Presentation to
Bills Committee on
Electronic Transactions Bills

4 November 1999

Hand Written Signature

To sign means “to write one’s name as a signature to a document in attestation, confirmation, ratification.”

Signature has three main functions:

- **authentication;**
- **non-repudiation;**
- **integrity**

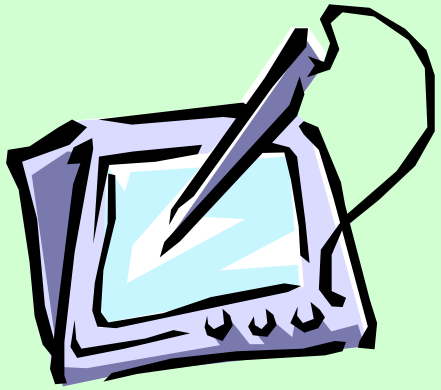
Reliable Signature

Hand-written Signature are reliable

- Signature Biometrics;
- Ink absorbs into the paper frabics;
- Detectable alteration, deletion and attestation.

Electronic Signature

" any letter, characters, numbers or other symbols in digital form attached to or logically associated with an electronic records, and executed or adopted for the purpose of authenticating or approving the electronic record."



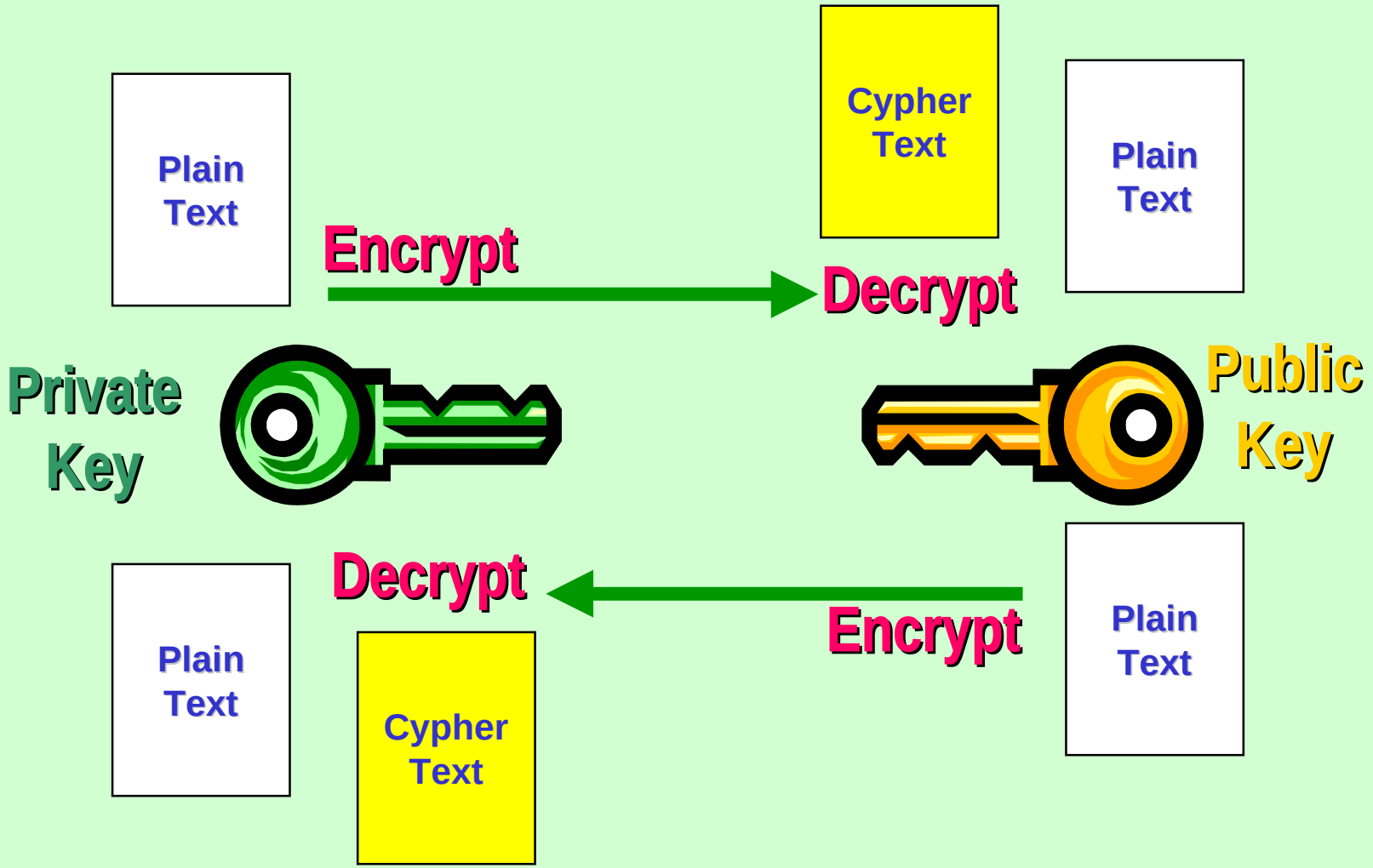
Digital Signature

" electronic signature of the signer generated by the transformation of the electronic record using an asymmetric crytosystems and a hash function such that a person having the initial untransformed electronic record and the signer's public key can determine —

(a) whether the transformation was generated using the private key that corresponds to the signer's public key; and

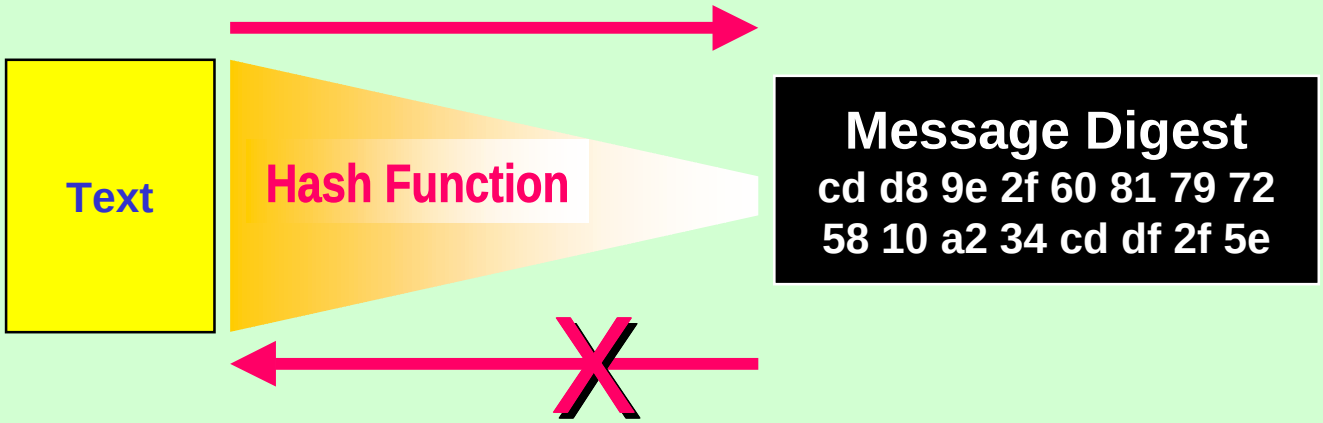
(b) whether the initial electronic record has been altered since the transformation was generated."

Asymmetric Key Cryptography



Public Key Cryptography

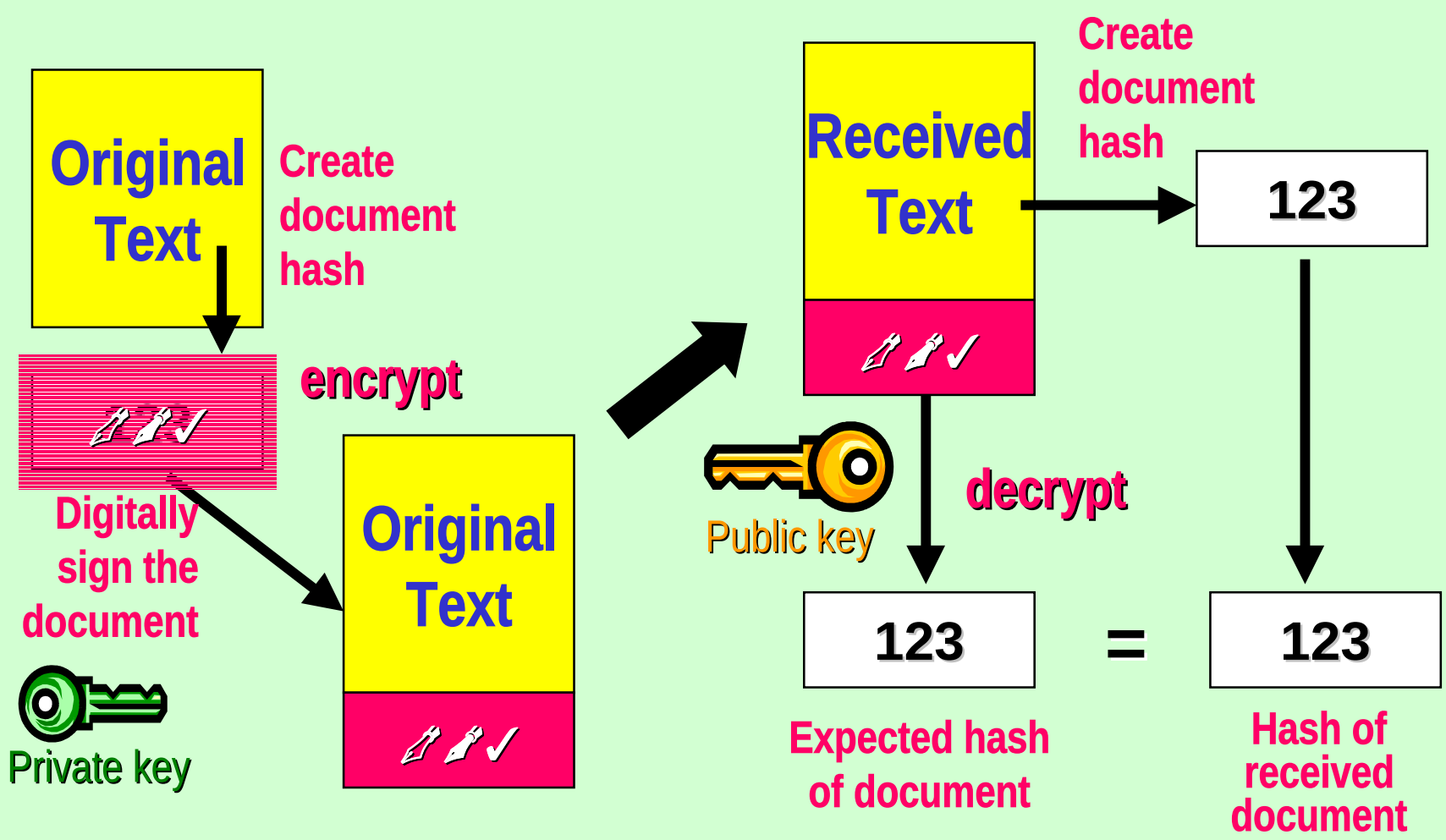
Hash Function



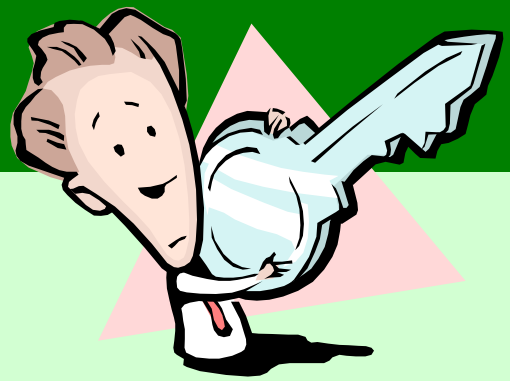
Hash Algorithm

Message Digest 5 (MD5)	*128 bits (16 bytes)*
Secure Hash Algorithm (SHA-1)	*160 bits (20 bytes)*

How Digital Signature Works?

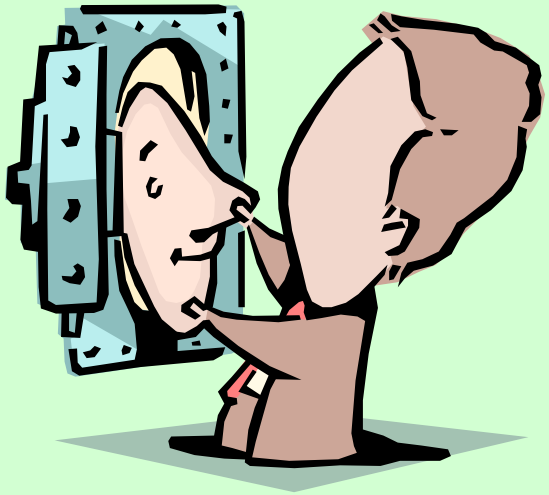


The Dilemma



Any one can

- produce private/public keys
- name the owner of the private key
- put the public key in a public directory

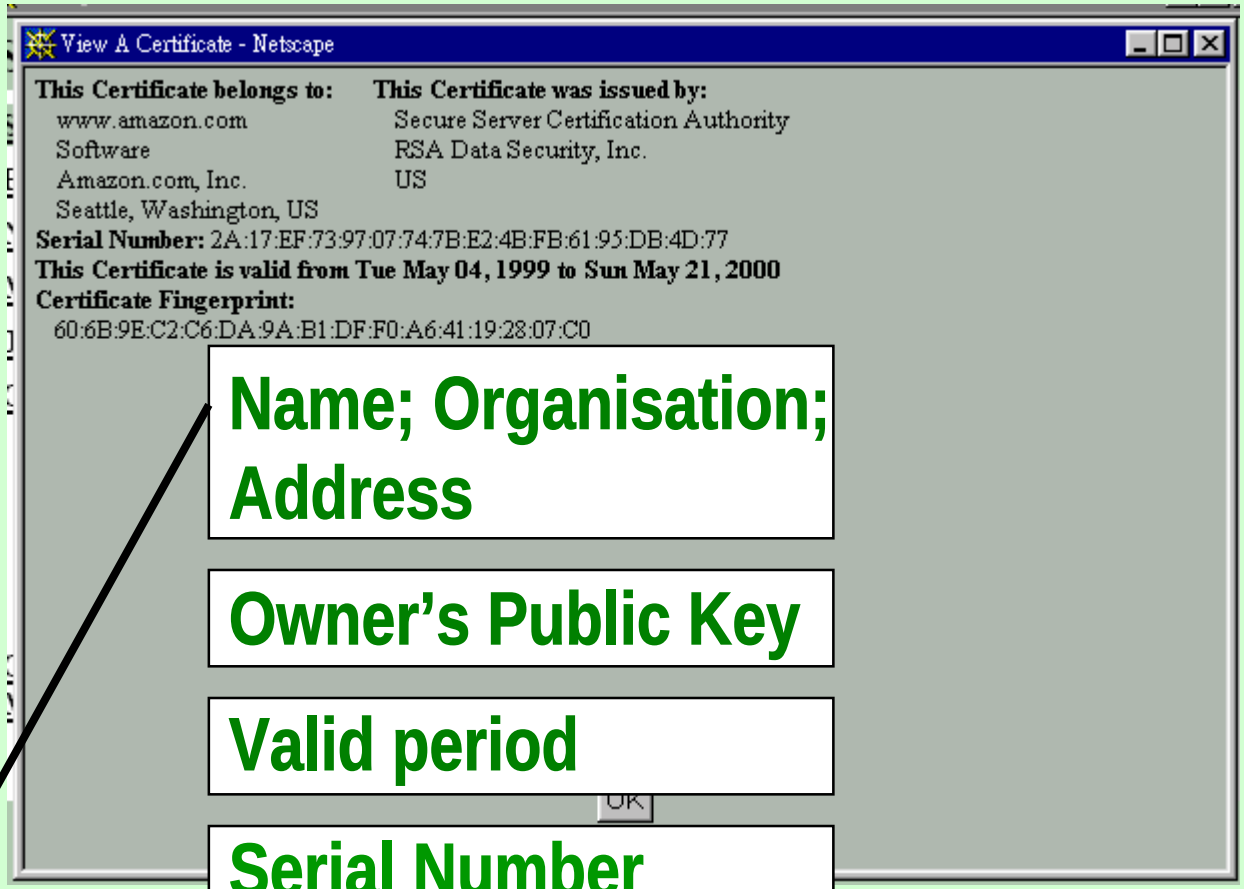


The problem is how to ensure the key is belong to the person it claimed.

Certification Authority

- Digital certificate can bound the relation with the owner of the private key
- Digital certificates issued by a Trusted Third Party is trustworthy
- Trusted third party issuing digital certificate is a Certification Authority

Digital Certificate



Message

Digital Signature

Digital Certificate

- Name; Organisation; Address
- Owner's Public Key
- Valid period
- Serial Number
- Issuer's digital signature