Cryptography, PKI, *and* Digital Signatures

Topics

- Cryptography
  - Background
  - Services
- RSA Digital Signature Creation
- Digital Signature Process
- Public Key Infrastructure
  - Certificates

Cryptography Defined

- Original definitions sprang from its literal meaning, that is from the original Greek, (“kryptos” as “hidden” and “-graphy as “writing”.)

As technology evolved however, so did its definition. For example, the U.S. Army Field Manual FM 34-40-2 defines cryptology as

- “… the branch of knowledge which concerns secret communications in all its aspects.

- A more contemporary and complete definition, from NIST:

  “… a branch of mathematics that is based on the transformation of data and can be used to provide several security services: confidentiality, data integrity, authentication, authorization and non-repudiation.” [SP 800-32]

Cryptographic Services

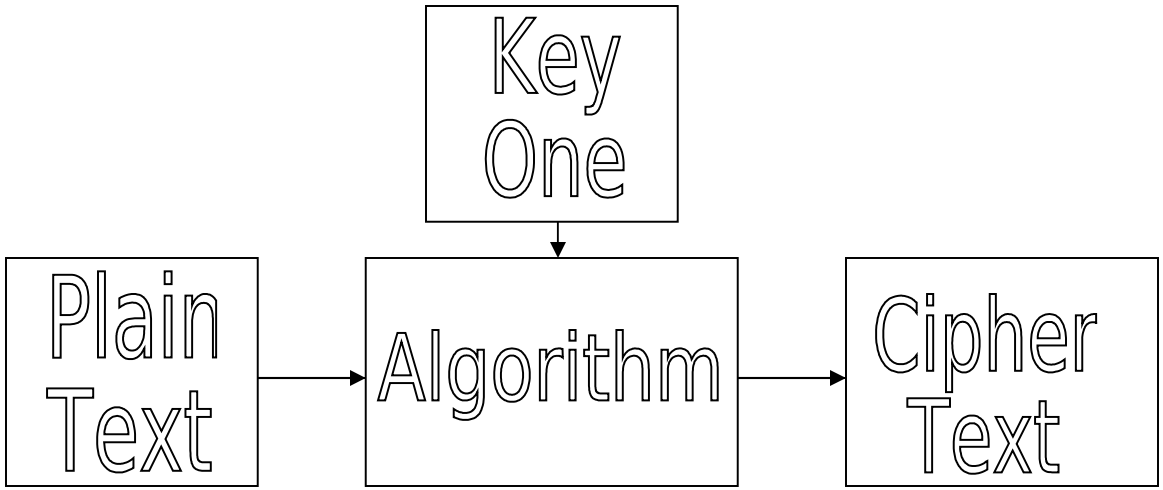
- Confidentiality -- Encryption
  - Only authorized people –e.g., the sender and recipient of a message, not eavesdroppers – can know the message.
- Integrity – Message Digests (MAC or MIC), and Digital Signatures
  - When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
- Authentication – PKI and Digital Signatures
  - When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
- Nonrepudiation – MAC and Digital Signatures
  - Alice cannot later deny that the message was sent.
  - Bob cannot later deny that the message was received.

  - *Note: cryptography is not concerned with availability.*

Confidentiality/Encryption Goal

- Make obtaining or altering information too expensive, in time or money, to be worthwhile.
- Encryption strength is context sensitive.
  - Related to time as well as to the information's perceived value to the opponent.
- Cryptography doesn't need to be perfect, it just has to be stronger than your opponent's methods and resources.
  - Jay's rule – A cryptographic implementation should cost less than bribing the clerk that holds the information.

Encryption Process



- Key One and plain text are inputs into the encryption algorithm.
- Cipher text is the output.
  - In contrast to plain text, cipher text maintains confidentiality when sent through an insecure communications channel.

Cryptography Defined

- Original definitions sprang from its literal meaning, that is from the original Greek, (“kryptos” as “hidden” and “-graphy as “writing”.)

As technology evolved however, so did its definition. For example, the U.S. Army Field Manual FM 34-40-2 defines cryptology as

- “… the branch of knowledge which concerns secret communications in all its aspects.

- A more contemporary and complete definition, from NIST:

  “… a branch of mathematics that is based on the transformation of data and can be used to provide several security services: confidentiality, data integrity, authentication, authorization and non-repudiation.” [SP 800-32]

Cryptographic Services

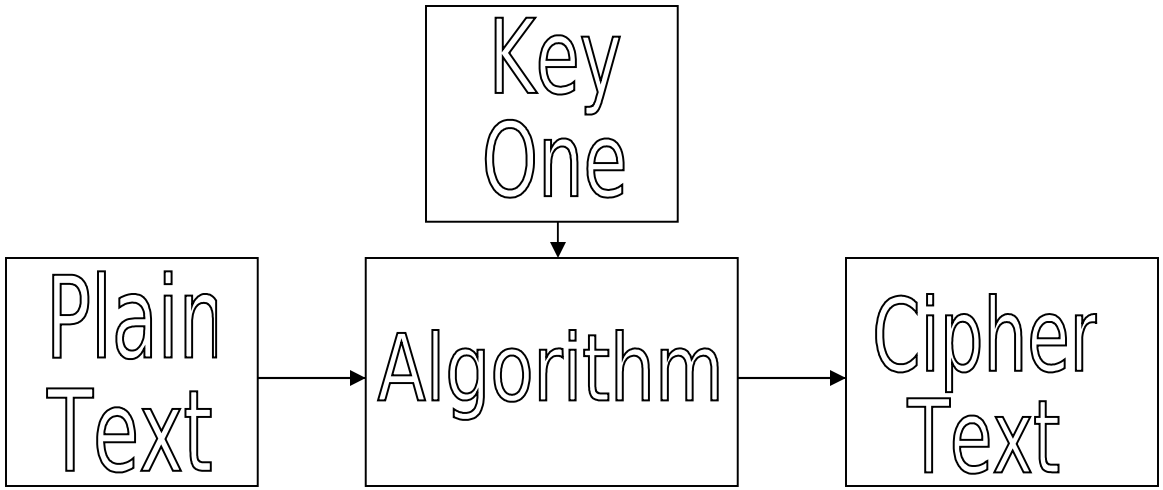
- Confidentiality -- Encryption
  - Only authorized people –e.g., the sender and recipient of a message, not eavesdroppers – can know the message.
- Integrity – Message Digests (MAC or MIC), and Digital Signatures
  - When Bob receives a message, he can be sure that it was not modified en route after Alice sent it.
- Authentication – PKI and Digital Signatures
  - When Bob receives a message that purports to be sent by Alice, Bob can be sure that the message was really sent by Alice.
- Nonrepudiation – MAC and Digital Signatures
  - Alice cannot later deny that the message was sent.
  - Bob cannot later deny that the message was received.

  - *Note: cryptography is not concerned with availability.*

Confidentiality/Encryption Goal

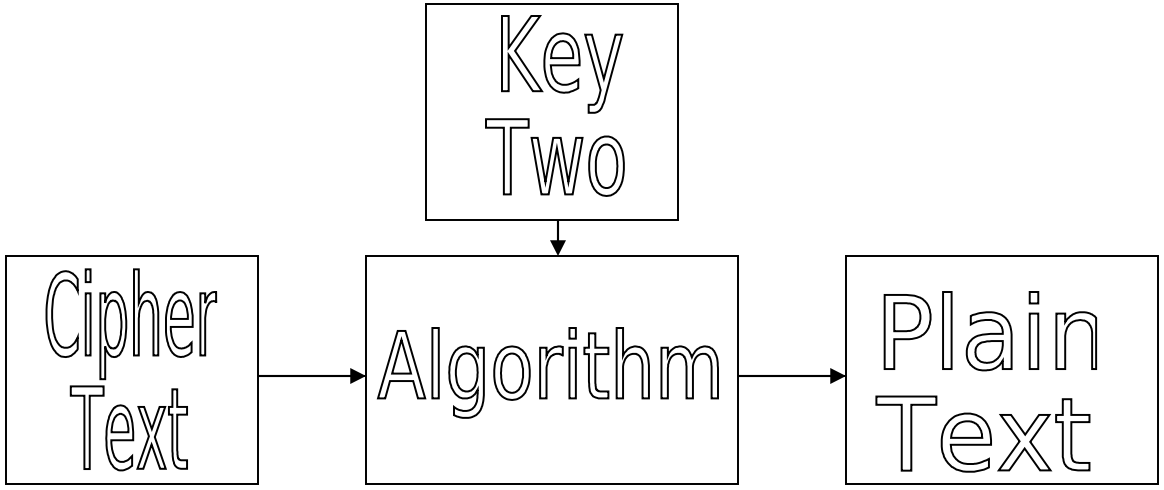
- Make obtaining or altering information too expensive, in time or money, to be worthwhile.
- Encryption strength is context sensitive.
  - Related to time as well as to the information's perceived value to the opponent.
- Cryptography doesn't need to be perfect, it just has to be stronger than your opponent's methods and resources.
  - Jay's rule – A cryptographic implementation should cost less than bribing the clerk that holds the information.

Encryption Process



- Key One and plain text are inputs into the encryption algorithm.
- Cipher text is the output.
  - In contrast to plain text, cipher text maintains confidentiality when sent through an insecure communications channel.

Decryption Process



- Key Two and cipher text are inputs into the decryption algorithm. Plain test is the output.
  - When using a symmetric algorithm, Key One and Key Two are identical.
  - When using an asymmetric algorithm, Key One and Key Two are different.

    Asymmetric notes
    - For confidentiality, sender uses the recipient's public key.
    - Then, since the recipient, is the only person with the private key, the recipient is the only person that can decrypt the cipher text.

An Integrity Process

- A Hash, or message digest, enables you to discern whether or not a document has been altered.
  - That is, it proves or disproves data integrity.
  - This process is also called a Message Integrity Code (MIC)
  - A hash is considered bound to a document.
    - Sometimes called a digital fingerprint.
- Process utilizes a one way function, called a hash.
  - Hash process takes a variable length document as input and produces a fixed length document as output.
- Hashes can also be components of digital signatures and Message Authentication Codes (MACs).
- This is an example of a keyless hash process.
  - Later, we will cover keyed integrity processes called message authentication codes (MACs or HashMACs).

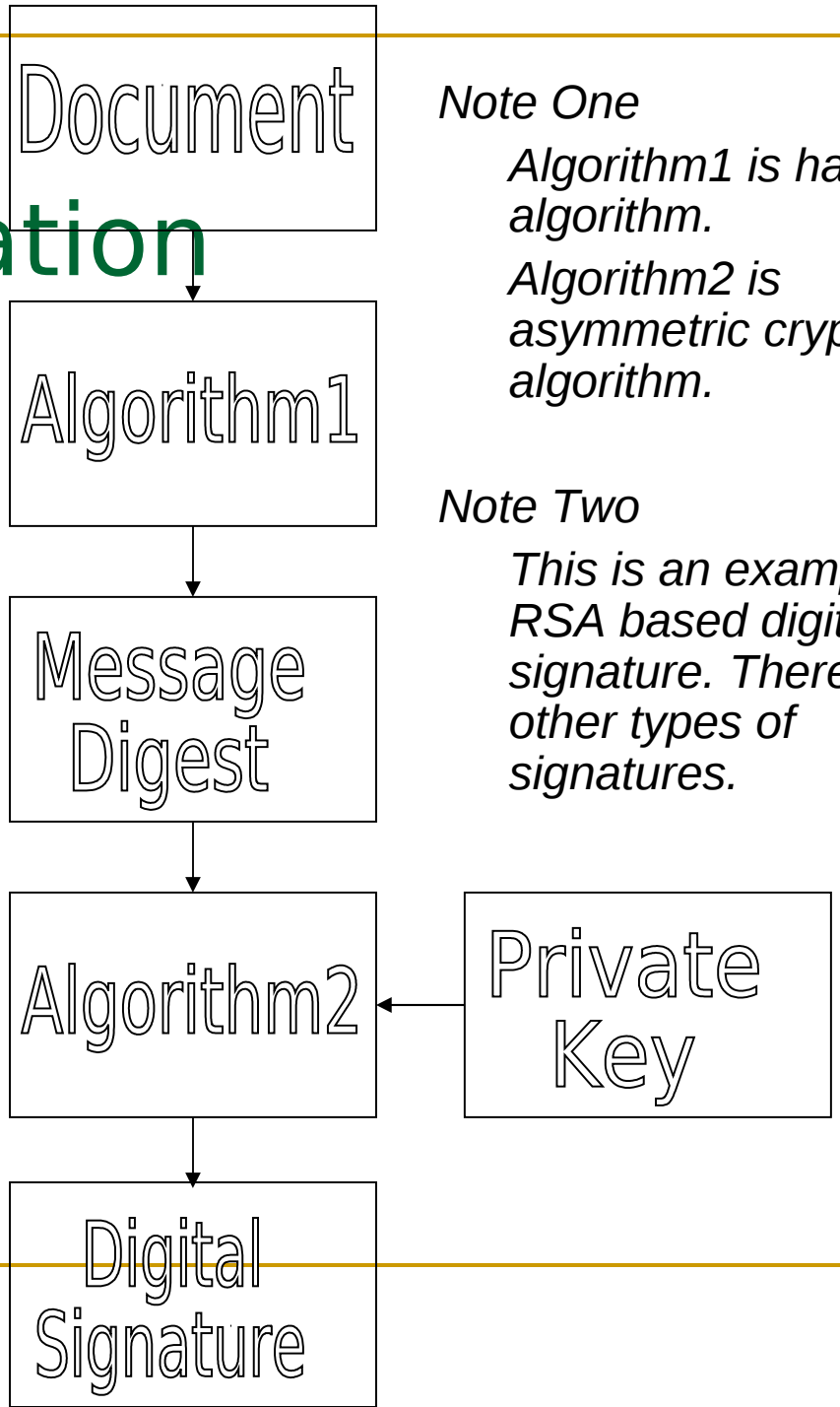
Authentication and NonRepudiation Goals and Process

- Authentication verifies that a message came from whom it is represented to come from.
- Non repudiation provides evidence so that a message can not be disavowed at a later time.

- Process utilizes a secret known to only one person (private key).
- Methods include digital signatures.

RSA Digital Signature Creation

1. Hash document to create digest
2. Encrypt hash with senders private key
3. Attach to encrypted hash communication
4. Upon delivery, recipient decrypts hash with senders public key
5. Creates new document hash and compares
6. If hashes are identical, documents have integrity.



Note One

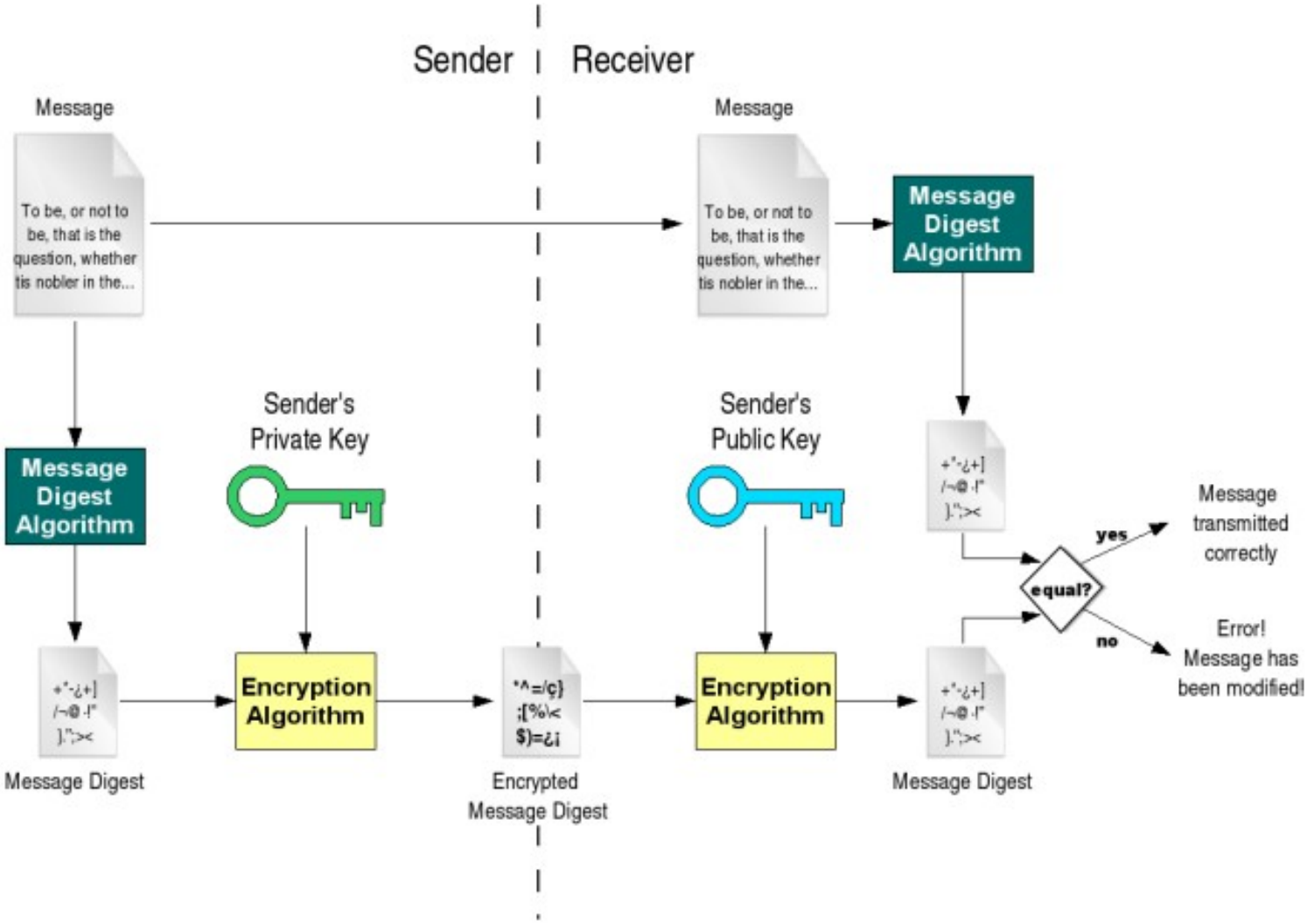
Algorithm1 is hash algorithm.

Algorithm2 is asymmetric crypto algorithm.

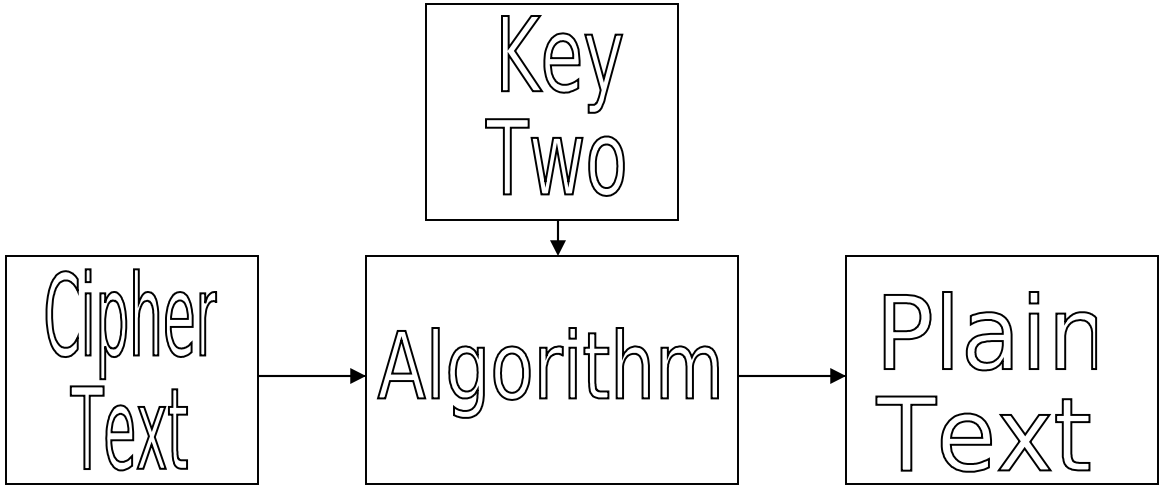
Note Two

This is an example of an RSA based digital signature. There are other types of signatures.

Digital Signature Process



Decryption Process



- Key Two and cipher text are inputs into the decryption algorithm. Plain test is the output.
  - When using a symmetric algorithm, Key One and Key Two are identical.
  - When using an asymmetric algorithm, Key One and Key Two are different.

    Asymmetric notes
    - For confidentiality, sender uses the recipient's public key.
    - Then, since the recipient, is the only person with the private key, the recipient is the only person that can decrypt the cipher text.

An Integrity Process

- A Hash, or message digest, enables you to discern whether or not a document has been altered.
  - That is, it proves or disproves data integrity.
  - This process is also called a Message Integrity Code (MIC)
  - A hash is considered bound to a document.
    - Sometimes called a digital fingerprint.
- Process utilizes a one way function, called a hash.
  - Hash process takes a variable length document as input and produces a fixed length document as output.
- Hashes can also be components of digital signatures and Message Authentication Codes (MACs).
- This is an example of a keyless hash process.
  - Later, we will cover keyed integrity processes called message authentication codes (MACs or HashMACs).

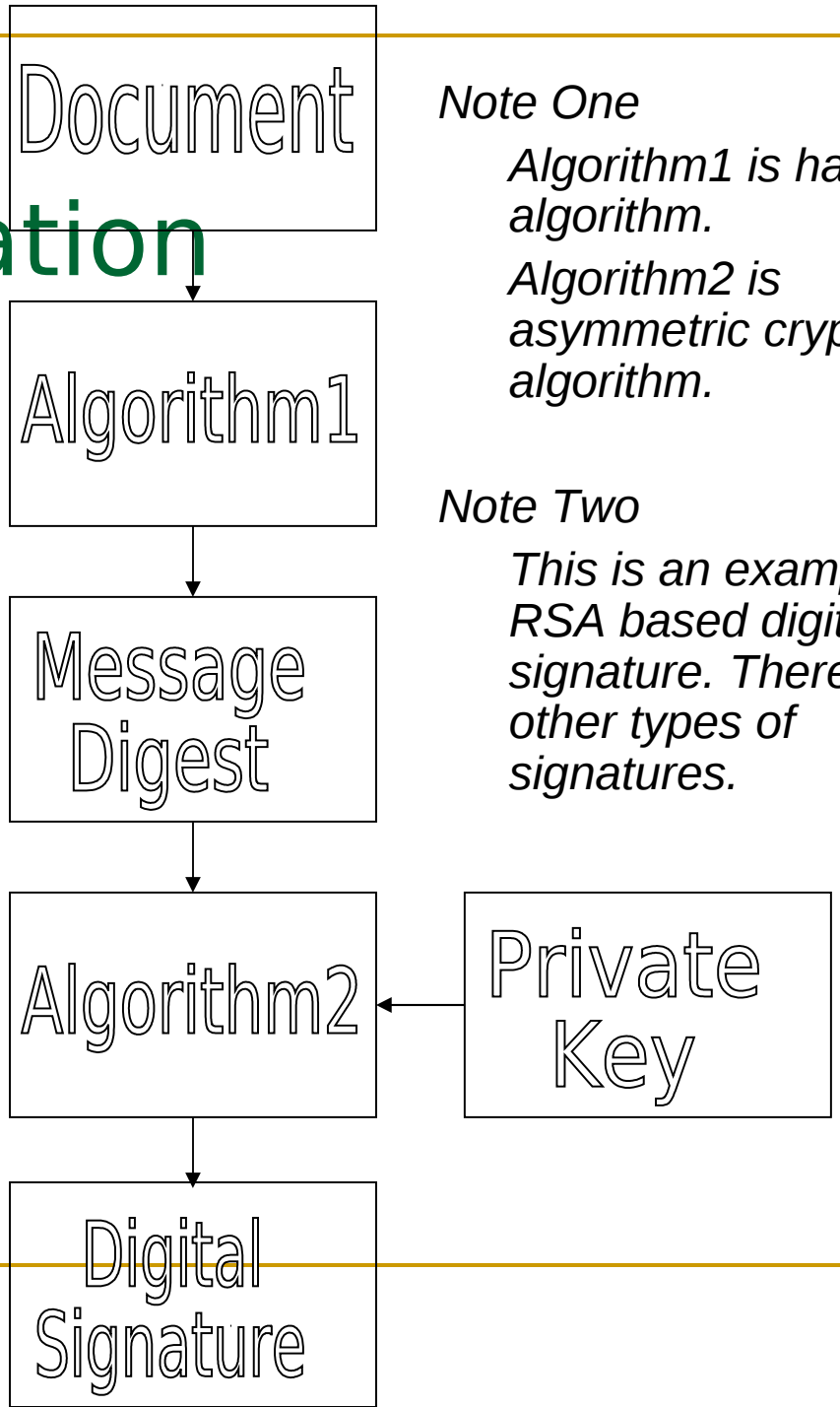
Authentication and NonRepudiation Goals and Process

- Authentication verifies that a message came from whom it is represented to come from.
- Non repudiation provides evidence so that a message can not be disavowed at a later time.

- Process utilizes a secret known to only one person (private key).
- Methods include digital signatures.

RSA Digital Signature Creation

1. Hash document to create digest
2. Encrypt hash with senders private key
3. Attach to encrypted hash communication
4. Upon delivery, recipient decrypts hash with senders public key
5. Creates new document hash and compares
6. If hashes are identical, documents have integrity.



Note One

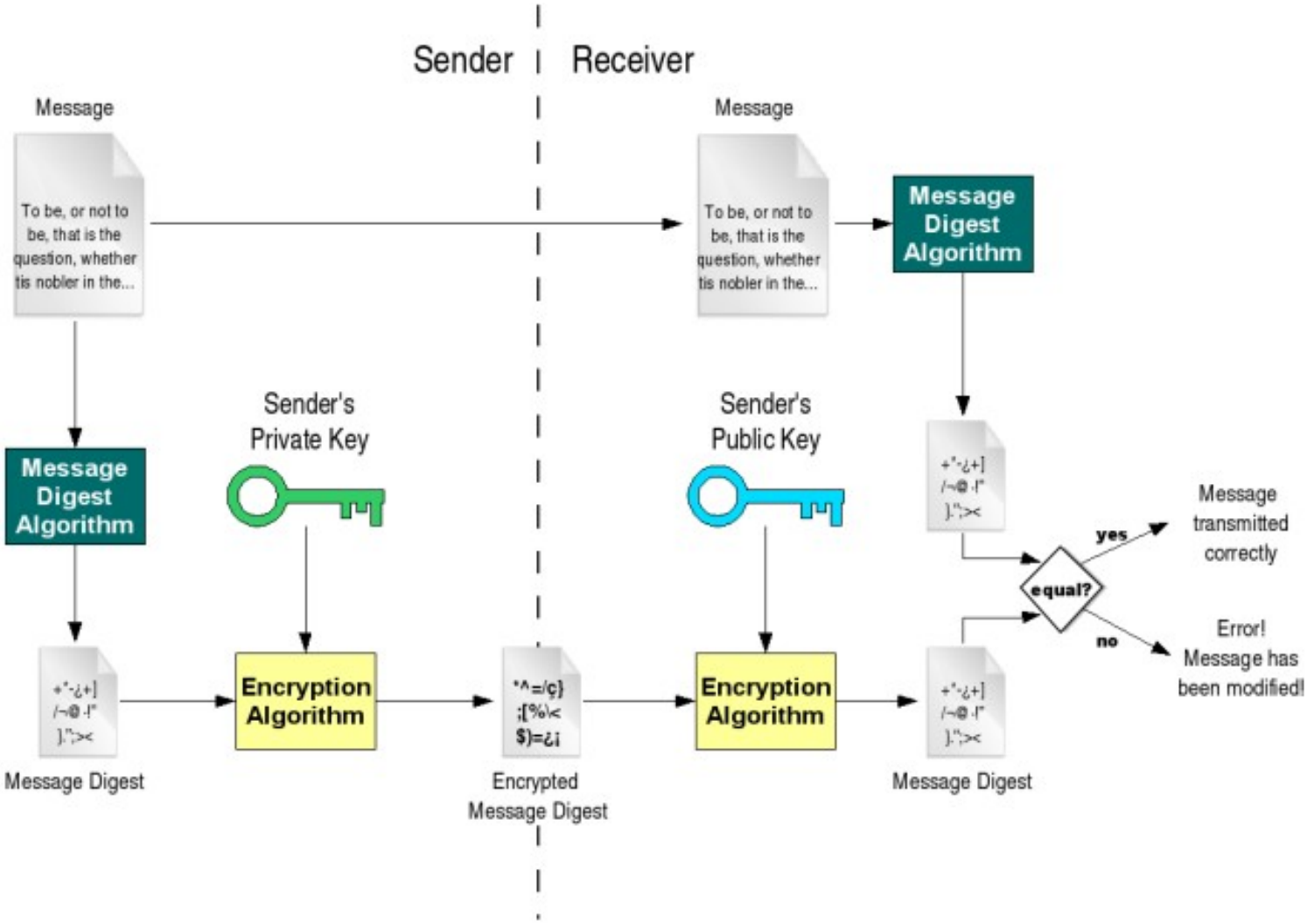
Algorithm1 is hash algorithm.

Algorithm2 is asymmetric crypto algorithm.

Note Two

This is an example of an RSA based digital signature. There are other types of signatures.

Digital Signature Process



Public Key Infrastructure Defied

Digital Key Signatures are part of a Public Key Infrastructure (PKI) that:

- Binds public keys to entities
- Enables other entities to verify public key bindings
- Provides the services needed for ongoing management of keys in a distributed system.

-- NIST 800-32

Provides confidence that:

- The person or process identified as sending the transaction is actually the originator.
- The person or process receiving the transaction is the intended recipient.
- Data integrity has not been compromised.

Public Key Infrastructure

- Public key infrastructure enables enterprises to protect the security of their communications and business transactions on networks.
  - An enterprise-wide network security architecture, PKI integrates:
    - Digital certificates
    - Public key cryptography
    - Certification authorities.
  - Facilitates specific security services including:
    - Public key exchange
    - User authentication
    - Nonrepudiation.

Public Key Infrastructure Issues

Specific Public Key Infrastructure (PKI) issues include:

- Key Authentication and Non-repudiation
  - Nothing about a key proves to whom it belongs
- Revoking keys
  - Nothing about a key indicates whether it has been revoked
- Policy enforcement
  - Any organization utilizing PKI needs to create and enforce a local policy.

PKI Architecture Overview

- PKI architecture consists of:
  - A Trust Model
  - Servers (Certificate, Revocation, Registration)
  - Certificates/Data format standards
    - Public key mechanism standards
- All components work together to enable trusted and secure communications.

PKI Hierarchical Trust Model

1. Hierarchical Trust
   - Sets up an independent certificate authority (CA) with authority to sign digital certificates.
   - A CA can revoke a certificate
   - Facilitates enforcement of a local policy
   - Most complex, most efficient trust model

   - *Note that there are other trust models.*

PKI Support Infrastructure

- Includes
  - Certificates
    - X.509 Standard
  - Certificate Authority
    - Trusted entity that maintains and issues digital certificates.
  - Registration Authorities
    - Performs certificate registration duties
    - Acts as a broker between users and CA
  - Certificate revocation process
    - CA maintains a Certificate Revocation List (CRL)
  - Local Policies and Procedures
  - Non-repudiation service
    - Digital Signature

Certificate Servers

- Certificate servers validate, or certify, keys.
- A certificate server holds a large number of:
  - Certificates
  - Associated data sets
  - Revocation lists
- Three data structures
  1. Certificates
  2. Certificate revocation lists
  3. Attribute certificates.
- Include:
  - Certificate Authorities
  - Registration Authorities

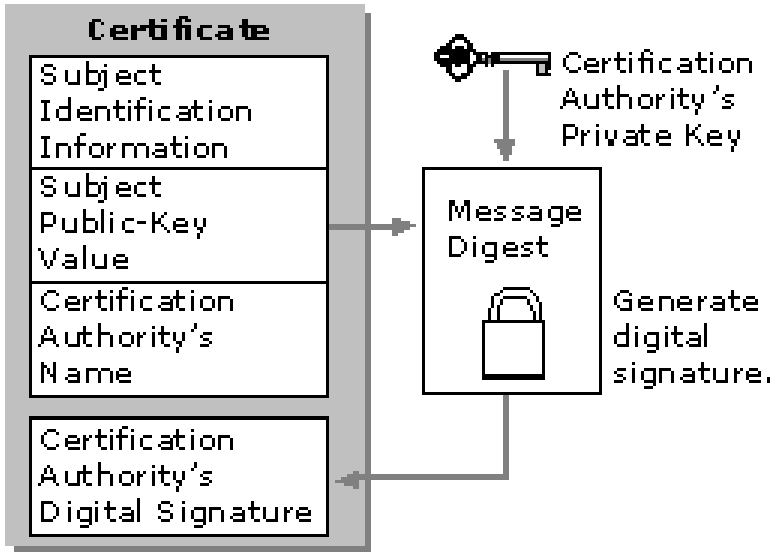
X.509 Certificate Standard

- ITU/CCITT X.509
  - X.500 component
  - Initially intended to provide X.500 authentication
    - Produced by a ISO and ITU collaboration
- Describes digital certificate format.
  - Several versions.
- PKIX – IETF working group
  - Specifies protocols for managing digital certificates as well as protocols for their use.
  - RFC 2459

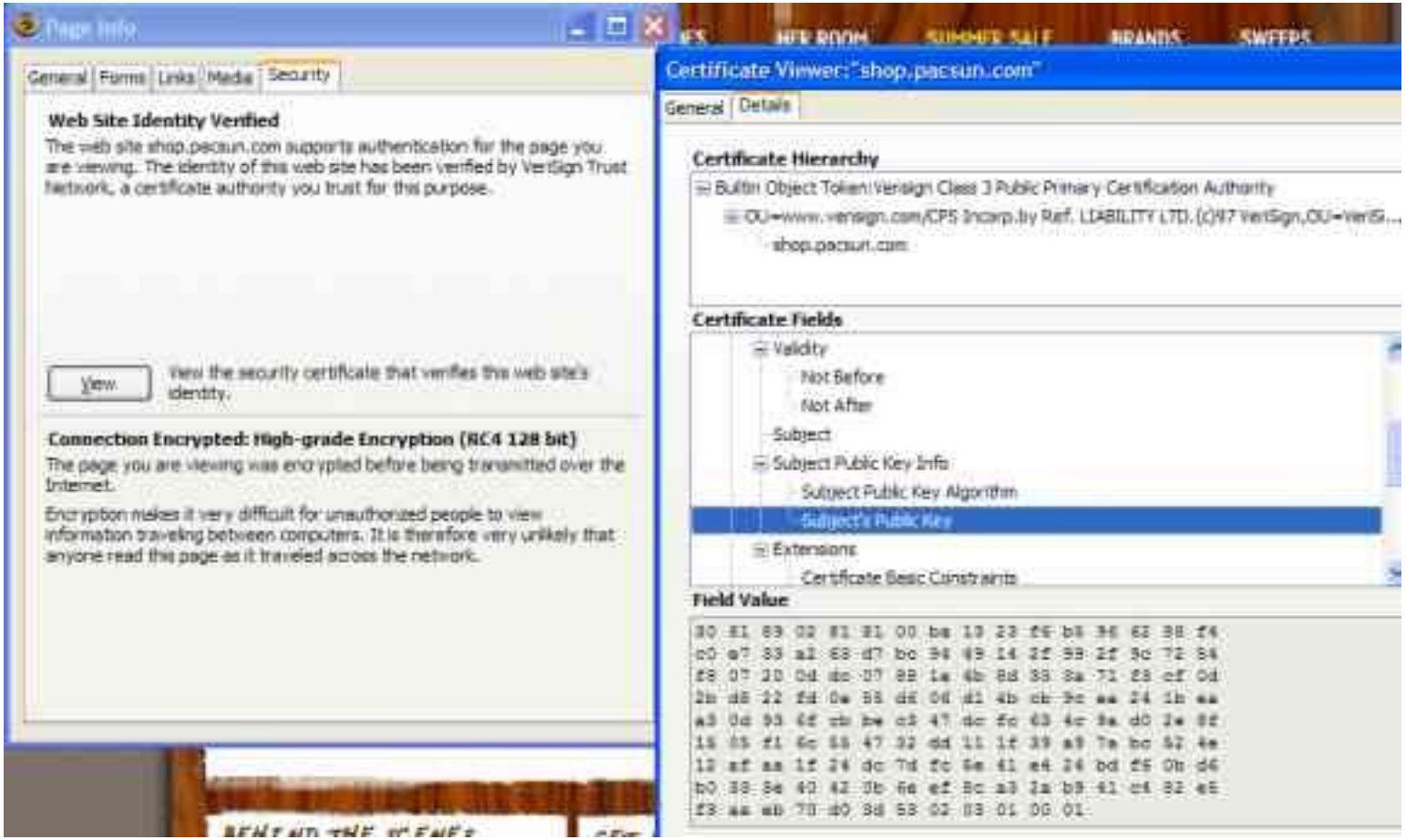
Public Key Certificates

Sample digital certificate components

1. Public key
2. Certificate attributes
   - "Identity" information about user, including name, user ID…
1. One, or more, digital signatures from the Certificate Authority.



Example Certificate



Certificate Revocation Process

- Utilizes Certificate Revocation Lists (CRLs)
  - A revocation list is a signed list (usually signed by CA) in which the serial numbers of revoked certificates are detailed.
- A revocation list is replaced by an updated version from the Trust Center at regular intervals, or as necessary.
  - Validity period determined by Trust Center
  - Usually one day

Questions?

Selected References

http://csrc.nist.gov/publications/PubsSPs.html

http://en.wikipedia.org/wiki/Digital_signature

http://www.simonsingh.net/Crypto_Corner.html

http://www.schneier.com/