Генерация ключей

Пусть $\underline{N_1 ... N_q}$ запись числа N в двоичной системе счисления. Будем искать ключи M так же в виде двоичной записи $\underline{M_1 ... M_q}$.

Рассмотрим ключи, которые первый раз отличаются от N в a-м бите, то есть $N_1 = M_1, N_2 = M_2, \dots N_{a-1} = M_{a-1}$ и $N_a \neq N_b$. Так как $M < N$, то $N_a = 1$ и $M_a = 0$. Таким образом, у M есть $q - a$ «свободный» бит, среди которых должно быть $K - b$ единичных, где b — число единичных бит на общем префиксе N и M. Это можно сделать C_{l-a}^{K-b} способами, где C_n^k — число сочетаний из n по k.

Таким образом, ответом на задачу является сумма C_{l-a}^{K-b} для всех a, для которых $N_a = 1$.

При заданных ограничениях число сочетаний можно было считать либо в длинной арифметике по формуле $C_n^k = \frac{n!}{k!(n-k)!}$, либо треугольником Паскаля по модулю 998 244 353.