ECE 404: Introduction to Computer Security

Purdue University

Spring 2021: Midterm-I

Instructions

1. Write or type your answers and email them in PDF form to the provided email address. You do not have to write your answers in this booklet (i.e. you can write them on a separate sheet).
2. Your answers for each questions must be clearly legible and labelled for the respective question. You may lose points if your work is illegible.
3. This is an open book, open notes exam.
4. Unless otherwise instructed, justify your answers fully.
5. **Answers that are directly copied from the lecture notes will not be accepted.**
6. **You must not consult other students or anyone else for help with answers to the exam questions.**
7. **Purdue Honor Pledge: As a Boilermaker pursuing academic excellence, I pledge to be honest and true in all that I do.**

You must include the following information in your submitted PDF:

Name :

Student ID :

Email :

Signature (For PDFs, use Adobe Reader's Signature tool. For DOCX files,in Word go to Insert →Shapes→Lines →Scribble) :

Problem 1 [20 points]

1. The Rosetta stone was a monumental discovery for linguistics and archaeology. Ancient Egyptian hieroglyphics had been undecipherable until archaeologists excavated a stone tablet at Rosetta which contained the same message written in both Ancient Egyptian and legible Greek scripts. Using this tablet, historians could decipher the long lost Egyptian language leading to massive strides in Egyptology.

   Now imagine yourself in the shoes of an Egyptologist who has stumbled upon a similar stone inscription as shown below:

   RNFEMMS OBAIME JEFDW AHB UPW PEPTMNSVLOD JF ------ NKE --------

   You are currently unfamiliar with Ancient Egyptian but thanks to the Rosetta stone, you now know that the Egyptian alphabet shares a similar frequency distribution as the English alphabet. These frequency distributions are given in Figure 1 on the next page. Using these distributions, can you fill in the missing letters on the inscription? **[3 points]**

2. There is now a new piece of information: the text at the bottom of the inscription was generated using a Vigenere cipher and the first two words of the plaintext are to be:

   RAIDERS BEWARE —— — — ——— – —— — ———

   The cipher was generated using a 6-letter keyword which is still unknown. Furthermore, the text symbols used for constructing the key for the cipher are only the 23 letters (A-W) shown in Figure 1.

   - Determine the key for the Vigenere cipher. Show your work. **[5 points]**
   - Recover the rest of the message using the key. **[3 points]**
   - How would you solve the cipher if the key length was not known? **[2 points]**

3. Convert the following ASCII string to Base64: *3DES*

   You must show your work to receive credit. You may find the website http://www.asciitable.com/ useful. **[7 points]**

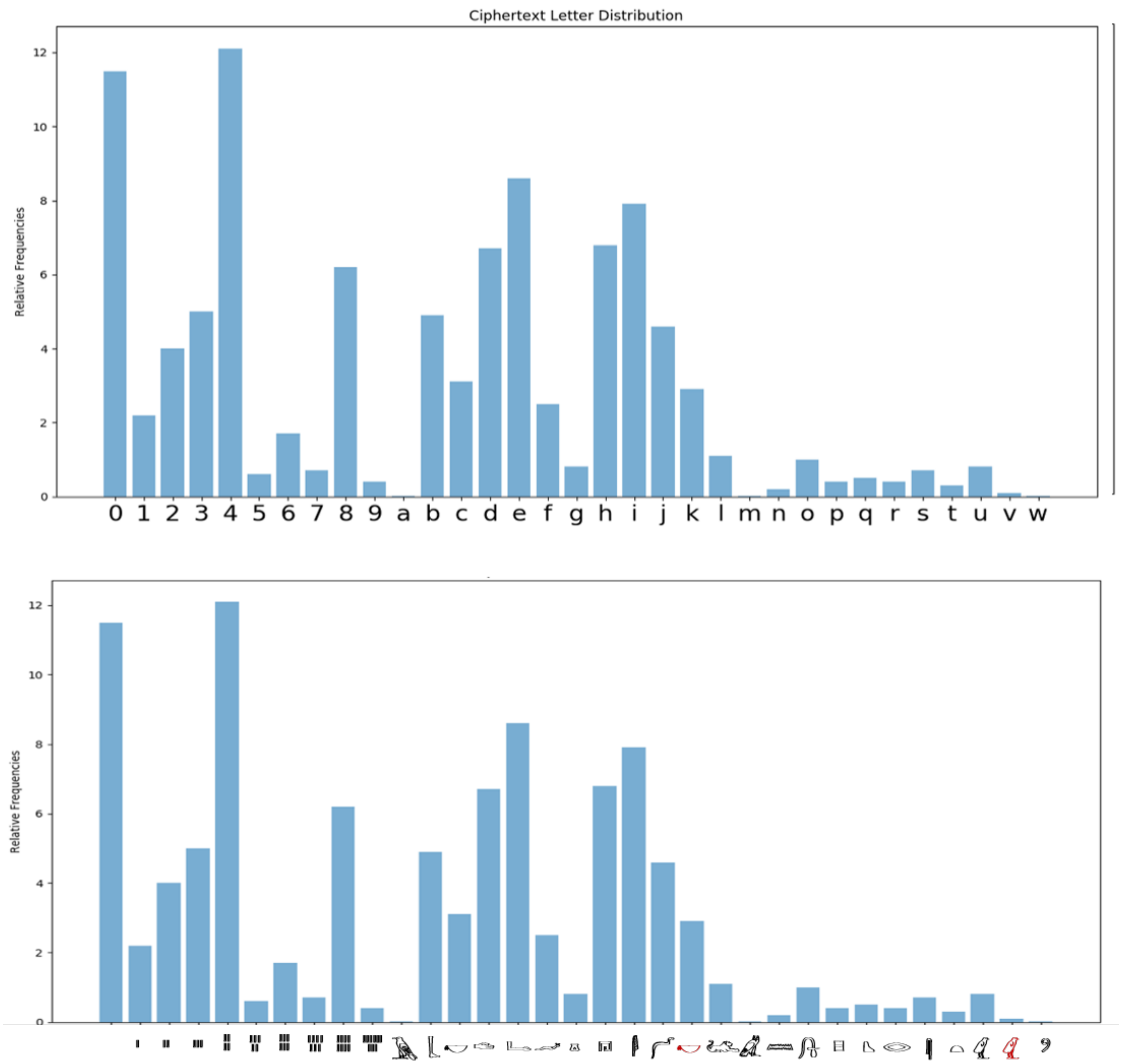
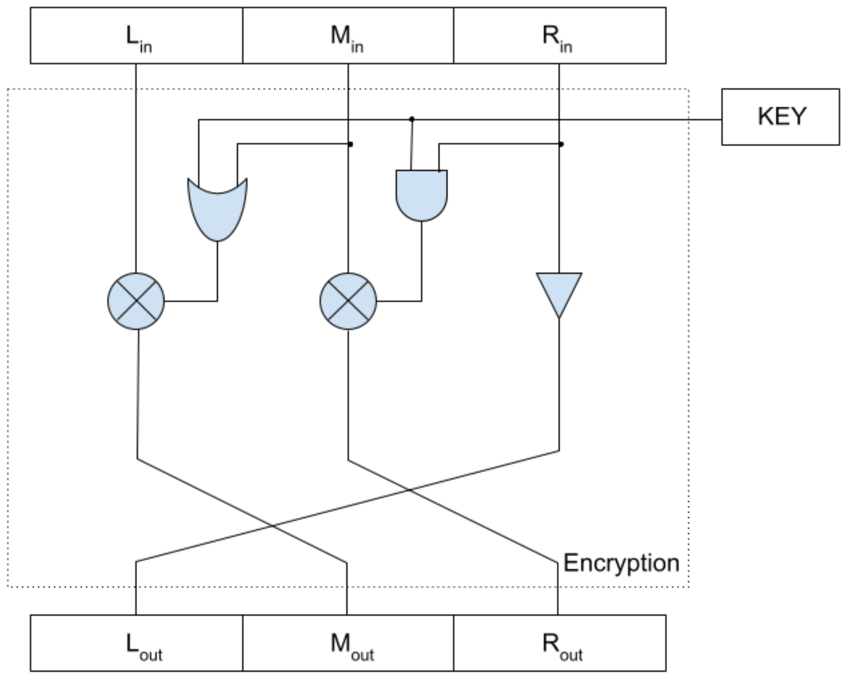


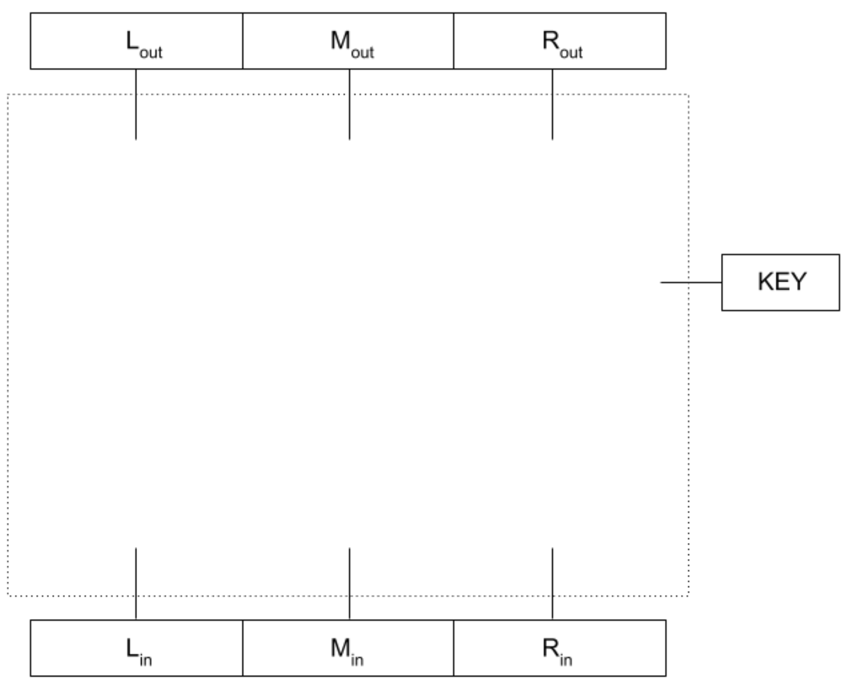
Figure 1: Frequency distributions for the Egyptian and English alphabet

Problem 2 [30 points]

1. Consider the following block encryption structure. The input block is divided into 3 sub-blocks: L_{in} (left sub-block), M_{in} (middle sub-block), and R_{in} (right sub-block). The encrypted output block is composed of L_{out}, M_{out}, and R_{out} as in the input block.
 You can assume the key size is the same as the block size (the exact size is not important).



Design the decryption structure: **[10 points]**



Show how the decryption works. Formulate the encryption and decryption equations. Use these equations to show how L_{in}, M_{in}, and R_{in} can be recovered from L_{out}, M_{out}, and R_{out}. [**10 points**]

2. In the DES Feistel function, if the values in the S-boxes were all set to 0, the DES output ciphertext would be equal to the input plaintext. Explain why this is the case. [**5 points**]

3. What would happen in DES encryption if, in addition to all the S-boxes set to 0, all the numbers in the P-box are set to zero? Your answer should explain what happens to the final ciphertext as well as what happens to the P-box output block (i.e. the immediate output after applying the new P-box permutation). [**5 points**]

Problem 3 [23 points]

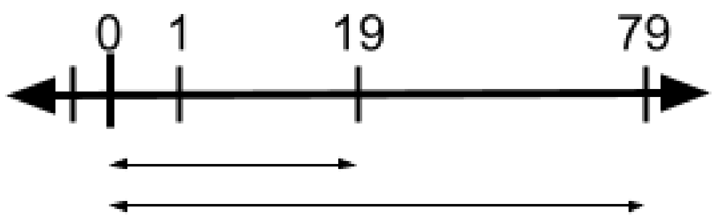
1. Let $\mathbb{C}$ be the set of all complex numbers such that $x \in \mathbb{C}$ if $x = a + b \times i$, where $a, b \in \mathbb{R}$ and $i = \sqrt{-1}$. We know that $\mathbb{C}$ forms an abelian group under arithmetic addition. Complete the following:

   (a) Does the set of all complex numbers under arithmetic addition and multiplication $\{\mathbb{C}, +, \times\}$ form a ring, an integral domain or a field? Explain in detail by showing the properties that are satisfied. [**3 points**]

   (b) The set of real numbers, $\mathbb{R}$ forms a subset under $\mathbb{C}$ by setting $b = 0$, for all $x = a+b\times i, x \in \mathbb{C}$. We know that $\mathbb{R}$ under arithmetic addition and multiplication $\{\mathbb{R}, +, \times\}$ forms a field.

   Similarly, the set of imaginary numbers, $\mathbb{I}$ is formed by setting $a = 0$ for all $x = a + b \times i, x \in \mathbb{C}$. Is $\{\mathbb{I}, +, \times\}$ also a field? If not, what is it? Explain your answer by showing the properties that are satisfied. [**5 points**]

2. Suppose you are on the integer number line and you can only take steps of 79 or 19 either to the left or right. How would you go from 0 to 1? (The diagram below is **not** to scale). [**5 points**]



3. If $a \mid bc$ (i.e. a is a divisor of bc) and $gcd(a, b) = 1$, prove that $a \mid c$. [**5 points**]

4. Find $(n-1)! \mod n$ given that n is a prime number. Explain how you got your answer. [**5 points**]

Problem 4 [16 points]

1. For the irreducible polynomial $x^3 + x^2 + 1$ in $GF(2^3)$, compute the following results for the bitstrings $B_1 = 110, B_2 = 011$. You can use whichever method you like to solve them (bitwise operations <u>or</u> convert them to polynomials and solve).

   (a) $B_1 \times B_2$ [**3 points**]

   (b) B_1 / B_2 [**4 points**]

2. The following problems are related to Euclid's Algorithm

   (a) Show that Euclid's algorithm can be used to find the GCD of three integers [**4 points**]

   (b) Given below is the Python implementation of the Euclid's algorithm to find the GCD of two integers. Modify the code to find the GCD of three integers: [**2 points**]

```python
#!/usr/bin/env python
## GCD.py
import sys
if len(sys.argv) != 3:
    sys.exit("\nUsage: %s <integer> <integer>\n" % sys.argv[0])

a,b = int(sys.argv[1]),int(sys.argv[2])

while b:
    a,b = b, a%b

print("\nGCD: %d\n" % a)
```

   (**NOTE:** You do not need to provide a working script - only present the implementation logic with pseudocode.)

   (c) You are given three positive integers a, b, c such that $gcd(a, b, c) = 1$. Which of the following statements is true for the integers pairs (a, b), (a, c) and (b, c)?

      i. All three pairs are also relatively prime.

      ii. At least one of the pairs is relatively prime.

      iii. Information is not sufficient to answer.

   Justify your answer. [**3 points**]

Problem 5 [11 points]

1. Below is a Python code snippet from an incorrect implementation of the row shifting step of the AES algorithm. There is a bug in the code due to it being an incorrect implementation. Find the bug in the code and correct it. [**5 points**]

```python
def row_shifting(input_block):
    # Form the state array as a list of bytes
    byte_array = [input_block[byte_index * 8:(byte_index + 1)* 8]for byte_index in range(16)]
    shift_block = BitVector(size=0)
    # Compute the new columns after row shifting
    col_1 = byte_array[0] + byte_array[13] + byte_array[10] + byte_array[7]
    col_2 = byte_array[4] + byte_array[1] + byte_array[14]] + byte_array[11]
    col_3 = byte_array[8] + byte_array[5] + byte_array[2] + byte_array[15]
    col_4 = byte_array[12] + byte_array[9] + byte_array[6] + byte_array[3]
    # Construct the shifted block
    shift_block += col_1 + col_2 + col_3 + col_4
    return shift_block
```

2. Explain the vulnerability in using block ciphers (such as AES or DES) in electronic codebook (ECB) mode. Then explain in general how the other modes of operation for block ciphers avoid this (while these modes have their differences, the general mechanism by which they avoid the vulnerability is the same). [**6 points**]

[*You can use this page if you run out of room on the other ones*]