McGill
APRIL 2013
Final Examination

FINAL EXAMINATION

Computer Science COMP-547B
Cryptography and Data Security

29 APRIL 2013, 9h00

Examiner:	Prof. Claude Crépeau	Assoc Examiner:	Prof. Patrick Hayden

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 6 questions on 3 pages, title page included.

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

Question 1. Perfect RSA ? (10 +10 = 20 points)

Consider an RSA crypto-system with keys **(N,e,d)** as usual except that only **N** is publicly available.

I) By definition, we know that m^{ed} **mod N** ≡ **m** for **m** s.t. **gcd(m,N)=1**. Using the Chinese remainder theorem show that m^{ed} **mod N** ≡ **m** for **m** s.t. **gcd(m,N)>1** as well.

II) Assume Alice and Bob use **(e,d)** as the private encryption-decryption keys of an RSA crypto-system **mod N** for exactly one message **m**, **0<m<N**. Explain whether this one-time system is perfect according to Shannon's definition.

Question 2. DDES (8 + 7 = 15 points)

Consider the 128-bit block cipher DDES obtained by combining two instances of DES in a two-round Feistel network. The total key-size of this new cipher would be 112 bits.

- Let **x** be a 128-bit input and **k** be a 112-bit key. Give an explicit formula for the encryption and decryption functions of DDES.
- Discuss the pseudo-random nature of the permutation defined by DDES.

Question 3. Rivest (10 + 10 = 20 points)

Remember the construction by Rivest of a private-key crypto-system based on the existence of an arbitrary private-key authentication scheme.

a) Show that the definition of security of the MAC is not sufficient for the resulting crypto-system to have undistinguishable encryptions in the presence of an eavesdropper.

b) Define a stronger security notion for MACs such that the construction of Rivest yields a crypto-system with undistinguishable encryptions in the presence of an eavesdropper.

Question 4. Number Theory vs Crypto (5 + 5 + 5 = 15 points)

For each of the following Number Theoretical concepts, name a Cryptographic concept which is related and explain the relation.

1) Chinese remainder theorem.

2) Quadratic Residuosity.

3) $\mathbb{F}_{2^k}$, for $k \geq 1$.

Question 5. Elgamal Details (10 +10 = 20 points)

Instantiate all the parameters of an Elgamal encryption scheme from a prime **p=47** and give me an encryption of **m=10**. Give me all the details of the crypto-system, taking into account all the implementation details seen in class.
(All your calculations can be done by hand.)

Question 6. Merkle-Damgård... (8 + 7 = 15 points)

In Construction 4.13 the size L of the input string x is such that $L<2^{l(n)}$. It is very peculiar that if we hash a string x of length $2^{l(n)}-1$ using H^s, the time needed to hash the string is greater than the time needed to find a collision of h^s by a birthday attack. This seems to imply that hashing exponentially long strings is insecure.

i) Explain why this is not contradicting the security statement (Theorem 4.14) that if h^s is collision-resistant then H^s is also collision-resistant.

ii) Why do we still use an exponential bound ($L<2^{l(n)}$) in Construction 4.13 and not a polynomial bound such as $L<l(n)^k$?