Занятие 95: практическое

ИНСТРУКЦИОННАЯ КАРТА № 41

на выполнение практического занятия по МДК.03.02
" Безопасность функционирования информационных систем "
для студентов специальности 09.02.02 Компьютерные сети

Тема: Основные принципы работы инфраструктуры открытых ключей (PKI)

Цель работы: Изучить основы инфраструктуры открытых ключей (PKI)
Норма времени: 2 ак. часа
Оснащение рабочего места: ПК, инструкционные карты, конспект.
Информационное обеспечение:
Что такое PKI? Главное об инфраструктуре открытых ключей. – https://habr.com/ru/post/655135/
Инфраструктура открытых ключей. – https://dic.academic.ru/dic.nsf/ruwiki/151605
Компетенции, умения и навыки, которыми должны овладеть обучающиеся: ОК9, ПК.3.1
После выполненных работ студент должен **знать:** инфраструктуры открытых ключей; кл Область применения PKI; Стандарты и протоколы; **уметь:** выполнять шифрование с использованием р=основных алгоритмов.

Теоретические сведения

Общие сведения об инфраструктуре открытых ключей (PKI)

Public Key Infrastructure (PKI) - совокупность сервисов для управления ключами и цифровыми сертификатами пользователей, программ и систем.

Упрощенно,

PKI представляет собой систему, основными компонентами которой являются удостоверяющий центр и пользователи, взаимодействующие между собой используя сертификаты, выданные этим удостоверяющим центром.

PKI использует технологию открытых ключей для:

- идентификации участников электронного обмена (пользователей, программ, систем),
- обеспечения конфиденциальности информации,
- контроля за целостностью информации,
- установления происхождения информации.

В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

- ❑ закрытый ключ известен только его владельцу;
- ❑ удостоверяющий центр создает сертификат открытого ключа, таким образом удостоверяя этот ключ;
- ❑ никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- ❑ удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

PKI оперирует в работе сертификатами.

Сертификат — это электронный документ, который содержит электронный ключ пользователя, — открытый или же ключевую пару (keypair), — информацию о пользователе, которому принадлежит сертификат, удостоверяющую подпись центра выдачи сертификатов (УЦ) и информацию о сроке действия сертификата.

Функции PKI

- **Регистрация (Registration)** - процесс сбора информации о пользователе и проверки ее подлинности, которая затем используется при регистрации пользователя, в соответствии с правилами безопасности.
- **Выдача сертификата (Certificate Issuance)**. Как только CA подписал сертификат он выдается просителю и/или отправляется в хранилище сертификатов. CA проставляет на сертификатах срок действия, требуя таким образом периодического возобновления сертификата.
- **Аннулирование сертификата (Certificate Revocation)**. Сертификат может стать недействительным до окончания срока действия в силу различных причин: пользователь уволился из компании, сменил имя или если его част-

ный ключ был скомпрометирован. При этих обстоятельствах CA аннулирует сертификат, занося его серийный номер в CRL.

- **Восстановление ключа (Key Recovery)**. Дополнительная функция PKI позволяет восстанавливать данные или сообщения в случае утери ключа.
- **Управление работой (Lifecycle Management)** - постоянная поддержка сертификатов в PKI, включающая обновление, восстановление и архивирование ключей. Эти функции выполняются периодически, а не в ответ на специальные запросы. Автоматизированное управление ключами наиболее важная функция для больших PKI. Ручное управление ключами может ограничить масштабируемость PKI.

Информация, необходимая для работы PKI, содержится в стандарте **X.509**

Основные алгоритмы шифрования, используемые в PKI

Алгоритм Диффи—Хеллмана используется для обмена секретными ключами без передачи их по открытому каналу связи

В соответствии с алгоритмом Диффи—Хеллмана для успешного решения задачи абоненты должны выполнить следующие действия. Прежде всего они открыто договариваются о том, что будут использовать одностороннюю функцию $Y = D^x \bmod P$. Затем они договариваются о значениях параметров D и P. Пусть, например, они договорились, что D = 7 и P = 13, то есть функция имеет вид $Y = 7^x \bmod 13$. Еще раз подчеркнем, что в соответствии с алгоритмом Диффи—Хеллмана вся эта информация не является секретной.

Дальнейшие действия участников обмена описываются в табл.1.

Таблица 1. Действия Алисы и Боба в соответствии с алгоритмом Диффи—Хеллмана

	Действия Алисы		Действия Боба	
1	Алиса секретным образом выбирает произвольное число A (закрытый ключ Алисы)	Пусть, например, A = 2	Боб также секретно выбирает произвольное число B (закрытый ключ Боба)	Пусть, например, B = 4
2	Алиса вычисляет значение а односторонней функции Y, используя в качестве аргумента свое секретное число A: то есть $a = D^A \bmod P$ (открытый ключ Алисы)	$a = D^A \bmod P = 7^2 \bmod 13 = 10$	Боб также вычисляет значение b односторонней функции У, используя в качестве аргумента свое секретное число B: $b = D^B \bmod P$ (открытый ключ Боба)	$b = D^B \bmod P = 7^4 \bmod 13 = 2401 \bmod 13 = 9$
3	Алиса посылает Бобу свой открытый ключ *a*	10	Боб посылает Алисе свой открытый ключ *b*	9
4	Алиса, получив от Боба число *b*, вычисляет по формуле $K = b^A \bmod P$ (разделяемый секретный ключ)	$K = b^A \bmod P = 9^2 \bmod 13 = 81 \bmod 13 = 3$	Боб, получив от Алисы число *a*, вычисляет по формуле $K = a^B \bmod P$ (разделяемый секретный ключ)	$K = a^B \bmod P = 10^4 \bmod 13 = 10000 \bmod 13 = 3$

В результате описанной процедуры на шаге 4 Алиса и Боб получили одно и то же число 3. Это и есть общий секретный ключ.

Обмен сообщениями по протоколу RSA происходит следующим образом:
1. Абонент-получатель шифрованных сообщений Б генерирует открытый и закрытый ключи.
2. Открытый ключ получатель Б рассылает всем отправителям (в том числе А).
3. Отправитель (А) шифрует сообщение открытым ключом получателя Б и отправляет его получателю.
4. Получатель Б расшифровывает сообщение своим закрытым ключом.

Пусть пользователь Алиса хочет передать пользователю Бобу сообщение «8275».

1. В этом случае вначале пользователь Боб должен подготовить открытый и закрытый ключи. Пусть им выбраны, например, следующие параметры:

два случайных простых числа (для простоты расчетов примем очень маленькие числа) $P = 3$ и $Q = 11$, тогда

$N = P \cdot Q = 3 \cdot 11 = 33 \qquad F = (P-1)\cdot(Q-1) = 2 \cdot 10 = 20$

2. Затем пользователь Боб выбирает любое число *D*, **не имеющее общих делителей с *F***. Пусть $D = 13$. Это число будет одним из компонентов открытого ключа: (D, N) = (3, 33).

Далее необходимо найти число *E*, которое можно будет использовать в качестве закрытого ключа для расшифровки сообщения. **Значение *E* должно удовлетворять соотношению $ED \bmod F = 1$** . В нашем случае подходит *E* =17. (Проверяем: 13*17 mod 20 = 221 mod 20 = 1.) Это – закрытый ключ.

3. Теперь пользователь Боб должен запомнить свой закрытый ключ 17 (число *E*), отправить открытый ключ (13, 33) пользователю Алисе и уничтожить числа $P = 3$ и $Q = 11$.

4. Пользователь Алиса, получивший открытый ключ (13, 33), увидев, что N=33, разбивает исходное сообщение на три блока, причем значение каждого меньше N. В нашем случае получаем три блока m_1=8, m_2=27, m_3,=5. Затем пользователь А шифрует каждый блок: $c_i = m_i^D \bmod N$:

$c_1 = 8^{13} \bmod 33 = 17 \qquad c_2 = 27^{13} \bmod 33 = 15 \qquad c_3 = 5^{13} \bmod 33 = 26$

Вычисление модуля от степени числа упрощается при использовании следующего правила:

$$(Y^{a+b+c}) \bmod P = (Y^a \bmod P \times Y^b \bmod P \times Y^c \bmod P) \bmod P$$

Зашифрованное сообщение, состоящее из трех блоков (17, 15, 26), передается пользователю Бобу.
5. Далее Боб, используя свой закрытый ключ $E = 17$ и $N=33$, расшифровывает сообщение: $m_i = c_i^E \bmod N$:
$m_1 = 17^{17} \bmod 33 = 8$ $m_2 = 15^{17} \bmod 33 = 27$ $m_3 = 26^{17} \bmod 33 = 5$
Таким образом, абонент Б расшифровал сообщение от абонента А.

Ход работы

Задание 1. Изучение основ работы инфраструктуры открытых ключей (PKI)

1. Изучить основные сведения об инфраструктуре открытых ключей (PKI). Записать результаты изучения в отчет.

Задание 2. Шифрование с использованием алгоритма Диффи-Хеллмана

1. Два абонента используют алгоритм Диффи—Хеллмана для получения общего секретного ключа. Они используют функцию $Y = D^x \bmod P$ (задается преподавателем). Вычислить открытый ключ абонента А, который он отправит абоненту Б.

2. Два абонента используют алгоритм Диффи—Хеллмана для получения общего секретного ключа. Они используют функцию $D^x \bmod P$ (задается преподавателем). Абонент А отправил абоненту Б свой открытый ключ (задается преподавателем). Вычислить общий секретный ключ.

Задание 3. Шифрование с использованием алгоритма RSA

1. При шифровании по алгоритму RSA открытый ключ абонента Б равен (D,N) (задается преподавателем). Выполнить шифрование двух чисел (задаются преподавателем) с использованием открытого ключа.

2. При шифровании по алгоритму RSA открытый ключ абонента Б равен (D,N), закрытый ключ равен Е. Выполнить дешифрование сообщения, переданного абоненту (исходные данные задаются преподавателем).

Содержание отчета о занятии

Определение PKI: …
PKI представляет собой систему, основными компонентами которой являются: …
Основные принципы PKI: …
Сертификат — это …
Функции PKI (только названия) …
Процесс развертывания PKI состоит из нескольких этапов: …
Алгоритм Диффи-Хеллмана:
D = …, N = … Открытый ключ абонента А:
D = …, N = … B = … Общий секретный ключ
Алгоритм RSA:
Открытый ключ абонента Б: …. Исходное сообщение: … Зашифрованное сообщение: …
Открытый ключ абонента Б: …. Закрытый ключ абонента Б: …
Зашифрованное сообщение: … Результат расшифровки: …

Инструкционную карту составил преподаватель Дубик Н.А.