Recitation 3/2/18 – Lesson Plan

Jonathan Frankle

Agenda

- Questions
- Review content on block ciphers
- Discuss the design of AES in more detail
- Cipher modes of operation
- Explore the process by which AES came to be

Review of Block Ciphers

- A block cipher takes a fixed-length key and a fixed-length input and produces a fixed length output (typically of the same size as the input)
    - We'll deal with variable-length input in a little while.
- What properties must a block-cipher have?
    - It must be invertible
    - It must be "secure." How is secure defined?
        - Ideal cipher model: for every key, a cipher is a random function from its inputs to its outputs. Clearly this would be bit to use in practice.
        - In general, so long as the key is secret, the attacker shouldn't be able to find any patterns in the output of the cipher that reveal information about the key or input.
        - Cryptanalysis: people should work very hard to try to break it. If they fail, that's a good thing. (People usually attack a small number of rounds of the cipher, and the cipher is given a number of rounds such that it can't be broken with known techniques, plus a safety margin)
        - Statistical tests
            - Output is indistinguishable from random.
            - Flipping one bit of the key or plaintext flips half the bits of the ciphertext in a random-looking way.
    - It is efficient. In software? In hardware?
    - It is easy to implement?
- How are block ciphers designed?
    - Feistel structure
        - Link to the SPECK cipher, which uses a variation on the Feistel cipher.
    - Confusion/Diffusion model.
        - Show the stick figure guide to AES

Cipher Modes of Operation

- Key question: how do you use a cipher on a message that is longer than its block size?
- Idea 1: Pick a cipher and use the key for each block independently.
    - Called “electronic codebook” (ECB) mode.
    - Problem: Encrypting the same block twice yields the same output.
    - See a visual representation of this problem on Wikipedia.
- Idea 2: Just use a different key for every block.
    - Incredibly inefficient.
- Idea 3: Cipher block chaining. (CBC)
    - Start with an initialization vector. XOR that with the first block of the message. Run the result through the cipher to get the output of the first block.
    - Use the output of the first block as the initialization vector for the second block.
    - Benefits: No two encryptions of the same block will look different.
    - Downside: If part of the message is corrupted, the whole message is impossible to recover.
- Idea 4: Cipher feedback mode (CFB)
    - Encrypt the initialization vector with the block cipher, then XOR it with the first plaintext block to get the first ciphertext block.
    - Encrypt the first ciphertext block with the key, then XOR it with the second plaintext block to get the second ciphertext block. Repeat.
    - You’re essentially generating a long sequence of bits that you XOR with the plaintext to get the ciphertext. Like stretching the key. The plaintext also affects the pattern of these bits.
- Idea 5: Output feedback mode (OFB)
    - Compute E(IV). The output of the first block is E(IV) xor Plaintext block 1.
    - To compute the next block, compute E(E(IV)) and do the same.
    - Essentially, use the cipher and key to generate a string of bit. XOR those bits with the plaintext to get the ciphertext.
    - This turns a block cipher into a “stream cipher,” which we will discuss later in the course.
- Idea 6: Counter mode (CTR)
    - Generate the bits to XOR with the message by repeatedly encrypting arbitrary values.
    - Usual case: encrypt the numbers 1 through n, where n is the number of blocks.
    - You can’t repeat an input. This is why using numbers in order is a good choice.
    - Benefit: highly parallelizable.

Developing an Encryption Standard

- Discussion: What should the process look like for developing a good cryptographic standard?
    - How do you do it in a way that is resistant to inserting back doors?

    - How do you prove to the public that no back doors were inserted?
    - How do you ensure the cipher is secure?
- Example: Report on the Development of AES
    - Work though the report to show how the process worked, what NIST was looking for, etc.