Вопросы (протоколы аутентификации и идентификации)

1. Определение криптографического протокола, участники протокола, раунд протокола, шаг протокола. Виды протоколов (различные способы классификации).
2. Функции безопасности: аутентификация сторон, аутентификация источника, разграничение доступа, конфиденциальность, целостность, невозможность отказа.
3. Нарушитель, противник, стойкость протокола. Требования к протоколам (goals). Атаки на протоколы: подмена, повторное навязывание, отражение, человек посередине и др.
4. Протоколы идентификации, многофакторная идентификация. Симметричные и асимметричные протоколы идентификации.
5. Односторонняя идентификация по паролю, использование хэш-функций в парольной аутентификации. „Подсоленные“ пароли. Определение криптографической хэш-функции. Идентификация Лэмпорта. Достоинства и недостатки.
6. Односторонняя идентификация на основе временных меток. Достоинства и недостатки. Назначение nonce. Требования к генератору nonce.
7. Односторонняя идентификация типа запрос-ответ: на основе симметричного шифрования. Достоинства и недостатки. Односторонняя идентификация типа запрос-ответ: на основе асимметричного шифрования. Достоинства и недостатки.
8. Односторонняя идентификация типа запрос-ответ: на основе ЭЦП. Достоинства и недостатки. Протокол односторонней аутентификации с привязкой к сессии.
9. Двусторонняя аутентификация. Объяснить, почему нельзя симметрично использовать два протокола односторонней аутентификации: привести пример атаки. Протокол Нидхема-Шредера. Атака типа „человек посередине“ на этот протокол.
10. Протокол подбрасывания монеты по телефону. Требования к протоколу, реализация. Протокол вручения обязательства (bit commitment, BC), стадия вручения, стадия раскрытия. Требования привязки (binding) и маскировки (hiding).
11. Дать определение теоретико-информационной и вычислительной стойкости для требований привязки и маскировки. Протокол BC на основе криптографической хэш-функции, объяснить его стойкость (для привязки и для маскировки).
12. Протокол BC Педерсена (схема COMMIT_1), объяснить его стойкость (для привязки и для маскировки). Протокол BC типа Эль-Гамаля COMMIT_2, объяснить его стойкость (для привязки и для маскировки).

13. Доказать, что не существует протокола ВС, который был бы стойким в теоретико-информационном смысле как для требования привязки, так и для требования маскировки.

14. Протоколы идентификации с нулевым разглашением. Определение. Протокол Шнорра. Доказать, что противник, не знающий секретного ключа, не сможет подменить легальную доказывающую сторону.

15. Доказать, что протокол Шнорра — это протокол с нулевым разглашением (рассмотреть случай, когда проверяющая сторона не мошенничает).

16. Протокол идентификации Гиллу-Кискате. Доказать, что противник, не знающий секретного ключа, не сможет подменить легальную доказывающую сторону.

17. Доказать, что этот протокол является протоколом с нулевым разглашением (рассмотреть случай, когда проверяющая сторона не мошенничает).

18. Протокол Окамото. В чем преимущества этого протокола перед протоколом Шнорра и протоколом Гиллу-Кискате?

19. Протокол идентификации Штерна (Стерна). Протокол идентификации Жиро (Girault M.).

20. Двусторонние протоколы распределения ключей.

Вопросы (протоколы распределения ключей)

1. Классификация протолов распределения ключей. Их принципиальные отличия, области применения. Понятия forward/backward-безопасности.

2. Двусторонние протоколы передачи ключей (без третьей доверенной стороны). Примеры на основе симметричного шифрования, на основе асимметричного шифрования, на основе криптографической хэш-функции.

3. Протокол Нидхема-Шредера. Анализ forward/backward-безопасности протокола.

4. Протокол Керберос. Анализ forward/backward-безопасности протокола.

5. Протокол Отвея-Рииса. Анализ forward/backward-безопасности протокола.

6. Распределение ключей с помою центров сертификации. Достоинства, недостатки. Цепь доверия. forward/backward-безопасность таких протоколов.

7. Схема протокола SSL. Почему вместо HMAC не используют цифровую подпись?

8. Алгоритмы проверки целостности сообщений MAC: на основе хэш-функций, на основе блоковых шифров, HMAC. В каком случае используются MAC? В каком случае используются цифровые подписи?

9. Трехпроходной протокол Шамира. Пример слабой и сильной реализации протокола.
10. Схемы одновременного обеспечения целостности и конфиденциальности ключей (3 основных типа). Обоснование стойкости протокола HMAC.
11. Зафиксированный (fixed), эфемерный (ephemenral), анонимный (anonymous) протокол Диффи-Хэллмана.
12. Предварительное распределение ключей. Схема Блома. В чем отличие от генерации ключей?

Вопросы (схемы разделения секрета и многосторонние вычисления)

1. Схема разделения секрета (СРС), участники протокола, протокол разделения секрета, протокол восстановления секрета.
2. Определение правомочной коалиции (восстанавливающее множество), структуры противника, структуры доступа. Совершенные СРС, идеальные СРС, пороговые СРС.
3. Чем разбиение секрета отличает от разделения секрета?
4. СРС Шамира. Докажите, что СРС Шамира - совершенная.
5. Реплицированная СРС.
6. Схема визуальной криптографии Наора-Шамира.
7. Определение протокола многостороннего вычисления функции. Протокол защищенного голосования (сумма секретных аргументов).
8. Протокол защищенного установления соответствия (произведение аргументов из множества $\{0,1\}$).
9. Протокол многостороннего вычисления арифметического выражения (схема).