Author: Brian Erichsen Fagundes

CS6014; MSD; UofU
Spring semester - 2024
Crypto Homework
Homework 4 - Blocks & Streams

Question 1

A block cipher with an 8-bit block size is very easy to break with a known-plaintext attack (assuming each block is just encrypted independently with the same key). **Describe how you would do so.**

Know-Plaintext-Matching: Since the known plaintext is only an 8 bit block cipher, it means that there are only 256 possible input values from (2^8). With known-plaintext; if I were an attacker, I could **create a table** mapping each possible plaintext block to its corresponding ciphertext block since the encryption process here is deterministic.This would create some sort of dictionary for the encryption function. Once a table is created; I could use the **table to look up** the cipher blocks for any given plaintext blocks and since the same key is used then that table can decrypt any ciphertext by finding the corresponding entry for that block in the table.

Exhaustive Search: Through analysis of decrypted blocks and patterns in the key space; the attacker could recover the encryption key used in the ciphers.

In summary, given the small block size of 8 bits, the key space is very limited and an exhaustive search becomes feasible.

Question 2

Assume you're sending a long message using a block cipher (like AES) with the following scheme: split the message into block-sized chunks, then encrypt each with the same key. Basically Alice sends Bob AES(m1, k), AES(m2, k), AES(m3, k), etc.

- Part A: **Even if they can't decrypt blocks, what information can an eavesdropper discern from this scheme?** Hint: Imagine that Alice is sending a table of data where each cell is exactly one block of data.

Even if an eavesdropper cannot decrypt blocks, they can still observe and discern some crucial information and patterns. Take into consideration that repetition is likely to happen since each block is encoded with the same key which can lead to figuring out specific blocks of message without knowing the actual content of the messages. An eavesdropper can

also determine the type of communication based on the number of block ciphers if a specific type of communication has a fixed length.

Part B (4 points): **Things are actually even worse! A malicious attacker can actually CHANGE the message that Bob receives from Alice (slightly). How?** This is particularly bad if the attacker knows the structure of the data being sent (like in part A).

if an attacker knows the structure of the data being sent then the attacker can perform block replacement attack, block substitution attack; among other types of attacks.

In block substitution; the attacker intercepts encrypted messages and replaces certain blocks with different blocks of their choosing. Since the blocks are encrypted with the same key, the attacker does not need to know the specific key, they only need to manipulate and change the ciphertext.

In block replacement attack; the attacker can reorder blocks of ciphertext without affecting the decryption. In this replacement, a given attacker leverages its understanding of the data to make targeted modifications. These attack tactics can lead to severe implications since the intended message has its structure changed; specially when a given message has a predefined structure.

- Part C: **How could you modify the scheme to mitigate/prevent these types of attack?**

To enhance the security of the scheme and mitigate potential attacks, it is crucial to use authenticated encryption modes such as AES-GCM or AES-CCM which encrypt and provide integrity protection by ensuring that ciphertext has not been tampered. AES (Advanced Encryption Standard) algorithms involves several key steps, including the use of subBytes where each byte of the blocks is substituted with another byte; the use of shift-rows where the rows of the blocks are shifted by different offsets; the use of mix-columns where columns of the block are mixed to provide diffusion and the use of Add-Round-Key where the block is XORed with the round key derived from the original encryption key.

In the current scheme, where each block of the message is independently encrypted with the same key, an attacker could possibly exploit the lack of integrity protection by performing block replacement attacks. By adopting authenticated encryption modes, a defender ensures that any authorized modifications to the ciphertext are detected.

Authenticated encryption modes usually incorporate additional authentication tags that are calculated based on the ciphertext and a secret key. These tags serve as a cryptographic check that allows the recipient to verify the integrity of the received ciphertext; if any alterations have occurred during transmission, the authentication check will fail, indicating potential tampering.

Programming Part 1: A (bad) block cipher

- Try modifying 1 bit of the ciphertext and then decrypting with the correct passwords. What do you see?

When I tried to modify 1 bit of the ciphertext and then decrypt with the correct password; the decrypted message was different from the original message. This shows that even minor changes in the message causes significant alteration in the decrypted message.

Programming Part 2: RC4 Cipher

- What do you expect to see if you xor the two encrypted messages?

Encrypting two messages using the same keystream in a ciphertext, like CR4, is usually insecure. This happens because if two messages are encrypted with the same key and the same keystream, an attacker can perform a bitwise XOR operation on the ciphertext of the two messages that leads to XOR of the original messages.

I expect to observe certain patterns and vulnerability due to key repetition when XOR the two encrypted messages. For instances; from the two messages that are encrypted where each encryption is message XOR keystream; when we XOR the two ciphertext together we get ciphertext1 (message1 XOR Keystream) XOR (message2 XOR Keystream) where Keystream XOR Keystream cancels each other which leads to message1 XOR message2. This reveals the bitwise XOR of the original messages, providing potential information about the content of both messages. An attacker could analyze the patterns and frequencies of XOR results to make educated guesses about the content of the original messages.

I also would expect to see a series of null bytes if the both encrypted messages are identical since each byte XORed with itself is 0.