Fundamentals of Cryptography

Homework 3

Dr. Mohammad Dakhilalian

Fall 2024

Theory Part

Thoroughly review **Chapters 5 & 6** of the book *Understanding Cryptography* to confidently address the questions.

Question 1

Consider a scenario where you need to implement a highly secure communication system using block ciphers. Answer the following questions by analyzing different block cipher modes, their strengths, weaknesses, and potential attacks:

1. Encryption Mode Selection: You are tasked with selecting a block cipher mode of operation to encrypt large files while maintaining both confidentiality and integrity. What mode(s) of operation would you select and why? Discuss their properties, especially in terms of confidentiality, integrity, and computational performance.

2. Security Against Attacks: Explain how a substitution attack could exploit a weakness in the ECB mode and why CBC mode is better at mitigating such an attack. Discuss how the initialization vector plays a crucial role in this process.

3. Multiple Encryption and Its Efficacy: Consider a situation where the system requires stronger encryption than standard AES. Would you recommend using double encryption or triple encryption? Justify your answer by explaining the meet-in-the-middle attack and how it affects the security of double encryption. Why is triple encryption considered more secure?

Question 2

We consider known-plaintext attacks on block ciphers by means of an exhaustive key search where the key is k bits long. The block length counts n bits with $n > k$.

1. How many plaintexts and ciphertexts are needed to successfully break a block cipher running in ECB mode? How many steps are done in the worst case?

2. Assume that the initialization vector IV for running the considered block cipher in CBC mode is known. How many plaintexts and ciphertexts are now needed to break the cipher by performing an exhaustive key search? How many steps need now maximally be done?

3. How many plaintexts and ciphertexts are necessary if you do not know the IV?

4. Is breaking a block cipher in CBC mode by means of an exhaustive key search considerably more difficult than breaking an ECB mode block cipher?

Question 3

Verify that Euler's Theorem holds in Z_m, $m = 6, 9$, for all elements a for which $gcd(a, m) = 1$. Also verify that the theorem does not hold for elements a for which $gcd(a, m) \neq 1$.

Question 4

With the Euclidean algorithm, we finally have an efficient algorithm for finding the multiplicative inverse in Z_m that is much better than an exhaustive search. Find the inverses in Z_m of the following elements a modulo m:

1. $a = 7$, $m = 26$
2. $a = 19$, $m = 999$

Note that the inverses must again be elements in Z_m and that you can easily verify your answers.

Question 5

Using the basic form of Euclid's algorithm, compute the greatest common divisor of

1. 7469 and 2464
2. 2689 and 4001

For this problem use only a pocket calculator. Show every iteration step of Euclid's algorithm, i.e., don't write just the answer, which is only a number. Also, for every gcd, provide the chain of gcd computations, i.e.,

$$gcd(r_0, r_1) = gcd(r_1, r_2) = ...$$

Programming Part

Question 6

Here you have to implement an AES in CBC mode with Python. What are the advantages and disadvantages of this mode? (Note that you can use the Crypto library)

Question 7

Write a Python program that uses the Extended Euclidean Algorithm to compute the greatest common divisor(GCD) of two numbers and finds the linear coefficients(s and t) such that $s * a + t * b =$ GCD(a, b). Then, verify that these coefficients satisfy the equation.