Introduction to Cryptography
Lab 2

1) *LCG as a PRNG:*
Given the following PRNG, used as a stream-cipher, defined by the following two functions:

```
InitializeSeed(s):
    seed = s
GetRandomNumber():
    next <-  (seed * 134775813 + 1) mod 2^32
    seed <- next
    return next
```

Also given:
   a) An encryption/decryption program *"encdec.exe"*
      i) Please launch to understand how it works (you may also try few examples)
   b) A ciphertext "*cipher.txt*"
   c) The 20th random number is 37193295

Decipher the 21th message and above.

2) Given the following PRNG, used as a stream-cipher, defined by the following two functions:

```
InitializeSeed(s):
    seed = s
GetRandomNumber():
    seed <-  seed * 1103515245 + 12345
    return (seed / 65536) % 32768
```

   a) Assuming you have the i-th random number, can you determine the rest of the used seeds in a manner similar to the first question?
   b) Assuming you know two consecutively generated keys A and B. Can you determine the used seed?

Requirements:

1) *encdec.exe* - an encryption/decryption program used in exercise 1
2) *cipher.txt* - an example cipher used in exercise 1