

## Cryptography Assignment 9

1. A Chinese Remainder code works as follows: Fix primes  $p_1 < p_2 < \dots < p_n$  such that  $p_n < 2p_1$ . The code of a message  $y$  is the tuple  $(y \bmod p_1, \dots, y \bmod p_n)$ . Note the alphabet size  $q = p_n$ .

If  $y$  is chosen from  $\{0, \dots, m-1\}$  what is the distance and rate of the code. Express these values as a function of  $q$ ,  $n$  and  $m$ .

2. A Hamiltonian cycle in an undirected graph is a cycle that hits every vertex exactly once. It is NP-complete to determine if a given undirected graph has a Hamiltonian cycle.

Give a zero-knowledge protocol for Hamiltonian cycle. (A specific protocol for Hamiltonian cycle, not a reduction to another protocol.)

3. Here is a zero-knowledge proof of identity that Peggy knows a discrete logarithm. Suppose  $p$  is a large prime and  $\alpha$  is a primitive root and  $\beta = \alpha^a \bmod p$ . The number  $p$ ,  $\alpha$  and  $\beta$  are public and Peggy wants to prove she knows  $a$ .

- Peggy chooses a random integer  $k$ ,  $1 \leq k < p-1$  computes  $\gamma = \alpha^k \bmod p$  and sends  $\gamma$  to Victor.
- Victor chooses a random integer  $r$ ,  $1 \leq r < p-1$  and sends  $r$  to Peggy.
- Peggy computes  $y = k - ar \bmod p-1$  and sends  $y$  to Victor.
- Victor checks whether  $\gamma = \alpha^y \beta^r \bmod p$ .

- (a) Show that if Peggy follows the procedure above then Victor's check will always be true.
- (b) Give a simulation of the protocol to show that Victor learns nothing new.
- (c) Show that if Peggy can make Victor's test pass for more than one  $r$  than Peggy must "know"  $a$ .