CIPHER NAME: **nbXOR^{80}**

CHARACTER SET (in order):
`~1!2@3#4$5%6^7&8*9(0)-_=+qQwWeErRtTyYuUiIoOpP[{]}\|aAsSdDfFgGhHjJkKlL;:’”zZxXc
CvVbBnNmM,<.>/?
SOURCE: The 95 printable characters available on a US 101-key keyboard starting in the top left no shift and then shift, ending in space, with no tab or enter

BLOCK SIZE: 80 columns (exclusively from defined character set) **PAD CHARACTER**: “ ”

NON-BITWISE EXCLUSIVE OR: An anomalous function derived of defining text as positions in the character set array and applying non-standard Modular arithmetic to mimic results similar to binary exclusive OR (XOR) functionality. AKA using string manipulation and simple arithmetic to provide for a substitution mechanism that is reversible by nature of providing one of the original values to determine the other based on the final value.

JOIN FUNCTION: The product of two 80 column lines combined to one 80 column line by a one-for-one non-bitwise XOR (nbXOR) of the respective columns.

MIX/UNMIX FUNCTION: Write-ahead substitution based on the non-bitwise XOR of the character set. The input is “space”-padded to 80 characters. The function starts with the first column and writes the nbXOR of the first + second column in the second column. The process continues to the right from there until the last column is nbXOR’d with the first column. This is defined as a round. There shall be 80 rounds.

STIR/UNSTIR FUNCTION: Write behind substitution based on the non-bitwise XOR of the character set. The function starts with the first column and writes the nbXOR of the first + second column in the first column. The process continues to the right from there until the last column is nbXOR’d with the first column. This is defined as a round. There shall be 80 rounds.

ENCRYPT/DECRYPTION FUNCTION: The encrypt function consists of a combination of:

1. passphrase and message text enter the algorithm
2. the passphrase sent into keyhash to produce three product keys
3. the plaintext is divided into 80 character blocks padded with spaces if needed
4. the first block is joined with the 3rd hash of the passphrase (key#3)
5. the mix function is applied
6. the mixed data is then joined with the 1st hash of the passphrase (key#1)
7. the stir function is applied
8. the stir result is then joined with the 2nd hash of the passphrase (key#2)
9. If there is not more data, the function terminates after writing the ciphertext.
10. If there are additional blocks
    a. key#3 is replaced using the join of cipher and plaintext from above
    b. and the process is repeated from step 4 for the next line.