Introduction to Cryptography
Lab 1

1) *Two-time pad attack*
    a) Take two large texts (e.g. from Wikipedia) - save them as files in a pre-created directory (*m1,m2*)
    b) Normalize the file sizes (see *tools-instructions* below for further instructions)
    c) Create a random key (see *tools-instructions* below for further instructions) of the same size and save it as a file (e.g. *'key'*) within the pre-created directory
    d) Xor both files with the same key and save the output in two different files. You now have *c1 = m1 XOR k, c2 = m2 XOR k*
    e) Compute *c1 XOR c2*
    f) Try to extract some information regarding the original text from the result

Requirements:

1) Python3 (on a debian system, install using sudo-apt-get install python3)
2) Files Xor Script (See *moodle*)
3) Word Dup Script (See *moodle*)

Tools Instructions:

File size normalization - use *dd* tool as follows:
dd if=input_file of=output_file bs=1 count=desired_size

Random key creation - *use* https://www.random.org/bytes (choose save as a file option)

Hexadecimal Dump - Use *hexdump* tool as follows:
hexdump -C 'file'