Bài tập 5. Xây dựng mô hình có đầy đủ chức năng bảo mật, chứng thực, chữ kí số.

||

S

Compare

M



K

K

S

E{K, [M||E(Pra,H(M,S)]}

PUa

PRa

Giải thích mô hình:

M qua hàm phi S và được băm qua hàm băm (chữ kí số), sau đó được mã hoá bởi khoá K. Người nhận nhận được sẽ giải mã bằng khoá K thu được M thông điệp ban đầu (bảo mật) , và chuỗi băm được mã hoá. Tiếp tục đưa chuỗi băm qua mã hoá với khoá công khai PUa (chứng thực), và so sánh hàm băm này với hàm M vừa được giải mã và đi qua hàm băm ở đường trên (tính toàn vẹn).

Ưu điểm: Bảo mật hơn, chứng thực, toàn vẹn, chữ kí số

Nhược điểm: Phức tạp, tốn thời gian hơn