Digital Signatures

Digital Signatures are used to "Sign" messages to validate the source and integrity of the contents.

Digitized Written Signature??

- Simply taking a digital picture of a written signature does not provide adequate security.
- Such a digitized written signature could easily be copied from one electronic document to another with no way to determine whether it is legitimate.
- Electronic signatures, on the other hand, are unique to the message being signed and will not verify if they are copied to another document.

Digital signatures are used just like handwritten signatures.

- Digital signatures are used just like handwritten signatures.
- When you add them to a document, you are "signing" that document as a way of endorsing or agreeing with what the document says.
- Unlike handwritten signatures, digital signatures are used only with computers. They are electronic signatures that can be used to sign electronic documents, like word processing files or spreadsheets.

What is a digital signature?

- A digital signature is a kind of ID. You can use it on the Internet to identify yourself in a secure manner. This is extremely useful in areas such as electronic commerce. For instance, when making a credit card purchase on the Internet, you can use your digital signature to "sign" that purchase. This helps to ensure that only you can make purchases with your credit card number.

Requirements for a Digital Signature

- The signature must be a bit pattern that depends on the message being signed
- The signature must use some information unique to the sender, to prevent both forgery and denial.
- It must be relatively easy to produce digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

How is a Digital Signature Produced?

- Very briefly, a typical digital signature works like this:
  - A signature in the form of a code is generated by applying an algorithm, such as RSA, and the sender's private key to some or all of the message contents.
  - The recipient verifies the signature by decrypting it using the sender's public key.

Message Authentication

- Message authentication is playing an important role in a variety of applications, especially those related to the Internet protocols and network management, where undetected manipulation of messages can have disastrous effects.

Conventional Encryption for Signatures and MACs

- There is no shortage of good message authentication codes, beginning with DES-MAC, as defined in FIPS PUB 113.
- Conventional (symmetric) encryption could be used for digital signatures - DESMAC specified by FIPS
- However, message authentication codes based on encryption functions such as DES, which were designed for hardware implementation, may be somewhat limited in performance for soft-ware, and there is also the question of U.S. export restrictions on encryption functions.

Conventional Encryption for MACs

- When secret key cryptography is used, a message authentication code (MAC) is calculated from and appended to the data.
- To verify that the data has not been modified at a later time, any party with access to the correct secret key can recalculate the MAC. The new MAC is compared with the original MAC, and if they are identical, the verifier has confidence that the data has not been modified by an unauthorized party.
- FIPS 113, Computer Data Authentication, specifies a standard technique for calculating a MAC for integrity verification.

Microsoft Word Document

Secret Key Electronic Signatures Issues

- If two parties share a secret key, and one party receives data with a MAC that is correctly verified using the shared key, that party may assume that the other party signed the data.
- This assumes, however, that the two parties trust each other. Thus, through the use of a MAC, in addition to data integrity, a form of electronic signature is obtained.
- Using additional controls, such as key notarization and key attributes, it is possible to provide an electronic signature even if the two parties do not trust each other.

Digital Signatures and Privacy

- Can combine techniques - signed by private A, encrypt by public B
- A forms: X = encrypt(PUBB, encrypt(PRVA, M))
- B extracts: M = decrypt(PUBA, decrypt(PRVB, X))

Digital Signatures and Privacy

- Digital signatures use asymmetric encryption to provide assurance of authentication of the origin of a message and, sometimes, the integrity of its contents.
- They can also prevent repudiation (denial) as they can be used to prove, that providing the private key has not been disclosed, the signature is that of the sender.

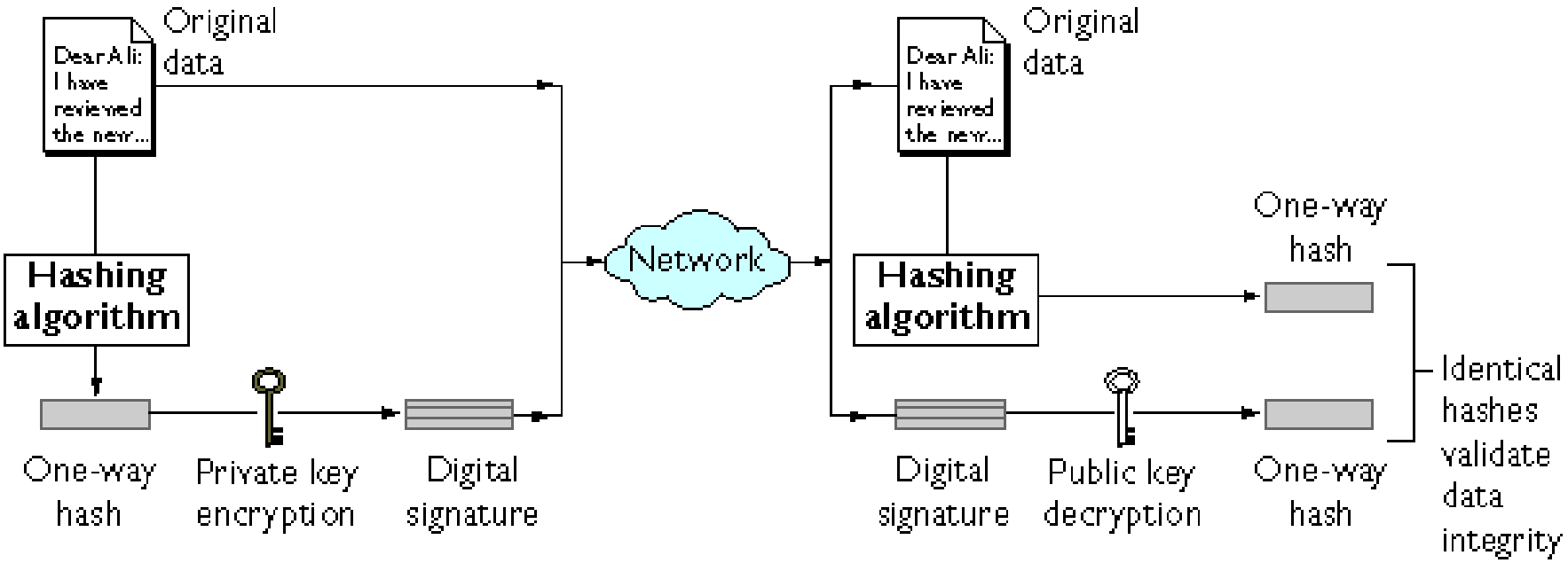
Public Key Electronic Signatures

- Another type of electronic signature called a digital signature is implemented using public key cryptography.
- Data is electronically signed by applying the originator's private key to the data.
- To increase the speed of the process, the private key is applied to a shorter form of the data, called a "hash" or "message digest," rather than to the entire set of data.
- The resulting digital signature can be stored or transmitted along with the data.

Public Key Electronic Signatures

- The signature can be verified by any party using the public key of the signer.
- This feature is very useful, for example, when distributing signed copies of virus-free software. Any recipient can verify that the program remains virus-free.
- If the signature verifies properly, then the verifier has confidence that the data was not modified after being signed and that the owner of the public key was the signer.

Steps in making a digital signature



Steps in making a digital signature

- Public key cryptography verifies integrity by using of public key signatures and secure hashes.
- A secure hash algorithm is used to create a message digest. The message digest, called a hash, is a short form of the message that changes if the message is modified.
- The hash is then signed with a private key. Anyone can recalculate the hash and use the corresponding public key to verify the integrity of the message.

Importance of Digital Signatures

- Digital Signatures are a central component of modern cryptographic systems.
- In analogy to handwritten signatures on paper documents digital signatures are used to guarantee the authenticity of electronic documents.
- Thus they play an important role for example in secure and reliable systems for electronic commerce.

What makes a digital signature break?

- Digital signatures contain a special number. This number is generated by a complex mathematical formula when you sign a document. When the digital signature is added to a document, the document is passed to the formula. The formula examines the document and generates a number. This number is then saved as part of the digital signature.

What makes a digital signature break?

- When somebody uses your public key to decode your signature, the same process occurs. The document is again passed to the formula, and the formula returns a number. The returned number is then compared to the number stored in the signature. If the numbers are the same, then the document hasn't been tampered with, and the signature is good. If the numbers are different, then something in the document has changed, and the signature will break.
- This means that once a document is signed, it can't be changed without breaking the signature.

How do I know the signature isn't a fake?

- Even if the signature isn't broken, you might be concerned that somebody has falsified a signature. For example, if your friend Bob managed to create his own digital certificate with your name on it, he could send documents with your signature on them. In effect, Bob would be forging your signature.

How do I know the signature isn't a fake?

- To make sure that a signature is authentic, you can check who issued or created the certificate. Each certificate is issued by what is called a certificate authority (CA). Certificate authorities can be anyone, from the government to your next door neighbor. Whenever you view a digital signature, you can see who the certificate authority was that issued the original certificate. You then have to decide for yourself whether you can trust that certificate authority.

How do I know the signature isn't a fake?

- For example, if you looked at a signature and saw that the certificate authority was the State of California, you would probably want to trust that signature. The State of California would have rigorous guidelines for issuing digital certificates. However, if the certificate authority was "Wild Bill", you might have second thoughts -- who knows what criteria Wild Bill might use?

How do I know the signature isn't a fake?

- Since digital certificates are stored on your desktop computer, the only other way for somebody to "forge" your signature is for them to get access to your computer. However, digital certificates can also be password protected, in order to prevent this from happening.

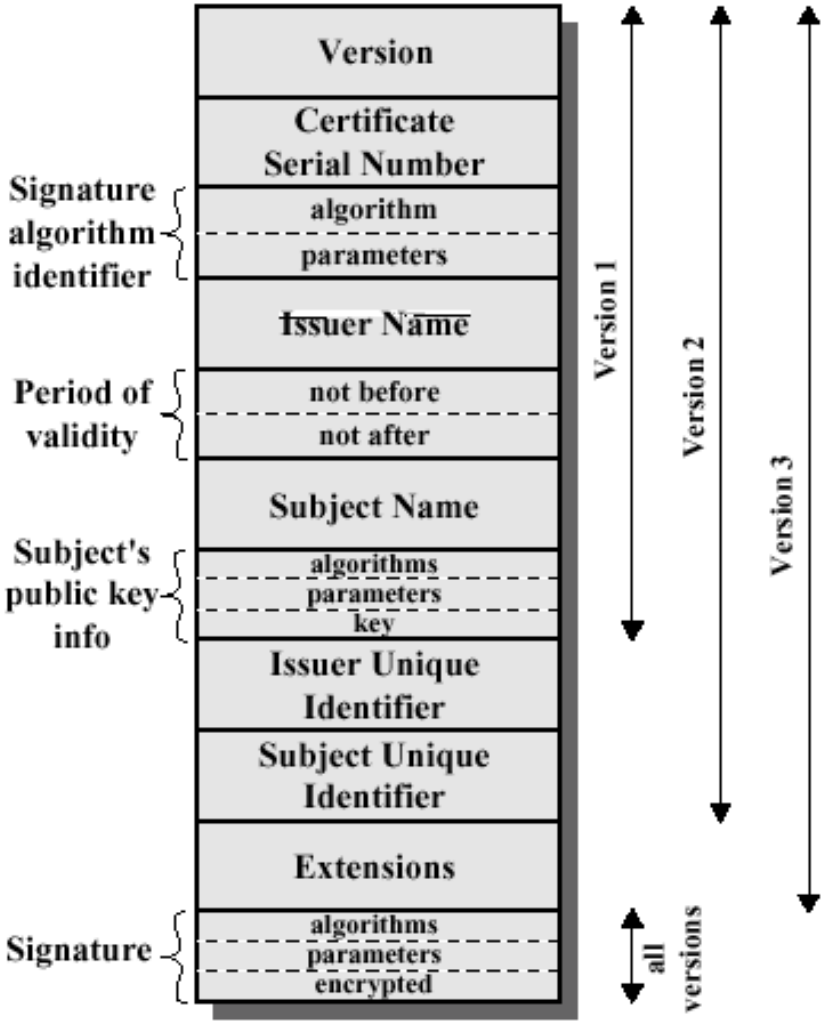
Are digital signatures being used today?

- Electronic commerce is also turning to digital signatures. "Smart cards," which are much like credit cards, can be used to store your digital certificate. You can then "swipe" these cards on your computer to sign things on the Internet, such as credit card purchases or bank deposits.
- Over the next year, the number of applications using digital signatures will continue to grow. It will likely become the standard for identifying yourself on the Internet.

Obtaining a Digital Certificate

- User Certificates are generated by a CA:
- Any user with access to the public key of the CA can recover the user public key that was certified
- No party other than the certification authority can modify the certificate without this being detected

Anatomy of a Digital Certificate



(a) X.509 Certificate