McGill

DECEMBER 20212
FINAL EXAMINATION

Cryptography and Data Security

COMP 547 section 001

15th Dec. 2025 18:00-21:00

EXAMINER:	Prof. Claude Crépeau	ASSOC. EXAMINER:	Prof. Robert Robere

STUDENT NAME:		**McGILL ID:**									

<table>
<tr><td rowspan="7">EXAM:</td><td>CLOSED BOOK ☐ OPEN BOOK ☒</td></tr>
<tr><td>SINGLE-SIDED ☐ PRINTED ON BOTH SIDES OF THE PAGE ☒</td></tr>
<tr><td>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.</td></tr>
<tr><td>ANSWER BOOKLET REQUIRED: YES ☒ NO ☐</td></tr>
<tr><td>EXTRA BOOKLETS PERMITTED: YES ☒ NO ☐</td></tr>
<tr><td>ANSWER ON EXAM: YES ☐ NO ☒</td></tr>
<tr><td>SHOULD THE EXAM BE: RETURNED ☒ KEPT BY STUDENT ☐</td></tr>
<tr><td>CRIB SHEETS:</td><td>PERMITTED ☒ <u>Specifications</u>: no page limit.
NOT PERMITTED ☐</td></tr>
<tr><td>DICTIONARIES:</td><td>TRANSLATION ONLY ☐ REGULAR ☒ NOT PERMITTED ☐</td></tr>
<tr><td>CALCULATORS:</td><td>NOT PERMITTED ☒
PERMITTED (Non-Programmable) ☐ PERMITTED (Programmable) ☐</td></tr>
<tr><td>ANY SPECIAL INSTRUCTIONS: e.g. molecular models</td><td>• This examination is worth 40% of your final grade.

• The exam consists of 10 questions on 3 pages (title page included).</td></tr>
</table>

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

Part I. Katz and Lindell

[10%] 3.29 What is the effect (on the decrypted plaintext) of a single bit flip in the ciphertext when using the **CBC**, **OFB**, and **CTR** modes of operation?

[10%] 4.23 Show that the polynomial-based difference-universal function seen in class (theorem 4.17) is not strongly universal.

[10%] 9.27 Let GenRSA be as in Section 9.2.4. Prove that if the RSA problem is hard relative to GenRSA then Construction 9.80 is a fixed-length collision-resistant hash function.

CONSTRUCTION 9.80

Define (Gen, H) as follows:

- Gen: on input 1^n, run $\mathsf{GenRSA}(1^n)$ to obtain N, e, d, and select $y \leftarrow \mathbb{Z}_N^*$. The key is $s := \langle N, e, y \rangle$.
- H: if $s = \langle N, e, y \rangle$, then H^s maps inputs in $\{0,1\}^{3n}$ to outputs in $\mathbb{Z}_N^*$. Let $f_0^s(x) \stackrel{\text{def}}{=} [x^e \bmod N]$ and $f_1^s(x) \stackrel{\text{def}}{=} [y \cdot x^e \bmod N]$. For a $3n$-bit long string $x = x_1 \cdots x_{3n}$, define

$$H^s(x) \stackrel{\text{def}}{=} f_{x_1}^s\left(f_{x_2}^s\left(\cdots\left(1\right)\cdots\right)\right).$$

Hint: Show that if you find a collision of H^s then you can compute $\mathrm{Dec}_{sk}(y)$.

[10%] 13.2 In class (book Section **13.4.1**) we showed an attack on the plain RSA signature scheme in which an attacker forges a signature on an arbitrary message using two signing queries. Show how an attacker can forge a signature on an arbitrary message using a single signing query. **HINT**: one of the two queries in the previous attack can be simulated using the public-key instead of the oracle.

[10%] 13.9 Assume revocation of certificates is handled in the following way: when a user Bob claims that the private key corresponding to his public key pk_B has been stolen, the user sends to the CA a statement of this fact signed with respect to pk_B. Upon receiving such a signed message, the CA revokes the appropriate certificate.

Explain why it is not necessary for the CA to check Bob's identity in this case. In particular, explain why it is of no concern that an adversary who has stolen Bob's private key can forge signatures with respect to pk_B.

Part 2. Perfect Encryptions

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 $k \in K$, $m \in M$. ("non-trivial" = "contains at least 2 elements")

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

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

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

[10%] **Part 3. CPA security**

You are given three encryption schemes Π_1, Π_2, and Π_3. You know that at least one of them is CPA-secure. Build an encryption scheme from these three that is guaranteed CPA-secure.

[10%] **Part 4. Existential Unforgeability**

You are given three digital signature schemes Π_1, Π_2, and Π_3. You know that at least one of them is existentially unforgeable under adaptive chosen-message attack. Build a digital signature scheme from these three that is guaranteed to be existentially unforgeable under adaptive chosen-message attack.