Cryptography

Problem set 8 - 12-13 VI 2013

Problem 1 Consider an additive group Z_n. An element $y \in Z_n$ is a quadratic resitue if and only if there exists an $x \in Z_n$ such that $2x = y \bmod n$.

- What are the quadratic residues in Z_p for p – an odd prime?
- Let $n = pq$ be a product of two odd primes p and q. What are the quadratic residues in Z_n?
- Let n be an even integer. What are the quadratic residues in Z_n?

Problem 2 Let $N = pq$ with p, q distinct, odd primes. Prove that if $x \in QR_N$ (quadratic residues over Z_N^*) then $[x^{-1} \bmod N] \in QR_N$, and if $x \in QNR_N^{+1}$ (quadratic non-residues) then $[x^{-1} \bmod N] \in QNR_N^{+1}$.

Problem 3 Let N be the product of 5 distinct odd primes. If $y \in Z_N^*$ us a quadratic residue, how man solutions are there to the equation $x^2 = y \bmod N$?

Problem 4, 5, ... to be continued