University of New Brunswick
Faculty of Computer Science
CS4355/6355: Cryptanalysis and DB Security
Course Projects, ***Due Time, Date*** *5:00 PM, December 3, 2019*

Student Name: _____ Matriculation Number: _____

Instructor: Rongxing Lu
The marking scheme is shown in the left margin and [100] constitutes full marks. [A / B]: A and B are schemes for CS4355 and CS6355, respectively. There is no requirement for CS4355 in Final Project.

[**50/20**] 1. Programming Project I (Individual Project)

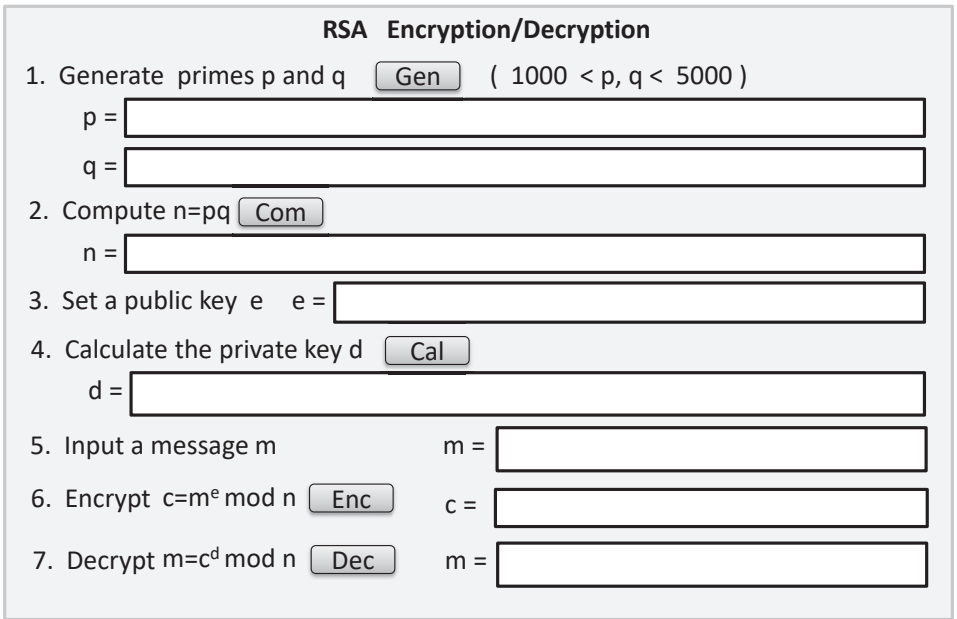
[10/5] (a) Use Java or other programming languages you are familiar to implement the Extended Euclidean algorithm.

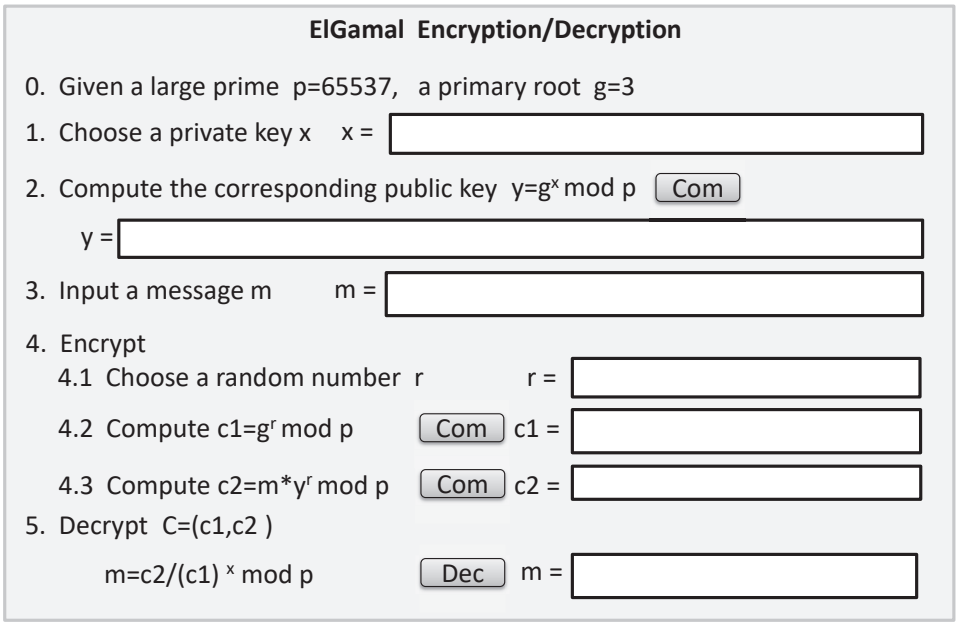
- Input: two large positive random numbers (a, b) of length 1024 bits, i.e., $|a| = |b| = 1024$
- Output: two numbers (c, d), where $c = a^{-1} \bmod b$ is the inverse of a under modulus b, and $d = b^{-1} \bmod a$ is the inverse of b under modulus a

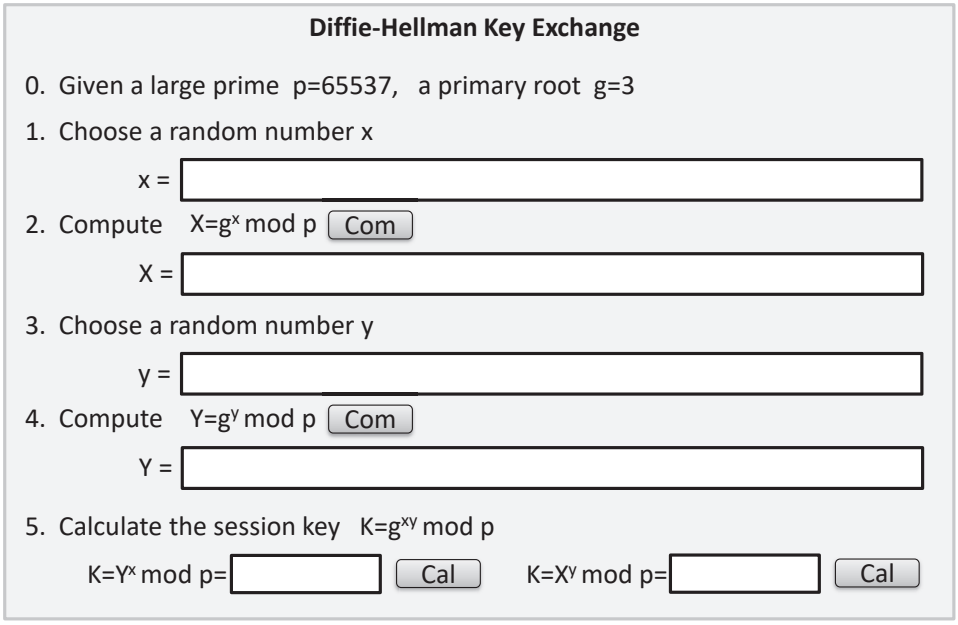
[10/5] (b) Use Java or other programming languages you are familiar to implement the Miller-Rabin primality test

- Input: one large positive random numbers a of length 1024 bits, i.e., $|a| = 1024$
- Output: output 1 if a is a prime, and 0 otherwise.

[30/10] (c) Use Java or other programming languages you are familiar to implement the demonstrations of RSA Encryption/Decryption algorithm, ElGamal Encryption/ Decryption algorithm, and Diffie-Hellman key exchange protocol. The functions and user interfaces of demonstrations should be designed similarly as the following figures.







[**15/5**] 2. Programming Project II (Individual Project)

The following ciphertext $\mathcal{C}$ has been generated with the Vigenere Cipher. Please cryptanalyze the ciphertext and recover the corresponding plaintext $\mathcal{M}$ and the used key $\mathcal{K}$. For the cryptanalysis, you only know the length of the used key $\mathcal{K}$ is 4. Please use Java or other programming languages you are familiar to implement an algorithm, which takes $\mathcal{C}$ and other required information as input, and automatically outputs the recovered $\mathcal{M}$ and $\mathcal{K}$. In addition to provide the source code, please also write down the detailed strategy you have applied to recover $\mathcal{M}$ and $\mathcal{K}$. Note that, the relative frequencies of letters in

text are shown in the following figure.

OOFWGTXYE - FKVY MHIULX WTOGLE TH AMBELFS MV XAIAAPL, KQSDAAPL, ZQROLD AGK YUVO YOKL - FONJT NXHDLR LHEKF MSILOT HM PABSK LBMQ IG AADT-F'E MHKQRG DAREK. FEVOZOEVSY BZ BOPLDEW UAT CBET UF EIEPOOG JTIIZ MN-W LXEVADIVPFY, UBF BR ATE VYQAMPHIMF MNW PZGXUGIMF AF VVYPNAQR LJUE-GAUSMZ IHH ADAGZXAML EOVPQTR'Z ZEXKE AGK IAGAE IGAA PKVPUVAE TAHF CTU UMIYAVX IATA ZACBLFY TUP TAL QCHUAMR.

The relative frequencies of letters

a	8.2%	j	0.2	s	6.3
b	1.5	k	0.8	t	9.1
c	2.8	l	4.0	u	2.8
d	4.3	m	2.4	v	1.0
e	12.7	n	6.7	w	2.4
f	2.2	o	7.5	x	0.2
g	2.0	p	1.9	y	2.0
h	6.1	q	0.1	z	0.1
i	7.0	r	6.0		

The most frequent diagrams in English on a relative scale of 1 to 10:

Diagram	Frequency	Diagram	Frequency
TH	**10.00**	**HE**	**9.05**
IN	**7.17**	**ER**	**6.65**
RE	**5.92**	**ON**	**5.70**
AN	**5.63**	**EN**	**4.76**
AT	**4.72**	**ES**	**4.24**
ED	**4.12**	**TE**	**4.04**
TI	**4.00**	**OR**	**3.98**
ST	**3.81**	**AR**	**3.54**
ND	**3.52**	**TO**	**3.50**
NT	**3.44**	**IS**	**3.43**
OF	**3.38**	**IT**	**3.26**
AL	**3.15**	**AS**	**3.00**

The most frequent trigrams in English:

ENT ION AND ING IVE TIO FOR OUR THI ONE

[**35/5**] 3. Design Project (Individual Project)

Alice has a set of files $\mathcal{F} = \{F_1, F_2, \cdots, F_n\}$, each file is around 100 M. Because files are huge in size, Alice plans to store them in a cloud. Later, when Alice wants to retrieve one of them, she just needs to launch a query and the cloud server will return the desired one. However, since the cloud server is not fully trusted, we usually consider it as semi-trusted, i.e., honest-but-curious model. Under this trust model, please help Alice design a scheme for secure file storing and retrieval in cloud server, and the following requirements should be met:

- Even though files $\mathcal{F} = \{F_1, F_2, \cdots, F_n\}$ are stored in the cloud, the cloud server cannot read the content of each file.
- Even though the cloud server also has one file F_c, which is exactly the same as one file in the set $\mathcal{F} = \{F_1, F_2, \cdots, F_n\}$ stored in the cloud, the cloud server cannot identify the file in the set $\mathcal{F}$.
- When Alice launches a query on some file F_i, if F_i really exists in the cloud, the cloud server can return the result with $O(\log n)$ processing time or less.

Please write down your design as much detail as possible. You do not necessarily implement your design with some programming language, but extensive security analysis and performance evaluation should be provided.

[**0/70**] 4. Final Project – CS6355 (Group-based Project)

Write a survey of no more than 3000 words (not including references) on your selected topic. Your survey must contain the following section headings: (1) abstract, (2) introduction, (3) detailed description of the topic, (4) related work in this area, (5) your thoughts and remarks on how to use the algorithms and protocols in the class to achieve some security requirements in your selected topic, and (6) references (additional sections are not allowed).

Note that the survey can be based on papers published within the last six years including: various IEEE/ACM Journals, Magazines, and security related conferences. Your survey must contain at least 6 references to papers of the above mentioned journals, magazines and conferences. You are not allowed to use the Wikipedia as a source.

Form disjoint groups: each consisting of 4-5 students. Notify the instructor of the group members' information via email (rlu1@unb.ca) by October 01, 2019 before class. Those students who are not in any group by October 01, 2019 will be arranged into groups to the instructor's discretion.

Available topics: you can select a topic from the list of available topics appended at the end of this document, or you may propose your own project to the instructor no later than October 01, 2019. Your proposed project is subject to the instructor's approval. Note that any given project can only be taken by one group; projects will be awarded on a first-come first-serve basis, being judged by the "Sent" time of the emails.

Peer Review: Each group's survey will be reviewed by each of the other groups (see schedule below). Prepare a one-page review report per group for each survey you review, and submit the review report according to the schedule below. Your review reports must include comments organized into the following two sections: (1) scientific/practical merit: correctness, accuracy, significance, and non-triviality, and (2) presentation: clarity, organization, and English usage. Additional sections are not allowed. Improve your survey based on the comments you receive from other groups and resubmit according to the schedule below. Your review reports are worth 15 of your final project. Your review reports will be evaluated according to their diligence.

Present your project: in the week of November 25, 2019 and afterwards (schedule of presentations will be generated randomly). Your presentation must last no more than 30 minutes. The use of supporting material such as slides, whiteboard, handouts, software tools, etc., is encouraged. Your presentation is worth 5 of your final project, and will be evaluated according to their soundness, clarity, precision, and conciseness. Note that, excellent presentations will gain additional 5 bonus points in your final project based on the instructor's discretion.

Grade of final project in this course: Your final project is worth 28% (=40%*0.7) of your final grade for this course, including 20% for your final survey report, 6% for your review reports, and 2% for your presentation. Note that, additional 2% bonus from your excellent presentation may be exercised.

Item	Submission Date		
Submit **survey draft** to the other project groups via instructor	**October 31**		
Submit **review reports** to instructor and corresponding authors via instructor		**November 08**	
Submit **final version** only to instructor			**December 3**

A list of available topics:

(a) Trust Management in Pervasive Computing

- Evolution of trust management, pervasive computing, security requirements and challenges, possible solution for at least one challenge

(b) Security in Bluetooth Enabled Devices

- Evolution of Bluetooth, security requirements and challenges for Bluetooth Enabled devices, possible solution for at least one challenge

(c) Smart Card Security

- Evolution of Smart card, security requirements and challenges, possible solution for at least one challenge

(d) Security Assessment on Google Android

- Evolution of Google Android, security requirements and challenges, possible solution for at least one challenge

(e) Smart Grid Security

- Evolution of smart grid, security requirements and challenges, possible solution for at least one challenge

(f) Addressing the Insider Threat

- Evolution of insider threat, security challenges, possible solution for at least one challenge

(g) Privacy-Aware Role-Based Access Control

- Evolution of Privacy-Aware Role-Based Access Control, security requirements and challenges, possible solution for at least one challenge

(h) RFID Technology Security

- Evolution of RFID Technology, security requirements and challenges, possible solution for at least one challenge

(i) Security in eHealthcare System

- Evolution of eHealthcare system, security requirements and challenges, possible solution for at least one challenge

(j) Security and Privacy in Online Social Network

- Evolution of online social network, security requirements and challenges, possible solution for at least one challenge

(k) Security in Electronic Voting

- Evolution of Electronic Voting system, security requirements and challenges, possible solution for at least one challenge

(l) Security in Wireless Sensor Networks

- Evolution of wireless sensor network, security requirements and challenges, possible solution for at least one challenge

(m) Security in Vehicular Ad Hoc Networks

- Evolution of Vehicular Ad Hoc Network, security requirements and challenges, possible solution for at least one challenge

(n) Security in Wireless Mesh Networks

- Evolution of Wireless Mesh Networks, security requirements and challenges, possible solution for at least one challenge