Fundamentals of Cryptography

Homework 1

Dr. Mohammad Dakhilalian

Fall 2024

Theory Part

Thoroughly review **Chapters 1 & 2** of the book *Understanding Cryptography* to confidently address the questions.

Question 1

1. What is the multiplicative inverse of 7 in $\mathbb{Z}_9$, $\mathbb{Z}_{10}$, and $\mathbb{Z}_{11}$?
2. What is the multiplicative inverse of 9, 10, and 11 in $\mathbb{Z}_7$?

Question 2

Compute x as far as possible without a calculator. Where appropriate, make use of a smart decomposition of the exponent.

1. $x = 3^3 \bmod 13$
2. $x = 3^{100} \bmod 13$
3. $x = 6^2 \bmod 13$
4. $x = 6^{100} \bmod 13$

Question 3

In an attack scenario, we assume that the attacker Oscar manages somehow to provide Alice with a few pieces of plaintext that she encrypts. Show how Oscar can break the affine cipher by using two pairs of plaintext–ciphertext, (x_1, y_1) and (x_2, y_2). What is the condition for choosing x_1 and x_2?

Question 4

Compute the first two output bytes of the LFSR of degree 8 and the feedback polynomial $x^8+x^4+x^3+x+1$, where the initialization vector has the value FF in hexadecimal notation.

Question 5

We conduct a known-plaintext attack on an LFSR-based stream cipher. We know that the plaintext sent was:

1001001001101101100100100110

By tapping the channel we observe the following stream:

1011110000110001001010110001

Note that the degree of the key stream generator (m) is 3.

1. What is the initialization vector?
2. Determine the feedback coefficients of the LFSR.
3. Draw a circuit diagram and verify the output sequence of the LFSR.

Cryptool Part

"CrypTool" is a widely used open-source e-learning software that illustrates cryptographic and cryptanalytic concepts. Please download it and complete the following exercises using this useful cryptology tool. **Include a screenshot of the software's output for each exercise in your answer file.**

Question 6

Encipher the following quote using the substitution cipher, use the given cipher alphabet as the key, and offset = 3. (To do this exercise select Encrypt/Decrypt → Symmetric (classic) → Substitution/Atbash).

- **Cipher text:** "Hkmmwhh yh asj jtw iwc js tbddyawhh. Tbddyawhh yh jtw iwc js hkmmwhh. Ye csk oslw ztbj csk bgw qsyar, csk zyoo nw hkmmwhheko." Bonwgj Hmtzwyjvwg
- **Cipher alphabet:** qwertyuiopasdfghjklzxcvbnm

Question 7

Decipher the following cipher text, enciphered with Vigenere cipher, using CrypTool analytical tools. What is the key? What do you guess the drawn diagram is?
(To break the cipher select Analysis → symmetric Encryption (classic) → Ciphertext-only → Vigenere)

Cipher text: Zkvbmdq ujagxkyw uy c hpuzkhyx lkjjp zjfr ruezqqy qs nduvjafopl rtk ksrqmtnrk, iqsdujgsrugnnrk, gpi yhgkqynonnrk uh iyfg cx gf ou ypmturgfzgi yoxqxq ax uymdkf nl zkvbmdqu. Nr utxtjhku f pmtij mr vtfafoejq mtf yconptjamkjq pkunezkf ym eghjeggti lqzytpwy hwmy iagcd zjwcmzu, xson cx szgwyfaxkecp gehcey, ffrm htjyongx, kmryfpq, gpi bqtkfj-al-ujphoej yfzchie. Qgd cxkojlfy qk lqzytpw yghsdovd gzinzbq lkwcignqq, utvwseoqs bqzghruup xwezgrq, qtewwbzktl, mtf xcoatj nduvtaaru qgwk UXJ/FRU. Fq oedjp fntjyfy gamxbg, wmnauy lqzytpw yghsdovd ge kuxczzkfj rut jleatnls zjj qmlgyw al ujleovntq opkmdscygat, rfpfoezjmxnd gz yghraxu qgwk hnlmtej, fqgnyfogtj, yzj ittqxprczz.