CS547A Homework set #5 (REVISED)

<u>**Due Wednesday December 3, 2003 in class at 13:30**</u>

Exercises (from Stinson's book)

<u>A MUST PROBLEM AND EXTRAS:</u>

• 5.11 (new) •

EXTRAs

(c) Is the result of **• 5.10 •** still valid using the decryption method of **• 5.11 •** ? Explain your answer.

(d) Using MAPLE™ find two random **100**-digit primes **p** and **q** with the property that **|gcd(p-1,q-1)|>75** digits.

(e) Find exponents **a,a',b** such that **|a|=|b|=|n|=200** digits whereas **|a'|<125** digits. Verify on **10** random examples that $(m^b)^{a'}$ **mod n = m**.

<u>ANY TWO OF THE FOLLOWING THREE PROBLEMS:</u>

• 4.5 (new) •

• 6.7 (new) •

• 7.6 (formerly 6.5) •

<u>Other Exercises</u>

<u>Blum-Goldwasser</u>

Let **n=p*q**, the product of two primes $p \underline{=} q \underline{=} 3$ **(mod 4),** be a modulus suitable for the **Blum-Goldwasser** cryptosystem. Suppose that we modify the cryptosystem and that in order to encrypt an **l-bit** message **x** we use the **BBS** generator **2l+t+1** times instead of only **l+1**. The initial **l+t** extra bits are used to authenticate **x** into a **t-bit** tag as $w=ax|_t(+)b$ where **a** is from F_2^l and **b** is from F_2^t.

The encryption would then be (y, w, s_{2l+t+1}) where **y** is from the original scheme.

(1) Explicit the decryption/verification algorithm of this encryption/authentication scheme.

(2) Show that even this modified scheme fails under **chosen cyphertext** attack.

(Assume that the decryption device returns the original plaintext **x** only when (y, w, s_{2l+t+1}) is correctly authenticated, otherwise an error message is issued)

More on back

Jacobi symbol and least significant bit

Let $n=p*q$, the product of two primes, and let $n-1$ be an element of $QNR_n[+1]$ i.e. the Jacobi symbol $(^{n-1}/_n) = +1$. Let **e** be an RSA public exponent **mod n**.

1) Give explicit conditions on **p** and **q** to have the Jacobi symbol $(^{n-1}/_n) = +1$.

Let **M** be a random variable describing the random choice of a plaintext $0<M<n$.

2) Show that $H[\ lsb_n(M)\ |\ (M^e/n)\ ] = H[\ lsb_n(M)\ ]$.

3) Use MAPLE™ to show that this may be false if the Jacobi symbol $(^{n-1}/_n) = -1$.

Goldwasser-Micali

Let $n=p*q$, the product of two primes, and let **y** be an element of $QNR_n[+1]$. Remember that the *Goldwasser-Micali* cryptosystem with public parameters **(n,y)** encrypts a **zero** bit by [a random square] x^2 **mod n** and a **one** bit by [a random pseudo-square] x^2y **mod n**.

Let $GM(m_1),GM(m_2)$ be the *Goldwasser-Micali* encryption of messages m_1 and m_2 as computed and sent by Bob to Alice. Suppose Bob applied his personal signature to the encryption of each bit.

Imagine the government witnessed Bob's transmission of both messages to Alice and they wish to have some minor information about the messages as follows.

(a) Show how Bob can prove that both $GM(m_1),GM(m_2)$ were encryptions of the same message $m_1=m_2$ without disclosing anything else about it.

(b) Show how Bob can prove that $GM(m_1),GM(m_2)$ were encryptions of messages m_1 and m_2 that differed in an **even** (including zero) or **odd** number of positions, without disclosing anything else about them.

(c) Assume m_1,m_2 have even length, $|m_1|=|m_2|=2k$. Show how Bob can prove that $GM(m_1),GM(m_2)$ were encryptions of different messages $m_1 \neq m_2$ by disclosing nothing except for the fact that they differed somewhere among all but one of the positions. (Bob can put aside one encrypted bit at a fixed position of $GM(m_1)$ and $GM(m_2)$, and then prove that the remaining truncated messages are different without disclosing anything about them except for the fact that they differ). Explain why we need messages of even length **2k**.

(d) How much uncertainty is left about m_1,m_2 when only learning that they differ ? How much uncertainty is left about m_1,m_2 when learning that they differ by the method suggested in (c) ?

(in both cases assume that the a priori uncertainty was maximum.)