яка модифікація шифру Цезаря дозволяє збільшити стійкість?**

A) Використання кількох ключів

B) Використання випадкових перестановок

C) Використання афінного шифру ✅

D) Використання хеш-функцій

1. **Який підхід у квадраті Полібія допомагає покращити безпеку?**

A) Використання випадкового алфавіту ✅

B) Використання великих блоків

C) Використання багаторівневого шифрування

D) Використання двох таблиць

1. **Який основний недолік квадрата Полібія?**

A) Слабкість перед частотним аналізом ✅

B) Потреба у складних обчисленнях

C) Великий розмір ключа

D) Неможливість шифрування цифр

1. **Як називається процес розшифрування шифру гамування без знання ключа?**

A) Частотний аналіз

B) Відновлення потоку ключа ✅

C) Дешифрування з використанням словника

D) Криптоаналіз за допомогою квантових обчислень

1. **Який із зазначених методів є найстарішим?**

A) Шифр Вернама

B) Шифр Цезаря ✅

C) Шифр гамування

D) Квадрат Полібія

1. **Яке основне обмеження шифру Цезаря?**

A) Використовує випадкові перестановки

B) Може бути зламаний частотним аналізом ✅

C) Використовує відкритий ключ

D) Не можна застосовувати до цифр

1. **Яким способом можна підвищити безпеку шифру Цезаря?**

A) Використання випадкових перестановок ✅

B) Використання квантових алгоритмів

C) Використання довгих ключів

D) Використання додаткових таблиць

1. **Який із класичних шифрів вважається абсолютно стійким?**

A) Шифр Вернама ✅

B) Шифр Цезаря

C) Квадрат Полібія

D) Афінний шифр

1. **Яка головна проблема шифру гамування?**

A) Потрібен довгий ключ, як і текст ✅

B) Не підтримує алфавітні символи

C) Використовує тільки двійкові дані

D) Використовує відкритий ключ

1. **Як працює афінний шифр?**

A) Використовує лінійне перетворення ✅

B) Використовує перестановку літер

C) Використовує випадкові підстановки

D) Використовує двійкове кодування

1. **Яка операція використовується в шифрі гамування?**

A) XOR ✅

B) Додавання

C) Ділення

D) Множення

1. **Чому шифр Вернама не можна використовувати для багаторазового шифрування?**

A) Виникають закономірності у тексті ✅

B) Використовується відкритий ключ

C) Він не підтримує символи кирилиці

D) Потребує дуже коротких ключів

1. **Який шифр є прикладом потокового шифру?**

A) Шифр гамування ✅

B) Шифр Цезаря

C) Квадрат Полібія

D) DES

1. **Як можна зробити шифр гамування безпечнішим?**

A) Використовувати криптографічно стійкий генератор ключів ✅

B) Використовувати один і той самий ключ багато разів

C) Використовувати цифровий підпис

D) Використовувати тільки ASCII-символи

1. **Чому квадрат Полібія є простим для розшифрування?**

A) Він зберігає частотний розподіл літер ✅

B) Використовує двійковий код

C) Використовує квантові алгоритми

D) Використовує одноразовий ключ

1. **Який принцип використовує шифр Цезаря для шифрування?**

A) Зсув літер на фіксовану кількість позицій ✅

B) Використання випадкових перестановок

C) Використання відкритого ключа

D) Використання афінного шифру

1. **Який із шифрів не відноситься до класичних методів шифрування?**

A) DES ✅

B) Шифр Цезаря

C) Квадрат Полібія

D) Шифр Вернама

***ІІІ. Блокові шифри: DES, AES, ДСТУ ГОСТ 28147-2009, ДСТУ 7624:2014 (довжина ключів, довжина блоку вхідного тексту, кількість раундів, крипостійкість, режими роботи згідно з ДСТУ ISO/IEC 10116:2019)***

1. **Яка довжина блоку вхідного тексту для AES?**

A) 32 біти

B) 64 біти

C) 128 біт ✅

D) 256 біт

1. **Скільки раундів має шифр DES?**

A) 8

B) 12

C) 16 ✅

D) 24

1. **Яка головна відмінність між DES і AES?**

A) DES використовує менше раундів

B) AES має більшу довжину ключа ✅

C) DES є асиметричним шифром

D) AES використовує старший алгоритм

1. **Яка довжина ключа використовується в DES?**

A) 64 біти

B) 56 біт ✅

C) 128 біт

D) 256 біт

1. **Яка максимальна довжина ключа в AES?**

A) 128 біт

B) 192 біт

C) 256 біт ✅

D) 512 біт

1. **Яка кількість раундів у шифрі AES-256?**

A) 10

B) 12

C) 14 ✅

D) 16

1. **Який режим роботи блочного шифру не використовує зворотний зв’язок?**

A) CBC

B) ECB ✅

C) CFB

D) OFB

1. **Який основний недолік режиму ECB?**

A) Повільність обчислень

B) Використовує занадто довгі ключі

C) Повторювані блоки шифруються однаково ✅

D) Використовує тільки 64-бітні блоки

1. **Який алгоритм є стандартом шифрування в Україні?**

A) ГОСТ 28147-89

B) ДСТУ 7624:2014 ✅

C) DES

D) RC4

1. **Який з наведених алгоритмів є блочним шифром?**

A) RC4

B) AES ✅

C) OTP

D) MD5

1. **Яка головна характеристика ГОСТ 28147-2009?**

A) Використання 64-бітного блоку ✅

B) Використання 128-бітного блоку

C) Використання симетричних ключів довжиною 512 біт

D) Відсутність S-блоків

1. **Який стандарт прийшов на заміну DES?**

A) ГОСТ 28147-89

B) AES ✅

C) RC4

D) Blowfish

1. **Який алгоритм блочного шифрування підтримує режим XTS?**

A) AES ✅

B) DES

C) RC4

D) ГОСТ 28147-2009

1. **Яка структура використовується в DES?**

A) Сеть Фейстеля ✅

B) Потокова схема

C) Квантова криптографія

D) Гібридна схема

1. **Яка головна відмінність між ГОСТ 28147-89 та AES?**

A) ГОСТ використовує 64-бітний блок, AES – 128-бітний ✅

B) ГОСТ використовує потокове шифрування

C) AES менш стійкий за ГОСТ

D) ГОСТ не використовує S-блоки

1. **Скільки основних режимів роботи блочних шифрів визначено в ДСТУ ISO/IEC 10116:2019?**

A) 3

B) 5 ✅

C) 7

D) 9

1. **Який режим роботи блочних шифрів дозволяє паралельну обробку блоків?**

A) ECB ✅

B) CBC

C) CFB

D) OFB

1. **Яка особливість режиму CBC?**

A) Використовує ініціалізаційний вектор ✅

B) Дозволяє незалежну обробку блоків

C) Використовує асиметричне шифрування

D) Не застосовується у криптографії

1. **Яка довжина ключа використовується в ДСТУ 7624:2014?**

A) 128, 256, 512 біт ✅

B) 64 біти

C) 1024 біти

D) 2048 біт

1. **Який режим роботи шифрування дозволяє потокову обробку даних?**

A) OFB ✅

B) ECB

C) CBC

D) CFB

1. **Яка особливість режиму CFB?**

A) Він працює у потоковому режимі ✅

B) Використовує XOR тільки для шифрування

C) Дозволяє паралельну обробку блоків

D) Використовується лише для збереження хешів

1. **Який механізм використовується для створення ключів у AES?**

A) Ключове розширення ✅

B) Генерація випадкового ключа

C) Логічні операції XOR

D) Використання цифрових підписів

1. **Яка особливість режиму XTS?**

A) Використовується для шифрування дисків ✅

B) Підтримує лише 64-бітні блоки

C) Використовується тільки в асиметричних шифрах

D) Не використовує ініціалізаційний вектор

1. **Чому ГОСТ 28147-89 вважається застарілим?**

A) Використовує малу довжину блоку ✅

B) Не підтримує сучасні режими шифрування

C) Вимагає квантових обчислень

D) Використовує нестійкий алгоритм

1. **Яка структура використовується в AES?**

A) SP-мережа ✅

B) Сеть Фейстеля

C) Симетричний потік

D) Комбінація потокового та блочного шифрування

1. **Яка головна особливість ДСТУ 7624:2014 у порівнянні з AES?**

A) Використовує змінну довжину блоку ✅

B) Використовує тільки 128-бітні ключі

C) Підтримує тільки режим ECB

D) Використовує відкритий ключ для шифрування

1. **Яка криптографічна атака є найбільш небезпечною для DES?**

A) Атака грубою силою ✅

B) Атака з боку відкритого тексту

C) Атака на основі хеш-функцій

D) Атака квантовим алгоритмом Гровера

1. **Що покращує безпеку AES у порівнянні з DES?**

A) Використання більших ключів і більшої кількості раундів ✅

B) Використання підстановочних таблиць (S-блоків)

C) Використання лише 56-бітного ключа

D) Використання блоку 64 біти

***ІV. Потокові шифри. RC4, STRUMOK (довжина ключів, крипостійкість)***

1. **Яка основна характеристика потокових шифрів?**

A) Використання блочного розбиття тексту

B) Шифрування по бітам або байтам ✅

C) Використання двох ключів

D) Обробка даних у великих блоках

1. **Який із наведених алгоритмів є потоковим шифром?**

A) AES

B) DES

C) RC4 ✅

D) ГОСТ 28147-89

1. **Яка максимальна довжина ключа у RC4?**

A) 40 біт

B) 128 біт

C) 256 біт ✅

D) 512 біт

1. **Що є основним компонентом генерації ключового потоку у RC4?**

A) Перестановка масиву байтів ✅

B) Використання таблиці підстановок

C) Рекурсивне шифрування

D) Блочна обробка даних

1. **Який основний недолік RC4?**

A) Велика довжина ключа

B) Вразливість у початкових байтах ключового потоку ✅

C) Повільна швидкість обчислень

D) Використання статичних таблиць

1. **Яка довжина ключа підтримується в STRUMOK?**

A) 128, 256, 512 біт ✅

B) 40 біт

C) 64 біти

D) 2048 біт

1. **Чим STRUMOK відрізняється від RC4?**

A) Використовує більш стійку генерацію ключового потоку ✅

B) Використовує блочну схему

C) Підтримує тільки 128-бітні ключі

D) Використовує фіксовану матрицю підстановок

1. **Яка головна перевага потокових шифрів?**

A) Можливість шифрувати дані потоково без розбиття на блоки ✅

B) Висока криптографічна стійкість для цифрових підписів

C) Використання відкритого ключа

D) Застосування тільки в квантовій криптографії

1. **Яка особливість генерації ключового потоку у STRUMOK?**

A) Використовує ініціалізаційний вектор

B) Використовує нелінійну трансформацію стану ✅

C) Використовує XOR з відкритим текстом

D) Використовує матрицю перестановок

1. **Яка головна особливість потокових шифрів у порівнянні з блочними?**

A) Вони працюють зі змінною довжиною блоку

B) Вони обробляють інформацію побайтово або побітово ✅

C) Вони використовують подвійний ключ

D) Вони не використовують криптографічні алгоритми

1. **Яка головна відмінність між потоковими та блочними шифрами?**

A) Потокові шифри працюють із окремими бітами або байтами ✅

B) Потокові шифри мають фіксований розмір блоку

C) Блочні шифри швидші за потокові

D) Блочні шифри не використовують ключовий потік

1. **Який механізм забезпечує криптостійкість STRUMOK?**

A) Використання нелінійних перетворень ✅

B) Фіксований ключовий потік

C) Відсутність ініціалізаційного вектора

D) Динамічна зміна довжини ключа

1. **Яка основна перевага потокових шифрів для шифрування потокових даних?**

A) Висока швидкість ✅

B) Використання блокової структури

C) Використання подвійного шифрування

D) Використання коротких ключів

1. **Яке призначення ключового потоку у потокових шифрах?**

A) Використовується для обчислення хешів

B) XOR-операція з відкритим текстом ✅

C) Розбиває текст на блоки

D) Генерує випадкові числа для ключа

1. **Який тип атаки найбільш ефективний для зламу RC4?**

A) Аналіз кореляції ключового потоку ✅

B) Атака грубою силою

C) Атака на диференціальне шифрування

D) Квантова атака

1. **Чому використання унікального ініціалізаційного вектора важливе у STRUMOK?**

A) Для уникнення повторення ключового потоку ✅

B) Для збільшення швидкості шифрування

C) Для зменшення довжини ключа

D) Для підвищення швидкості розшифрування

1. **Який алгоритм є стійкішим до атаки на повторення ключового потоку?**

A) STRUMOK ✅

B) RC4

C) DES

D) AES

1. **Як можна підвищити безпеку використання RC4?**

A) Відкидання перших байтів ключового потоку ✅

B) Використання фіксованого ключа

C) Використання коротких ключів

D) Використання асиметричного шифрування

1. **Яка головна перевага STRUMOK у порівнянні з RC4?**

A) Вища стійкість до атак ✅

B) Використання блочного шифрування

C) Менша швидкість шифрування

D) Використання відкритих ключів

1. **Яке середовище найбільш підходить для використання потокових шифрів?**

A) Потокове передавання даних ✅

B) Шифрування великих файлів

C) Статичне збереження даних

D) Використання у цифрових підписах

1. **Чому STRUMOK вважається безпечнішим за RC4?**

A) Має стійкіший генератор ключового потоку ✅

B) Використовує відкритий ключ

C) Працює лише з малими ключами

D) Підтримує тільки статичні ключі

1. **Яка операція є основною для змішування даних у потокових шифрах?**

A) XOR ✅

B) Додавання

C) Перемноження

D) Зсув бітів

1. **Яка атака є загрозливою для потокових шифрів?**

A) Аналіз повторюваних ключових потоків ✅

B) Факторизація великих чисел

C) Використання квантових алгоритмів

D) Використання цифрових сертифікатів

1. **Яка головна вимога до генератора псевдовипадкових чисел у потокових шифрах?**

A) Відсутність закономірностей у вихідних даних ✅

B) Генерація парних чисел

C) Використання фіксованої послідовності

D) Збереження відкритих ключів

1. **Який недолік можуть мати погано реалізовані потокові шифри?**

A) Прогнозованість ключового потоку ✅

B) Використання малих блоків

C) Збільшення розміру зашифрованих даних

D) Використання асиметричних ключів

1. **Чому важливо використовувати унікальний ключ для кожного сеансу у потокових шифрах?**

* A) Щоб уникнути повторення ключового потоку ✅
* B) Щоб підвищити швидкість шифрування
* C) Щоб спростити дешифрування
* D) Щоб використовувати менше пам’яті

1. **Як можна підвищити криптостійкість потокового шифру?**

* A) Використовувати криптографічно стійкий генератор випадкових чисел ✅
* B) Використовувати відкриті ключі
* C) Зменшити довжину ключа
* D) Використовувати один і той самий ключ для всіх сеансів

1. **Яка головна перевага потокових шифрів для мобільних пристроїв?**

* A) Висока швидкість обробки даних ✅
* B) Використання коротких ключів
* C) Захист від квантових атак
* D) Використання блочного кодування

***V. Псевдовипадкові послідовності в криптосистемах***

1. **Що таке псевдовипадкова послідовність?**  
   A) Послідовність, створена випадковим процесом  
   B) Послідовність, яка виглядає випадковою, але генерується за визначеним алгоритмом ✅  
   C) Набір простих чисел  
   D) Рівномірно розподілені значення
2. **Що таке генератор псевдовипадкових чисел (ГПВЧ)?**  
   A) Механізм для стискання даних  
   B) Алгоритм для генерації чисел, які виглядають випадковими ✅  
   C) Шифратор тексту  
   D) Апаратний пристрій для хешування
3. **Чим відрізняються псевдовипадкові числа від істинно випадкових?**  
   A) Вони менш рівномірно розподілені  
   B) Вони генеруються детерміновано ✅  
   C) Вони використовуються лише в шифруванні  
   D) Вони мають простіші значення
4. **Який елемент визначає вихід псевдовипадкового генератора?**  
   A) Швидкість обчислень  
   B) Початкове значення (seed) ✅  
   C) Розмір даних  
   D) Кількість бітів
5. **Чому важливо використовувати якісний seed для ГПВЧ?**  
   A) Це прискорює обчислення  
   B) Це забезпечує непередбачуваність послідовності ✅  
   C) Це зменшує обсяг пам'яті  
   D) Це змінює алфавіт
6. **Де застосовуються псевдовипадкові послідовності у криптосистемах?**  
   A) Для створення графічних інтерфейсів  
   B) Для генерації ключів, сольових значень, nonce ✅  
   C) Для стиснення текстів  
   D) Для підпису електронних документів
7. **Що таке криптографічно стійкий генератор псевдовипадкових чисел (CSPRNG)?**  
   A) Генератор, який може бути легко передбачений  
   B) Генератор, стійкий до криптоаналітичних атак ✅  
   C) Алгоритм для створення хешів  
   D) Апаратний модуль для обміну ключами
8. **Чому важливо використовувати CSPRNG для криптографічних цілей?**  
   A) Він забезпечує випадковість і непередбачуваність ✅  
   B) Він працює швидше  
   C) Він створює коротші ключі  
   D) Він генерує хеш-функції
9. **Який із наведених генераторів є криптографічно стійким?**  
   A) Linear Congruential Generator (LCG)  
   B) Blum Blum Shub ✅  
   C) Mersenne Twister  
   D) Fibonacci Generator
10. **Що таке атака на основі відновлення seed?**  
    A) Атака через брутфорс  
    B) Спроба визначити початкове значення генератора ✅  
    C) Зміна шифру  
    D) Підміна ключа
11. **Який з алгоритмів найчастіше використовується для генерації псевдовипадкових чисел у стандартних додатках (не для криптографії)?**  
    A) Mersenne Twister ✅  
    B) SHA-256  
    C) RSA  
    D) AES
12. **Яка головна властивість криптографічно стійкого генератора?**  
    A) Його важко передбачити ✅  
    B) Він створює прості ключі  
    C) Він використовує великі обсяги пам'яті  
    D) Він генерує короткі послідовності
13. **Що таке період генератора псевдовипадкових чисел?**  
    A) Час роботи генератора  
    B) Кількість значень перед повторенням послідовності ✅  
    C) Розмір блоку пам'яті  
    D) Кількість обчислень
14. **Який період у Mersenne Twister?**  
    A) − 1 ✅  
    B)   
    C)   
    D)
15. **Що може статися, якщо генератор псевдовипадкових чисел передбачуваний?**  
    A) Знижується швидкість шифрування  
    B) Зловмисник може відновити ключ або інші секретні дані ✅  
    C) Збільшується розмір шифртексту  
    D) Алгоритм стає повільнішим
16. **Як можна підвищити криптостійкість генератора?**  
    A) Використовувати хеш-функції для обробки seed ✅  
    B) Зменшити розмір seed  
    C) Зменшити період генератора  
    D) Додати додаткові біти
17. **Що таке атака "predictive attack" на псевдовипадковий генератор?**  
    A) Зловмисник намагається передбачити майбутні значення послідовності ✅  
    B) Зміна ключів  
    C) Атака на інтерфейс програми  
    D) Стирання seed
18. **Яке рішення захищає псевдовипадковий генератор від атак?**  
    A) Використання випадкового seed та хешування ✅  
    B) Зменшення обчислювальної складності  
    C) Стиснення даних  
    D) Використання симетричних алгоритмів
19. **Чому важливо уникати повторного використання seed?**  
    A) Це уповільнює роботу  
    B) Це може призвести до повторення послідовностей ✅  
    C) Це зменшує розмір файлу  
    D) Це змінює алфавіт
20. **Як псевдовипадкові послідовності використовуються у шифруванні потоків?**  
    A) Вони формують ключ потоку ✅  
    B) Виконують хешування  
    C) Стискають дані  
    D) Змінюють структуру пакета
21. **Чому генерація ключів потребує криптостійких генераторів?**  
    A) Щоб запобігти прогнозуванню ключів ✅  
    B) Щоб прискорити обчислення  
    C) Щоб зменшити кількість бітів  
    D) Щоб видалити випадкові біти
22. **Де застосовуються псевдовипадкові послідовності в мережевій безпеці?**  
    A) Для створення сесійних ключів, nonce, IV ✅  
    B) Для шифрування відеофайлів  
    C) Для створення IP-адрес  
    D) Для підпису електронних листів
23. **Що таке nonce у криптографії?**  
    A) Випадкове число, яке використовується один раз ✅  
    B) Вид ключа  
    C) Хеш-функція  
    D) Блок повідомлень
24. **Чому важливо, щоб nonce був унікальним?**  
    A) Щоб уникнути повторного шифрування однаковим ключем ✅  
    B) Щоб зменшити обсяг повідомлень  
    C) Щоб прискорити процес шифрування  
    D) Щоб змінити довжину повідомлення
25. **Яка основна вимога до генератора для криптосистеми?**  
    A) Висока швидкість роботи  
    B) Непередбачуваність вихідних значень ✅  
    C) Мінімальне використання пам'яті  
    D) Простота кодування
26. **Яке правило визначає криптостійкість ГПВЧ?**  
    A) Всі значення мають бути унікальними  
    B) Неможливість відновлення seed з вихідної послідовності ✅  
    C) Кожне третє число повинно бути парним  
    D) Використання тільки простих чисел
27. **Яка властивість відрізняє CSPRNG від звичайного ГПВЧ?**  
    A) Довший період  
    B) Стійкість до криптоаналізу ✅  
    C) Використання простих чисел  
    D) Можливість зміни seed під час генерації
28. **Як забезпечити кращу ентропію у генераторі?**  
    A) Використовувати апаратні джерела випадковості ✅  
    B) Використовувати однакові значення  
    C) Зменшити кількість ітерацій  
    D) Використовувати лише нулі
29. **Яка загальна мета використання псевдовипадкових послідовностей у криптографії?**  
    A) Забезпечення непередбачуваності ключів і процесів ✅  
    B) Зменшення обсягу даних  
    C) Створення хеш-функцій  
    D) Збереження паролів

***VІ. Умови стійкості шифрів***

1. **Що таке стійкість шифру?**  
   A) Його здатність до стиснення даних  
   B) Захищеність шифру від розкриття без знання ключа ✅  
   C) Рівень енергоспоживання  
   D) Здатність генерувати випадкові числа
2. **Що таке криптостійкість?**  
   A) Стійкість шифру до випадкових помилок  
   B) Стійкість шифру до криптоаналітичних атак ✅  
   C) Стійкість до фізичних впливів  
   D) Здатність шифру створювати цифрові підписи
3. **Який головний фактор впливає на стійкість шифру?**  
   A) Довжина ключа ✅  
   B) Кількість користувачів  
   C) Формат повідомлення  
   D) Вибір кольорів інтерфейсу
4. **Що таке атака грубої сили (brute-force)?**  
   A) Атака через соціальну інженерію  
   B) Перебір всіх можливих ключів ✅  
   C) Використання вірусів  
   D) Модифікація пакета даних
5. **Яка умова стійкості шифру до атаки грубої сили?**  
   A) Простий алгоритм шифрування  
   B) Велика кількість можливих ключів ✅  
   C) Наявність бекдору  
   D) Використання простих паролів
6. **Що таке криптоаналітична атака на шифр?**  
   A) Атака на фізичний сервер  
   B) Спроба розкрити шифр без знання ключа ✅  
   C) Викрадення паролів  
   D) Стиснення зашифрованого повідомлення
7. **Що таке стійкість до статистичного аналізу?**  
   A) Здатність шифру приховувати закономірності у даних ✅  
   B) Наявність резервного копіювання  
   C) Захист від DDoS-атак  
   D) Використання складних паролів
8. **Що таке дифузія у шифруванні?**  
   A) Зменшення розміру зашифрованого тексту  
   B) Розсіювання статистичних закономірностей у даних ✅  
   C) Додавання випадкових бітів  
   D) Використання двох ключів
9. **Що таке конфузія у криптографії?**  
   A) Невизначеність у шифруванні  
   B) Ускладнення залежності між ключем та шифртекстом ✅  
   C) Додавання додаткових нулів  
   D) Використання симетричних алгоритмів
10. **Що є найважливішим критерієм оцінки стійкості шифру?**  
    A) Зручність використання  
    B) Складність для криптоаналізу ✅  
    C) Колірна схема інтерфейсу  
    D) Кількість бітів у повідомленні
11. **Що таке атака з відомим відкритим текстом?**  
    A) Атака, де зловмисник знає частину оригінального повідомлення ✅  
    B) Атака на сервер  
    C) Викрадення ключа  
    D) Атака на мережу
12. **Що таке атака з вибраним відкритим текстом?**  
    A) Атака, де зловмисник може вибрати повідомлення для шифрування ✅  
    B) Атака за допомогою троянів  
    C) Перехоплення паролів  
    D) Стирання даних
13. **Що таке атака з вибраним шифртекстом?**  
    A) Атака, де зловмисник може вибрати шифртекст для аналізу ✅  
    B) Дозволяє змінити ключ  
    C) Здійснюється шляхом зміни пароля  
    D) Використовує фішинг
14. **Що таке атака на основі часткових даних?**  
    A) Аналіз відомих частин повідомлення ✅  
    B) Стирання даних  
    C) Викрадення ключа  
    D) Хешування повідомлення
15. **Який вид атаки є найнебезпечнішим для шифрів із коротким ключем?**  
    A) Статистичний аналіз  
    B) Атака грубої сили ✅  
    C) Стиснення даних  
    D) Використання хеш-функцій
16. **Що таке атакa "людина посередині" (Man-in-the-Middle)?**  
    A) Атака через випадковий збій системи  
    B) Перехоплення даних між двома сторонами ✅  
    C) Додавання шкідливого коду  
    D) Захоплення вебсайту
17. **Яка умова забезпечує стійкість до атак "людина посередині"?**  
    A) Двофакторна автентифікація  
    B) Використання цифрових підписів ✅  
    C) Блокування портів  
    D) Встановлення антивірусів
18. **Що таке атака на основі часу (timing attack)?**  
    A) Використання шкідливого ПЗ  
    B) Аналіз часу обробки операцій для визначення ключа ✅  
    C) Затримка сигналу  
    D) Викрадення пароля через кейлогери
19. **Як забезпечити стійкість до атак на основі часу?**  
    A) Використання константного часу обробки ✅  
    B) Додавання паролів  
    C) Перезавантаження серверів  
    D) Використання шкідливих скриптів
20. **Що таке бічні канали в криптографії?**  
    A) Альтернативні маршрути передачі даних  
    B) Непрямі джерела інформації, як-от споживання енергії чи час виконання ✅  
    C) Додаткові сервери  
    D) Підключені зовнішні пристрої
21. **Який шифр вважається стійким за визначенням Кергоффса?**  
    A) Той, який залишається безпечним навіть при відомому алгоритмі ✅  
    B) Шифр, де відомий лише ключ  
    C) Будь-який симетричний шифр  
    D) Шифр з подвійним ключем
22. **Що таке "ідеальний шифр"?**  
    A) Шифр без ключів  
    B) Шифр, який неможливо зламати, навіть маючи необмежені ресурси ✅  
    C) Симетричний шифр з коротким ключем  
    D) Шифр без зворотного дешифрування
23. **Який шифр вважається ідеально стійким?**  
    A) RSA  
    B) Шифр Вернама ✅  
    C) AES  
    D) DES
24. **Що таке лавинний ефект у шифруванні?**  
    A) Несподівана зупинка процесу  
    B) Невелика зміна у відкритому тексті викликає значні зміни у шифртексті ✅  
    C) Стиснення зашифрованого повідомлення  
    D) Втрата даних
25. **Чому важливо уникати коротких ключів у шифрах?**  
    A) Їх легко зламати перебором ✅  
    B) Вони займають більше пам'яті  
    C) Вони уповільнюють роботу системи  
    D) Вони збільшують обсяг шифртексту
26. **Яке значення має ентропія у стійкості шифру?**  
    A) Визначає кількість випадковості в ключі ✅  
    B) Визначає швидкість обчислень  
    C) Визначає розмір файлу  
    D) Залежить від частоти бітів
27. **Що таке криптоаналітична складність?**  
    A) Час, необхідний для злому шифру ✅  
    B) Розмір ключа  
    C) Обсяг повідомлення  
    D) Час створення ключа