Tutorial 4 - Bitwise operators and system commands.

Did you manage to solve last month's challenge problem? Here is the solution to compare with,

Challenge solution

```
#include <stdio.h>
#include <stdlib.h>
int newMask() {
  int mask = (double)rand()/RAND_MAX*254+1;
  return mask;
}

int main(int argc, char *argv[]) {
  int seed = 0xA3, mask = 0;
  char c;
  FILE *inputFile = 0, *outputFile = 0;

  srand(seed); /* Set the seed value. */

  /* Check the number of arguments */
  if(argc!=3) {
    printf(" Usage: %s <input file> <output file>\n",argv[0]);
    return 1; /* Report an error */
  }

  inputFile = fopen(argv[1],"r"); /* Open the input file. */
  if(!inputFile) return 2;

  outputFile = fopen(argv[2],"w"); /* Open the output file. */
  if(!outputFile) return 3;

  c = fgetc(inputFile); /* Get the first character. */

  /* Loop until end-of-file is reached. */
  while(c != EOF) {
    mask = newMask(); /* Get a new mask value. */
    printf("mask = %d\n",mask);
    c ^= mask; /* Exclusive-OR with the mask. */
    fputc(c,outputFile); /* Write to the output file. */
    c = fgetc(inputFile); /* Get another character. */
  }

  /* Close the files. */
  fclose(inputFile);
  fclose(outputFile);

  return 0;
}
```

The solution uses a new mask to encrypt each character. The numbers returned from newMask follow a series, which is repeatable for a given value of the input seed. Therefore, the encryption key is the random number seed.