Lindsay Haslam
CS6014
2/18/2024

Blocks and Streams

Question 1

Step 1: The first step is to collect enough pairs of plaintext and corresponding ciphertext.
Step 2: Analyze the encryption pattern. For each pair of plaintext-ciphertext, note how each plaintext byte is transformed into its ciphertext counterpart.
Step 3: Create a substitution table. Using the collected pairs, create a substitution table that maps every plaintext byte to its corresponding ciphertext byte.
Step 4: Decrypt the entire cipher text.
Step 5: Handle incomplete mappings. If your known plaintext doesn't cover all 256 possible byte values, you might not be able to decrypt portions of the ciphertext that use unmapped values.

Question 2

Part A

An eavesdropper can recognize patterns, which can help make inferences of the specific lettering or representation of the repeated blocks. They can also recognize message length, which would help them recognize the type of message or information being sent between parties.

Part B

The eavesdropper can reorder the blocks of the cipher text. A message that’s been reordered can alter the message will still qualify for a valid decryption on Bob’s end. They can also replace the blocks with different messages that still match the encryption key. An eavesdropper can also duplicate or delete blocks so that the overall message is unreadable.

Part C

You could implement cipher block chaining or counter modes so that there are dependencies between the blocks, so encryption of each block depends on the previous one.