Exercises E2: Viginere, Kasiski, Friedman

August 31, 2006

1 From *Making, Breaking Codes* by Paul Garrett

Original problem numbers in parens. Optional, DOUBLE and TRIPLE point scores. Garrett has appendix of problem answers.

1. Show that for m and n relatively prime and both > 2 the number of length mn keys is "lots" bigger than the number of length m keys times the number of length n keys. (4.1.05)

2. (Optional) Why is there no point to multiple-round Viginere encryption with all keys of the same length? (4.1.06)

3. Find the least common multiple of 24 and 36. (4.2.07)

4. Find the greatest common divisor or 51051 and 55913. (4.2.10)

5. Suppose (falsely but simply) that all 26 characters occur with equal probability in a character stream of length N. For a positive integer m, what is the probability (as a function of m and N) that no two identidcal characters occur any multiple of m apart? (4.3.01)

6. Referring to the previous exercise, if we concede that some letters are more likely to occur than others, does this increase or decrease the probability that no two identical ones will occur at a multiple of m apart? (4.3.03)

7. Why would it be silly to apply the Kasiski attack to the encryption of a plaintext consisting of a stream of 'random' characters? (4.3.05)

8. DOUBLE POINTS. If we apply the Kasiski attack to a plaintext, what does the outcome mean? How can the Kasiski attack tell that a text is encrypted? (4.3.08)

9. (Optional) What is the expected number of heads (before any tail comes up) as a result of tossing a coin that gives heads 3/5 of the time? (4.4.07)

10. What is the expected number of coin flips before a head comes up (with a fair coin)? (4.4.08)

11. What is the expected distance between two 'e's in a random character stream where 'e's occur 11% of the time? (4.4.10)

12. (Optional) DOUBLE POINTS. Choose two real numbers 'at random' from the interval $[0, 1]$. What is the expected value of their product? (4.4.14)

13. Consider an alphabet with just two characters, '0' and '1', and a language in which these characters occur with respective probabilities 2/3 and 1/3. Say that a stream of '0's and '1's is *random* if the '0's and '1's each occur with probability 1/2. Define an index of coincidence $I(y, z)$ for same-length character streams y, z of '0's and '1's. (4.5.01)

2 From Trappe and Washington

Section 2.13
Exercises: 10, 11, 12.