Crypto Homework 1: Blocks and Streams

Jeremy Rodgers

# Question 1

There are a few reasons why a block cypher with an 8 bit block are easy to break with a plain text attack. First, involves the property of block cyphers that the size of the cypher text is equal to the size of the plain text. As a result, the attacker knows the length of the message. Next, our block size happens to be very poorly chosen because 8 bit blocks happen to match the length of a character. Therefore, although each block goes through a series of substitution, shifting and xoring steps (implementations vary) the output of the cypher text will be the same for each character. Therefore, if the attacker knows the plain text of a message encrypted using the same key, the hacker will be able to easily decrypt other messages encrypted using the same key. This would be very similar to breaking a Cesar Cypher, although a more difficult as we are doing more than just shifting characters in our encryption.

# Question 2

1. Even if the attacker can’t decrypt blocks, they can still gain information about the message. In particular, if plain text message blocks contain duplicate information, they will become duplicate cypher text. For example, if the block size was right, the word the could get encrypted to abc over and over again. This could reveal information about the plain text even if the plain text is not decoded. For example, if the table had office salaries, the eavesdropper might be able to tell ( under the right circumstances) if multiple people had the same salaries or if salaries varied. Or more likely the structure of a document such as how many times a certain word repeats.
2. A malicious attacker can change the message Bob receives from Alice without decrypting the message in a few ways. First, if proper care isn’t taken, block cyphers are susceptible to bit flipping attacks. This means that a flipped bit in the cypher text would equate to a flipped bit in the plain text. Additionally, the attacker could rearrange, move, or delete blocks of the cypher text and it would result in a change to the plain text. If Bob doesn’t authenticate the message he has no way of knowing that the message he received is unchanged from the message he received from Alice. This is especially dangerous if the attacker knows the format of the underlying message because the attacker could strategically flip bits and alter the message Bob receives in an even more malicious way. For example, if the table being sent was a table of salaries, Mallory could increase her salary without Bob knowing.
3. To mitigate and prevent the above attacks, I’d modify the strategy from the Electronic Code Book Mode to the Galois Counter Mode. First, instead of using the same cypher, I would use a different cypher with each code block. This will prevent an eavesdropper from obtaining information about our data just by looking at the structure of the cypher text. We can do this by using a counter. We will take a counter (first message 1, second message 2 and so on) and or it with an initialization vector(IV) which we can then send to Bob in plain text. Then we’ll pass the IV || counter through the block cypher. This should give us a unique value that we can use to xor our plain text message against to produce our cypher text. Additionally, we need a way to authenticate our message to help protect against bitflip and other attacks that modify the cypher text without Bob knowing. To achieve this, we’ll send a message authentication code (MAC) to enable bob to detect whether a message has been tampered with or not.