**Задание на самостоятельную (контрольную) работу по предмету «Криптографические технологии» для ДО**

**2017/2018 учебный год**

Рекомендуется следующая структура контрольной работы:

Титульный лист

Теоретический вопрос:

Задание 1

Задание 2

Список источников

При выполнении контрольной работы необходимо САМОСТОЯТЕЛЬНО рассмотреть теоретический вопрос, показав тем самым знание и понимание материала дисциплины. Изложение вопросов должно опираться на ссылки использованных источников (литература, периодические издания, электронные издания, Интернет). Ссылка нумеруется в квадратных скобках по порядку упоминания источника, например [1].

В необходимых случаях ответ должны сопровождаться поясняющими его схематическими рисунками и формулами. Представляемые иллюстрации должны нести смысловую нагрузку (на них должны быть ссылки по тесту).

Рекомендуемый объем ответа на теоретический вопрос – **до 5-7 страниц** печатного текста. При ответе на вопрос рекомендуется пользоваться актуальной информацией из сети Интернет.

***Список источников***. Формируется и нумеруется в порядке упоминания источников, использованных при выполнении контрольной работы.

Примеры библиографического описания *электронных публикаций* в Интернете:

The Ten Most Critical Web Application Security Risks [Электронный ресурс] – Режим доступа: //www.owasp.org/images/7/72/OWASP\_Top\_10-2017\_%28en%29.pdf.pdf. - Дата доступа: 13.06.2018.

# ***Оформление контрольной работы***

Объем контрольной работы − 10-15 печатных страниц формата А4. Оформляется в текстовом процессоре MS Word: шрифт − Times New Roman, 12 пт; абзац – отступ первой строки – 1,5 см, одинарный междустрочный интервал; параметры страницы: поля – слева – 25 мм, остальные – по 15мм.

На титульном листе должны быть указаны: название дисциплины, номер группы, фамилия и инициалы студента, шифр (номер зачетной книжки).

**Теоретический вопрос**

Выбор номера теоретического вопроса контрольной работы осуществляется по двум последним цифрам зачетной книжки. Полужирным шрифтом указано наименования темы вопроса, обычным – что должно быть рассмотрено в вопросе. Если две последние цифры больше, чем 24, то при определении вариант берется только последняя цифра, если последняя цифра «0», то берется 10-й вариант.

|  |  |
| --- | --- |
| №  вопроса | Содержание вопроса |
|  | **Роль криптографических протоколов в системах защиты информации.**  Понятие криптографического протокола. Функции криптографических протоколов. Классификация криптографических протоколов (по функциям, числу участников, числу транспортируемых сообщений). Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. |
|  | **Роль криптографических протоколов в системах защиты информации.**  Моделирование криптографических протоколов. Уязвимости и атаки на криптографические протоколы. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Основные подходы к автоматизации анализа протоколов. |
|  | **Схемы электронной цифровой подписи.** Понятие электронной цифровой подписи. Схемы ЭЦП на основе симметричных и асимметричных шифрсистем. Схемы Эль-Гамаля, Фиата-Фейга-Шамира и Шнорра, их свойства. |
|  | **Схемы электронной цифровой подписи**. Стандарты США, РФ и РБ электронной цифровой подписи. Одноразовые ЭЦП. Схемы конфиденциальной ЭЦП и ЭЦП вслепую. Подписи с обнаружением подделки. Мобильная ЭЦП. |
|  | **Протоколы идентификации.** Понятия идентификации, аутентификации и авторизации. Протоколы идентификации на основе паролей, протоколы “рукопожатия” и типа «запрос-ответ». Идентификация с использованием систем открытого шифрования. Привести конкретные примеры протоколов. |
|  | **Протоколы идентификации.** Протоколы интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением. Протоколы Фиата-Шамира, Шаума, Шнорра и Окамото. Примеры применения. |
|  | **Протоколы идентификации.** Связь между протоколами цифровой подписи и протоколами идентификации. Протоколы с самосертифицируемыми открытыми ключами, построенными на основе идентификаторов. |
|  | **Инфраструктура открытых ключей.** Основные вопросы управления открытыми ключами. Организация и компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509. Государственная система управления открытыми ключами РБ. |
|  | **Инфраструктура открытых ключей.** Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа. Привести скрины примеров. |
|  | **Протоколы распределения ключей.** Протоколы генерации и передачи ключей на основе симметричных и асимметричных шифрсистем. Двух и трех сторонние протоколы передачи и распределения ключей. Функции доверенной третьей стороны и выполняемые ею роли. |
|  | **Протоколы распределения ключей.** Схемы предварительного распределения ключей. Неравенство Блома. Схемы предварительного распределения ключей Блома и на основе пересечений множеств. Протокол открытого распределения ключей Диффи-Хэллмана и способы его защиты от атаки «противник в середине». Аутентифицированные протоколы открытого распределения ключей. Групповые протоколы. Протоколы разделения секрета и распределения ключей для видеоконференцсвязи. |
|  | **Прикладные протоколы.** Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей. Особенности построения семейства протоколов IPsec. Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации. |
|  | **Прикладные протоколы.** Протоколы Oakley, ISAKMP, IKE. Протоколы SKIP, SSL/TLS и особенности их реализации. |
|  | **Протоколы открытых сделок.** Протоколы битовых обязательств и их свойства. Протоколы подбрасывания монеты и “игры в покер” по телефону. Забывающая передача информации. Протокол подписания контракта. Протокол сертифицированной электронной почты. Протоколы электронного голосования. Свойства неотслеживаемости и несвязывемости. Протоколы электронных платежей и цифровых денег. |
|  | **Протоколы открытых сделок.** Протокол сертифицированной электронной почты. Протоколы электронного голосования. Свойства неотслеживаемости и несвязывемости. Протоколы электронных платежей и цифровых денег. |
|  | **Технологии взлома механизмов защиты. Методы защиты от исследования программ.** Взлом механизмов, основанных на ключевом сравнении. Уязвимость криптографических систем защиты. Надежность цифровой подписи. Атака полным перебором. Эмуляция ключевых дисков.  Средства исследования программ. Защита программ от дизассемблирования. Защита программ от работы под контролем отладчика. |
|  | **Технологии взлома механизмов защиты. Методы защиты от исследования программ.** Средства исследования программ. Защита программ от дизассемблирования. Защита программ от работы под контролем отладчика. |
|  | **Криптографическая библиотека CryptoAPI. О**бласть применения. Поддерживаемые криптографические алгоритмы. Процедура обмена ключами. Цифровые сертификаты. Примеры функции. Шифрование с использованием паролей. |
|  | **Хеш-функции.** Методы контроля целостности сообщения.Определение односторонней функции. Понятие хеш-функции. Область применения хеш-функций. Требования к криптографическим хеш-функциям. Понятие коллизии относительно хен-функции. Работы алгоритмов хешерования MD5, SHA-1 и SHA-2, российский и белорусский стандарты хеширования. |
|  | **Код проверки подлинности сообщения (имитовставка).** Методы контроля целостности сообщения. Имитовставка по ГОСТ 28147-89. Алгоритм проверки подлинности сообщений (MAA - Message Authenticator Algorithm), CBC-MAC, двунаправленный MAC, HMAC. |
|  | **Симметричные криптосистемы.** Понятие симметричных криптографических алгоритмов. Сфера применения. Достоинства и недостатки. Характеристики (параметры) алгоритмов. Краткая характеристика алгоритмов DES, AES, ГОСТ 28147-89, RC2, RC5, RC4. |
|  | **AES.** Область применения. Описание режимов работы. Стойкость криптоанализу. |
|  | **ГОСТ 28147-89.** Область применения. Описание режимов работы. Стойкость криптоанализу. |
|  | **Стеганография.** Понятие.Компьютерная и цифровая стеганография. Алгоритмы. Применение. Атаки на стегосистемы. |
|  | **Технология блокчейн.** Умный контракт. Основные понятия: блок и цепочка транзакций, подтверждение. Применение. Майнинг криптовалют. Правовые аспекты использования криптовалют и майнинга. |

**Задание 1**

Сформировать электронную цифровую подпись c помощью алгоритма RSA сообщения, представляющего собой значение хеш-функции от своей фамилии, проверить ее правильность.

Исходные данные: простые числа p и q, хеш-функциют вычислять по формуле:

Hi = (Hi–1 + Mi) 2 mod n, где n = p·q.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер  варианта | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| p | 7 | 7 | 7 | 7 | 7 | 7 | 7 | 11 | 11 | 11 | 11 | 11 | 11 | 13 | 13 | 13 |
| q | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 11 | 13 | 17 | 19 | 23 | 29 | 13 | 17 | 19 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер  варианта | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| p | 13 | 13 | 17 | 17 | 17 | 17 | 19 | 19 | 19 | 23 | 23 | 29 | 31 | 37 | 37 | 37 |
| q | 23 | 29 | 17 | 19 | 23 | 29 | 19 | 23 | 29 | 23 | 29 | 29 | 7 | 7 | 11 | 13 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Номер  варианта | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| p | 37 | 37 | 37 | 37 | 37 | 37 | 41 | 41 | 41 | 41 | 41 | 41 | 41 | 41 | 41 | 41 |
| q | 17 | 19 | 23 | 29 | 31 | 37 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 |

**Задание 2**

Используя алгоритм гаммирования с конгруэнтным датчиком псевдослучайной последовательности, зашифровать сообщение. Сообщением является часть фамилии студента из первых 8 букв (если фамилия меньше 8 букв, то дописать именем), представленная в двоичном виде в кодировке ANSI (для одного символа – 8 бит). Параметры датчика конгруэнтного датчика ПСЧ: T(0)=5, A=17, C=7. Задание реализовать расчетным путем и программно.