Tutorial 1 Solutions

1. *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.*

5 ^ 7 mod 11
5^2 = 25 == 3
5^4 = 3^2 = 9
5^6 = 5^2 * 5^4 = 3 * 9 = 27 == 5
5^7 = 5^6 * 5 = 5 * 5 = 25 == 3

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

```
remainder

7403 % 4653 = 2750
4653 % 2750 = 1903
2750 % 1903 =  847
1903 %  847 =  209
 847 %  209 =   11
 209 %   11 =    0
```


3 *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.*

11x = 11
 8x = 1
 3x = 10

 8x = 1
 3x = 10
 5x = -9 == 2

 5x = 2
 3x = 10
 2x = -8 == 3

 3x = 10
 2x = 3
  x = 7

check: 8 * 7 = 56 == 1

5 / 8 = 5 * 7 = 35 == 2.

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?*

3 * ¼ * 2 + 2 * 1/8 * 3
= 3/2 + ¾
= 9/4

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?*

unicity distance = H(K) / D
H(K) = 8 * 1.5 (¾ for English) = 12
D = R – r = 4 – r = 2

So unicity distance = 12 / 2 = 6.