

Homework 10, due September 27

- (1) **New codebook:** ROT3. Let us invent our own codebook, called ROT3. The key  $k$  and input  $x$  are both 3-bit binary numbers. Define the output to be  $ROT3(k, x) = k \oplus \text{RotateLeft}(x)$ , where  $\text{RotateLeft}(x)$  cyclically rotates by 1 bit to the left. Note: the plaintext gets rotated, not the key. For example,  $ROT3(011, 100) = 011 \oplus \text{RotateLeft}(100) = 011 \oplus 001 = 010$ . You find the inverse codebook to ROT3 yourself.
- Let's use the ROT3 codebook above. Suppose we use the key 101 and plaintext 000111101. What is the ciphertext in each of the following modes?
- (a) Electronic Codebook mode (ECB).
  - (b) Cipher Block Chaining mode (CBC) using an Initial Value of 110.
  - (c) Cipher Feedback mode using Initial Value 110.
  - (d) Output Feedback mode using Initial Value 110.
  - (e) Counter Mode (CTR) using Initial Value 110. (Note that  $111 + 1 = 000$ , as we are working with 3-bit binary numbers.)
- (2) (Page 147, Problem 6) Suppose Triple DES is performed by choosing two keys  $K_1, K_2$  and computing  $E_{K_1}(E_{K_2}(E_{K_2}(m)))$ . Note that the order of the keys has been changed from the usual two-key Triple DES. Show how to attack this modified version with a meet-in-the-middle attack.
- (3) Read the Wikipedia article on passwords: <https://en.wikipedia.org/wiki/Password>. Then read the Wikipedia article on password cracking: [https://en.wikipedia.org/wiki/Password\\_cracking](https://en.wikipedia.org/wiki/Password_cracking). Note that you did this when you turn in your homework.

What did you learn from these two articles? Do you think you choose secure passwords?