AbdelRahman Adel
1701 2296

PAGE
DATE

Assignment 5

Theoratical Questions

(1) For computational ease, one typically chooses a value of e that is prime, has a few bits as possible equal to 1 for fast multiplication, and, at the same time is cryptographically secure. Typical values of e are 3, 17, & 65537 ($2^{16}+1$)

(2) No. Knowing the totient of the modulus doesn't directly break the RSA scheme, they would still need to factorize n to derive key d. The security of RSA lies in the difficulty of factoring large semiprime numbers into their prime factors. It can aid in certain attacks but it's not sufficient

(3) In a simplified RSA scheme with weak key generation attackers might exploit brute force attacks on the private exponent, common modules attacks, or weakness in the encryption process to recover plain text from ciphertext without access to the private exponent.