Программа поддерживает работу в трёх режимах (предусмотрен как интерактивный метод выбора режима, так и через аргумент программы) :

- keygen – генерация открытого и секретного ключей.

  На вход подаются два параметра: n - длина сверхвозрастающей последовательности, b - битовая длина элементов этой последовательности, значения обоих параметров вводятся в интерактивном режиме.

  В результате работы создаются 2 файла: pk.txt – файл, содержащий открытый ключ (последовательность из n чисел, записанных через пробел), и sk.txt – файл, содержащий секретный ключ (последовательность из $n + 2$ чисел, записанных через пробел, первое число – число a, взаимно простое с N, второе – число N – модуль открытого числа, остальные – сверхвозрастающая последовательность из n элементов).

- enc – шифрование сообщения.

  На вход подаются открытый ключ и сообщение, записанные в соответствующих файлах (предусмотрен как интерактивный метод ввод имени файла, так и через аргументы программы). Зашифруется количество бит, равное наименьшему из количества элементов открытого ключа и битовой длины сообщения.

  В результате работы создаётся файл text.txt, содержащий шифр-текст в кодировке base32.

- dec – расшифрование шифр-текста.

  На вход подаются открытый ключ и шифр-текст (последовательность символов в кодировке base64), записанные в соответствующих файлах (предусмотрен как интерактивный метод ввод имени файла, так и через аргументы программы).

  В результате работы создаётся файл ctext.txt, содержащий возможное значение сообщения в UTF8-кодировке или выдаётся сообщение о невозможности декодирования.

Ссылка на код: `https://github.com/tanyarubtsova/Homework/blob/master/MHcrack/MHcrack.py`