(1) Trong trường hợp nhóm m >= 2 người dùng chung giá trị n trong hệ mã RSA, nếu giả sử họ cùng chọn cùng một giá trị n, điều này có thể tạo ra một số vấn đề về an toàn của hệ thống RSA.

(2) Trong trường hợp k người cùng chọn cùng một giá trị e như nhau và các giá trị ni (modulus) khác nhau, điều này tạo ra một mô hình không an toàn cho hệ mã RSA. Dưới đây là một số lý do giải thích tại sao hệ mã RSA có thể bị tấn công trong tình huống này:

* Tấn công The Common Modulus (CM): Nếu nhiều người dùng chung cùng một giá trị n, và một số người dùng chọn cùng một giá trị e như nhau, một tấn công có thể được thực hiện bằng cách sử dụng thuật toán Euclidean mở rộng để tính đồng dư mở rộng của e đối với ni. Nếu tấn công thành công, kẻ tấn công có thể suy luận được khóa riêng tư của những người dùng khác.
* Tấn công The Common Exponent (CE): Nếu nhiều người dùng chia sẻ cùng một giá trị e, và một số người dùng chọn cùng một giá trị ni, một kẻ tấn công có thể sử dụng tấn công giả mạo để tạo ra chữ ký giả mạo cho các thông điệp đã biết. Điều này có thể dẫn đến việc giả mạo chữ ký và xâm phạm tính toàn vẹn của hệ thống.
* Khả năng phát hiện và tấn công hóa học dữ liệu: Khi nhiều người dùng chia sẻ cùng một modulus n, người tấn công có thể sử dụng các kỹ thuật như đo thời gian thực hiện phép toán để tìm hiểu thông tin về khóa riêng tư và thậm chí làm suy luận về giá trị khóa riêng tư.

Để ngăn chặn các loại tấn công này, quan trọng là mỗi người dùng nên chọn một modulus (ni) duy nhất và một cặp khóa công khai/riêng tư riêng biệt để đảm bảo tính toàn vẹn và an toàn của hệ mã RSA.