Faculty of Science

McGill

Final Examinations Winter 2020

1. Introduction

The purpose of this exam is to provide you with an opportunity to demonstrate what you have learned in this course. Because of the challenging situation imposed by COVID-19, the Faculty of Science wants to ensure that you are fully aware of the special measures we are taking to ensure the exam is fair and that you have enough time to complete and submit it.

Please read the complete cover page and sign your agreement to the academic integrity statement on page 2 before beginning your exam.

2. General information

Course (eg FCSI 101):	COMP 547
Type of exam:	Take-home
Date and time of exam release: (eg APR-20 09.00)	APR-29 09:00
Deadline for exam submission: (eg APR-23 09.00)	MAY-02 09:00
Method of submission:	myCourses Assignment
Examiner:	Prof. Claude Crépeau Dr. Giulia Alberini claude.crepeau@mcgill.ca
Associate Examiner:	Dr. Giulia Alberini giulia.alberini@mail.mcgill.ca

3. Terms and Conditions

a) Use of the following materials during the exam is permitted (check indicates allowed, all blank for closed book):
- course textbook..... ☑
- your own class notes..... ☑
- any book online..... ☑
- myCourses page..... ☑
- other..... ☐ If other please specify

b) Online searching of subject material/related exam questions is permitted: Yes ○ No ◉

c) Communicating with classmates regarding any aspect of the exam or course once you begin the exam **is not permitted**.

d) Posting or sharing the exam content, including exam questions, or your answers both during and after submission **is not permitted**.

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

Question 1. Operations à la mode **(5 + 10 + 10 = 25 points)**

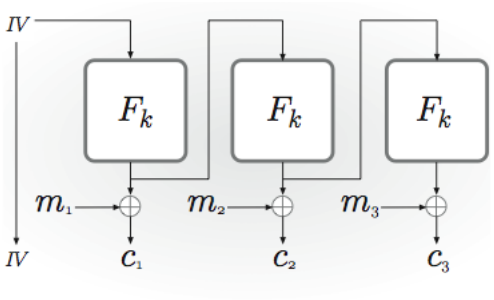

FIGURE 3.7: Output Feedback (OFB) mode.

In public-key encryption schemes some modes of operations are fairly useless because the decryption function is not necessary for the decryption process.

(i) Explain this problem in details for the **OFB** mode above (assuming F_k is a Public-key block cipher).

A suggested modification to resolve this issue is to give up on *providing the IV* as part of the ciphertext $\langle IV,c_1,c_2,c_3,\ldots\rangle$ but to provide instead a similar *TV* (for *terminal vector*) obtained at the end of the encryption process instead of the beginning $\langle c_1,c_2,c_3,\ldots,TV\rangle$.

(ii) Make this idea explicit for the **OFB** mode (assuming F_k is a Public-key invertible block cipher).

(iii) What other modes of operation can be adapted in a similar fashion ? Explain.

Question 2. El Gamal-like perfect encryption **(5 + 20 = 25 points)**

Let q and p=2q+1 both be primes. Let g be a generator of QR_p.
Let (p,q,g) be public parameters for some encryption system.
Consider the following two private-key probabilistic encryption schemes for messages $m \in QR_p$.
Alice and Bob agree on a random private-key x, s.t. $1 \le x \le q-1$.

$Enc_x(m)$: Choose r at random, $1 \le r \le q-1$ and send $[\, g^r , g^{xr}m \,]$
$Enc'_x(m)$: Choose r at random, $1 \le r < q-1$ and send $[\, g^r, g^{xr}\, m \,]$.

I. Tell me the decryption scheme of these two encryption algorithms.

II. One of these two schemes is perfectly secret whereas the other is not.
Tell me which is which and prove your answers.

Question 3. CPA+ **(10 + 10 + 5 = 25 points)**

When we discussed the AIGCD based public-key crypto-system I mentioned that in order to obtain a fully homomorphic scheme the user creating the public parameters must publish an encrypted version of the private-key. This inspires this question.

In the CPA-security experiment the adversary must provide a pair of *known* messages m_0, m_1 and try to distinguish the encryption of which one he later receives.

a) Extend the notion of CPA security to CPA+ security where the adversary *does not necessarily know the plaintexts* m_0, m_1. In particular describe a CPA+ security experiment where the adversary can provide two algorithms a_0, a_1 involving not only known messages but also secret parameters like the private-key k (known only to the experiment) to allow the experiment to compute plaintexts m_0, m_1.

b) Explain how satisfying your definition of CPA+ security would imply that publishing an encryption of the private-key is not a security concern.

c) Explain why a similar CCA+ security notion does not make much sense.

Question 4. OHNISHI **(25 points)**

In 1988 a japanese master student called Ohnishi realized 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: <u>compare</u> 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.

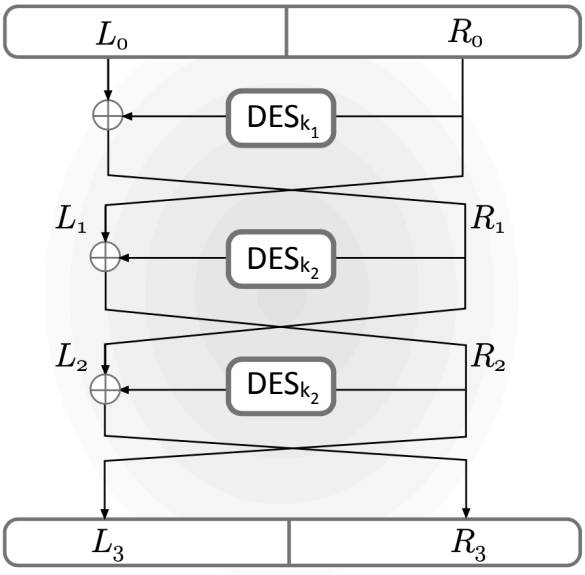

FIGURE 6.5: A three-round Feistel network.