Introduction to mathematical cryptography
Homework problems
Week 8

15. Suppose $N = pq$ where p, q are odd primes. Assume $1 \leqslant a \leqslant N$ such that $\gcd(a, N) = 1$. Prove that if the congruence $x^2 \equiv a \bmod N$ has any solutions, then it has exactly four solutions.

16. Suppose $N = pq$ where p, q are odd primes. Assume you have a machine which does the following. You can give any number $1 \leqslant a \leqslant N$ as an input. Then if $\gcd(a, N) = 1$, and $x^2 \equiv a \bmod N$ has any solutions, then the machine returns the four solutions; while if $\gcd(a, N) > 1$ or $x^2 \equiv a \bmod N$ has no solution, the machine returns the message `ERROR`. How could you use this machine to find the factorization of N?

Important: The two problems are related. Even if you cannot prove the statement in first one, you are free to use the fact that it is true.
Note: Please provide complete arguments everywhere.