CS 601.414 Cryptography

Tuesday, February 25, 2025 15:44

* 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.

- $2^8 = 256$ possible keys (0-255)
- Solution: try every single key til we find the right one
  ↳ Brute Force!
- Obtain know plaintext-ciphertext pairs
- For each possible key, encrypt the known plaintext using the block cipher and check if result equals corresponding ciphertext
- Confirm key be encrypting rest of plaintexts and comparing them to corresponding ciphertexts

* 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.

- "Deterministic nature" of encryption scheme
  ↳ same plaintext block always encrypts same ciphertext block

1. Patterns
   - since message is structured (each cell = 1 block), eavsdropper can identify repeated patterns in cipher text
2. Analyze frequency
   - Eavesdropper can start to infer meaning based on frequency of cipher text block
3. Message Length
   - Eavesdropper can determine exact length of the message in blocks
     This can reveal content (large message → probably large dataset)
4. Structure of data
   - if eavesdropper knows structure, structure of plaintext can be infered

PART B

- Things are actually even worse! A malicious attacker can actually change the message that Bob recieves from Alice (slightly). How? This is particularly bad if the attacker knows the structure of the data being sent (like in part A)
- So if the attacker knows the structure is a table with specific values in certain positions, they can replace cipher text blocks with ones they have already seen
  ↳ Block substitution
- Also if they know a specific ciphertext block that corresponds to a valid plaintext, they can insert that block into a different spot in the message
  ↳ Replay Attacks
- The attacker can change specific blocks which then changes the meaning of the message
  ↳ Partial Message Manipulation

PART C

- How could you modify the scheme to mitigate/prevent these types of attacks?

- Randomness! and Integrity Protection
  - Initialization vector — combined with plaintext BEFORE encryption
    so if the same plaintext block will encrypt to a different cipher text block, each time
  - Cipher Block Chaining also encrypts different ciphertext blocks but by XORing each plaintext block with previous cipher text block but before encryption
  - Message Authentication Code: Appends to message
    : computed using cryptographic hash function and secret key
    : Bob can verify integrity and also see if there was any tampering