Massachusetts Institute of Technology
6.857: Network and Computer Security
Professors Ronald L. Rivest and Yael Tauman Kalai

Handout R3
February 21, 2020
Christos Nestor Chachamis

Recitation 3: Block Ciphers and AES

Plan for today

1. Block Ciphers
2. Ideal Block Cipher
3. Modes of Operation
4. Advanced Encryption Standard

1 Block Cipher

A block cipher is a mapping from fixed-length keys and fixed-length inputs to fixed-length outputs. Usually, the length of the output is the same as the length of the input, so a Block Cipher can be viewed as a permutation, for every key.

We need to define an Encryption and a Decryption algorithm. Given the key, they have to be one-to-one and satisfy

$$Dec_K(Enc_K(M)) = M$$

Requires that the key is known to both the sender and the receiver of the ciphertext.

2 Ideal Block Cipher

Ideal Block Cipher is an abstraction for how a secure block cipher should behave. It is very useful for examining the security of schemes that use block ciphers as their components. The Ideal Block Cipher is treated as indistinguishable from a random permutation, for a given key. In addition, the permutations of the ideal block cipher are independent for different keys. Then, with a randomly chosen key the adversary cannot get any information about the message.

For a block cipher to be considered close to the ideal block cipher there must extensive (and fruitless) efforts to break its security. In addition, it is considered good practice if there are some margins of safety (for instance more encrypting rounds are used compared to what the state-of-the art techniques can break). Finally, the outputs of the block cipher encryption should be computationally indistinguishable from random.

3 Modes of Operation

A good block cipher is a great way to ensure confidential communication between two parties. But it requires that the message is of fixed length. How can we encrypt messages of variable length? The answer is to use some of the modes of operation we saw (will see) in class.

3.1 Electronic Code Book

In this mode, we encrypt every block of the message with the same key and then output all of the block ciphers. That is, if $M_1, M_2, \ldots, M_n$ is the message, then we outupt $C_1, C_2, \ldots, C_n$, where

$$C_i = Enc_K(M_i), \text{ for } i = 1, 2, \ldots, n$$

The disadvantage of this method is that we reveal whether or not two blocks are the same. Same blocks are encrypted to same ciphers.

3.2 Counter Mode

In this mode we generate random bytes and xor them with the messages bytes, similar to OTP. In order to generate the random bytes, we use the encryptions of the numbers $r, r+1, \ldots, r+n$, where n is the length of the message. That is, if $M_1, M_2, \ldots, M_n$ is the message, then we compute

$$X_i = Enc_K(r - 1 + i)$$

$$C_i = M_i \oplus X_i$$

Then the output is $r, (C_1, C_2, \ldots, C_n)$. We need to have a random r, otherwise we have the same problem as in OTP.

One limitation of the block ciphers and the modes of operation is that there is no way to identify ciphertext corruption. This is important in real applications, since we care not only about confidentiality, but also authenticity. In next lecture we will see how to achieve authenticity.

4 Advanced Encryption Standard

- AES is considered a great standard. Replaced DES. In practice used as an ideal block cipher.
- Input and output size is 128 bits
- The key can be of size 128, 192 or 256
- The key specifies the number of rounds. There are 10 rounds for size 128, 12 rounds for size 192 and 14 rounds for 256.
- All operations are in GF(2^8).
- Byte addition: Byte can be represented as a polynomial. That is, if $\{a_7a_6a_5a_4a_3a_2a_1a_0\}$ is a byte, then it corresponds to the polynomial $a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$. Then, byte addition is performed by XORing the corresponding coefficients. For example:

$$\{57\} \oplus \{83\} =$$

$$\{01010111\} \oplus \{10000011\} =$$

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) =$$

$$x^7 + x^6 + x^4 + x^2 = \{11010100\} = \{d4\}$$

- Byte Multiplication: Corresponds to the multiplication of polynomials modulo an irreducible polynomial of degree 8 ($m(x) = x^8 + x^4 + x^3 + x + 1$). For example:

  $$\{57\} \bullet \{83\} =$$

  $$\{01010111\} \bullet \{10000011\} =$$
  $$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) =$$
  $$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

  and
  $$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \text{ modulo (m(x))} = x^7 + x^6 + 1 = \{c1\}$$

- AES Encryption Algorithm: (For 10 rounds)
  - Generate 11 “round” keys through the AES key schedule
  - For 9 rounds do the following:
    - XOR “round” key
    - Substitute Bytes
    - Rotate rows
    - Mix each column
  - In round 10:
    - XOR “round” key
    - Substitute Bytes
    - Rotate rows
    - XOR “round” key