Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Практическое задание №4.2**

**Тема «Криптографическая защита информации»**

Руководитель: Ржеутская Н. В.

Выполнил:

Студент 2 курса 8 группы ФИТ

Солодкий ДВ

Минск 2022

**Задание №1**

Рассказать процесс работы алгоритма RSA.

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи.

Для начала нужно сгенерировать публичный и приватный ключ.

* Выбираю два простых числа. Пусть это будет p=3 и q=7.
* Вычисляю модуль — произведение p и q: n=p\*q=3\*7=21.
* Вычисляю функциюЭйлера: φ=(p-1)\*(q-1)=2\*6=12.
* Выбираю число e, отвечающее следующим критериям:

1. Оно должно быть простое
2. Оно должно быть меньше φ — остаются варианты: 3, 5, 7, 11
3. Оно должно быть взаимно простое с φ; остаются варианты 5, 7, 11. Пусть e=5. Это открытая экспонента.

Теперь пара чисел {e, n} — это мой открытый ключ. Я отправляю его кому-то, чтобы этот кто-то зашифровал своё сообщение. Но мне еще нужно получить закрытый ключ.

Мне нужно вычислить число d, обратное е по модулю φ. То есть остаток от деления по модулю φ произведения d\*e должен быть равен 1. d может мыть равен 17. Пара {d, n} — это секретный ключ, его я оставляю у себя. Его нельзя сообщать никому. Только обладатель секретного ключа может расшифровать то, что было зашифровано открытым ключом.

Теперь зашифрую какое-нибудь сообщение(число).

Пусть это будет число 19. Обозначу его P=19. Также имеется открытый ключ: {e, n} = {5, 21}. Шифрование выполняется по следующему алгоритму:

* Выбранное число возводится в степень e по модулю n. То есть, вычисляется 19 в степени 5 (2476099) и берётся остаток от деления на 21. Получается 10 — это закодированные данные.

Полученные данные E=10 отправляются назад отправителю.

Однако сообщение P=19 не должно быть больше n=21, иначе ничего не получится.

Теперь расшифрую то, что было зашифровано.

Я получил данные (E=10), и у меня имеется закрытый ключ  
{d, n} = {17, 21}.

Суть в том, что открытый ключ не может расшифровать сообщение, а закрытый ключ я никому не сообщал.

Начинаю расшифровывать:

* Я делаю операцию, похожую на шифровку, но вместо e использую d. Возвожу E в степень d: получаю 10 в степени 17. Вычисляю остаток от деления на 21 и получаю 19 — исходное сообщение.

Никто, кроме обладателя закрытого ключа не сможет расшифровать сообщение (ну почти никто).

**Задание №2**

Рассказать процесс работы алгоритма Диффи-Хеллмана.

Пусть есть 2 числа – g и p. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: первый абонент — число a, второй абонент — число b. Затем первый абонент вычисляет значение A = g^a mod p и пересылает его второму, а второй вычисляет B = g^b mod p и передаёт первому. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (т.е. у него нет возможности вмешаться в процесс передачи). На втором этапе первый абонент на основе имеющегося у него a и полученного по сети B вычисляет значение, B^a mod p = g^(a\*b) mod p, а второй абонент на основе имеющегося у него b и полученного по сети A вычисляет значение A^b mod p = g^(a\*b) mod p. Как нетрудно видеть, у обоих абонентов получилось одно и то же число: K = g^(a\*b) mod p. Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления g^(a\*b) mod p по перехваченным g^a mod p и g^b mod p, если числа p, a, b выбраны достаточно большими.

**Задание №3**

Рассказать процесс работы алгоритма Эль-Гамаля.

Схема была предложена Тахером Эль-Гамалем в 1984 году.Эль-Гамаль разработал один из вариантов алгоритма Диффи-Хеллмана. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и для обеспечения аутентификации. В отличие от RSA алгоритм Эль-Гамаля не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию. Считается, что алгоритм попадает под действие патента Диффи-Хеллмана.

Пусть имеются абоненты А, В, С, ..., которые хотят передавать друг другу зашифрованные сообщения, не имея никаких защищенных каналов связи. Фактически здесь используется схема Диффи-Хеллмана, чтобы сформировать общий секретный ключ для двух абонентов, передающих друг другу сообщение, и затем сообщение шифруется путем умножения его на этот ключ. Для каждого следующего сообщения секретный ключ вычисляется заново.

Шифрование

Допустим, что нужно зашифровать сообщение М = 5.  
  
1. Произведем генерацию ключей: пусть p = 11, g = 2. Выберем x = 8 - случайное целое число x такое, что 1 < х < (р - 1).

Вычислим y = g^x mod p = 2^8 mod 11 = 3.

Итак, открытым является тройка (p, g, y) = (11, 2, 3), а закрытым ключом является число x = 8.

2. Выбираем случайное целое число k такое, что 1 < k < (p - 1). Пусть k = 9.

3.Вычисляем число A = g^k mod p = 2^9 mod 11 = 512 mod 11 = 6.

4.Вычисляем число B = y^k\*M mod p = 3^9\*5 mod 11 = 19683\*5 mod 11 = 9

Полученная пара (a, b) = (6, 9) является шифротекстом.

Расшифрование

Необходимо получить сообщение M = 5 по известному шифротексту

(a, b) = (6, 9) и закрытому ключу x = 8.

Вычисляем M по формуле M = b\*(a^x)^-1 mod p = 9\*(6^8)^-1 mod 11 = 5.

Получили исходное сообщение M = 5.

Вывод: были изучены алгоритмы шифровки RSA, Диффи-Хеллмана, Эль-Гамаля.