

**CSC435 - Computer Security**

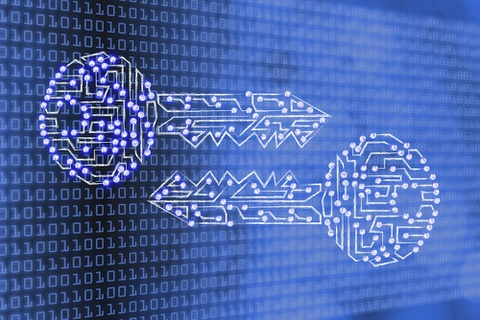
**Lab 4 - Cryptography**

**Group 7**

Roula Ghaleb

Abdallah Tourbah  
Louay Zeineldien  
Omar Shatila

For: Dr. Ayman Tajjedine



## Table of Contents

[**1. Consider RSA with p = 5 and q = 11. 3**](#_o8r3gz43tast)

[a. What are n and z? (Louay) 3](#_5zxu1kora1ap)

[b. Let e be 3. Why is this an acceptable choice for e? (Roula) 4](#_psgt4omoqxk3)

[c. Find d such that de = 1 (mod z) and d < 160. (Abdallah) 4](#_bjg5qpvngngd)

[d. Encrypt the message m = 8 using the key (n, e). Let c denote the corresponding ciphertext. Show all work. Hint: To simplify the calculations, use the fact: [(a mod n) . (b mod n)] mod n = (a . b) mod n (Omar) 4](#_9hp9d7qqu9fm)

[**2. Write a program that implements Caesar Cipher as follows [the code should be well-documented]: 5**](#_uri1o8y8msei)

[a. Your program should have the following options 5](#_8wwq598yeyfo)

[i. Encrypt (Roula and Omar) 5](#_ej48q878w4ch)

[ii. Decrypt (Louay) 5](#_oq6h12aujf10)

[iii. Brute Force (Abdallah) 5](#_kzzxo3c4fzx2)

[b. For the first two choices, the program should ask for a key and a text message (capital and/or small letters). Then the program should use Caesar Cipher to encrypt/decrypt the message entered by the user (keeping all non-letter characters as they are) and display the result. Note that a capital letter must remain capital after encryption/decryption; the same goes for the small letters. 5](#_p6crvxsmlf07)

[c. If brute force was chosen, your program should take in an encrypted message from the user and display all possible decryptions with the corresponding keys. 5](#_yrcdllcfq4jc)

## 

## 

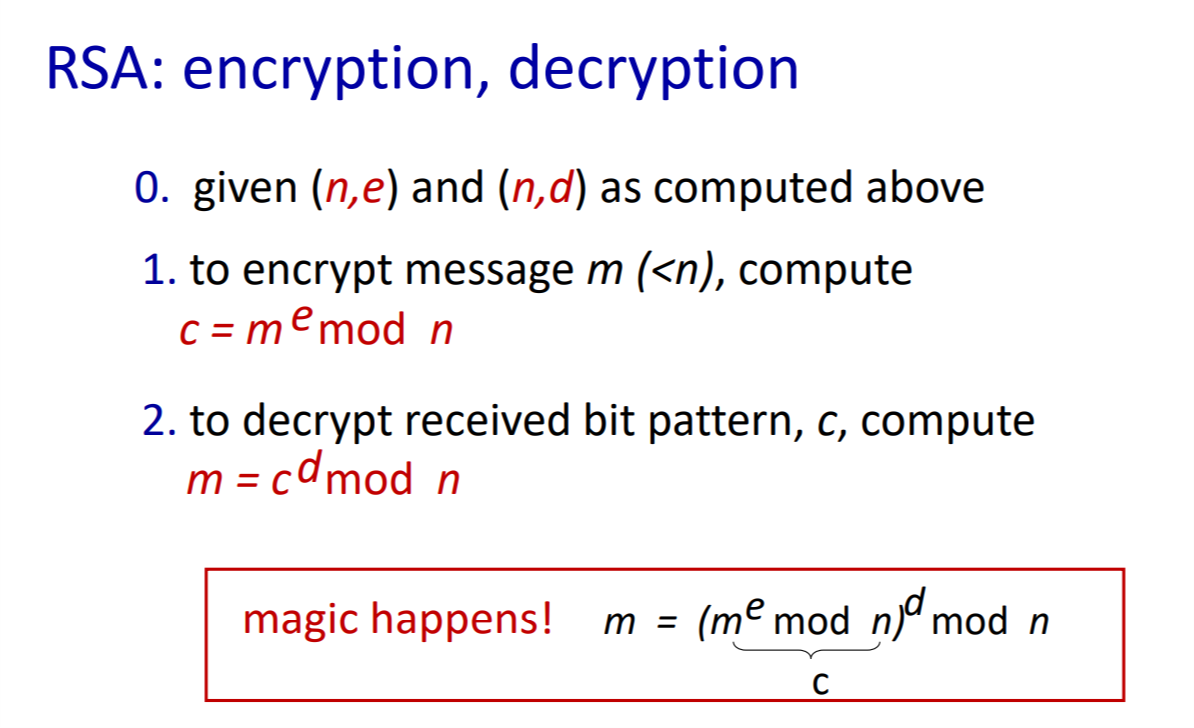
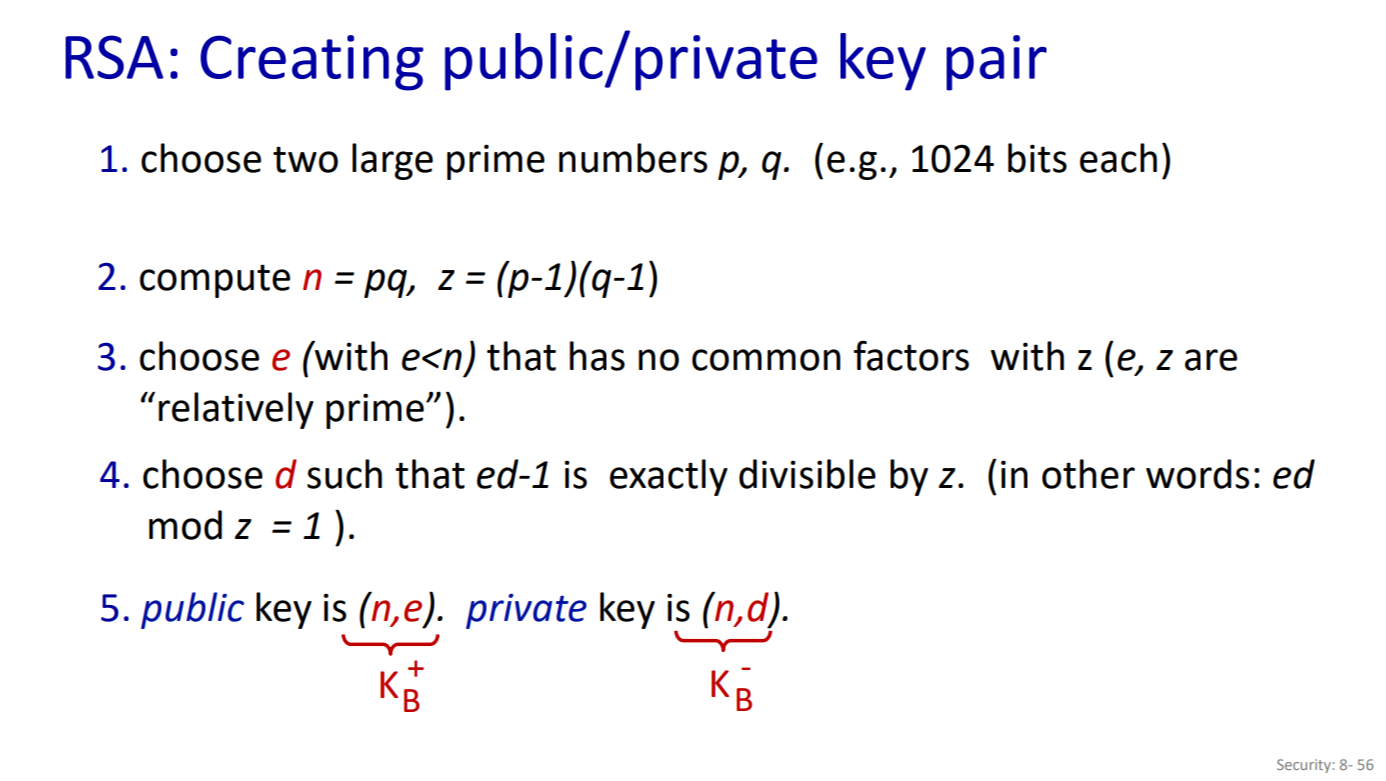
## 

## 

## 

## 1. Consider RSA with p = 5 and q = 11.

Part 1 of this lab can be solved using the following slides from Handout 7 Cryptography:



### a. What are n and z? (Louay)

* We have the formula n = pq from the first slide above in rule 2. So, n = p\*q = 5\*11 = 55
* We also have the formula z =(p-1)(q-1) = (5-1)\*(11-1) = 40

### b. Let e be 3. Why is this an acceptable choice for e? (Roula)

Assume e = 3. As per rule 3 of the first slide above, the e should be less than n and have no common factors with z (which means that e and z are relatively prime).

e = 3 is a valid choice because it satisfies these two conditions.

* The first condition is clearly valid since e<n → 3<55
* The second condition is also satisfied since the greatest common denominator of e and z is 1 (GCD(e, z)=1). That means e and z are relatively prime.

### c. Find d such that de = 1 (mod z) and d < 160. (Abdallah)

From rule 4 of the first slide, we can use the formula: ed.modz = 1.

To calculate this formula, we will replace with the values we found and find d. We have e = 3 and z = 40. We also have de = 1modz

3d.mod40 = 1 → 3d = 1mod40 → d = 27 since 27\*3=81 mod40 = 1.

### d. Encrypt the message m = 8 using the key (n, e). Let c denote the corresponding ciphertext. Show all work. Hint: To simplify the calculations, use the fact: [(a mod n) . (b mod n)] mod n = (a . b) mod n (Omar)

From the second slide and the given hint:

* me = 83 = 512
* c = me mod n = 83 mod 55 = 17

## 2. Write a program that implements Caesar Cipher as follows [the code should be well-documented]:

### a. Your program should have the following options

#### i. Encrypt (Roula and Omar)

#### ii. Decrypt (Louay)

#### iii. Brute Force (Abdallah)

### b. For the first two choices, the program should ask for a key and a text message (capital and/or small letters). Then the program should use Caesar Cipher to encrypt/decrypt the message entered by the user (keeping all non-letter characters as they are) and display the result. Note that a capital letter must remain capital after encryption/decryption; the same goes for the small letters.

### c. If brute force was chosen, your program should take in an encrypted message from the user and display all possible decryptions with the corresponding keys.

For part 2, we will attach a .py file and a readme file.

Readme error photo: 