McGill

DECEMBER 2011
Final Examination

FINAL EXAMINATION

Computer Science COMP-547A
Cryptography and Data Security

16 DECEMBER 2011, 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 4 pages, title page included.

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

Question 1. Pseudo-random function ? (5+5+5+5 = 20 points)

Let f_k for $k \in \{0,1\}^n$ be a candidate pseudo-random function family.

i) Suppose f_k and $f_{\bar{k}}$ are actually the same exact function, for all possible values of k. Does that contradict the pseudo-randomness of f_k ? Explain your answer.

ii) Suppose $f_k(\mathbf{000\ldots0}) = \mathbf{000\ldots0}$ for all possible values of k. Does that contradict the pseudo-randomness of f_k ? Explain your answer.

iii) Suppose $f_k(\mathbf{000\ldots0}) = k$ for all possible values of k. Does that contradict the pseudo-randomness of f_k ? Explain your answer.

iv) Suppose $f_k(k) = k$ for all possible values of k. Does that contradict the pseudo-randomness of f_k ? Explain your answer.

Question 2. Number Theory (8+7 = 15 points)

Let N=**143** be an RSA modulus.

- Find all the square roots r ($1 \le r \le N$) of **1** (mod N).
- Give r_0 and r_1 that are two square roots of 1 such that $r_0 \not\equiv \pm r_1 \pmod{N}$.
- What are $\gcd(r_0 - r_1, N)$ and $\gcd(r_0 + r_1, N)$?

7.10 Corollary 7.21 shows that if $N = pq$ and $ed = 1 \bmod \phi(N)$ then for all $x \in \mathbb{Z}_N^*$ we have $(x^e)^d = x \bmod N$. Show that this holds for all $x \in \mathbb{Z}_N$.

Hint: Use the Chinese remainder theorem.

Question 3. Negligible (5+5+5 = 15 points)

Remember

DEFINITION 3.4 A function **f** is _negligible_ if for every polynomial $p(\cdot)$ there exists an N such that for all integers $n > N$ it holds that

$$f(n) < 1/p(n)$$

A) Give an example of a negligible function and prove it is.

We can define non-negligible by simply changing as follows

DEFINITION 3.4* A function **f** is _non-negligible_ if there exists a polynomial $p(\cdot)$ such that for all integers n it holds that

$$f(n) > 1/p(n)$$

B) Give an example of a non-negligible function and prove it is.

C) Give an example of a function which is _neither negligible nor non-negligible_ and prove it is.

Question 4. Mac & Signature (7+7+7 = 21 points)

1) Explain why the term “Signature” is only used for the public-key setting.

2) Explain why textbook RSA is NOT existentially unforgeable.

3) It is possible to have MACs that are secure without computational assumptions. Why not signatures ?

Question 5. CPA security vs insecurity… (10+8+8+8 = 34 points)

i) Suppose pseudo-random permutations exist. Give two constructions of **CPA**-secure encryption schemes (for arbitrary-length messages) with identical key space.

You are given two **CPA**-secure encryption schemes $\mathbf{E_1}$=(**Gen**,$\mathbf{Enc_1}$,$\mathbf{Dec_1}$), and $\mathbf{E_2}$=(**Gen**,$\mathbf{Enc_2}$,$\mathbf{Dec_2}$) that share the same key-space and have the same key generation algorithm **Gen**.

ii) Consider the combined cryptosystem where encryption is the pair ($\mathbf{Enc_{1,k_1}}(\boldsymbol{m})$,$\mathbf{Enc_{2,k_2}}(\boldsymbol{m})$) where encryptions are done using INDEPENDENT KEYS $\boldsymbol{k_1}$, $\boldsymbol{k_2}$. Explain why this resulting system is still **CPA**-secure.

iii) Consider the combined cryptosystem where encryption is the pair ($\mathbf{Enc_{1,k}}(\boldsymbol{m})$,$\mathbf{Enc_{2,k}}(\boldsymbol{m})$) where both encryptions are done using THE SAME KEY $\boldsymbol{k}$. Explain why this resulting system might NOT be **CPA**-secure.

Suppose I give you a **CPA**-secure encryption $\mathbf{E_0}$=($\mathbf{Gen_0}$,$\mathbf{Enc_0}$,$\mathbf{Dec_0}$).

iv) Using $\mathbf{E_0}$, give an example of such systems $\mathbf{E_1}$, $\mathbf{E_2}$ with properties as in **iii)**. (You should involve $\mathbf{E_0}$ into the construction of $\mathbf{E_1}$ and of $\mathbf{E_2}$ so that they are as secure individually as $\mathbf{E_0}$ but not together…)

HINT: Put an apparent useless part in encrypted messages that will reveal the key when you get both $\mathbf{Enc_{1,k}}(\boldsymbol{m})$ and $\mathbf{Enc_{2,k}}(\boldsymbol{m})$,.