Question 1

Suppose we have a set of blocks encrypted with the RSA algorithm and we don't have the private key. The public key is {n,e}. You are an attacker and are trying to break the private key. Suppose someone tells you they know one of the plaintext blocks has a common factor with n. Does this help you in any way to determine the private key? If yes, describe how.

SOLUTION:

In RSA, the form of the public and the private key is as follows:

Private key - {n,d}
Public key - {n,e}

We know the public key value i.e. (n,e).
Thus we can get one component of the private key since we know that 'n' is common in both the keys.
We just need to calculate the value 'd' to find the private key.

We know that, in RSA:

$d = (e^{-1}) \bmod (PHI)$
$PHI = (p-1) \times (q-1)$ [where p and q are prime numbers].

Yes! If someone tells me that one of the plaintext box has a common factor with 'n', it does help me to determine the private key.

The steps I would use to determine the private key are:

1. We are told that one of the plain text box has a common factor with n.
2. This will help us in factoring n.
3. We can factor n to find 'p' and 'q'.
4. We can use 'p' and 'q' to calculate 'PHI' as PHI = (p-1) x (q-1).
5. Now using Euclid's algorithm, we can compute $d = (e^{-1}) \bmod (PHI)$.
6. Thus, we can find 'd' and determine the private key.

It is important to note that 'step 3' which is the factoring of 'n' is a non trivial step. However, If a plaintext block has a common factor with n modulo n then the encoded block will also have a common factor with n modulo n. Because we encode blocks, which are smaller than 'p & q', the factor must be p or q and the plaintext block must be a multiple of p or q. We can test each block for primality. If prime, it is p or q. In this case we divide into n to find the other factor. If not prime, we factor it and try the factors as divisors of n

Knowing that the plaintext box has a common factor with 'n', it helps in factorization and thus reduces the effort required to perform cryptanalysis to determine the private key.

NOTE:

Reference to PPT - Computer Security 7 : Cryptography — Public Key Version: 2012/02/15 16:15:24
Department of Computer Science
University of Arizona
Link - http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Handouts/Handout-7.pdf

Reference - Cryptography and Network Security: Principles and Practice - William Stalling
Chapter 9 - Public Key Cryptography and RSA