Коллоквиум 2

Петров Глеб 590-1

Билет 7
Приведите описание алгоритма с открытым ключом RSA.
Каково назначение комплекса криптоалгоритмов PGP?
Опишите понятие “червя”.

Вопрос №1 – «Приведите описание алгоритма с открытым ключом RSA»

RSA (Rivest–Shamir–Adleman) — криптографический алгоритм, использующий открытый и закрытый ключи. Вот шаги алгоритма RSA:

1. Генерация ключей:
- Выбор двух простых чисел p и q
- Вычисление их произведения $n = p \times q$.
- Вычисление функции Эйлера от n: $\varphi(n) = (p-1) \times (q-1)$
- Выбор открытой экспоненты e, которая является взаимно простой с $\varphi(n)$ (чаще всего выбирается простое число, например, 65537).
- Вычисление закрытой экспоненты d, такой, что $d \times e = 1 \ (mod\ \varphi(n))$.

В результате генерируются открытый ключ (n, e) и закрытый ключ d. Открытый ключ распространяется, а закрытый ключ хранится в секрете.

2. Шифрование:
- Любой может использовать открытый ключ (n, e) для шифрования сообщения M.
- Шифротекст C вычисляется по формуле: $C = M^e \ (mod\ n)$

3. Дешифрование:
- Только владелец закрытого ключа может дешифровать шифротекст C и восстановить исходное сообщение M.
- Дешифрование выполняется по формуле: $M = C^d \ (mod\ n)$.

Алгоритм RSA основан на трудности решения задач факторизации больших чисел. Без знания секретного ключа, раскладывание произведения двух больших простых чисел на множители является сложной задачей, даже при наличии открытого ключа и шифротекста.

RSA широко используется для шифрования данных в сети, подписи цифровых документов, аутентификации и других криптографических приложений. Однако, в последнее время, с развитием квантовых

компьютеров, появляются методы, которые могут подвергнуть риску безопасность RSA.

Вопрос №2 – «Каково назначение комплекса криптоалгоритмов PGP?»

PGP (Pretty Good Privacy) представляет собой комплекс криптографических алгоритмов, который используется для обеспечения конфиденциальности, аутентификации и целостности данных. Ниже перечислены основные цели и назначение PGP:

1. Конфиденциальность данных:
   - PGP используется для шифрования данных, чтобы обеспечить их конфиденциальность. Он применяется для защиты текстовых сообщений, файлов и других данных от несанкционированного доступа.

2. Аутентификация:
   - PGP поддерживает механизмы аутентификации, который позволяет убедиться в том, что отправитель данных действительно тот, за кого он себя выдает. Это достигается с использованием цифровых подписей.

3. Цифровые подписи:
   - PGP использует цифровые подписи для подтверждения подлинности отправителя и целостности данных. Отправитель подписывает данные своим закрытым ключом, и получатель может проверить подпись с использованием открытого ключа отправителя.

4. Жизненный цикл ключей:
   - PGP обеспечивает инфраструктуру для управления ключами, включая их генерацию, распределение, хранение, отзыв и обновление. Это важно для обеспечения безопасного использования криптографии с открытыми ключами.

5. Комплексный набор алгоритмов:
   - PGP включает в себя различные алгоритмы, такие как алгоритмы шифрования (например, IDEA, CAST5, AES), алгоритмы хэширования (например, SHA-256), алгоритмы создания цифровых подписей (например, DSA, RSA). Это обеспечивает гибкость и адаптивность к изменяющимся требованиям безопасности.

6. Безопасный обмен ключами:
   - PGP позволяет пользователям безопасно обмениваться открытыми ключами для установления защищенного канала связи. Это особенно важно в контексте электронной почты, где PGP широко применяется для шифрования и подписи сообщений.

PGP является одним из наиболее широко используемых инструментов для обеспечения конфиденциальности и цифровой подписи данных в различных областях, таких как электронная почта и файловый обмен.

Вопрос №3 – «Опишите понятие “червя”»

В информационной безопасности и компьютерной терминологии "червь" (worm) обозначает вредоносный программный код, который способен самостоятельно распространяться по компьютерным сетям, системам или устройствам. В отличие от вирусов, черви не требуют хост-файла или программы-носителя для передачи с машины на машину. Они могут самостоятельно копировать и запускаться на новых хостах без человеческого вмешательства.

Основные характеристики червей включают:

1. Способность саморепликации: Червь содержит механизмы автономной репликации, который позволяет ему распространяться от системы к системе без вмешательства пользователя.

2. Использование сетевых уязвимостей: Черви часто используют известные уязвимости в сетевых протоколах, службах или приложениях для вторжения в новые системы.

3. Способность самозапуска: Черви могут активироваться и запускаться на целевых системах без дополнительного воздействия.

4. Разнообразие воздействия: Целью червей может быть не только самораспространение, но и выполнение различных вредоносных действий, таких как уничтожение данных, украденных конфиденциальных данных, установка задней двери и так далее.

5. Способность изменять свой код: Некоторые черви обладают способностью изменять свой код или варьировать методы вторжения, что делает их более сложными для обнаружения и устранения.

Черви могут причинить значительный ущерб сетевым инфраструктурам, поскольку они способны многократно копировать себя и распространяться с высокой скоростью. Для защиты от червей важны регулярные обновления программного обеспечения, устранение известных уязвимостей, использование антивирусного программного обеспечения и сетевых механизмов безопасности, а также осмотрительность пользователей при работе с вложенными файлами или ссылками в сети.