McGill

DECEMBER 2010
Final Examination

FINAL EXAMINATION

Computer Science COMP-547A
Cryptography and Data Security

6 DECEMBER 2010, 9h00

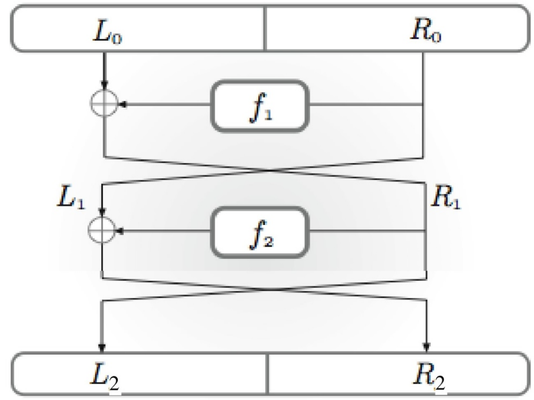
Examiner:	Prof. Claude Crépeau	Assoc Examiner:	Prof. David Avis

INSTRUCTIONS:

- This examination is worth 50% of your final grade.
- The total of all questions is 100 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 4 questions on 3 pages, title page included.

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

Question 1. Super Secure AES? (4+8+8+10 = 30 points)



Start with 256-bit **AES**. Mr Paranoid, who wants a super secure block cipher, considers embedding this version of **AES** in a Fiestel structure as shown on the right. Assume he instantiates the pseudo-random functions f_1 and f_2 with **AES** as above, using two completely independent keys.

i) What would be the resulting block size and key size of this new cipher ?

ii) Show that the resulting block cipher does not behave as a pseudo-random permutation.

iii) What can you say about the security of the resulting block cipher ??

iv) Consider randomized versions of this block cipher:

version A : to encrypt an R_0, choose a random L_0 and apply the new block cipher.
version B : to encrypt an L_0, choose a random R_0 and apply the new block cipher.

Compare these two versions in terms of **CPA**-security.

Question 2.  MAC (10+6+8 = 24 points)

You are given a (**CPA**-secure) Public-key encryption scheme **E**=(Gen$_{\mathbf{E}}$,Enc,Dec), a (secure†) digital signature scheme **S**=(Gen$_{\mathbf{S}}$,Sig,Vrfy$_{\mathbf{S}}$) and a (secure†) private-key authentication scheme **A**=(Gen$_{\mathbf{A}}$,Auth,Verfy$_{\mathbf{A}}$). The (private-key) latter is substantially more efficient than the (public-key) formers.

Bob has never met Alice before, but through a trusted **CA**, Bob knows Alice's (encryption) public-key $pk_{\mathbf{A}}$ and (signature) public-key $qk_{\mathbf{A}}$ and Alice knows Bob's (encryption) public-key $pk_{\mathbf{B}}$ and (signature) public-key $qk_{\mathbf{B}}$.

i) Explain how you may combine (only) these three ingredients (**E**, **S** and **A**) and allow Bob to authenticate an enormous amount of data to Alice, as efficiently as possible. Justify your choices.

ii) Give specific systems to instantiate each of **E**, **S** and **A**.

iii) Explain why having either only **E**, **A** or only **S**, **A** is fairly useless for the same task as in **i)**…

† existentially unforgeable under an adaptive chosen-message attack.

Question 3. Short and sweet (8+8 = 16 points)

7.5 Compute the final two (decimal) digits of 3^{1000} (by hand).

Hint: The answer is $[3^{1000} \bmod 100]$.

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 $x \in \mathbb{Z}_N$. (even if $\mathbf{gcd}(x,N) > 1$)

Hint: Use the Chinese remainder theorem.

Question 4. El Gamal vs Al Gemel (5+7+6+7+5 = 30 points)

A) Let p be a random 1024-bit prime. If g is a generator of the entire group $\mathbb{Z}^*_{p\text{-}1}$, is it likely that the decisional Diffie-Hellman problem be hard $\mathbf{mod}\ p$? Justify your answer.

B) Consider a variation on El Gamal crypto-system called "Al Gemel" :

to encrypt a message m in $\mathbb{Z}^*_q$, choose a random k and send « h^k, $g^k{\times}m^2$ »

where the private parameter is a and the public parameters are « $p := 2q+1$, g, $h := g^a$ » with a prime q and a generator g of the quadratic residue sub-group of $q := (p\text{-}1)/2$ elements.

i) Given a, show how we can efficiently compute an exponent b such that $g^k = (h^k)^b$.

ii) Explain all the details of the resulting decryption algorithm.

iii) Show that (when $q = (p\text{-}1)/2$ is prime) the Al Gemel crypto-system is essentially the same as the El Gamal crypto-system !!!

iv) Why is this not the case when q is not prime ??