

P and Q are prime numbers. If you enter a number that is not prime for P or Q, the next larger prime number is displayed.

$N = PQ$ and $(P-1)(Q-1)$ are calculated from P and Q.

E is a positive integer relatively prime to $(P-1)(Q-1)$. If you enter a number for E that is not relatively prime to $(P-1)(Q-1)$, the next larger number that is relatively prime is displayed. By default, the smallest integer relatively prime to $(P-1)(Q-1)$ is displayed.

To use the program, choose parameters P, Q, E. The program calculates D. Publish N and D, keep E secret.

Enter a message in plaintext and push the Encrypt button. The message is converted character-by-character into ASCII code and translated into binary. Characters are grouped two at a time to form blocks. Blocks are transformed by raising the numerical value of the block to the E power modulo N. Often the ASCII code for the result does not consist of printable characters, so it shows on the display as a blank or as an empty rectangle. .

- 1) Encrypt several test messages to see how ASCII code works. Try consecutive capital letters (e. g. "ABCDE"), consecutive lower case letters, and consecutive numbers to see how it works.
- 2) Check out the conversion from ASCII to binary;'. It is nothing tricky. I will show you how it works if you don't see the pattern.
- 3) Observe how two characters are encoded in the same block. What happens at the end when there is a plaintext message of odd length?
- 4) Use your calculator to verify the $T^E \pmod N$ encoding for a "small" block or two. You need to calculate T^E , divide by N, and report the remainder. Note that you don't need to know P, Q, or D to encode the message, but if you happened to know P as well as N you could calculate Q easily, find D, and decode the message at will.
- 5) For decryption the process is reversed. With the same parameters P, Q, and E the original message is recovered. Push the Decrypt button to see how the original message is reconstructed step by step.
- 6) With default parameters decrypt the secret message 12126 3036 26912 40701 3865 2767. Pay attention to the spaces to separate blocks.
- 7) With $P=569$, $Q=379$, and $E=11$ try to decrypt the message above. Gibberish, right? Try the message 47979 137307. It was encoded with those parameters.
- 8) If the primes are too small the process as laid out doesn't work because there aren't enough residues mod N to represent the codewords. Get N above about 40000 and there won't be any problems. Try some small values for P and Q and see what goes wrong.
- 9) A stupid spy publishes $N = 12007001$ and $E=7$. Find the obvious factorization of N and use it to decrypt the "secret" message 3973692 165810 6506132 5228823 11249839 4543968