2.7 Re-Use of a Module

Question: What happens if two different participants use the same RSA module n?

In other words, A and B use (n, e_A) and (n, e_B) as public keys.

Obviously A and B may read each other's messages since both can factorize n and hence compute the other's private key. Thus a common module makes sense only in a cooperative situation where A and B absolutely trust each other.

However it's even worse: A message a sent to both A and B is readable *by everyone*. The ciphertexts are:

$$c_\mathrm{A} = a^{e_\mathrm{A}} \bmod n, \quad c_\mathrm{B} = a^{e_\mathrm{B}} \bmod n.$$

Assuming e_A and e_B coprime is no significant loss of generality. Then the attacker, using the extended Euclidean algorithm, finds coefficients x and y with

$$xe_\mathrm{A} + ye_\mathrm{B} = 1.$$

Necessarily x and y have opposite signs, assume $x < 0$. If $\gcd(c_\mathrm{A}, n) > 1$, then the attacker can decompose n and is done. Otherwise she computes

$$g := c_\mathrm{A}^{-1} \bmod n$$

by congruence division and gets

$$g^{-x} \cdot c_\mathrm{B}^{y} \equiv (a^{e_\mathrm{A}})^x \cdot (a^{e_\mathrm{B}})^y \equiv a \pmod{n},$$

breaking the ciphertext without computing the private keys d_A and d_B.

Hence the common module n is secure only when A and B trust each other and moreover keep the module secret. But in this situation it makes much more sense to use a symmetric cipher.