Петров Глеб 590-1 Коллоквиум 1
Билет 7
Опишите способ подписи документа на основе криптографии с открытыми ключами.
В чем заключается тест Казисского?
Определите понятие абсолютной нормы языка.

Вопрос №1 – “Опишите способ подписи документа на основе криптографии с открытыми ключами.”

Подписание документа с использованием криптографии с открытыми ключами осуществляется с помощью цифровой подписи. Вот общий способ такой подписи:

1. Генерация ключей:
- Открытый ключ (Public Key): Этот ключ распространяется открыто и используется для проверки подписи. Он связан с конкретным пользователем или организацией.
- Закрытый ключ (Private Key): Этот ключ хранится в секрете и используется для создания подписи. Только владелец закрытого ключа может создать подпись, которую можно проверить с использованием соответствующего открытого ключа.

2. Хэширование документа:
- Создайте хеш (криптографическую сумму) документа с использованием хеш-функции (например, SHA-256). Это создаст фиксированный размер хеш-значения, уникальное для каждого уникального входного документа.

3. Подписание документа:
- Владелец закрытого ключа использует свой закрытый ключ для создания электронной подписи для хеш-значения документа. Это обычно делается с использованием алгоритма ЭЦП (электронной цифровой подписи).

4. Добавление подписи к документу:
- Полученная подпись добавляется к документу. Теперь у вас есть оригинальный документ и соответствующая ему цифровая подпись.

5. Проверка подписи:
- Кто угодно, имеющий доступ к открытому ключу подписанта, может проверить подлинность документа. Для этого:
  - Получатель извлекает хеш-значение из подписанного документа.
  - Получатель использует открытый ключ подписанта для проверки подписи. Если подпись действительна, это доказывает, что документ не был изменен после его подписания.

Преимущества использования цифровой подписи с открытыми ключами включают стойкость к подделке, возможность проверки подписи без раскрытия закрытого ключа и возможность однозначной идентификации подписанта.

Важно обеспечить безопасное хранение закрытого ключа, так как доступ к нему предоставляет полномочия на создание подписей от имени владельца.

Вопрос №2 – «В чем заключается тест Казисского?»

Тест Казисского (Cassis test) является методом атаки на криптографические системы с открытым ключом, основанный на слабостях алгоритмов шифрования. Этот тест был предложен в 1976 году бельгийским математиком и криптографом Анри Гильдасом Казиссом (Henri Gilbert Cassiers). Он описывает метод атаки, который использует комбинаторные методы для поиска секретного ключа, используемого в криптосистемах с открытым ключом.

Процесс атаки может быть кратко описан следующим образом:

1. Предположение о структуре ключа:
   - Атакующий предполагает определенную структуру секретного ключа. Например, предположим, что ключ состоит из нескольких частей.

2. Создание шифрованных текстов:
   - Атакующий выбирает различные открытые тексты и шифрует их, используя открытый ключ, чтобы получить соответствующие шифротексты.

3. Анализ шифротекстов:
   - Атакующий анализирует шифротексты, пытаясь выявить закономерности и зависимости между различными частями шифротекстов.

4. Поиск секретного ключа:
   - На основе анализа атакующий пытается выявить закономерности, которые могут помочь в поиске секретного ключа.

5. Тестирование секретного ключа:
   - После нахождения предполагаемого секретного ключа, атакующий проверяет его, шифруя произвольный открытый текст и сравнивая полученный шифротекст с фактическим.

6. Итерации:

- Если найденный ключ не является правильным, атакующий может изменить предположения о структуре ключа и повторить процесс.

Тест Казисского подчеркивает важность использования криптографических алгоритмов с открытым ключом, устойчивых к подобным атакам. Например, алгоритмы, основанные на задачах, которые считаются вычислительно сложными, таким как факторизация больших чисел (RSA), или решение задачи дискретного логарифма (как в DSA и Diffie-Hellman), могут предоставлять более стойкую защиту от таких методов атак.

Вопрос №3 – «Определите понятие абсолютной нормы языка.»

Абсолютная норма языка равна максимальному количеству битов, которое может быть передано каждым символом при условии, что все последовательности символов равновероятны. Если в языке L символов, то абсолютная норма равна: $R = log_2 L$

Это максимум энтропии отдельных символов. Для английского языка с 26 буквами абсолютная норма равна $Log_2 26$, или около 4,7 бит/буква. Следует отметить, что действительная норма английского языка намного меньше, чем абсолютная, так как естественные языки обладают высокой избыточностью.