Основные атаки на алгоритм Эль Гамаля

1. Атака малого модуля

Атака состоит в том, что мы будем искать решение h = g^x mod p, зная h, g и p (имеет малое значение), алгоритмом baby step giant step.

Пусть есть уравнение h = g^x в цикличекой группе порядка p. Положим, что x = i\*m - j, где m - заранее выбранная константа (обычно используют округленное вверх значение квадратного корня из p). i называют giant step, т.к увеличение параметра увеличивает x на m, а i - baby step (противоположность giant step).

Очевидно, что любое x из промежутка [0,p) можно представить в такой форме. Тогда уравение принимает вид: h = g^(m\*i - j) => h\*(g^(-m))^i = g^j

Алгоритм предварительно вычисляет g^j для некоторых j. Потом корректируется значение m и пробуются различные значения i.

Давайте рассмотрим пример:

20 = 5^x (mod 53)

В данном случае g = 5, h = 20 и p = 53, и мы хотим узнать x. Для начала определим квадратный корень из p-1, и округлим до ближайшего целого:

m = ceil(sqrt(p-1)) = ceil(sqrt(52)) = 7

Затем мы вычислим g^j (mod p) от 1 до m и занесем информацию в виде {g^j (mod p), j}

{1: 0, 5: 1, 25: 2, 11: 3, 42: 4, 51: 5, 43: 6, 3: 7}

Например: Если i = 0, мы получаем 5^6 mod 53 дает 43 {43:6}

Теперь у нас есть список пар от 0 до квадратного корня из p-1. Затем мы проходимся по значениям h (g^-m)^x (mod p) пока мы не найдем совпадения в таблице. Тогда мы умножаем число на m и добавляем число, которое сопоставлено в таблице.

Для решения задачи была написана программа , которая по заданным в файле значениям h, g, p вычисляет x.

Рассмотрим примеры ее работы:

Пример 1.

h = 1849836

g = 11

p = 2097151

Ответ:

Пример 2.

h = 4338246301

g = 1208

p = 9048610007

Ответ:

Это были очень маленькие значения. Попробуем что-то большее!

Добавить примеры

Как можно избежать данной атаки? Во-первых, следует использовать достаточно большие значения модуля p (порядка 2^10 — 2^11 знаков). Во-вторых, нужно использовать числа Софи Жермен.

Простое число p является простым числом Софи Жермен, если 2p+1 также является простым.

Пример: 11 - простое число, 2\*11+1 = 23 - связанное с ним простое, значит 11 - число Софи Жермен.

Первые несколько чисел Софи Жермен: 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131, 173, 179 ....

Числа 2p+1, объединенные простотой Софи Жермен, называются безопасными простыми. (Безопасное простое - это простое число вида 2p+1, где p - число Софи Жермен) Понятие безопасной простоты можно усилить до сильной простоты, для которой p-1 и p+1 имеют большие простые множители, которые, в свою очередь, имеют достаточно большие простые делители. (Сильное простое - безопасное простое число p, для которого p-1 и p+1 имеют большие простые делители, которые, в свою очередь, имеют достаточно большие простые делители)

Если для Z/pZ каноническое разложение числа p-1=2q (т.к p -простое, то p-1 четное), где q - безопасное или сильное простое число, то взлом криптосистемы Эль Гамаля методами "baby step", "baby step giant step" становится весьма затруднительными, практически невозможными.

2. Атака одинаковых k

Предположим, что при отправке двух разных сообщений m и m' был использован один и тот же секретный ключ k. (Параметры p,g,h,x тоже одинаковые). Допустим, что злоумышленник каким-то образом смог получить информацию о первом сообщении m. Тогда

m: s1 = g^k mod p, s2 = m\*(h^k) mod p

m': s1' = g^k mod p, s2' = m'\*(h^k) mod p

Во-первых, s2'/s2= m'/m => m' = (s2'/s2')\*m, т.е мы спокойно можем получить информацию о другом сообщении, которое было передано с таким же k.

Во-вторых, если злоумышленник каким-либо образом вычислит k, то он сможет узнать и секретный ключ по формуле ... А это позволит не только расшифровывать все сообщения, но и подписывать сообщения.

Для того, чтоб избежать атаки такого типа, нужно для каждого сообщения M генерировать новый сеансовый ключ k.