Семинар 5. Алгоритм RSA

Алгебра в криптографии, осенний семестр 2021 г.

ФАКУЛЬТЕТ МАТЕМАТИКИ, НИУ ВШЭ

Задача 1 (Шифр Юлия Цезаря)**.** Текст зашифрован программой, заменяющей взаимно однозначно каждую букву на некую другую. Докажите, что этот текст можно расшифровать, применив определённое число раз шифрующую программу.

Задача 2 (Детский RSA[1])**.** Арина выбрала натуральные числа a, b, a', b' (их она потом уничтожила) и по ним вычислила *открытый множитель* $e = a'(ab-1)+a$, *закрытый множитель* $d = b'(ab-1)+b$, и *модуль*

$$n = \frac{ed-1}{ab-1}.$$

Числа e и n Арина передала своему агенту Богдану, а число d держит у себя в сейфе. Богдан шифрует сообщение x (=целое число от 0 до $n-1$) с помощью функции:

$$f(x) = ex \pmod{n}$$

и пересылает результат Арине по открытому каналу связи.

(а) Как Арине расшифровать сообщение Богдана (то есть найти x по $f(x)$)?

(б) Шпион Вася перехватывает сообщение Богдана (а также открытый множитель e и модуль n). Как Васе взломать шифр (сейф Арины он взломать не может)?

Задача 3 (Алгоритм RSA)**.** Пусть $n = pq$ (*модуль*) — произведение двух простых чисел, а e (*открытая экспонента*) — число взаимно простое с $\varphi(n) := (p-1)(q-1)$ и меньшее, чем $\varphi(n)$. Для произвольного остатка x (*сообщения*) по модулю n определим остаток $f(x)$ (*зашифрованное сообщение*) по формуле

$$f(x) = x^e \pmod{n}.$$

Предложите способ расшифровки сообщения, то есть, вычисления x по $f(x)$, если также известны p, q и e. В частности, объясните почему функция $x \mapsto f(x)$ переводит разные остатки по модулю n в разные.

Задача 4. (а) Зашифруйте сообщение 21 22 с помощью модуля 35 и открытой экспоненты 5.

(б) Расшифруйте сообщение 02 09, зашифрованное тем же открытым ключом, что и в пункте (а).

Задача 5. Шифр использует открытый ключ из модуля 143 и экспоненты 103, а также следующее соответствие между буквами и цифрами:

$$\text{И} = 1,\ \text{Н} = 2,\ \text{Е} = 3,\ \text{А} = 4,\ \text{О} = 5,\ \text{Т} = 6,\ \text{Л} = 7,\ \text{Р} = 8,\ \text{С} = 9,\ \text{В} = 0.$$

Сообщение перевели в цифры, разбили на блоки по две цифры и зашифровали. Получилось 10 03. Расшифруйте сообщение.

Задача 6. В слове (русского языка) заменили каждую букву на её порядковый номер в алфавите и записали последовательность номеров как одно число (без пробелов). Полученное число зашифровали алгоритмом RSA с помощью открытого ключа:

$$n = 32\ 193\ 888\ 639\ 167\ 989, \quad e = 3.$$

Получилось число 7868291377216450. Восстановите исходное слово.

[1]Этот шифр придумал американский математик Нил Коблиц