McGill

DECEMBER 2023

FINAL EXAMINATION

Cryptography and Data Security

COMP 547, section 001

18 December 2023, 14:00

EXAMINER: Claude Crépeau

ASSOC. EXAMINER: Giulia Alberini

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 16 of the Code of Student Conduct and Disciplinary Procedures. ANSWER BOOKLET REQUIRED: **YES** ☒ NO ☐ EXTRA BOOKLETS PERMITTED: **YES** ☒ NO ☐ ANSWER ON EXAM: YES ☐ **NO** ☒
	THE EXAM SHOULD BE: **RETURNED** ☒ KEPT BY STUDENT ☐
CRIB SHEETS:	**PERMITTED** ☒ Specifications: **no 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 10 questions on 3 pages (title page included).**

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

Part 1.

[10%] 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%] Exhibit a function family $f_k : \{0,...,7\} \rightarrow \{0,1\}$ which is strongly universal.

[10%] We know it is possible to have **MAC**s that are secure without computational assumptions. Why not signatures ?

[10%] 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%]

Part 2. CPA security

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

[10%]

Part 3. Existential Unforgeability

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

Part 4. 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)** $\text{Enc}_k(m) := m + k \mod p$

[10%] **(ii)** $\text{Enc}_k(m) := m \cdot k \mod p$

[10%] **(iii)** $\text{Enc}_k(m) := m^k \mod p$

Part 5. OHNISHI

[10%] In 1988 a japanese master student called Ohnishi realized and proved that a Feistel network of 3 rounds using 2 (instead of 3) pseudo-random functions is enough to obtain a pseudo-random permutation. I give an example below using DES with 2 independent keys k_1 and k_2.

My question is rather open-ended : compare this DES variation to triple-DES with two or three keys as we learned it in class. Be as exhaustive as possible about as many aspects as possible.

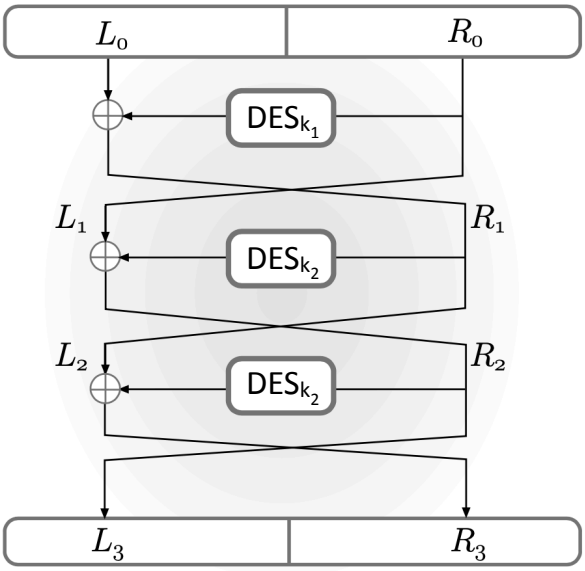

FIGURE 6.5: A three-round Feistel network.