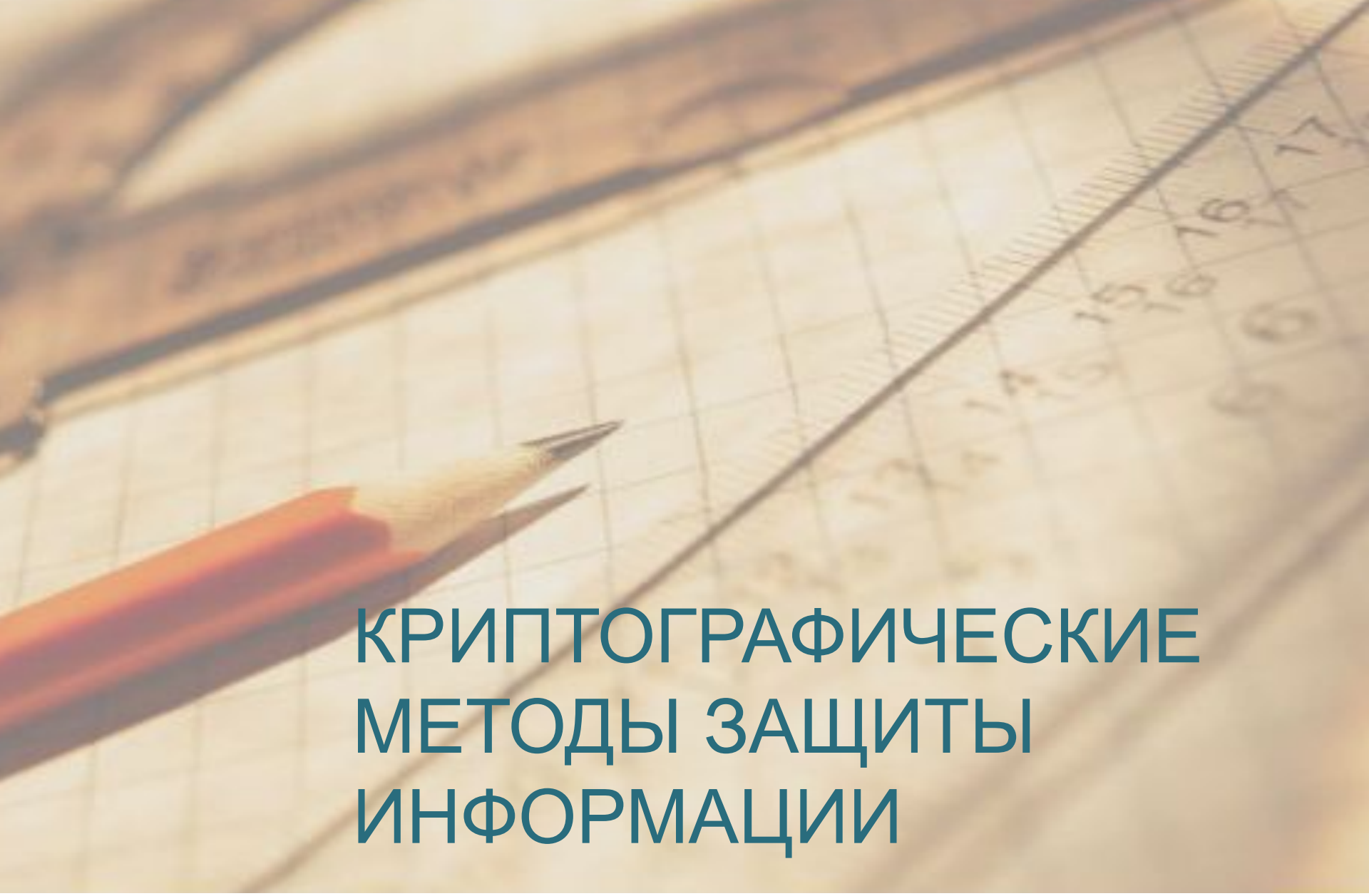

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Лектор - Хорев Павел Борисович
Бакалавры 8 семестр

Литература

1. Хорев П.Б. Криптографические протоколы.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си.
3. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости.

Литература

4. Хорев П.Б. Практикум по криптографическим методам защиты информации.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях.
6. Столлингс В. Основы защиты сетей. Приложения и стандарты.

Лекция 1. Введение и основные понятия

1. Основные понятия современной криптографии.
2. Понятие и классификация криптографических протоколов.
3. Атаки на криптографические протоколы и методы их анализа.

Основы криптографической защиты информационных ресурсов

- К открытому тексту применяется функция шифрования, в результате чего получается шифротекст (или криптограмма).
- Для восстановления открытого текста из шифротекста к последнему применяется функция расшифрования.

Шифрование и расшифрование

Функции шифрования (E) и расшифрования (D) используют один или более дополнительных параметров, называемых ключом:

$$E_k$$

P (открытый текст)--> C (шифротекст)

$$D_{k'}$$

C (шифротекст) --> P (открытый текст)

$$C=E_k(P);\ P=D_{k'}(C)$$

Виды криптографических систем

- Если ключ шифрования K совпадает с ключом расшифрования K′, то такую криптосистему называют симметричной; если для шифрования и расшифрования используются разные ключи, то такую систему называют асимметричной.
- В симметричной криптосистеме ключ должен быть секретным; в асимметричной системе один из ключей может быть открытым.

Виды криптографических ключей

- Ключ симметричного шифрования обычно называют сеансовым (session key).
- Пару ключей асимметричного шифрования образуют открытый ключ (public key) и личный (или закрытый) ключ (secret key, private key).

Применение криптографических методов защиты информации

- Обеспечение конфиденциальности информации, передаваемой по открытым линиям связи или хранящейся на открытых носителях информации.
- Аутентификация, обеспечение целостности и неоспоримости передаваемой информации.
- Защита информационных ресурсов от несанкционированного использования.

Современные симметричные криптографические системы

- AES
- DES, 3-DES, DESX
- ГОСТ 28147-89 («Магма»)
- ГОСТ Р 34.12-2015 («Кузнечик»)
- RC2, RC4, RC5, RC6
- IDEA, CAST, Blowfish

Различаются типом (блочные или потоковые), длиной ключа и количеством раундов в функции шифрования блока.

Принципы построения асимметричных криптосистем

Используются так называемые однонаправленные функции:

- Простое вычисление прямой функции $f(x)$.
- Существование обратной функции $f^{-1}(x)$.
- Сложное вычисление обратной функции без знания специальной информации («обходного пути»).

Механизм электронной подписи (ЭП) обеспечивает защиту документов от

- Посылки их от лица других абонентов («маскарада»).
- Отказа отправителя от авторства («ренегатства»).
- Подмены получателем содержимого документа.
- Изменения содержимого третьим лицом при передаче (хранении) документа («активного перехвата»).
- Повторной передачи документа.

Получение и проверка ЭП

1. Вычисление образа (хеш-значения) подписываемого документа.
2. Его шифрование асимметричным алгоритмом с помощью личного ключа автора

1. Вычисление образа для проверяемого документа.
2. Расшифрование полученной ЭП под ним асимметричным алгоритмом с помощью открытого ключа автора.
3. Сравнение вычисленного и расшифрованного образов проверяемого

Современные асимметричные криптосистемы

- RSA (основана на сложности задачи факторизации больших целых чисел).
- Диффи-Хеллмана (основана на сложности задачи дискретного логарифмирования).
- Эль-Гамаля (модификация системы Диффи-Хеллмана).
- Эллиптические кривые (основана на сложности задачи нахождения одной из двух точек эллиптической кривой, по которым была получена третья точка).

Аутентификация открытых ключей

- Подлинность открытых ключей (подтверждение связи между конкретным субъектом и его открытым ключом) обеспечивается выпуском сертификатов открытых ключей, заверяемых электронной подписью доверенного посредника (удостоверяющего центра, центра сертификации).

Понятие криптографической функции хеширования

- Односторонняя функция
- Для любого документа M длина его хеш-значения H(M) постоянна.
- Минимальная вероятность коллизий
- Сложность нахождения другого документа с тем же хеш-значением.

$$\neg\exists H^{-1} H^{-1}(H(M)) = M$$

$$p(H(M') = H(M) \mid M' \neq M) \leq p_{\max}$$

Применение функций хеширования

- Хранение образов паролей пользователей компьютерных систем в регистрационных базах данных.
- Генерация сеансовых ключей, одноразовых паролей и откликов на случайные запросы службы аутентификации.
- Обеспечение целостности электронных документов (конструкция HMAC, Hash-based Message Authentication Code).
- В механизме ЭП.

Современные функции хеширования

- MD2, MD4, MD5, MD6
- SHA
- ГОСТ Р 34.11-2012
- RIPEMD

Различаются длиной получаемого хеш-значения и сложностью алгоритма хеширования.

Ограничения криптографических методов защиты информации

- Проблема генерации «невырожденных» ключей, их надежного хранения и распространения.
- Не скрывается факт существования защищаемого информационного ресурса (обеспечивается невозможность его использования без знания ключа или «вскрытия» шифра)

Понятие протокола

- ***Алгоритм*** – конечная последовательность однозначно определенных действий, которые необходимо выполнить для получения результата. Алгоритм выполняется некоторым субъектом (вычислителем).
- ***Протокол*** – конечная совокупность однозначно определенных действий, выполняемых в заданной последовательности двумя или более субъектами с целью достижения

Характеристики протокола

- Результативность.
- Конечность.
- Известность протокола его участникам.
- Согласие участников следовать протоколу.
- Непротиворечивость (отсутствие возможности его недопонимания участниками)
- Полнота (каждой возможной ситуации при выполнении протокола должно соответствовать определенное действие).

Криптографические протоколы

Криптографические протоколы – протоколы, в которых используются криптографические алгоритмы. Их целью может быть не только обеспечение конфиденциальности и целостности, но и желание подписать одновременно какой-либо контракт, провести электронную жеребьевку, идентифицировать участников телеконференции и т.п. Их применение в компьютерных сетях обусловлено использованием различных механизмов межсетевого взаимодействия на сетевом и

Цели использования криптографических протоколов

- Предотвращение или обнаружение нарушений (мошенничества или вредительства) в условиях возможного взаимного недоверия участников протокола.
- Невозможность для участников узнать или сделать больше, чем определено в протоколе.

Классификация криптографических протоколов

- Протоколы с посредником.
- Протоколы с арбитражем (судейством).
- Самоутверждающиеся (самодостаточные) протоколы.

Протоколы с посредником

Посредник – незаинтересованная третья (при двух основных участниках) сторона, которой доверено завершение протокола. Незаинтересованность означает отсутствие интереса к определенному результату выполнения протокола или склонности к одному из его участников. Доверие означает принятие всеми участниками протокола каждого действия посредника, согласие с истинностью его решений и уверенность в выполнении им своей части протокола.

Недостатки протоколов с посредником

- Посредник может не пользоваться у других участников безусловным доверием.
- Необходимость оплаты услуг посредника.
- Увеличение времени реализации протокола.
- Поскольку посредник контролирует каждый шаг протокола, его участие может стать узким местом при его реализации. Увеличение числа посредников приведет к росту накладных расходов на реализацию протокола.
- Т.к. все участники должны пользоваться услугами посредника, он будет

Протоколы с арбитражем

Состоят из двух частей:

- Протокола без посредника, используемого при желании участников выполнить протокол.
- Протокола с посредником (арбитром или судьей), приглашаемым в исключительных ситуациях (при наличии разногласий между участниками).

Особенности арбитров

В отличие от обычного посредника арбитр (судья) не принимает непосредственного участия в каждой отдельной реализации протокола, а приглашается участниками только для проверки честности его выполнения всеми сторонами.

Самоутверждающиеся протоколы

- Не требуют присутствия посредника для завершения каждого шага протокола и не предусматривают наличия судьи для разрешения конфликтных ситуаций.
- Если один из участников мошенничает, другие смогут моментально распознать его нечестность и прекратить выполнение дальнейших шагов протокола.
- На практике в каждом конкретном случае приходится конструировать свой специальный самоутверждающийся протокол.

Атаки на криптографические протоколы

- Атаки на криптографические алгоритмы, которые используются в протоколе.
- Атаки на криптографические средства, применяемые для реализации алгоритмов.
- Атаки на сами протоколы.

Атаки непосредственно на криптографические протоколы

1. *Пассивная атака* (посторонний пытается перехватить информацию, которой обмениваются участники). Атакующий при этом может только накапливать данные и наблюдать за ходом событий, но не в состоянии влиять на него. Пассивная атака подобна криптоанализу на основе знания только шифротекста. Поскольку участники протокола не обладают надежными средствами обнаружения пассивной атаки, для защиты от нее используются протоколы, дающие возможность предотвращать возможные неблагоприятные последствия пассивной атаки.

Атаки непосредственно на криптографические протоколы

2. *Активная атака* (атакующий может попытаться внести изменения в протокол ради собственной выгоды). Нарушитель может выдать себя за участника протокола, внести изменения в сообщения, которыми обмениваются участники протокола, подменить информацию, которая хранится в компьютере и используется участниками протокола для принятия решений.

Защита от атак на протоколы

- Защита протокола от активных действий нескольких нарушителей представляет собой весьма нетривиальную проблему. Тем не менее при некоторых условиях эту задачу удается решить, предоставив участникам протокола возможность вовремя распознать признаки активного мошенничества.
- Защиту от пассивных атак должен предоставлять любой протокол.

Внутренние и внешние атаки на протоколы

Внутренний нарушитель – лицо, имеющее легальные полномочия внутри организации, подвергающейся атаке с его стороны, или участник протокола, пытающийся нанести определенный ущерб другим его участникам. Внутренний и внешний нарушители могут быть активными или пассивными.

- Атака с привлечением внутреннего нарушителя называется ***внутренней атакой***.
- Атака, в которой участвуют только внешние нарушители, называется ***внешней атакой***.

Наиболее опасные атаки

Возможен такой вид атак, когда внешние и внутренние нарушители объединяются, что создает наиболее серьезные угрозы безопасной эксплуатации криптосистем. Если нарушитель находится среди разработчиков, то возможны атаки на основе встроенных потайных ходов в алгоритмах формирования ключевых параметров и трудно обнаруживаемых вредоносных программных закладок.

Понятие безопасного криптографического протокола

Под ***безопасным*** будем понимать такой ***криптографический протокол***, в котором его участники достигают своей цели, а нарушители – нет.

Формальные методы анализа криптографических протоколов

- *Моделирование и проверка работы протокола*. Могут использоваться специализированные языки и инструментальные средства.
- *Создание экспертных систем*, которые могут применяться для апробирования различных сценариев выполнения протоколов.
- *Моделирование требований к семейству криптографических протоколов*. Можно использовать специальную логику, разработанную для анализа таких свойств