Để kiểm tra tính toàn vẹn của dữ liệu đã được mã hóa RSA trong trường hợp không tin tưởng người gửi, ta có thể sử dụng chữ ký số (digital signature) cùng với mã hóa RSA. Dưới đây là các bước cơ bản để thực hiện điều này:

1. Người gửi tạo chữ ký số: Trước khi mã hóa dữ liệu, người gửi sẽ tạo một chữ ký số bằng cách sử dụng khóa riêng (private key) của họ. Điều này thường được thực hiện bằng cách sử dụng hàm băm (hash function) để tạo một bản tóm tắt của dữ liệu và sau đó ký bản tóm tắt này bằng khóa riêng. Kết quả là một chữ ký số đi kèm với dữ liệu đã được mã hóa RSA.
2. Gửi dữ liệu và chữ ký số: Người gửi sẽ gửi dữ liệu đã được mã hóa RSA cùng với chữ ký số cho người nhận.
3. Người nhận giải mã dữ liệu: Người nhận sẽ sử dụng khóa công khai (public key) của người gửi để giải mã dữ liệu RSA và thu được bản gốc.
4. Kiểm tra chữ ký số: Sau khi giải mã dữ liệu, người nhận sẽ sử dụng cùng một hàm băm mà người gửi đã sử dụng để tạo bản tóm tắt của dữ liệu gốc. Sau đó, họ sẽ sử dụng khóa công khai của người gửi để giải mã chữ ký số. Nếu bản tóm tắt của dữ liệu gốc và bản tóm tắt được giải mã từ chữ ký số trùng khớp, thì dữ liệu được xem là nguyên vẹn và chưa bị sửa đổi.

Nếu bất kỳ thay đổi nào được thực hiện trên dữ liệu sau khi được ký bằng chữ ký số, bản tóm tắt sẽ không còn trùng khớp và quá trình kiểm tra tính toàn vẹn sẽ thất bại. Điều này cho phép người nhận phát hiện bất kỳ sửa đổi nào trong dữ liệu đã được gửi.

Trong quá trình thực hiện các bước này, quan trọng nhất là bạn phải có khóa công khai của người gửi để giải mã chữ ký số và khóa công khai này phải được tin tưởng. Nếu bạn không tin tưởng khóa công khai này, bạn có thể gặp khó khăn trong việc xác minh tính toàn vẹn của dữ liệu. Do đó, quản lý và xác minh khóa công khai là một phần quan trọng của quá trình này.