Crypto Homework 1: Blocks and Streams

Muyuan Zhang

2023-03-01

Question 1

A block cypher 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.

- If we know for sure that some words appeared in the ciphertext message, then we could have determined the (plaintext, ciphertext) pairings for the letters involved and create a substitution table. If we have recorded all of the ciphertext transmissions, we can find the decrypted version of one of the transmissions.

Question 2

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

a Even if they can't decrypt blocks, what information can an eavesdropper discern from this scheme?

- That the plaintext content of a pattern is the same as that of another duplicate pattern.

b Things are actually even worse! A malicious attacker can actually CHANGE the message that Bob receives from Alice (slightly). How?

- Misplace the known patterns in the cipher text, swap or delete the blocks by flipping some of its bits to tamper the message.

c How could you modify the scheme to mitigate/prevent these types of attack?

- Cipher-Block Chaining - mix some randomness into the ciphertext so that identical plaintext blocks produce different ciphertext blocks.
- RSA algorithm - makes extensive use of arithmetic operations using modulo-n arithmetic.
- Session Keys - use RSA in combination with symmetric key cryptography.