Faculty of Science
Final Examination

Computer Science 308-547A
Cryptography and Data Security

Examiner:	Prof. Claude Crépeau	**Date:**	Dec 9, 2003
Associate Examiner:	Mr. George Savvides	**Time:**	14:00 – 17:00

INSTRUCTION:

∞ This examination is worth 50% of your final grade.
∞ The total of all questions is 105 points.
∞ Each question is assigned a value found in parenthesis next to it.
∞ This is an **open book** examination. All documentation is permitted.
∞ Faculty standard calculator permitted only.
∞ This examination consists of 6 questions on 3 pages, including title page.

Suggestion:
read all the questions and their value before you start

QUESTION 1. EASY BITS OF EL GAMAL (15 POINTS)

Let $\mathbf{p}$ be an odd prime and α be a primitive element $\mathbf{mod\ p}$.

a) Show that given $\mathbf{p}, \alpha, \alpha^x \mathbf{\ mod\ p}$, the predicate $\mathbf{lsb_{p-1}(x)}$ is easy to compute.

Let $(\mathbf{p}, \alpha, \beta = \alpha^a \mathbf{\ mod\ p})$ be an *El Gamal* public key and $\mathbf{a}$ be the private key.

b) Show that given (γ, δ) the *El Gamal* encryption of a message $\mathbf{m}$, there is a predicate of $\mathbf{m}$ that is easy to compute.

c) Give a condition on the private $\mathbf{a}$ such that given only δ from the *El Gamal* encryption of a message $\mathbf{m}$, this same predicate of $\mathbf{m}$ is still easy to compute.

QUESTION 2. EQUALITY VERIFICATION (20 POINTS)

Alice and Bob would like to compare very large documents without disclosing each other what these documents are. Their goal for any two documents $\mathbf{D_A}, \mathbf{D_B}$ is to find out whether they are equal $(\mathbf{D_A=D_B})$ or not $(\mathbf{D_A \neq D_B})$ but nothing else. Alice and Bob are not assumed to have met before or shared any secret key.

A) Explain how this can be done using notions such as PRBG, PRΦG, Cryptographic Hash Functions, Bloc Ciphers, etc.

B) Propose a most efficient implementation of your proposal using tools we learned in class, but make sure you use up-to-date tools in terms of security (e.g. don't use **DES**)…

QUESTION 3. RSA EXPONENT 3 (15 POINTS)

Let Bob, Chuck and Dan be three friends of Alice. All three of them have a public RSA modulus $\mathbf{N_B}$ (resp. $\mathbf{N_C}, \mathbf{N_D}$) of 512 bits and public encryption exponent **3**. Suppose Alice sends the same message $\mathbf{m < N_M = \min\{N_B, N_C, N_D\}}$ to each of them, encrypted as $\mathbf{C_B}$ to Bob, $\mathbf{C_C}$ to Chuck and $\mathbf{C_D}$ to Dan, where $\mathbf{C_{Id} = m^3 \mathbf{\ mod\ } N_{Id}}$, for $\mathbf{Id=B,C,D}$.

a) Show that using the Chinese Remainder Theorem, anyone who has observed all ciphertexts $\mathbf{C_B}, \mathbf{C_C}, \mathbf{C_D}$ can recover the unique $\mathbf{C < N_M^3}$ such that

$$\mathbf{C_B \equiv C \ (mod\ N_B)}$$
$$\mathbf{C_C \equiv C \ (mod\ N_C)}$$
$$\mathbf{C_D \equiv C \ (mod\ N_D)}$$

b) Show that indeed $\mathbf{m}$ is simply $\sqrt[3]{\mathbf{C}}$ over the integers.

c) Describe an efficient general algorithm to simply compute $\sqrt[3]{\mathbf{X}}$ over the integers.

QUESTION 4. DES -- HASH FUNCTION? (15 POINTS)

Consider the following function hashing **120** bits down to **64**, **h:** $\{0,1\}^{56} x \{0,1\}^{64} \rightarrow \{0,1\}^{64}$

$$\langle k,x \rangle \rightarrow DES_k(x)$$

A) Argue whether **h** is secure against PreImage attacks.

B) Argue whether **h** is secure against Second PreImage attacks.

C) Argue whether **h** is secure against Collision attacks.

QUESTION 5. SHORT AND *SWEET* (25 POINTS) <u>**JUSTIFY YOUR ANSWERS.**</u>

(a) (5 points)
Explain why **DES** had to be replaced by **AES**.

(b) (5 points)
Compare the computational efficiency of the Blum-Blum-Shub and Blum-Micali PRBGs.

(c) (5 points)
Give two random variables **X** and **Y** over **{0,1}** such that $0<H(X)=H(Y)<1/2$ but $X \neq Y$.

(d) (5 points)
Let **(n,e)** and **d** be RSA public and private keys. Suppose $|n|=|e|=|d|=512$ **bits**.
What is the unicity distance of this public-key cryptosystem ?

(e) (5 points)
In practice, many people use a hybrid combination of a public-key cryptosystem and a secret-key cryptosystem: they use the PKC to transmit a "session key" used in a SKC. All encryption of messages are actually done using the session key. Explain the advantages and disadvantages of this method.

QUESTION 6. SHAFI & SILVIO (15 POINTS)

A) (5 points)
Show that the *Goldwasser-Micali* probabilistic encryption scheme exhibits a property similar to the RSA multiplicative property, i.e. $GM(b) \times GM(b') = GM(b \oplus b')$.

B) (10 points)
Show that if there exists an efficient algorithm **QR** that decides whether **X mod N** (with $(X/N)=+1$) is a quadratic residue or a quadratic non residue with probability **51%** (on average over all elements with $(X/N)=+1$) then there exists an efficient algorithm **DEC** that decrypts *Goldwasser-Micali* encrypted messages with probability nearly **100%.**