MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough
gpete at utsc dot utoronto dot ca

Homework Assignment 1 (Due Feb 8 Tue)

Don't just give the answers, but indicate clearly the arguments you have followed.

Problem 1. What is 49^{-1} (mod 50)? And (mod 700)? And (mod 701)? **(3 pts)**

Problem 2. Show that if $\gcd(a, n) = 1$ and $a \mid mn$, then $a \mid m$. **(2 pts)**

Problem 3. Find all integer solutions (x, y) to $1234x + 5678y = 910$. (Do not forget to argue that those you have found are all the ones.) **(4 pts)**

Problem 4. Suppose a language has only 3 letters, a, b, c, with frequencies .7, .2, .1, and not much dependence between neighbouring letters in a typical text. The ciphertext "ABACABCBBB" is encrypted with Vigenère (mod 3). You are told that the keyword length is 1,2, or 3. What is the most probable keyword? **(2 pts)**

Problem 5. Alice regularly sends quotations from her favorite Zen master Shunryu Suzuki to Bob, always encrypted with a Hill cipher, using the same 3×3 matrix (mod 26). Eve has been following the messages for a while, and since "BKJDBC" and "SSFUSY" are the two most frequent segments in the ciphertexts, she guesses that the first stands for "Buddha" and the second for "Suzuki".

(a) What is the key matrix used by Alice? **(1.5 pts)**

(b) What does the ciphertext "WNA TAU CEL LUC SLS SPE SYK NSY NSZ OSR THO TWK VCQ WNU NOW IDP AHI ANP EZH AHI" mean? (This is a bit long to do by hand, so if you get bored, then either use a computer program (Mathematica, Maple, Matlab, C) to do the matrix multiplications, or just decode the first few words.) **(1.5 pts)**

Problem 6. An LFSR sequence generated by a length 3 recurrence starts 001110. What is the next element of the sequence? **(2 pts)**

Problem 7. Consider an Enigma machine with 3 rotors with known wirings and with a plugboard with 6 pairs of plugs. (See Section 2.12 in the book.)

(a) In the computation of the size of the keyspace, the book has a factor 100391791500 corresponding to the 6 pairs of plugs. Why is this the correct number? **(2 pts)**

(b) Does Enigma have Shannon's diffusion and confusion properties? **(2 pts)**

(Max possible score: **20 pts**)