Travis Allan
2/4/2016
CSCE 4050
Homework 1
Stream Cipher Design

For my stream cipher, I'm choosing to do a manipulation of each individual character such that there can be only one corresponding character in the key, thereby creating perfect secrecy. This could be considered as a modified version of the one time pad(OTP).

The process starts with converting each character to a number that correlates to that character: (other characters not listed here and numbers will not be permitted as this program is designed to only encrypt sentences.)

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
25	0	24	1	23	2	22	3	21	4	20	5	19	6	18	7	17	8	16	9	15	10	14	11	13	12

	.	,	?	!	;	:	“	(	)
26	27	28	29	30	31	32	33	34	35

Next, we multiply each number by a prime number: 23 for this example
In the program the prime number will be randomly chosen from a pool of primes.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
575	0	552	23	529	46	550	69	525	92	460	115	437	138	414	161	391	184	368	207	345	230	322	253	299	276

	.	,	?	!	;	:	“	(	)
598	621	644	667	690	713	736	759	782	805

Finally, we shift each number: 5 for this example
In the program, the offset will will be a random number between 1 and 9.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
570	-5	547	18	524	41	545	64	520	87	455	110	432	133	409	156	386	179	363	202	340	235	317	248	294	271

	.	,	?	!	;	:	“	(	)
593	616	639	662	685	708	731	754	777	800

Now, we have a key that is completely different from its original form and a challenge to trace back to. I think it's important to note that this is only perfect in theory and can be easily traced back once the key formula "(([, a, b,…z] => [0, 1, 2,…26]) x prime) - number" is discovered.

Important Information:

- The key size for this cypher is 36 characters, as seen in the charts. Please do not use any other characters than the ones listed.
- The message can be anywhere from 1 to 2000 characters long. If you would like it to be bigger, you will need to change the buffer size, as well as all of the for loops that have 2000 as their limit.

Running the program:

This program was written in C++.

- To run it, just type "StreamCypher.cpp" and hit enter, and then type "./a.out" and hit enter.
- The program reads from a file called "input.txt", and outputs to "output.txt"
- The program will print the Prime used, followed by the offset value, onto the screen.
- To change the list of primes, change the information in primes.txt; however, be sure to change the prime buffer's capacity to the new number of primes.

Special notes:

- The file "output.txt" has each character printed in order, on individual lines, starting from the top.
- The program will return 1 if it ran successfully and 0 if there was an error.