CS 408 – Cryptography & Internet Security (Fall 2024)

Assignment #1

(due October 3, 2024, in the beginning of class (2:30pm))

Please provide very detailed answers. If in doubt, provide more details than less details.
The assignment must be typed and printed. You are allowed to draw diagrams/figures by hand.

Problem 1 (25 points)

(a) Caesar wants to arrange a secret meeting with Marc Antony at one of two locations, either at the Tiber (the "RIVER") or at the Coliseum (the "ARENA"). He sends the ciphertext EVIRE to Antony. However, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar? (*Hint*: This is a trick question.)

(b) After sending the ciphertext, Caesar realized there is a problem with his previous message, and wants to send a second message. How would you solve the problem if you were Caesar?

(c) If an encryption function E_K produces the same result as the decryption function D_K, then key K is said to be an involutory (in other words, $E_K(p) = D_K(p)$, for all plaintexts p). Find all involutory keys in the Shift cipher over $\mathbb{Z}_{26}$, over $\mathbb{Z}_{22}$, and over $\mathbb{Z}_{23}$ (a Shift cipher over $\mathbb{Z}_{26}$ means a Shift cipher over an alphabet of 26 letters).

Problem 2 (25 points)

The operator of a Vigenere encryption machine is bored and encrypts a plaintext consisting of the same letter of the alphabet repeated several hundred times. The key is a six-letter English word. Eve is an attacker that cryptanalyses the ciphertext and knows that the key is a word, but does not yet know its length.

(a) What property of the ciphertext will make Eve suspect that the plaintext is one repeated letter and will allow her to guess that the key length is six?

(b) Once Eve recognizes that the plaintext is one repeated letter, how can she determine the key? Will the key be unique? Motivate your answer.

(*Hint:* You need to assume the fact that no English word of length six is a shift of another English word.)

Problem 3 (30 points)

(a) *The complementation property of DES:* Given $Y = DES_K(X)$, prove that $\overline{Y} = DES_{\overline{K}}(\overline{X})$, where $\overline{X}$ denotes the bitwise complement of X (*i.e.*, $\overline{X}$ is obtained from X by changing all the 1s to 0s and all the 0s to 1s).

(*Hint:* This has nothing to do with the structure of the S-boxes. You also need to leverage the fact that operations such as permutations and shifts are not affected by bitwise complementation. To solve the problem, just *work through all the other steps of the encryption*

algorithm and provide a detailed justification for your answer.
You might also need to use the fact the for any two bits a and b, we have $a \oplus b = \overline{a} \oplus \overline{b}$, and $\overline{a \oplus b} = \overline{a} \oplus b$)

(b) Use the complementation property in point **(a)** above to show how can an adversary reduce in half the expected number of keys to be tried in a brute-force chosen-plaintext attack (from 2^{55} to 2^{54} keys).

(*Hint:* You can assume that the attacker can execute a chosen-plaintext attack, so the adversary has access to the following pairs of plaintext/ciphertext: (M_1, C_1) and $(\overline{M_1}, C_2)$, where $C_1 = E_K(M_1)$ and $C_2 = E_K(\overline{M_1})$.)

Problem 4 (20 points)
When DES is used with a *weak key* K, then $E_K(E_K(p)) = p$.
When we use a pair of keys K_1, K_2, with $K_1 \neq K_2$, such that $E_{K_1}(E_{K_2}(p)) = p$, then such keys are known as *semi-weak keys*.

(a) How would you describe a pair of semi-weak keys in terms of the round keys they generate? (Your answer should provide a justification for the property of semi-weak keys described above)

(b) What is the danger of using such a key pair K_1, K_2 of semi-weak keys? Provide a detailed explanation for your answer. (*Hint:* You need to understand how does DES decryption work and then use that knowledge in your answer.)