RSA

# Trapdoor function

Идея: trapdoor функция f и ловушка t могут быть сгенерированы за полиномиальное время алгоритмом Gen. Тем не менее получить обратную функцию сложно, пока значение t не известно.

Если f – trapdoor функция, то существует такая секретная информация y, что имея f(x) и y легко вычислить x.

Функция выступает в роли замка, а секретная информация в роли ключа. Замок можно защелкнуть без ключа, просто нажав на защелку. Чтобы закрыть замок, нужен ключ. Ключ это trapdoor, а замок trapdoor функция.

См. работу Диффи-Хеллмана (1976г)

Trapdoor функции это набор односторонних функций