# CS 478/513: Computer Security
# Spring 2022
# Total Points: 100
## Homework 2

Due: Tue., 2/23/22, before class

Please complete the following problems, being sure to explain your conclusions or show your work when such details are requested. Your solutions must be submitted to Canvas as a PDF file.

This assignment is to be completed individually — plagiarism and cheating are strictly prohibited and are punishable. Please cite your references (except textbook), as described in the syllabus.

**Chapter 3:**

1. (5 points) Complete Problem 2 (a, b) from the text.
   Sol: Stream ciphers cannot be proven secure, as the keystream must eventually repeat. In one-time pads, the key never repeats is is chosen at random. Also, if we encrypt two different plaintexts with the same keystream (which we must, at some point), that would create ciphertext in depth. This might give an adversary enough information to guess the key.
2. (10 points) Complete Problem 3 (a, b) from the text.
   Sol: 3 a) $C_0 = P_0 \oplus K_0, C_1 = P_1 \oplus K_1, \ldots, C_n = P_n \oplus K_n$. If an adversary knows a single $(P_i, C_i)$ pair, she can recover $K_i = C_i \oplus P_i$, and similarly she can recover keys for all the plaintext/ciphertext pairs she knows.
   3 b) Assume adversary picks a plaintext $P'_0, P'_1, \ldots, P'_n$. Adversary then computes $C'_0 = P'_0 \oplus K_0, C'_1 = P'_1 \oplus K_1$, which is the same as $C'_0 = P'_0 \oplus P_0 \oplus C_0, C'_1 = P'_1 \oplus P_1 \oplus C_1, \ldots, C'_n = P'_n \oplus P_n \oplus C_n$. When this is decrypted by Bob, he gets $P'_0, P'_1, \ldots, P'_n$.
3. (15 points) Complete Problem 4.
   Sol: a) X: max. is 6, min is also 6, so avg is 6 times.
   b) Y: max. is 6, min is also 6, so avg is 6 times
   c) Z: max. is 6, min is also 6, so avg is 6 times.
   d) All 3 registers step 2 times.
   e) Exactly 2 registers step 6 times.
   f) Exactly 1 register steps 0 times (you need at least 2 to agree on majority bit to step).
   g) No register steps 0 times (at least 2 will always agree on the majority bit and step).
4. (5 points) Complete Problem 11 (a, b, c, d) from the text.
   Sol: 11 a) is just a description of a Feistel cipher.
   11 b, c) DES isa Feistel cipher, AES is not, although it needs to be invertible. TEA is not.

5. (5 points) Complete Problem 16 from the text.
   Sol: The adversary will build a table, where first column is $E_{K_1^{2^1}}(P), \ldots, E_{K_1^{2^{56}}}(P)$. The second column will be $E_{K_2^{2^1}}(C), \ldots, E_{K_2^{2^{56}}}(C)$. There will be a match at some point, and adversary can guess $K_1, K_2$.
6. (10 points) Complete problem 18.
   Sol: a) You'd need to compute both left and right columns for a known plaintext/ciphertext pair. You can't always use the same chosen plaintext for brute-forcing multiple DES keys.
   b) Left column requires computing $2^{56}$ entries, right column involves computing $2^{56}$ entries. Expected work is $2^{56}$ – on an average.
7. (10 points) Complete Problem 22 (a, b) from the text. Explain the reasoning behind your answer for part (a).
   An IV provides randomization, so it needs to be random, If 2 IV are the same for the same plaintext, the resulting ciphertext will also be the same. IV should never be chosen in a predictable way – either in sequence or otherwise, since it will enable an adversary to perform a chosen plaintext attack (details not expected in this assignment).

8. I think the author is saying instead of using $K$ as an encryption key, why not use $(IV + i)$ as the key for the $i^{th}$ round of encryption? This is clearly insecure, since as the IV is publically known, anyone can know/guess what $(IV + i)$ should be for the $i^{th}$ round of encryption.
9. (10 points) Complete Problem 25 (a, b) from the text.
   Sol: 25 a) Decryption: $P_0 = D(C_0 \oplus IV, K), P_1 = D(C_1 \oplus C_0, K), P_2 = D(C_2 \oplus C_1, K), \ldots, P_n = D(C_n \oplus C_{n-1}, K)$.
   25 b) This is insecure since it defaults to EBC mode. Adversary just XORs every ciphertext with the previous ciphertext to get $C_i = E(K, P_i)$. Also, every block of ciphertext depends on the previous block of ciphertext, rather than the previous block of plaintext. This goes contrary to Shannon's property of *confusion*. So, if there's an error in a block of plaintext, it might not propagate all the way down.
10. (10 points) Complete Problem 31 (a, b, c) from the text. Provide rationale to defend your answer for part (c).
    Sol: 31 a) Same IV means CBC gives no advantage over the insecure ECB mode.
    31 b) In CTR mode, if the same IV is used for encrypting different messages, there could be a chance that different plaintexts get encrypted using same key. Attacker can XOR the ciphertexts as in an one-time pad, and obtain the XOR of the plaintexts.
    31 c) CBC is marginally better, since two plaintexts need to identical for the attacker to succeed. In CTR, attacker can succeed even if 2 plaintexts are different.
11. (10 points) Assume a particular Feistel cipher uses the round function $F(X, K) = X \oplus K$, and number of rounds $n = 4$. Let the plaintext block $P$ be the 8-bit binary number 10110101, and the subkeys $K_1$ through $K_4$ as follows: 1011, 0100, 0101, 1010. Run the cipher on this input, and show the values of $L_i$ and $R_i$ for each round $i$, as well as the final ciphertext block that is obtained. *You do not have to compute each step by hand — you may write a simple program which gives the required outputs.*

    Sol: Intermediate values in encryption: $L_1 = 0101, R_1 = 0101, L_2 = 0101, R_2 = 0100, L_3 = 0100, R_3 = 0100, L_4 = 0100, R_4 = 1010$, ciphertext = (01001010).
    Intermediate values in decryption: $R_3 = 0100, L_3 = 0100, L_2 = 0101, R_2 = 0100, L_1 = 0101, R_1 = 0101, L_0 = 1011, R_0 = 0101$, plaintext = (10110101).