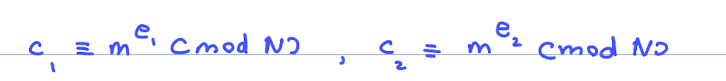
**Task 1 Analysis of RSA algorithm**

By using the standard common-modulus attack, Even can compute the plaintext without knowing the private key of Alice.

Assume that Bob’s plaintext is m and Eve intercepts:



and Eve will know N since N is the public key, e1 is the first encryption exponent and e2 is the second encryption exponent.

Mathematical explanation

If gcd (e1, e2) = 1, Eve can use the extended Euclidean algorithm to find integers a, b with:

A blue handwritten text on a white background

AI-generated content may be incorrect.

Raise c1 to a and c2 to b and multiply:



If a or b is negative, Eve can interpret as which enables Eve to compute the modular inverse of the ciphertext modulo N. This requires that the ciphertext to be invertible modulo N (gcd (m, N) = 1). This means that under the usual conditions (coprime exponents and m invertible mod N) Eve can recover m directly.

What went wrong:

Alice or Bob reused the same modulus N to encrypt the same plaintext under two different public exponents. This common modulus usage with the same modulus leaks the message m when gcd (e1, e2) = 1. The correct way to do encryption is by using randomized padding so that the two ciphertexts are different encryptions with different padded message.

If Eve cannot find m:

* Any information that lets Eve compute a modular inverse exponent (an integer d with ) which is one of the private keys or a factorization of N. With the factorization of N. With the factorization of N Eve can compute and then recover m from either ciphertexts.
* Or if she gets extra independent ciphertexts with exponents that together form a combination giving 1.