Programming assignment. You are given an oracle-access to a function `dec(c)` that inverts the *RSA* (d, N) function: on input c it computes $m \equiv c^d \pmod{N}$ for all but one cipher text. We call this cipher text a challenge cipher text $C*$. The parameters $(N, e, d, C*)$ are fixed. You'll find all public parameters in the file `params.txt` . Your task is to decrypt the challenge $C*$.

To accomplish the task you should follow the instruction below (Important! You will need to have the GMP library installed on your machine (www.gmplib.org).

Instructions (for Linux):

1. Download the two files `dec.o` and `dec.h` from the web-page.

It provides the function

```
char *dec ( const char *c_inp )
```

that returns the decryption of a cipher text `c_inp` given as a string for fixed (d, N). You can also provide a cipher text of the `GMP` long int type by calling

```
char *dec ( mpz t *c_inp )
```

2. To use the above function, either create your own `.cpp` file and include `dec.h` as a header or download the template file `hw1.cpp` from the web-site. To compile this `.cpp`

file with the `dec.o` run in terminal

```
g++ hw1 . cpp dec . o -lgmp
```

Don't forget to link it with the `GMP` library!

3. As the result, you should get a .out file which you can then execute.

As this is an attack on a public key *crypto-system* and you are given e, you should implement the corresponding encryption function by yourself. You should submit both the resulting $m = dec(C*)$ and your code.