

Парадокс дней рождения и криптографические хэш функции.

1. Построить коллизию для функции $h(x) = MSB_n(STREEBOG(x))$.
(используя базовый алгоритм, основанный на парадоксе дней рождения)
2. Построить осмысленную коллизию для функции $h(x) = MSB_n(STREEBOG(x))$.
(используя итеративный алгоритм, основанный на парадоксе дней рождения)
3. Построить графики зависимости времени построения коллизии от n для алгоритмов из пунктов 1 и 2.

Условие на коллизию: коллизию образуют сообщения x_1 и x_2 , где x_i являются изображениями X и Y .

(X, Y выбрать на свой вкус. Например, X - кот, Y - собака)