McGill

APRIL 2015
Final Examination

FINAL EXAMINATION

Computer Science COMP-547B
Cryptography and Data Security

27 APRIL 2015, 14h00

Examiner:	Prof. Claude Crépeau	Assoc Examiner:	Prof. David Avis

INSTRUCTIONS:

• This examination is worth 50% of your final grade.

• The total of all questions is 105 points.

• Each question heading contains (in parenthesis) a list of values for each sub-questions.

• This is an **open book** exam. **All documentation is permitted.**

• Faculty standard calculator permitted only.

• The exam consists of 5 questions on 3 pages, title page included.

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

Question 1. Perfect RSA ? (5 +10+10 = 25 points)

Consider an RSA crypto-system with keys **(n, e, d)** except that only **n=p*q** is publicly available (but neither **e** nor **d**).

I) How many key pairs **(e,d)** are possible for a fixed **n** ? **HINT**: use function **φ**.

Assume Alice and Bob use **(e,d)** as the secret encryption-decryption keys of an RSA crypto-system **mod n** for exactly one message **m** in $\mathbb{Z}_n^*$.

II) Explain whether this one-time system is perfectly secure or not.

Assume Alice and Bob use **(e,d)** as the secret encryption-decryption keys of an RSA crypto-system **mod n** for exactly one message **b** in **{0,1}** encoded as a random even number from $\mathbb{Z}_n^*$ if **b=0** and encoded as a random odd number from $\mathbb{Z}_n^*$ if **b=1**.

III) Explain whether this one-time system is perfectly secure or not.

Question 2. Pseudo-random permutation (10 + 10 = 20 points)

Let **Π** be a pseudo-random **permutation** family.

- Explain why it must be difficult to compute **k** using oracle access to **Π_k**.
- Explain why it must be difficult to compute **$\Pi_k^{-1}(k)$** using oracle access to **Π_k**.

Question 3. Computational Assumption (15 points)

Consider the Discrete Logarithm Assumption modulo **n**, where **n=p*q**. Suppose we have an efficient algorithm **D** to completely break this assumption, that is

given a modulus **n**, a base **b**, and a target **t**, **D(n,b,t)=x** such that **$t \equiv b^x \pmod{n}$**.

Show an efficient algorithm for factoring **n** using algorithm **D**.
HINT: Think of RSA and once again use algorithm RSA-factor.

Question 4. CBC-MAC (15 points)

4.15 Show that appending the message length to the *end* of the message before applying basic CBC-MAC does not result in a secure MAC for arbitrary-length messages.

HINT: show how you can extend such a message by adding a new length at the *end*.

Question 5. Hashing (5+5+5+5+10 = 30 points)

Let **h** : $\{0,1,\ldots,9\}^8 \rightarrow \{0,1,\ldots,9\}^4$ be the following hash function

$$\mathbf{h(d_1d_2d_3d_4d_5d_6d_7d_8) = d_1{+}d_2 \bmod 10 \mid d_3{+}d_4 \bmod 10 \mid d_5{+}d_6 \bmod 10 \mid d_7{+}d_8 \bmod 10}$$

a) Show that **h(55555555) = 00000**.

b) Show that **h(a0b0c0d0) = h(0a0b0c0d) = abcd**.

c) What is **h(03512493)** ?

d) Find a collision of **h**.

e) Compute the value of **H(423879623045)** where **H** is the Merkle-Damgård transform of **h**.

*** Show all your calculations so I can follow them even if you make errors ***