PMAT 4282 – Cryptography Winter 2001 — Assignment #4

1. By $\mathbb{Z}_n^*$ we will denote the set $\{a \in \mathbb{Z}_n \,|\, \text{GCD}(a,n) = 1\}$. A *quadratic residue* modulo n is any element x of $\mathbb{Z}_n^*$ that is a square (ie $x = y^2$ for some $y \in \mathbb{Z}_n^*$). What are the quadratic residues for

   (a) $\mathbb{Z}_{23}^*$

   (b) $\mathbb{Z}_{26}^*$

   (c) $\mathbb{Z}_{27}^*$

   In a few weeks we will see in class how to determine whether a given element $x \in \mathbb{Z}_p^*$ is a quadratic residue, where p is a prime. For instance, we'll learn how to answer the question: Is 789 a quadradic residue in $\mathbb{Z}_{5683}^*$?

2. Below is a schematic diagram for the function $f : \{0,1\}^{12} \to \{0,1\}^{12}$, which is used in each round of computation of an NDS-like cryptosystem in which $n = 12$ and $r = 16$.

   The specifications of this cryptosystem are such that s_0 is the identity function, s_1 is the complement function, and the permutation in the final step of f simply reverses the order of the 12 bits.

   You have gained access to an implementation of the encryption algorithm for this cryptosystem, using the key s_k that Alice and Bob have as their secret. This implementation is online at `http://www.math.mun.ca/~dapike/crypto/`.

   (a) How many possible choices are there for the key s_k?

   (b) Perform a chosen plaintext attack on the cryptosystem, and thereby determine s_k.