HW #1 : CST 407

5). Gilbert Vernam devised a simple system that encrypts and decrypts by bitwise XOR of the text and key. Provide a proof that this system works. It should be mathematicab based and targeted towards a CST 130 student.

Let: P = Plaintext
C = cipher
k = key

Here I will demonstrate with boolean algebra that $\boxed{P = C \oplus k}$

Starting with the basic fact that

$P \oplus k = C$

$P \oplus k = C$ ← xoring P with k will create the cipher

$(P \oplus k) \oplus k = C \oplus k$ ← Property of equality

$P \oplus (k \oplus k) = C \oplus k$ ← associative property

$k \oplus k = \bar{k} \cdot k + k \cdot \bar{k} = 0$ ← complement axiom

$0 + 0 = 0$

$P \oplus 0 = C \oplus k$

$\bar{P} \cdot 0 + P \cdot \bar{0} = C \oplus k$ ← definition of XOR

$\bar{P} \cdot 0 = 0$ ← null elements axiom

$0 + P \cdot \bar{0} = C \oplus k$ ← can omit 0 (Identity)

$P \cdot \bar{0} = C \oplus k$ ← $\bar{0}$ is 1

$P \cdot 1 = C \oplus k$ ← identity

$P = C \oplus k$ ✓