Cpt S 450 Homework #10

Please print your name!

1. First read the notes. Now, this is what you know:
my public key: $(e = 49, n = 10539750919)$,
the baby-ASCII-table,
the cipher text: ITG!AAEXEX IRRG!IGRXI OIXGEREAGO
Tell me what is the plaintext? and HOW did you get it? (It is ok if you download some tools from the Internet to break the code)

2. Read Huffman code algorithm from the text or from the Internet. Recall that the algorithm is to code a word in bits (i.e., a binary tree is constructed). Now, we use digits instead of bits, can you design a Huffman code algorithm?

3. Try to read from the Internet and summarize (in half page) on current techniques in finding whether a cryptographic protocol has a flaw or not.