Fundamentals of Cryptography

Homework 1

Dr. Mohammad Dakhilalian

Fall 2023

1 Theory Part

Question 1

We consider the ring $\mathbb{Z}_4$. Construct a table which describes the addition of all elements in the ring with each other:

+	0	1	2	3
0	0	1	2	3
1	1	2	...	
2	...			
3				

1. Construct the multiplication table for $\mathbb{Z}_4$.

2. Construct the addition and multiplication tables for $\mathbb{Z}_5$.

3. There are elements in $\mathbb{Z}_{12}$ and $\mathbb{Z}_{15}$ without a multiplicative inverse. Which elements are these? Why does a multiplicative inverse exist for all nonzero elements in $\mathbb{Z}_{11}$?

4. Find all integers n between $0 \leq n \leq m$ that are relatively prime to m ($\mathbb{Z}_m^*$) for $m = 8, 22$. What is $\phi(m)$ for $m = 8, 22$? (ϕ : Euler's phi function).

Question 2

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 3

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. $x = 6^{100} \bmod 13$

5. $7^x = 11 \bmod 13$

Question 4

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 5

Assume an OTP-like encryption with a short key of 128 bits. This key is then used periodically to encrypt large volumes of data. Describe how an attack works that breaks this scheme.

Question 6

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 7

Given is a stream cipher that uses a single LFSR as a keystream generator. The LFSR has a degree of 256.

1. How many plaintext/ciphertext bit pairs are needed to launch a successful attack?
2. Describe all attack steps in detail and develop the formulae that need to be solved.
3. What is the key in this system? Why doesn't it make sense to use the initial contents of the LFSR as the key or as part of the key?

Question 8

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.

2 Cryptool Part

"CrypTool" is an open-source widespread e-learning software that illustrates cryptographic and cryptanalytic concepts. Download it and do the following exercises using this helpful cryptology tool. For each part, put the output of the software in your answer file.

Question 1

Encrypt your full name using the Caesar cipher with key = 'S'.
(To do so select Encrypt/Decrypt → Symmetric (classic) → Caesar)

How many letters is the alphabet shifted by?

Question 2

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:** Pbhtqy Pbpqboy'h mbg
- **Cipher alphabet:** qwertyuiopasdfghjklzxcvbnm

Question 3

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: udgaxgat tw nqzj jdqftfdq iyh wmaj xg gap qswqyk af qoisx nzv lqinlazo aigbtp etace gjkxesydialq ub lpka kzrlmqyw kqdpvsx lpqgzaevsfqzr wjixtdqa elsf ici vqatkfql es tq dpvq qidc la nzpdae lrv nzpec pwhr ltm xeltmxelukd mffw dqsxt xefmopetxm dxwba.

Question 4

In cryptography, the one-time pad is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key the same size as, or longer than, the message being sent. In this technique, a plaintext is paired with a random secret key. Answer the following questions regarding this encryption technique.

1. With the help of Cryptool, encrypt the following plaintext using the given key as a one-time pad.
   (to do this exercise select Crypt/Decrypt → Symmetric (classic) → OTP)
2. Use your full name as the OTP key and encrypt the same plaintext with the same algorithm. (don't forget to write the key in your answer file)
3. Try to find the OTP key of each of the two cipher texts in the previous parts using the Cryptool analytical tools and put the results, especially the predicted length of the key, in your answer file; Compare the security of the keys based on the results of analysis.
   (To do this part select Analysis → Symmetric Encryption → cipher text only → XOR)

- **Plaintext:**
  Today, Internet service providers (ISPs) try to deliver more and more valueadded services integrated with their residential Internet access offer, such as triple-play (voice, Internet, and video). This situation generates the need for more powerful and expensive home devices to cover these needs. This device receives different names, from customer premise equipment (CPE) to residential router and to home gateway (HGW), but all have a common ground: the trade-off between low-cost and rich functionalities, with a potentially negative effect on the device security. As a result, vHGW was one of the first scenarios that were adopted within the NFV paradigm, to demonstrate its potential in terms of efficiency and security. In this chapter, we are going to describe the NFV architecture that Telefonica designed and implemented in a commercial trial, to evaluate its potentiality.

- **OTP Key:**
  Thksp, Afuqfgwj abnqkku xdhsqlbfo (TYTd) jom th kifbxdy sevo kxr atlj wedxe-utpxk yehxmtsb gfuqyzfbjo smpx trwul vmnqlbjqcsp Nfuqfgwl qxarge otlru, evsf ed teqjoi-fswi (zhwte, Kuqqeyeb, fbb lqlbm). Iwsh yoxbwdpif lstjhrcqq npd cgoh dpq sevq thouvnzg oes igmgfzmxz tcva vnxmtqq ne hqxdy xkiui vgohc. Ykqw fadxms dgdqmxzi vjfwedryj seofc, vuyc towrfagz zsqqzqg bugijwknz (NES) nv vmnqlbjqcog osodqr lzd fa tbcr sshdgtc (ZEX), fbq imw vbmq v quhgif lpipzd: fvx urhga-kjd cqlupmm ecp-yeej oes hwfd oufliysvspnrcfy, zeto w tbsuecccfpp iebsvlei mnjgbd xo xki hfmwte wtokvnvi. Xw k tepqbv, vZEX azk ghf ee whl eypbh cvoxxtkpc ykkp funx uvdnckd exbguv rzg SMF ksrhggfq, th kirqnnmhrcy sru xrlzsngth ne pveeb az dklapguzsf wle cwnmlfeu. Ar bgua ejsyimv, zs gjs nikhd th kmhotxcy uag SMV jkydtnklxxiy uaus Wejpztesxs riduetwz bbo ygcaybmfuqb hc a dgehoxmpqe ufyzh, ca slznihte dhp iwlnjqcspnhj.U