Tutorial 1

1. Calculate 1 / 8 mod 11 (the inverse of 8) by hand using the equation subtracting algorithm. Use your result to calculate 5 / 8 mod 11.

2. Calculate gcd(7403, 4653) by hand using Euclid’s remainder algorithm.

3. Calculate 5 ^ 7 mod 11 by hand using repeated squaring and the homomorphism theorem. (5 to the power 7 mod 11). Verify that the calculations would be much harder if you left the mod 11 calculation to the end.

4. Define the term "The entropy of a set of messages" and show how it can be calculated. A language contains 5 symbols: A, B, C, D and E. A, B, C each occur ¼ of the time, while D and E occur 1/8 of the time. What is the entropy of this language?

5. Define the term "unicity distance." What information is needed to calculate it, and how useful is the concept of unicity distance? A newly invented language has 16 different symbols in its alphabet and is quite precise. On average each letter in the alphabet conveys 2 bits of information. A message in this language is encrypted with an 8 character key. It is known that users will choose English language keys all in lower case. What is the unicity distance of these encrypted messages?