**RSA**

**Шаг первый. Подготовка ключей**

Я должен проделать предварительные действия: сгенерировать публичный и приватный ключ.

* Выбираю два простых числа. Пусть это будет p=3 и q=7.
* Вычисляем *модуль* — произведение наших p и q: n=p×q=3×7=21.
* Вычисляем *функцию Эйлера*: φ=(p-1)×(q-1)=2×6=12.
* Выбираем число e, отвечающее следующим критериям: (i) оно должно быть простое, (ii) оно должно быть меньше φ — остаются варианты: 3, 5, 7, 11, (iii) оно должно быть взаимно простое с φ; остаются варианты 5, 7, 11. Выберем e=5. Это, так называемая, *открытая экспонента*.

Теперь пара чисел {e, n} — это мой открытый ключ. Я отправляю его вам, чтобы вы зашифровали своё сообщение. Но для меня это ещё не всё. Я должен 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. Запишем это в обозначениях, принятых во многих языках программирования: (d×е)%φ=1. Или (d×5)%12=1. d может быть равно 5 ((5×5)%12=25%12=1), но чтобы оно не путалось с e в дальнейшем повествовании, давайте возьмём его равным 17. Можете проверить сами, что (17×5)%12 действительно равно 1 (17×5-12×7=1). Итак d=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.

**Шаг второй. Шифрование**

Теперь пришла ваша очередь шифровать ваше сообщение. Допустим, ваше сообщение это число 19. Обозначим его P=19. Кроме него у вас уже есть мой открытый ключ: {e, n} = {5, 21}. Шифрование выполняется по следующему алгоритму:

* Возводите ваше сообщение в степень e по модулю n. То есть, вычисляете 19 в степени 5 (2476099) и берёте остаток от деления на 21. Получается 10 — это ваши закодированные данные.

Строго говоря, вам вовсе незачем вычислять огромное число «19 в степени 5». При каждом умножении достаточно вычислять не полное произведение, а только остаток от деления на 21. Но это уже детали реализации вычислений, давайте не будем в них углубляться.

Полученные данные E=10, вы отправляете мне.

Здесь надо заметить, что сообщение P=19 не должно быть больше n=21. иначе ничего не получится.

**Шаг третий. Расшифровка**

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

Обратите внимание на то, что открытый ключ не может расшифровать сообщение. А закрытый ключ я никому не говорил. В этом вся прелесть асимметричного шифрования.

Начинаем раскодировать:

* Я делаю операцию, очень похожую на вашу, но вместо e использую d. Возвожу E в степень d: получаю 10 в степени 17 (позвольте, я не буду писать единичку с семнадцатью нулями). Вычисляю остаток от деления на 21 и получаю 19 — ваше сообщение.

Заметьте, никто, кроме меня (даже вы!) не может расшифровать ваше сообщение (E=10), так как ни у кого нет закрытого ключа.

**Эль-Гамаля**



