Fundamentals of Cryptography

Homework 2

Dr. Mohammad Dakhilalian

Fall 2024

Theory Part

Thoroughly review **Chapters 3 & 4** of the book *Understanding Cryptography* to confidently address the questions.

Question 1

Consider the full DES encryption process:

1. DES algorithm performs a sequence of operations, including initial and final permutations. Describe in detail why these permutations are necessary, even though they do not contribute to the cryptographic strength of DES.
2. Given the importance of S-Boxes in the security of DES, discuss how the design of S-Boxes contributes to resistance against differential cryptanalysis. What properties of the S-Boxes are critical in this regard?
3. Prove that after 16 rounds of DES, every output bit is a function of every bit of the plaintext and the key. Provide a mathematical explanation of how diffusion spreads through the rounds.

Question 2

Due to the small key size, DES is often criticized for its vulnerability to brute-force attacks.

1. Explain the process of exhaustive key search against DES. How does the structure of DES make this type of attack feasible, and why is it still difficult to implement in certain scenarios?
2. Triple DES (3DES) was introduced to extend the security of DES. However, discuss why 3DES still has limitations, particularly in terms of computational efficiency and security against modern cryptographic attacks.

Question 3

Consider the irreducible polynomial $P(x) = x^4 + x + 1$:

1. Compute $A(x) + B(x) \bmod P(x)$ in $GF(2^4)$.
2. Compute $A(x) * B(x) \bmod P(x)$ in $GF(2^4)$.
   - $A(x) = x^2 + 1$, $B(x) = x^3 + x^2 + 1$
   - $A(x) = x^2 + 1$, $B(x) = x + 1$

Question 4

Find all irreducible polynomials:

1. of degree 3 over $GF(2)$.
2. of degree 4 over $GF(2)$.

(The best approach is to consider all polynomials of lower degree and check whether they are factors.)

Question 5

We consider AES with 128-bit block length and 128-bit key length. What is the output of the first round of AES if the plaintext consists of 128 ones, and the first subkey also consists of 128 ones?
You can write your final results in a rectangular array format if you wish.

Question 6

Consider the role of the different layers in AES encryption:

1. Explain how the "ShiftRows" and "MixColumns" layers contribute to diffusion in AES. Why is diffusion important for the security of AES?
2. Describe the key addition layer in AES. How does XOR operation in this layer ensure the incorporation of the key into the encryption process?
3. Why is it essential for the S-Box used in the Byte Substitution layer to be non-linear? What would happen if a linear S-Box were used instead?

Programming Part

Question 7

You are provided with a 56-bit key, which is composed of the first three letters of your first name and the first four letters of your last name in the ASCII code. You are tasked with verifying whether this key can create **confusion** and **diffusion** in the DES algorithm on random input texts. To do this, you need to write a Python program that uses this key and available libraries to encrypt several random input texts and analyze the results by assessing the bit-level changes between the original and encrypted texts.