Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА-Российский технологический университет»

РТУ МИРЭА

Кафедра КБ-1 «Защита информации»

ПРАКТИЧЕСКАЯ РАБОТА № 9

по дисциплине «Криптографические методы защиты информации»

Идентификация и аутентификация (RSA, схемы Шнорра и Фейге-Фиата-Шамира)

РТУ МИРЭА – 2020 г.

Идентификация (англ. identification) - процесс распознавания сущностей путем присвоения им уникальных меток (идентификаторов, логинов).

Аутентификация (англ. authentication) - проверка соответствия (подлинности) сущности предъявленному ею идентификатору. (Заметим, что происхождение русскоязычного термина «аутентификация» не совсем понятно. Английское «authentication» скорее можно прочитать как «аутентикация»; трудно сказать, откуда в середине взялось еще «фи» – может, из идентификации? Тем не менее, термин устоялся и закреплен в РД Гостехкомиссии РФ).

Для полноты картины приведем определение термина авторизация, который не следует путать с двумя вышеприведенными. **Авторизация** (англ. authorization) - предоставление сущности возможностей в соответствии с положенными ей правами или проверка наличия прав при попытке выполнить какое-либо действие.

Идентификация и аутентификация – это первая линия обороны, «входная дверь» в информационное пространство организации.

Идентификация позволяет субъекту (пользователю, процессу, действующему от имени определенного пользователя, или иному аппаратно-программному компоненту) назвать себя (сообщить свое имя). Посредством аутентификации вторая сторона убеждается, что субъект действительно тот, за кого он себя выдает.

Идентификация сродни присвоении имени ребенку (не совсем точное сравнение, но все же). В любой ИС должны быть определены все субъекты, участвующие в информационном обмене. Часть из них может быть сгруппирована, если они наделены одинаковыми (схожими) правами и обладают одинаковыми (схожими) характеристиками. Каждый субъект (группа субъектов) должен обладать уникальным именем (обозначением).

Аутентификация бывает **односторонней** (обычно клиент доказывает свою подлинность серверу) и **двусторонней** (взаимной). Пример односторонней аутентификации – процедура входа пользователя в систему.

Субъект может подтвердить свою подлинность, предъявив один из следующих **аутентификаторов**:

- нечто, что он знает (пароль, личный идентификационный номер, криптографический ключ и т.п.);

- нечто, чем он владеет (паспорт, личную карточку или иное устройство аналогичного назначения);

- нечто, что есть часть его самого (голос, отпечатки пальцев, образец ДНК и т.п.).

В том случае, если в ходе процедуры аутентификации клиент должен предъявить сразу несколько аутентификаторов, аутентификация называется **многофакторной**. Например, в ходе двухфакторной аутентификации клиент должен знать пароль и воспользоваться личной карточкой.

Широкое распространение при идентификации и аутентификации получили протоколы на базе асимметричного шифрования. Существует десятки разновидностей таких

протоколов, наиболее известными из которых являются протоколы на основе алгоритмов RSA, схемы Фейге-Фиата-Шамира, Шнорра и т.д.

Протокол на основе алгоритма RSA.

Этап 1. Генерация ключей.

1. **А** генерирует открытый и закрытый ключи ((e=5, n=91) и d=29).

2. **А** передает открытый ключ **Б**.

Этап 2. Аутентификация.

Таблица 1. Аутентификация на основе алгоритма RSA

№ п/п	Описание операции	Пример
1	Б выбирает случайное число **k** ∈ {1, …, n-1}, вычисляет **r** = k^e mod n и посылает **r А**.	k = 23 r = 23^5 mod 91 = 4
2	А вычисляет **k'** = r^d mod n и посылает **k' Б**.	k' = 4^{29} mod 91 = 23
3	**Б** проверяет соотношение **k** = **k'** и, если оно истинно, принимает доказательство, в противном случае - отвергает.	k = 23 k' = 23

Схема Клауса Шнорра.

Этап 1. Генерация ключей (выполняет **А**).

Таблица 2. Генерация ключей по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	Выбираются два простых числа **p** и **q** такие, что (p - 1) mod q = 0.	p = 23, q = 11
2	Выбирается секретный ключ **x** ∈ {1, …, q-1}.	x = 8
3	Выбирается **g** такое, что g^q mod p = 1.	g=3 3^{11} mod 23 = 1
4	Вычисляется открытый ключ **y** такой, что (g^x * y) mod p = 1.	y = 4 (3^8 * 4) mod 23 = 26244 mod 23 = 1
5	Публикация открытого ключа **y**.	

Этап 2. Аутентификация.

Таблица 3. Аутентификация по схеме Клауса Шнорра

№ п/п	Описание операции	Пример
1	**A** выбирает случайное число **k** ∈ {1, …, q-1}, вычисляет **r** = g^k mod p и посылает **r Б**.	k = 6 r = 3^6 mod 23 = 16
2	**Б** выбирает случайное число **e** ∈ {0, …, 2^t-1}, где t - некоторый параметр, и посылает **e A**.	e = 4
3	**A** вычисляет **s** = (k + x * e) mod q и посылает **s Б**.	s = (6 + 8 * 4) mod 11 = 5
4	**Б** проверяет соотношение **r** = (g^s * y^e) mod p и, если оно выполняется, принимает доказательство, в противном случае - отвергает.	16 = (3^5 * 4^4) mod 23

Для обеспечения стойкости протокола в 1989 г. Шнорр рекомендовал использовать **p** длиной 512 бит, **q** длиной 140 бит и **t** = 52.

Упрощенная схема аутентификации Фейге-Фиата-Шамира.

Этап 1. Генерация ключей (выполняет Посредник).

Таблица 4. Генерация ключей по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример
1	Выбирает модуль **n**, равный произведению двух простых чисел.	p = 5, q = 7, n = 35
2	Выбирает число **v** (открытый ключ), являющееся квадратичным вычетом по модулю **n** и имеется обратное значение $\mathbf{v^{-1}}$ по модулю **n**. **Квадратичный вычет** – число, удовлетворяющее выражению x^2 mod n = v, где 1 ≤ x ≤ n. Для модуля n = 35, квадратичными вычетами являются 1 (x = 1, 6, 29, 34), 4, 9, 11, 14, 15, 16, 21, 25, 29, 30. Обратное значение вычисляется по формуле (v * v^{-1}) mod n = 1. У квадратичных вычетов 14, 15, 21, 25 и 30 нет обратных значений по модулю. Таким образом, v ∈ {1, 4, 9, 11, 16, 29}.	v = 16 v^{-1} = 11 (16 * 11) mod 35 = 176 mod 35 = 1
3	Определяет закрытый ключ **s**, как наименьшее значение, удовлетворяющее следующему выражению s^2 mod n = v^{-1}.	s = 9 9^2 mod 35 = 11
4	Публикация открытого ключа – **v** и **n**. Передача закрытого ключа **s A**.	

Этап 2. Аутентификация.

Таблица 5. Аутентификация по схеме Фейге-Фиата-Шамира

№ п/п	Описание операции	Пример	
1	**А** выбирает случайное число **r** ∈ {1, …, n-1}, вычисляет **z** = r^2 mod n и посылает **z** **Б**.	r = 8 z = 8^2 mod 35 = 29	
2	**Б** посылает **А** случайный бит **b**.	b = 0	b = 1
3	Если **b**=0, то **А** посылает **Б** **r**, иначе - **y** = (r * s) mod n.	r = 8	y = (8 * 9) mod 35 = 2
4	Если **b**=0, то **Б** проверяет, что **z** = r^2 mod n, иначе - **z** = (y^2 * v) mod n.	29 = 8^2 mod 35	29 = (2^2 * 16) mod 35

Рассмотренный порядок операций, выполненный 1 раз называется **аккредитацией**. Если первую операцию поменять местами со второй, то **А**, даже не зная закрытого ключа **s**, может подобрать такое значение **r**, которое будет приводить к успешной аккредитации в обоих случаях (b=0 и b=1). Подобрать же такое **r**, которое будет приводить к успешной аккредитации в обоих случаях одновременно невозможно. Таким образом, если **А** не знает закрытого ключа **s**, то вероятность успешной аккредитации (подбора **r**) равна 1/2. Аккредитация повторятся **t** раз, пока не будет достигнута требуемая вероятность $1/2^t$, что А не знает закрытого ключа **s**.

Задание на практическую работу.

Составить отчет о проделанной практической работе. В отчете **должны** содержаться **выполненные задания**, указанные ниже

1) Ответить на контрольные вопросы.

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».

2. Что может служить в качестве аутентификатора?

3. Перечислите основные способы организации идентификации и аутентификации.

4. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.

2) Привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:

- на основе алгоритма RSA;

- по схеме Шнорра;

- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа (k или r) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.