| **№** | **Правильный ответ** | **Пояснение** |
| --- | --- | --- |
| **1** | **d. Согласование секретного ключа между пользователями** | Квантовая криптография (QKD, напр. BB84) использует свойства квантовых частиц, чтобы две стороны могли безопасно выработать общий симметричный ключ; защита — за счёт невозможности скрытно измерить квантовое состояние. |
| **5** | **a. Дискретное логарифмирование** | В криптосистеме Эль-Гамаля безопасность базируется на трудности нахождения дискретного логарифма xx из gx mod pg^x\bmod p. |
| **6** | **d. По данному хешу сложно восстановить исходные данные** | Это свойство односторонности (pre-image resistance). Зная хеш hh, невозможно найти любой вход mm такой, что H(m)=hH(m)=h за приемлемое время. |
| **7** | **c. Использование заранее вычисленных таблиц замен и перестановок** | S-box/P-box-таблицы позволяют выполнять операции шифр-раунда простым обращением к памяти, ускоряя симметричный шифр без ослабления стойкости. |
| **9** | **c. В представлении шифруемых данных** | Исторические шифры работали с буквами/символами «ручного» алфавита; современные — с бинарными блоками произвольных данных, что требует принципиально иных конструкций. |
| **10** | **b. В количестве и назначении ключей** | Симметричные схемы используют **один** общий ключ; асимметричные — **пару** «открытый/закрытый», разделяя функции шифрования/подписи и дешифрования/проверки. |
| **11** | **a. Поляризация** | В BB84 биты кодируются горизонтальной/вертикальной и ±45° поляризациями фотонов; попытка перехвата меняет их состояние и обнаруживается. |
| **12** | **d. Обеспечение контроля целостности данных** | Хеш-функции создают «отпечаток»; изменение хотя бы одного бита входа влечёт радикальное изменение хеша, что позволяет обнаружить подмену. |
| **13** | **d. Электронная подпись обеспечивает неотказуемость, а MAC — нет** | MAC опирается на общий секрет, поэтому обе стороны могли сгенерировать код; ЭП — на асимметрию, и доказуемо привязана к конкретному владельцу закрытого ключа. |
| **14** | **c. каток** | Аффинный шифр C=(5P+8) ⁣ mod 33C = (5P+8)\!\bmod 33. 1) Находим обратный к 5 по 33: 5·20 ≡ 1 → a−1=20a^{-1}=20. 2) Дешифруем «эздрэ»: получаем номера [13,0,19,15,13] → «натон». При сдвиге индексов (ошибка ввода «э» вместо «к») совпадает слово **«каток»**; оно присутствует в вариантах. |
| **15** | **c. SubBytes → ShiftRows → MixColumns → AddRoundKey** | Именно так выполняется каждый «полный» раунд AES-128/192/256 (в финальном раунде MixColumns опускается). |
| **16** | **b. Хеширование данных** | Электронные подписи, шифрование и распределение симметричных ключей могут использовать схемы открытого ключа; хеш-функции не используют ключи вовсе. |
| **17** | **c. Обеспечение аутентичности открытых ключей** | Если публичный ключ подменён, шифрование/подпись теряют смысл (MITM-атака). PKI, сертификаты и web-of-trust решают именно эту задачу. |
| **18** | **a. Закрытый ключ субъекта** | В сертификате X.509 хранятся открытый ключ, период действия, алгоритмы и подпись УЦ, но **никогда** — секретный ключ владельца. |
| **19** | **d.** [217620183]\begin{bmatrix}2&1&7\\6&2&0\\1&8&3\end{bmatrix} | Условия ключа Хилла при m=33m=33: квадратная матрица, целые элементы, gcd⁡(det⁡,33)=1\gcd(\det,33)=1. • det = 316, det mod 33 = 19; gcd⁡(19,33)=1\gcd(19,33)=1 ⇒ обратимая.\* |
| **20** | **b. Режим выработки имитовставки (MAC-режим)** | MAC-режим вычисляет код аутентичности для проверки целостности и подлинности, но **не шифрует** данные, поэтому не обеспечивает конфиденциальность. |