Chữ ký điện tử

-chữ ký là bawbgf chứng thể hiện người ký có chue định khi ký vb

-chữ ký thể hiện chủ quyền ,nó cho ai là người ký vb-chữ ký không thể tái sử dụng,là một phần của vb và không thể sao chép sang vb khác

-vb đã ký ko thể thay đổi

2 chữ ký điện tử

-nguồi gửi ký vb bằng cách mã hóa nó với khóa bí mật

-người gửi chuyển vb đã ký cho người nhận

-người nhận kiểm tra chũ ký bằng việc sử dụng chìa khóa công khai của người gửi để gải mã vb

Có hai loại khóa:+ private key : tạo chứ ký và publie key: cả lớp biết

-là thông tin đi kèm theo dữ liệu nhằm mục đích xác nhận người chủ của dữ liệu đó

- các chữ ký đt đc sinh ra chứa hai thaanhf phần:

+ thuật toán ký sig()

* Input: Private key,văn bản. Đầu ra là chữ ký

+thuật toán xác minh công khai ver()

* Intput: chữ ký, và publie key. Output:1 là đúng và 0 là sai

\*Chữ ký đt ko phải là

* Ck tay đc scan và lưu ở tệp ảnh
* Ko là ck đc in trên giấy
* 1 người ko chỉ có 1 ck
* 1 p tiện để ngăn chặn hackcer

Hệ chữ ký đt là một hệ gồm 5 phần(p,a,k,s,v) thỏa mãn

1. P là tập hữu hạn các bức điện
2. A là tập hữu hạn các ck
3. K là không gian khóa với mỗi khóa k thuôc K tồn tại một thuật toán sigk thuộc S và 1 thuật toán xác định verk thuộc V.mỗi sigk:p-> A và verk P\*A-> (TRUE.FALSE) là những hàm soa cho mỗi bức x thuộc P và mỗi chữ ký y thuộc A thỏa mãn pt:

ii. hệ ck RSA