Yêu cầu:Xây dựng giải pháp để nhân viên và trưởng dự án xác định thông tin lương có đúng là do trưởng dự án thiết lập không.

1) Giải pháp đưa ra:

Sử dụng chữ ký điện tử.

2) Cách thực hiện:

- Ta khởi tạo cặp khóa public/private key bằng một thuật toán mã hóa bất đối xứng( ví dụ rsa) cho trưởng dự án.

- Ở bảng Nhân Viên ta thêm một cột thuộc tính là PUBKEY, cột này lưu giá trị public key của nhân viên nếu là trưởng dự án đã khởi tạo ở trên và được phân quyền sao cho tất cả tài khoản của nhân viên khác đều có thể truy cập được.

- Ở cùng bảng Nhân Viên ta thêm một cột thuộc tính là Signature,giá trị ở cột này do trưởng dự án thêm vào chữ ký số khi thiết lập dữ liệu lương của một nhân viên. Cột này cũng được phân quyền sao cho tất cả nhân viên đều có thể truy cập được

- Giá trị ở cột Signature sẽ được khởi tạo như sau: lấy giá trị cột lương( của nhân viên mà trưởng dự án thiết lập) đưa qua một hàm hash( ví dụ md5,sha1). Sau đó giá trị ouput sẽ được mã hóa bằng private key của trưởng dự án -> Signature.

-Khi muốn kiểm tra giá trị lương có phải do trưởng dự án thiết lập hay không,ta lấy giá trị Signature giải mã bằng public key được lưu của trưởng dự án, sau đó đối chiếu với giá trị lương được đưa qua hàm hash. Nếu 2 giá trị này giống nhau thì đó là do trưởng dự án thiết lập