**5: Vernam Cipher System Proof**

Given plaintext X and key Y in bits, there is a ciphertext Z such that X ⊕ Y = Z, and Z ⊕ Y = X using two’s complement and bitwise XOR.

Let X = 1 0 1 1 and Y = 1 1 0 0,

Then, X ⊕ Y = 1 0 1 1 ⊕ 1 1 0 0 = 0 1 1 1 = Z. [Bitwise XOR, Two’s complement]

With Z = 0 1 1 1,

Z ⊕ Y = 0 1 1 1 ⊕ 1 1 0 0 = 1 0 1 1 = X. [Bitwise XOR, Two’s complement]

Since (X ⊕ Y = Z) encrypts X to give Z and (Z ⊕ Y = X) decrypts Z to produce X using key Y, the above statement is true, and therefore, Vernam Cipher System does work.