1. My Public key = ($e=49$, $n = 10539750919$)

1 2 3 4 5 6 7 8 9 0
Baby ASCII - A E G I O R T X ! &

Ciphertext = ITG!AAEXEX IRRG!IGRXI OIXGEREAGO

$C1 = 4739112828$ $C2 = 4663943684$ $C3 = 5483262135$

What is plain text? And How did you get it?

I used an online tool to calculate $p = 43481$ and $Q = 242399$, before following the steps outlined in the notes, and writing my own very basic C-program to do the harder calculations. I've shown the major steps below:

$(e \cdot d) \% (p-1)(q-1) = 1$. Using my C-program, $D = 3226366849$

$M_1 = (C_1^d \bmod n) = (4739112828^{3226366849} \bmod 10539750919) = 36217$

$M2 = (C_2^d \bmod n) = (4663943684^{3226366849} \bmod 10539750919) = 98483$

$M3 = (C_3^d \bmod n) = (5483262135^{3226366849} \bmod 10539750919) = 57847$

//Using my C-program to do the large calculations.

Plaintext = GREAT!XIXGOTXIT

2. Now, we use digits instead of bits, can you design a Huffman code algorithm?

Huffman coding is a lossless data compression algorithm. First, you create a huffman tree, and then traverse it to find code. Yes, if we use digits rather than bits, we could still design a Huffman code algorithm. Rather than encoding the string into bits, we can encode the string into ASCII value numbers and perform searches the same way as a normal Huffman code algorithm using bits. The only change would be the amount of memory required to store the Huffman tree.

3. Summarize (half-page) current techniques in finding whether a cryptographic protocol has a flaw or not.

There is an automated cryptographic protocol verifier developed by ENS called ProVerif. This verifier tool takes a protocol script as input and can automatically prove secrecy, authenticity, and equivalences. It works by translating the protocol into Horn clauses and determines whether the desired security properties are true by the clauses. This is one of the many tools currently available for determining if a cryptographic protocol has a flaw or not. These tools have gotten very accurate over the years and are very reliable to finding whether a protocol has a flaw or not.