**Destination B**

**Source A**

E(PRa,[M||H(M||S)])

E(PUb,E(PRa,[M||H(M||S)]))

E(PRa,[M||H(M||S)])

PRa

**Destination B**

compare

S

M

PUa

PRb

PUb

M

S

M

Ưu điểm của mô hình: +) Tính bảo mật cao (sử dụng cả khóa bí mật và khóa công khai của người nhận và người gửi)

+) Đa dạng chức năng (bảo mật, chứng thực, mã hóa, giải mã,...)

+) Bảo đảm tính toàn vẹn của dữ liệu nhờ hàm băm

Nhược điểm của mô hình: +) Tốc độ xử lí lâu do phải trải qua nhiều công đoạn

+) Về phía người dùng: bất tiện cho cả người dùng lẫn người nhận do phải trải qua bước OTP

+) Quản lí khóa: Khóa công khai và riêng tư cần phải được quản lí cẩn thận và bảo mật

Giải thích hoạt động:

+) Ban đầu M sẽ kết hợp với mã OTP và đi qua hàm băm. Sau đó kết quả thu được sẽ kết hợp với M ban đầu và sẽ tiến hành mã hóa bằng khóa bí mật của người gửi

+) Sau khi đã mã hóa bằng khóa bí mật của người gửi, ta sẽ mã hóa tiếp bằng khóa công khai của người nhận và gửi

+) Người nhận nhận được thông tin sẽ dùng khóa bí mật để giải mã ra thông điệp đã bị mã hóa bởi khóa bí mật người người gửi

+) Người nhận sẽ tiếp tục dùng khóa công khai của người gửi để giải mã ra thông điệp M cùng bảng băm.

+) Thông điệp M sau khi giải mã sẽ kết hợp với mã OTP và đi qua băm lại, cuối cùng là so sánh với hàm băm đã giải mã ở trên để xem dữ liệu có bị hay đổi hay thất thoát gì không