1. **Common Modulus Attack**

Suppose Bob1 and Bob2 choose the same modulus but coincidentally choose coprime encryption exponents. Thus we have \((n, e_1)\) and \((n, e_2)\) with \(\gcd(e_1, e_2) = 1\).

(a) Alice wants to send \(P\) to both of them so she sends \(C_1 \equiv P^{e_1} \mod n\) to Bob1 and \(C_2 \equiv P^{e_2} \mod n\) to Bob2.

(b) Suppose Eve gets ahold of both \(C_1\) and \(C_2\).

(c) Since \(\gcd(e_1, e_2) = 1\) she can find \(\alpha\) and \(\beta\) with \(\alpha e_1 + \beta e_2 = 1\) and then she can find \(P\) via:

\[
C_1^\alpha C_2^\beta \equiv (P^{e_1})^\alpha (P^{e_2})^\beta \equiv P^{\alpha e_1 + \beta e_2} \equiv P^1 \equiv P \mod n
\]

2. **Hastad Broadcast Attack**

This generalizes but the simple version is to suppose that Bob1, Bob2, and Bob3 each use encryption exponent \(e = 3\) because they want encryption to be fast with a low power but they use pairwise coprime moduli \(n_1\), \(n_2\), and \(n_3\).

(a) Alice wants to send \(P\) to all three of them so she sends \(C_1 \equiv P^3 \mod n_1\) to Bob1, \(C_2 \equiv P^3 \mod n_2\) to Bob2, and \(C_3 \equiv P^3 \mod n_3\) to Bob3.

(b) Suppose Eve obtains \(C_1\), \(C_2\), and \(C_3\). She solves the following system via the CRT:

\[
\begin{align*}
x &\equiv C_1 \mod n_1 \\
x &\equiv C_2 \mod n_2 \\
x &\equiv C_3 \mod n_3
\end{align*}
\]

She obtains \(x\), the least nonnegative residue \(\mod n_1 n_2 n_3\). But since \(C_1 \equiv P^3 \mod n_1\) and \(C_2 \equiv P^3 \mod n_2\) and \(C_3 \equiv P^3 \mod n_3\) Eve knows that \(x \equiv P^3\) \(\mod n_1 n_2 n_3\) and then since they’re pairwise coprime she knows that \(x \equiv P^3 \mod n_1 n_2 n_3\).

(c) However \(P < n_1\), \(P < n_2\) and \(P < n_3\) so in fact \(P^3 < n_1 n_2 n_3\) and so \(P^3 = x\) and so \(P = \sqrt[3]{x}\).

3. **Interception/Resend Attack**

Suppose Bob uses public key \((n, e)\) and private key \((n, d)\).

(a) Alice wants to send \(P\) to Bob so she sends \(C \equiv P^e \mod n\).

(b) Eve intercepts this \(C\) Of course she can’t read it but instead she chooses some \(r\) with \(\gcd(r, n) = 1\) and sends \(\bar{C} \equiv Cr^e \mod n\) on to Bob.

(c) Bob receives \(\bar{C}\) and attempts to decrypt it, finding:

\[
(\bar{C})^d \equiv (Cr^e)^d \equiv (P^e r^d)^d \equiv P^{ed} r^d \equiv Pr \mod n
\]

Which looks like garbage to him so he throws it in the trash.

(d) Eve retrieves it and multiplies by \(r^{-1}\) to get \(P\).