McGill

DECEMBER 2021
FINAL EXAMINATION

Cryptography and Data Security

COMP 547 section 001

21st Dec. 2021 9:00-12:00

EXAMINER:	Prof. Claude Crépeau	ASSOC. EXAMINER:	Prof. Prakash Panangaden

STUDENT NAME:		**McGILL ID:**									

EXAM:	CLOSED BOOK ☐ OPEN BOOK ☒
	SINGLE-SIDED ☐ PRINTED ON BOTH SIDES OF THE PAGE ☒
	MULTIPLE CHOICE ANSWER SHEETS: YES ☐ NO ☒ NOTE: The Examination Security Monitor Program detects pairs of students with unusually similar answer patterns on multiple-choice exams. Data generated by this program can be used as admissible evidence, either to initiate or corroborate an investigation or a charge of cheating under Section 17 of the Code of Student Conduct and Disciplinary Procedures. ANSWER BOOKLET REQUIRED: YES ☒ NO ☐ EXTRA BOOKLETS PERMITTED: YES ☒ NO ☐ ANSWER ON EXAM: YES ☐ NO ☒
	SHOULD THE EXAM BE: RETURNED ☒ KEPT BY STUDENT ☐
CRIB SHEETS:	PERMITTED ☒ Specifications: no page limit. NOT PERMITTED ☐
DICTIONARIES:	TRANSLATION ONLY ☐ REGULAR ☒ NOT PERMITTED ☐
CALCULATORS:	NOT PERMITTED ☒ PERMITTED (Non-Programmable) ☐ PERMITTED (Programmable) ☐
ANY SPECIAL INSTRUCTIONS: e.g. molecular models	• This examination is worth 40% of your final grade. • The exam consists of 2 questions (13 sub-questions) on 4 pages (title page included).

Suggestion: read all the questions and their values before you start answering.

Question 1. In c^o^de [1] **(10+5+5+5+5+10+5+10+10+5 = 70 points)**

Let $n = pq$ be an RSA modulus. Let $\mathbb{G}_n = \mathrm{GL}(2, \mathbb{Z}_n)$ be the set of invertible 2×2 matrices where all operations are modulo n. A useful fact is that $|\mathbb{G}_n| = n\phi(n)^2(p+1)(q+1)$.

[10%] **1)** Show how to factor n given n and $|\mathbb{G}_n|$.

Let A and C be two non-commuting matrices of $\mathbb{G}_n$ (such that $AC \neq CA$).

[5%] **2)** Find a matrix $C \in \mathbb{G}_{15}$ that does not commute with $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

Let $B = C^{-1}A^{-1}C$ and $G \leftarrow C^r$ for some random $r \leq n^4$ (a good approximation of $|\mathbb{G}_n|$). Let (n, A, B, G) be the public parameters of a public-key encryption scheme and C be the corresponding private key.

[5%] **3)** Prove that $GC = CG$.

Consider the <u>encryption pre-processing</u> as follows :

Let $D \leftarrow G^s$ for some random $s \leq n^4$
Let $E := D^{-1}AD$
Let $K := D^{-1}BD$

[5%] **4)** Using big-O notation, establish a good upper bound on the running time of this pre-processing algorithm.

Consider the encryption procedure $\text{Enc}(\mu)$ as follows :

Let $\mu' := K\mu K$ where μ is the plaintext 2×2 matrix.
The pair (E, μ') is the cipher-text.

[5%] **5)** Establish a good upper bound on the running time of this encryption algorithm.

Consider the decryption procedure $\text{Dec}(E, \mu')$ as follows :

Let $L := C^{-1}EC$
Let $\mu := L\mu' L$ be the plaintext.

[10%] **6)** Show that $L = K^{-1}$ and thus that $\text{Dec}(\text{Enc}(\mu)) = \mu$ for all matrix $\mu \in \mathbb{G}_n$.

[5%] **7)** Establish a good upper bound on the running time of this decryption algorithm.

[10%] **8)** Compare the performances of this scheme with the El-Gammal scheme.

[10%] **9)** Formulate a computational assumption on which the security of this scheme rests.

This scheme was briefly considered as a good alternative to the RSA/El-Gammal public-key encryption scheme because of its relative efficiency. Unfortunately, it was soon after broken.

[5%] **10)** Prove that if you have any multiple $C' := \nu C$ where ν is a scalar modulo n, you can decrypt using C' instead of C. (Hint: set $L' := C'^{-1}EC'$.)

To obtain a multiple of C, notice that $CG - GC = CB - A^{-1}C = 0$ imposes 8 public linear constraints on $C = \begin{pmatrix} c_{00} & c_{01} \\ c_{10} & c_{11} \end{pmatrix}$ with only 4 unknowns. It turns out **[2]** the solution space of these 8 constraints is the line $\ell = \nu C$. Using a little bit of linear algebra, according to Q10, any point on that line can be used to decrypt.

---

[1] "In C^{o}de: a mathematical journey" by Sarah Flannery with David Flannery. Algonquin books of Chapel Hill. 2002.
[2] "A Brief Retrospective Look at the Cayley-Purser Public-key Cryptosystem, 19 Years Later", by Douglas R. Stinson. Cryptology ePrint Archive, Report 2018/270, 2018. https://ia.cr/2018/270.

Question 2. Perfect Encryptions **(10 + 10 + 10 = 30 points)**

Let q and p = 2q+1 both be primes. Let g be a generator of QR_p.
Let (p,q,g) be publicly known parameters in relation to some private-key encryption system.
For each of the following private-key encryption algorithm give me

- the decryption algorithm corresponding to the encryption,
- a (non-trivial) key-space K, and a (non-trivial) message-space M such that the given encryption scheme is perfectly secret, for all $k \in K$ $m \in M$.

[10%] **(i)** $Enc_k(m) := m+k \bmod p$

[10%] **(ii)** $Enc_k(m) := m \cdot k \bmod p$

[10%] **(iii)** $Enc_k(m) := k^m \bmod p$