Глоссарий

Атажа Понытка противника раскрыть шифр. Аутентификация Установление подпинивности источных сообщения. Блочный шифр Вероятностное пифрование Пибфрование с использованием случайных параметров. Гибвий шифр Набор критгоаспротичов, выбираемых в зависимости от секретног ключа. Гибридная криптосистема (Критгосистема, в которой распределение ключей осуществляется с помощью двужключевой системы, а защифрование – с помощью одпоключевой. Даужключевая криптография с даужи коментор достума Даужключевая криптография с даужи коментор достума Даужключевая криптография с даужи коментор достума Даржинтография с даужи коментор достума Даржинтография с даужи коментор достума даржина криптография с достужет достументы достужения с достужет достужения с достужет достужения с достужет достужения достужени	Аппаратный шифр	Шифр, реализованный в виде электронного устройства.
Аутентификация Установление подлинности источника сообщения Пифрование Пифрования блоков, данных фиксировавнного размера. Пифрование Пифрование с пспользованием случайных параметров. Пибридная кринтосистема Кринтосистема, в которой распределение ключей осуществляется одноключевой системы, а запифрование – с помощью двухключевой системы, а запифрования, другой для расшифрования, причем вычисление любого из этих ключей при условии, что известел пругой ключ, возможно ввилу обиективности отображений запифрования, причем вычисление любого из этих ключей при условии, что известел ругой ключ, возможно ввилу обиективности отображений запифрования при условии, что известел ругой ключ, возможно ввилу обиективности отображений запифрования при условии, что известел ругой ключ, возможно ввилу обиективности отображений запифрования при условии, что известел ругой ключ, возможно ввилу обиективности отображений запифрования для от наконами при условии, что известел ругой ключ, возможно ввилу обиективности отображений запифрования для от наконами при условии, что известел ругой ключ, возможно выди и председавляет вычислительно тручно задачу. Запита от наконами доловнительно тручную задачу. Преобразование набромании для се защатия пожных сообпеций путем передачи небольшой дополнительной информации для сереного ключа паи процесе вынидения самого ключа по неходиму тексту и и соответствующему шифртексту. Криптографическое преобразование криптографическое доловного криптор най процессов инфрртексту. Криптографическое доловного криптор най процессов инфрртексту. Криптографической примитив распоразования (апториты) - составная часть боле сложного крипторафического преобразования, которое рассматривается как композования (апториты) - составная часть боле сложного ключа по неходному какоча дна вычислять выдерживать различные атаки. Криптоситема с закрытым ключом Криптографический драбнеекий дригиский дадачи от некстам дригиским дадачи. Программы вышем програм нежений дригиский драбнеекий дригиский дада		
Шифр для защифрование от Пифрование от Пифрование с использованием случайных параметров. Набор крытгоапторитьюв, выбіраемых в зависимости от секретног ключа. Пифрования с использованием случайных параметров. Пибридная криптосистема (Криптосистема, в которой распределение ключей осуществияется отмонью даухключевая криптография (Криптосистема, в которой распределение ключей осуществияется отмонью даухключевая криптография (Криптосистема с двумя ключами: один для зашифрования, другой для распифрования, причем вычисление любого вз этих ключей при условии, что заместен другой ключ, возможно ввиду бисктивности отобряжений зашифрования, но представляет вычислятельно трунури задачу. Преобразование информации для се защить от песанкционирования для се защить от песанкционирования для се защить от песанкционированию достовать достовать представляет вычислятельно трунури задачу. В другом друго		
Пифрование с использованием случайных параметров. Набор криптоалгоритмов, выбираемых в зависимости от секретног ключа. Криптосистема, в которой распределение ключей осуществляется с помощью длужключевой системы, а запифрования, другой для распифрования, притем вычисление любого из этих ключей при условии, что известен для убисктивности отображений зашифрования даниму бисктивности отображений зашифрования даниму пределатально трудную задачу. Пресобразование наформации для се защиты от несанкционированиюто доступа. Зашита от навъзвывания дожных сообщений путем передачи небольной дололингальной информации для се защиты от несанкционированного доступа. Крипторафическая контрольная сумма. Крипторафическая контрольная сумма. Крипторафическая контрольная сумма. Крипторафическое протексту и соответствующему информации контрольной кому секретного ключа пли процесе вычеления самого ключа по исходиому тексту и и соответствующему информации для решения других крипторафический примития Крипторафический протокол Крипторафический протоком К		
Гибкий пифр Набор криптоалгоритмов, выбираемых в зависимости от секретног ключа. Гибридная криптосистема Криптосистема, в которой распределение ключей осуществляется с помощью одноключевой системы, а зашифрование – с помощью одноключевой. Днухключевая криптография Криптосистема с двумя ключами: один для запифрования, другой для распифрования, причем вычисение любого из этих ключей при условии, что известен другой ключ, возможно ввиду бисктивности отображений зашифрования/расшифрования, но представляет вычисительно грудную задачу. Запифрование Преобразование информатии для се запиты от несавкию опредставляет вычисительно грудную задачу. Имитозащита Зашита от навязывания ложных сообщений путем передачи небольшей заполанительной информации (контрольной сумы). Имитованита Криптографическая контрольная сумма. Ключ Секретный параметр, управляющий процессом пифрования. Криптографическая польчительной сумы. Криптографическая контрольная сумма. Криптографическое проформации (контрольная сумита секретного ключа или врешесе вычисления самого ключа по исходному тексту и соответствующему пифрования данных или для решения других кратографическом пифртексту. Криптографической примитив Субъект, пытавошийся вычислить ключ по исходному тексту и соответствующему пифртексту. Криптографической примитив криптографической примитив Криптографической примитив криптографической примуты других креобразования, которое расматримы с примуты друг		
Криптосистема криптосистема (криптосистема, в которой распределение ключей осуществляется с помощью двужключевой системы, а защифрование — с помощью двужключевой системы, а защифрования — с помощью одноключевой. Двужключевая криптография (криптосистема с двумя ключами: один для запифрования, другой для расшифрования, притем вычисление любого из этих ключей при условии, что известен другой ключ, возможно визиу биективности отображений зашифрования/расшифрования, но представляет вычислительно трудную задачу. Зашифрование (предования информации для её защиты от несанкционированиюто доступа. Имитозащита (предование информации для её защиты от несанкционированиюто доступа. Криптографическая контрольная сумма. Ключ (скретный параметр, управляющий процессом пифрования. Криптографическая контрольная сумма. Криптованализ (процес ослучения исходного текста по шифртексту без знания скретного ключа или процесс вычисления самого ключа и кохднюму тексту и соответствующему шифртексту. Криптографическое (процедура инфровации ключного ключа или ворческом дини фрокации ключа и передура нифровация или выческом доможно вырутих криптографический примитив (криптографических задач). Криптографический примитив (криптографических задач). Криптографический протокол (инструкция, предуматинарнования клигиографических алгоритмов. Криптографический протокол (инструкция, предуматинанопия в заимосяйствие двух для более сторон с использованиям криптографических алгоритмов. Криптосистема с закрытым (криптосистемы выдерживать различные атаки.) Завинный эффект (посебность криптосистемы выдерживать различные атаки.) Программный шифр (протокол) (протокол) протокол, позволяещий выди программы. Прогокол, позволяещий выди протраммы. Прогокол, позволяещим криптографических алгоритмов. (криптосистемы выде программы.) Программный шифр (протокол) (протокол) протокол, позволяещим криптографических алгоритмов. (криптования) (протокол) протокол протокол, позволяещим криптографических алгоритмов. (криптования) (протокол) протокол протокол прот		
Тибридная криптосистема Криптосистема, в которой распределение ключей осуществляется с помощью двужлючевой системы, а защифрование – с помощью одноключевой. Двухключевая криптография Криптосистема с двумя ключами: один для защифрования, другой для расшифрования, причем вычисление любого из этих ключей при условии, что известен другой ключ, возможно ввиду биективности отображений защифрования дост из этих ключей при условии, что известен другой ключ, возможно ввиду биективности отображений защифрования дост информации для её защиты от несенькционирования ложных сообщений путем передачи небольшой долоплительной пиформации (контрольной суммы). Имитозащита Защита от навязывания ложных сообщений путем передачи небольшой долоплительной информации (контрольной суммы). Имитоващита Криптографическая контрольная сумма. Ключ Секретный параметр, управляющий процессом пифрования. Криптоанализ Процесс получения исходного текста по шифргексту без знания ключам али вычислить ключам по исходному тексту и соответствующему шифртексту. Криптографическое процесура шифрования к вичислить ключ по исходному тексту и соответствующему шифртексту. Криптографический примитив Процедура шифрования клиных кли для решения друтих криптографический примитиво исходному тексту и соответствующему шиф текстури преобразования к котором долем преобразования в зами преобра	т полит штүү	
для расшифрования, причем вычисление пюбого из этих ключей при условии, что известен другой ключ, возможно ввиду биективности отображений зашифрования/расшифрования, но представляет вычислительно трудную задачу. Зашита преобразование информации для её защиты от несанкционированию го доступа. Имитоващита Защита от навязывания ложных сообщений путем передачи небольшой дополнительной циформации (контрольной суммы). Имитовставка Криптографическая контрольная сумма. Ключ Секретный параметр, управляющий процессом шифрования. Криптогафанализ Процесс получения исходного текста по шифртексту без знания секретного ключа или процесс вычисления самого ключа по неходному тексту и и соответствующему шифртексту. Криптографическое Процедура шифрования данных или для решения других криптографическог принцура шифрования данных или для решения других криптографический примитив криптографическия операция (алгориты) = составная часть более сложного криптографическог операбразования, которое рассматривается как композиция криптографических примитивов Инструкция, предусматривающая канитографических примитивов Инструкция, предусматривающая канитографических примитивов Инструкция, предусматривающая канитографических примитивов Инструкция, предусматривающая канимором, известным двум или более пользователям. Криптоситемы с закрытивы ключом, известным двум или более пользователям. Криптоситемы к размномень инфрамация (алемномень или знаки иссобразуваций биты или знаки иссобразуваций биты или знаки иссобразуваций биты или знаки иссобразуваций	Гибридная криптосистема	Криптосистема, в которой распределение ключей осуществляется с помощью двухключевой системы, а зашифрование – с помощью одноключевой.
Преобразование информации для её защиты от несанкционировании для её защиты от несанкционировании для её защиты от несанкционирования дожных сообщений путем передачи небольшой дополнительной информации (контрольной суммы). Имитовставка Криптографическая контрольная сумма. Криптоганализ Процесс получения исходного текста по шифртексту без знания секретного ключа или процесс вычисления самого ключа по исходному тексту и и соответствующему шифртексту. Криптоганалитик противника Субъект, пытанощийся вычислить исходный текст по шифртексту без знания ключа или вичестить исходный текст по шифртексту без знания ключа или вычислить исходный текст по шифртексту осответствующему шифртексту. Криптографическое прообразование криптографических задача. Криптографический примитив Криптографическая операция (алгориты)= составная часть более сложного криптографического преобразования, которое рассматривается как композиция криптографических примитивов Инструкция, предусматривающая взаимодействие двух или более сторно с использованием криптографических алгоритмов. Криптосистема с закрытым Криптостойкость Способность криптосистемы кразиномы, известным двум или более пользователям. Криптостойкость Способность криптосистемы кразиномы, известным двум или более пользователям. Криптосистемы кразиномы, известным двум или более пользователям Криптосистемы кразиномы, известным двум или внаки исходного текста. Программный шифр Протокол рукопожатия Программный шифр Протокол рукопожатия Программный шифр Протокол, позволяющий двум пользователям, владеющим общим секретному ключу Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим секретному ключу Раскрытия секрета. Обратное преобразование по отношению к защифрованно, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Сратово подпись крытного текста по его шифртексту и секретному ключу Сратово подпись наконительных серетв. Криптосистема с закрытым ключом. Сратово подпись наконитель	Двухключевая криптография	для расшифрования, причем вычисление любого из этих ключей при условии, что известен другой ключ, возможно ввиду биективности отображений зашифрования/расшифрования, но
небольшой дополнительной информации (контрольной суммы). Кринторафическая контрольная сумма. Ключ Секретный параметр, управляющий процессом шифрования. Кринтоанализ Процесс получения исходного текста по шифртексту без знания секретного ключа или процесс вычисления самого ключа по исходному тексту и соответствующему шифртексту. Криптоаналитик противника Субъект, пытающийся вычислить исходный текст по шифртексту без знания ключа или вычислить ключ по исходному тексту и соответствующему шифртексту. Криптографическое преобразование Криптографическое преобразование Криптографический примитив Криптографический примитив Криптографический примитив Криптографический протокол Криптосистема с закрытым Криптосистема с закрытым Криптосистема с одним секретным ключом, известным двум или более отользованием криптографических алгоритмов. Криптостойкость Способность криптосистемы к размножению ошибок. Лавинный эффект Свойство криптосистемы к размножению ошибок. Поточный шифр Программный шифр Программный шифр Программный шифр Протокол рукопожатия Протокол рукопожатия Протокол рукопожатия Протокол, позволяющий друм пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытия секрета. Вычисление электронной цифровой подписи, которое подписывающий осуществить ключом. Симметричная криптосистема Сратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытия секрета. Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованнох сообщению). Стеганография Способ скрытной неразачи данных, способ формирования скрытного канала связи. Управление ключами	Зашифрование	Преобразование информации для её защиты от
Ключ Секретный параметр, управляющий процессом шифрования. Криптоанализ Процесс получения исходного текста по шифртексту без знания секретного ключа или процесс вычисления самого ключа или процесс вычисления самого ключа или исходному тексту и и соответствующему шифртексту. Криптоаналитик противника Субъект, пытающийся вычислить ключ по исходному тексту и соответствующему шифртексту. Криптографическое преобразование Процедура шифрования данных или для решения других криптографический примитив криптографическам операция (алгоритм)= составная часть более сложного криптографического преобразования, которое рассматривается как композиция криптографических примитивов Криптографический протокол Инструкция, предусматривающая взаимодействие двух или более сложного криптографических алгоритмов. Криптосистема с одним секретным ключом, известным двум или более пользователям Криптосистема с одним секретным ключом, известным двум или более пользователям Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы к размножению ошибок. Криптосиотема с одним секретным ключом, известным двум или более пользователям. Лавинный эффект Свойство криптосистемы к размножению ошибок. Криптосистема с закрытим инфрамению ошибок. Криптосистема к размножению ошибок. Протокол рукопожатия Программый шифр, последовательно преобразующий биты или знаки исходного текста.	Имитозащита	Защита от навязывания ложных сообщений путем передачи
Ключ Секретный параметр, управляющий процессом шифрования. Криптоанализ Процесс получения исходного текста по шифртексту без знания секретного ключа или процесс вычисления самого ключа или процесс вычисления самого ключа или исходному тексту и и соответствующему шифртексту. Криптоаналитик противника Субъект, пытающийся вычислить ключ по исходному тексту и соответствующему шифртексту. Криптографическое преобразование Процедура шифрования данных или для решения других криптографический примитив криптографическам операция (алгоритм)= составная часть более сложного криптографического преобразования, которое рассматривается как композиция криптографических примитивов Криптографический протокол Инструкция, предусматривающая взаимодействие двух или более сложного криптографических алгоритмов. Криптосистема с одним секретным ключом, известным двум или более пользователям Криптосистема с одним секретным ключом, известным двум или более пользователям Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы к размножению ошибок. Криптосиотема с одним секретным ключом, известным двум или более пользователям. Лавинный эффект Свойство криптосистемы к размножению ошибок. Криптосистема с закрытим инфрамению ошибок. Криптосистема к размножению ошибок. Протокол рукопожатия Программый шифр, последовательно преобразующий биты или знаки исходного текста.	Имитовставка	
Процесс получения исходного текста по шифртексту без знания секретного ключа или процесс вычисления самого ключа по исходному тексту и и соответствующему шифртексту. Криптоганалитик противника Субъект, пытающийся вычислить исходный текст по шифртексту без знания ключа или вычислить ключ по исходному тексту и соответствующему шифртексту. Криптографическое преобразование Процедура шифрования данных или для решения других криптографических задач. Криптографический примитив криптографического преобразования, которое рассматривается как композиция криптографических примитивов Инструкция, предусматривающая взаимодействие двух или более сторон с использователям. Криптосистема с закрытым Криптосистема с одним секретным ключом, известным двум или более пользователям. Способность криптосистемы выдерживать различные атаки. Свойство криптосистемы в размножению ошибок. Криптоситема и размный шифр Программный виде, последовательно преобразующий биты или знаки исходного текста. Программный шифр Протокол, позволяющий двум пользователям, владеющим общим секретном, осуществить взаимную проверку подлинности без раскрытия секрета. Обратное преобразование по отношению к запифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретном, осуществить взаимную проверку подлинности без раскрытия секрета. Криптосистема с закрытым ключом. Вычисление электронной шифровой подписи, которое подписывающий осуществляет для запифрованного сообщения (т.е. без допуска к ещё телялет для запифрованного сообщения (т.е. без допуска к ещё телялет для запифрованного сообщения скрытного канала связи. Способ скрытной передачи данных, способ формирования скрытного канала связи. Способ скрытной передачи данных, способ формирования скрытного канала связи. Способ скрытной передачи данных, способ формирования скрытного канала связи. Способ скрытной передачи данных, способ формирове		
без знания ключа или вычислить ключ по исходному тексту и соответствующему шифргексту. Криптографическое преобразование криптографических задач. Криптографический примитив криптографических эадач. Криптографический примитив криптографическог опреобразования, которое рассматривается как композиция криптографических примитивов Инструкция, предусматривающая взаимодействие двух или более сторон с использованием криптографических алгоритмов. Криптосистема с закрытым ключом более пользователям. Криптоситемы выдерживать различные атаки. Свойство криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы выдерживать различные атаки. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретном ключу Нахождение решения криптографической задачи за разумное врем: при использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Вычисление электронной цифровой подписи, которое подписывающий осуществить трия защифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и кличтожение ключей.		секретного ключа или процесс вычисления самого ключа по исходному тексту и и соответствующему шифртексту.
преобразование криптографических задач. Криптографический примитив криптографическая операция (алгоритм)= составная часть более сложного криптографического преобразования, которое рассматривается как композиция криптографических примитивов Криптографический протокол Инструкция, предусматривающая взаимодействие двух или более сторон с использованием криптографических алгоритмов. Криптостойкость Криптосистема с одним секретным ключом, известным двум или более пользователям. Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы выдерживать различные атаки. Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Программный шифр Прогокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Следая подпись Вычисление электронной цифровой подпись, которое подписывающий осуществляет дл	Криптоаналитик противника	без знания ключа или вычислить ключ по исходному тексту и
Криптографический примитив криптографическая операция (алгоритм)= составная часть более сложного криптографического преобразования, которое рассматривается как композиция криптографических примитивов Инструкция, предусматривающая взаимодействие двух или более сторон с использованием криптографических алгоритмов. Криптосистема с закрытым ключом Криптосистема с одним секретным ключом, известным двум или более пользователям. Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы к размножению ошибок. Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Программный шифр Шифр, реализованный в виде программы. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё не	Криптографическое	Процедура шифрования данных или для решения других
сложного криптографического преобразования, которое рассматривается как композиция криптографических примитивов Криптографический протокол Инструкция, предусматривающая взаимодействие двух или более сторон с использованием криптографических алгоритмов. Криптосистема с закрытым Криптосистема с одним секретным ключом, известным двум или более пользователям. Криптостойкость Способность криптосистемы выдерживать различные атаки. Обовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Программный шифр Шифр, реализованный в виде программы. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	преобразование	криптографических задач.
Криптографический протокол Инструкция, предусматривающая взаимодействие двух или более сторон с использованием криптографических алгоритмов. Криптосистема с закрытым ключом Криптосистема с одним секретным ключом, известным двум или более пользователям. Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы к размножению опинбок. Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщения). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечиваю	Криптографический примитив	сложного криптографического преобразования, которое
Криптосистема с закрытым ключом Криптосистема с одним секретным ключом, известным двум или более пользователям. Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавиный эффект Свойство криптосистемы к размножению ошибок. Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	Криптографический протокол	Инструкция, предусматривающая взаимодействие двух или более
ключом более пользователям. Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы к размножению ошибок. Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Программный шифр Шифр, реализованный в виде программы. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	Криптосистема с закрытым	
Криптостойкость Способность криптосистемы выдерживать различные атаки. Лавинный эффект Свойство криптосистемы к размножению ошибок. Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Протокол рукопожатия Шифр, реализованный в виде программы. Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	-	
Лавинный эффект Свойство криптосистемы к размножению ошибок. Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Программный шифр Шифр, реализованный в виде программы. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.		
Лобовая атака Криптоанализ путем перебора всех возможных ключей. Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Программный шифр Шифр, реализованный в виде программы. Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное времпри использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	•	
Поточный шифр Программный шифр, последовательно преобразующий биты или знаки исходного текста. Протокол рукопожатия Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное время при использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	11	
Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное врем при использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.		Программный шифр, последовательно преобразующий биты или
Протокол рукопожатия Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без раскрытия секрета. Расшифрование Обратное преобразование по отношению к зашифрованию, т.е. восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное время при использовании современных вычислительных средств. Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	Программный шифр	
восстановление исходного открытого текста по его шифртексту и секретному ключу Раскрытие (взлом) шифра Нахождение решения криптографической задачи за разумное время при использовании современных вычислительных средств. Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.		Протокол, позволяющий двум пользователям, владеющим общим секретом, осуществить взаимную проверку подлинности без
при использовании современных вычислительных средств. Симметричная криптосистема Криптосистема с закрытым ключом. Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	Расшифрование	восстановление исходного открытого текста по его шифртексту и
Симметричная криптосистема Криптосистема с закрытым ключом. Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	Раскрытие (взлом) шифра	Нахождение решения криптографической задачи за разумное время
Слепая подпись Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения (т.е. без допуска к ещё незашифрованному сообщению). Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	Симметричная криптосистема	
Стеганография Способ скрытной передачи данных, способ формирования скрытного канала связи. Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.		Вычисление электронной цифровой подписи, которое подписывающий осуществляет для зашифрованного сообщения
Управление ключами Совокупность мероприятий, обеспечивающих генерацию, распределение, хранение и уничтожение ключей.	Стеганография	Способ скрытной передачи данных, способ формирования
	Управление ключами	Совокупность мероприятий, обеспечивающих генерацию,
у правляемые операции — — Операции, выоираемые в зависимости от управляющего кода.	Управляемые операции	Операции, выбираемые в зависимости от управляющего кода.

Хеширование	Вычисление значения хеш-функции.
Хеш-функция	Функция, вычисляющая сжатый образ фиксированной длины для
	сообщения произвольной длины.
Цифровая подпись	Электронная цифровая подпись.
Шифр с открытым ключом	Двухключевая криптосистема.
Шифр	Совокупность алгоритмов зашифрования и расшифрования.
Шифрование	Преобразование информации под управлением ключа.
Шифратор	Электронное устройство или программа, осуществляющие
	шифрование информации.
Электронная цифровая подпись	Дополнительная информация, которая может быть сформирована
	только владельцем, обладающим некоторым секретом.