# <u>COMP-647B Advanced Cryptography</u>

## Problem set #1

due on ***<u>Tuesday January 30, 2007</u>***

### 1. <u>MA vs AM</u>

Prove that **MA** $\subseteq$ **AM**.

### 2. <u>Code equivalence in ZK.</u>

We say that two binary matrices G, G' generate two *equivalent* linear codes C=span(G) and C'=span(G') if there exists a permutation matrix P (each row and column contain all "0" except for one "1") and a base change matrix S (full rank) such that

$$G' = SGP.$$

Give a *perfect* zero-knowledge interactive proof for the language

$L_{eqv}$ = { (G,G') | G, G' generate *equivalent* linear codes }.

### 3. <u>Hamiltonian in ZK.</u>

Give a *computational* zero-knowledge interactive proof for the Hamiltonian circuit problem under suitable computational assumption. (A directed graph G is Hamiltonian if its edges contain a circuit visiting each vertex exactly once.)

### 4. <u>RSA integers in ZK.</u>

**4.A** Let **RSA** be integers with exactly two distinct prime factors. Give a Zero-Knowledge interactive proof for the **RSA** numbers.

**HINT:**

We define **RSA** = {$n$ | $n=pq$ where $p,q$ are distinct primes}.
You may use without proof the following two results:

**Theorem 1**. If $n=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_\kappa}$ (which is not a square) has exactly $k$ distinct prime factors then exactly $2^{1-k}$ of the $x$ in $Z_n$* with Jacobi symbol +1 are quadratic residues mod $n$.

**Theorem 2**. Let $n$ be a composite number. If $n=p_1p_2\ldots p_k$ is a product of distinct primes then every $x$ in $Z_n$* has an $n^{th}$ root mod $n$, i.e. a $y$ such that $x \equiv y^n$ mod $n$. On the contrary, if $p_i=p_j$ for some $1\le i<j\le n$, then at most half the $x$ in $Z_n$* has an $n^{th}$ root mod $n$.

Construct two zero-knowledge proofs for the languages **WRSA** of **Weak-RSA** numbers and **SF** of square-free numbers:

**WRSA**={$n$ | $n=p^\alpha q^\beta$ where $p,q$ are distinct primes and $\alpha,\beta>0$}
**SF**={$n$ | $n=p_1p_2\ldots p_k$ is a product of distinct primes}

Notice that **RSA** = **WRSA** ∩ **SF**.

**4.B** Finally, if we define

**BLUM** = {$n$ | $n=pq$ where $p \equiv q \equiv 3$ mod 4, are distinct primes}

then prove that **BLUM** has a *statistical* **ZK** interactive proof.

**HINT:**

Define the **Weak-BLUM** integers as

**WBLUM** = {n | -1 is in $QNR_n[+1]$ }

Notice that **BLUM** = **RSA** ∩ **WBLUM**.