

Instructions

- Answer each question completely; justify your answers.
1. Prove that the RSA cryptosystem is vulnerable to a chosen ciphertext attack. Specifically, show how to successfully decrypt a given ciphertext c to obtain its plaintext m by making use of a chosen ciphertext $\hat{c} \neq c$ and its corresponding plaintext \hat{m} .
 2. Suppose that Alice and Bob have published public RSA keys (n_A, e_A) and (n_B, e_B) respectively, such that $n_A \neq n_B$ but $\text{GCD}(n_A, n_B) \neq 1$. Show how Eve can determine Alice and Bob's private keys.
 3. Suppose that Alice wishes to send a single plaintext message m to each of Bob, Christine and David, all three of whom have published public RSA keys, say (n_B, e_B) , (n_C, e_C) and (n_D, e_D) where n_B , n_C and n_D are pairwise relatively prime but $e_B = e_C = e_D = 3$. Show how Eve can use the three ciphertexts c_B , c_C and c_D to determine the plaintext m that they represent (without factoring any of n_B , n_C or n_D).
 4. Use Pollard's $p - 1$ algorithm to factor n :
 - (a) $n = 16701131$
 - (b) $n = 451153742269$
 - (c) $n = 3129476997089035646236920257$