Exercise 7.6

Task

Let A be an algorithm that gets as input an RSA public key (n, e) and a ciphertext y. A will either return the correct plaintext x, or will return "no answer". Suppose A is able to decrypt if and only if y is in some subset S of Z_n^*. Assume also that the size of S is $\epsilon(p-1)(q-1)$, for $0 < \epsilon < 1$.

Construct a probabilistic algorithm B that uses A as a subrutine. B gets input public key (n, e) and ciphertext z, where z can be any number in Z_n. We will assume that z is not 0, as 0 is easy to decrypt anyway. You must construct B such that for any fixed z, B returns the correct plaintext for z with probability at least ϵ.

Solution

1. Input z, n, e
2. Compute $k = gcd(z, n)$
3. If $k \neq 1$ then
   - k is a multiple of p (or of q - it's the same). We can easily factor n, given p to find q. Decryption is easy when we have p and q. Terminate algorithm
4. If $k = 1$
   1. Choose a uniform random number b
   2. If $gcd(b, n) \neq 1$ then
   - We have the same situation as step 2. Terminate algorithm
   3. Calculate b' = $E_{n,e}(b)$ (encrypt b)
   4. Multiply b' and z
   5. Use A to decrypt $b' \times z$
   6. Divide the result by b
   7. If we decrypted successfully then
   - Answer found. Terminate algorithm
   8. Else go to step 3.1

Notes:

- The cases where $gcd(n, whatever) \neq 1$ are super unlikely, but it's worth trying.
- We have to choose a uniformly distributed b otherwise the A algorithm will be deterministic
- In steps 4.3 to 4.5 we use the Hint given in the book