CS290, Cryptanalysis, Spring, 2013, Homework 2

John Manferdelli

1. We learned that a 10 bit key generator that produced a 0 with probability .8 and all the other 10 bit strings with equal probability let attackers break a cipher in time ~$2^{2.7}$ instead of 2^{10}. Now that you know this, as the defender, how would you use this key generator in a safer manner? Later in the term, we'll learn some techniques for using an m bit entropy generator (m<n) use it to generate keys with n bits of entropy.
2. We'll learn techniques to defend against Mallory's one time pad attack in a few weeks. In the meantime, can you suggest ways, using only the one time pad primitive, of making the bank transfer safer?

Refer to the notes for the second lecture for the remaining problems.

3. Compute the 26 possible permutations realized by rotor II.
4. Carefully compute the running time of the attack used in the "method of batons" using the "probable word" method.
5. In WWII computing devices could operate at about 1 operation per millisecond. If Enigma was really 67 bits strong, how long would it take and adversary to break messages? (State your assumptions)
6. Prove H(X,Y)= H(Y)+H(X|Y) and H(X,Y)≤ H(X)+H(Y). Under what conditions (on X and Y) with the inequality in the second statement become an equality?