last name **first names** **id#**

cmput 210 W2016 **quiz 1** **45 min** **no devices** **closed book** **page 1/1**

1. Perform the first substitution recommended by Al Kindi on this ciphertext (you need not crack it) :

   `b p i b k i b p i l b p q z b g p i b a`

   `_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _`

   Explain why this method cannot be followed blindly (at most 15 words).

   •

2. Encrypt the text below using Vigenere cipher with keyword `arc`.

   `plaintext: i n d e c h i f f r a b l e`

   `ciphertext: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _`

   • The telegraph resulted in the popularity of the _____ cipher: security was needed because messages were easy to _____; this cipher was more secure than the _____ cipher, but easier to use than the _____ cipher.

3. Give Singh's two motivations for writing *The Code Book* ($\leq$ 15 words each):

   •

   •

4. Kerchoff says to assume this when discussing cryptosystem security ($\leq$ 15 words):

   •

   Some gave this numerical argument that the substitution cipher was unbreakable ($\leq$ 15 words):

   •

5. Encrypt with Kama Sutra key `ab cd ef gh ij kl mn op qr st uv wx yz` .

   `plaintext: i d o n o t l i k e g r e e n`

   `ciphertext: _ _ _ _ _ _ _ _ _ _ _ _ _ _ _`

   Crack this Caesar ciphertext `l g z t o a w z e d` .

   •