19CSE311 - COMPUTER SECURITY
UNIT-1
PART 3

January 21, 2022

Dr.Remya S/Mr. Sarath R
Assistant Professor
Department of Computer Science

AMRITA VISHWA VIDYAPEETHAM
DEEMED TO BE UNIVERSITY
School of Engineering

Outline

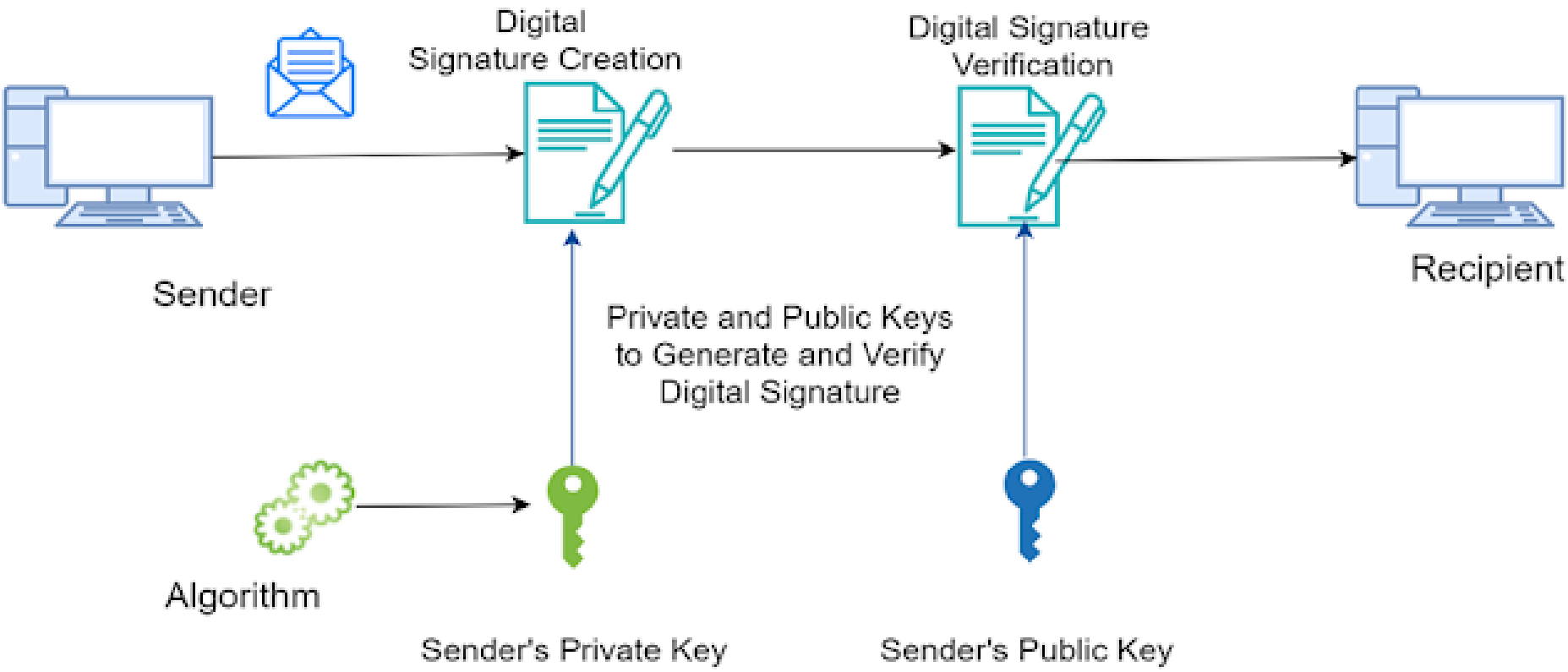
- Introduction to digital signature
  1. Definition
  2. Purpose of Digital Signature
  3. Process of Digital Signature
- Properties of Digital Signature
- Pros & Cons of Digital signature

What is Digital Signature?

- A digital signature is a mathematical technique used to validate the authenticity and integrity of a message or digital document.
- A digital signature is defined the signature generated electronically from the digital computer to ensure the identity of the sender and content of the message cannot be modified during transmission process.

Purpose of Digital Signature

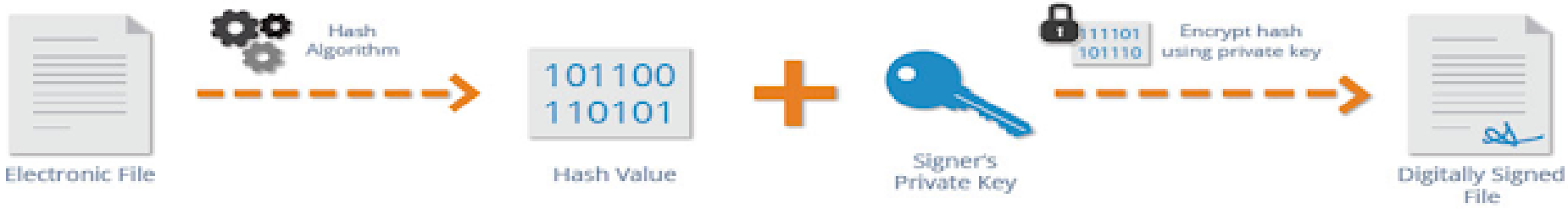
- Concept of digital signature is that sender of a message uses a signing key (Private key) to sign the message and send that message and its digital signature.
- The receiver uses a verification key (Public key) of the sender only to verify the origin of the message and make sure that it has not been tempered with while in transmission.
- Digital signature techniques achieve the authenticity and integrity of the data over internet


Digital
Signature Creation
Digital Signature
Verification
Sender
Recipient
Private and Public Keys
to Generate and Verify
Digital Signature
Algorithm
Sender's Private Key
Sender's Public Key

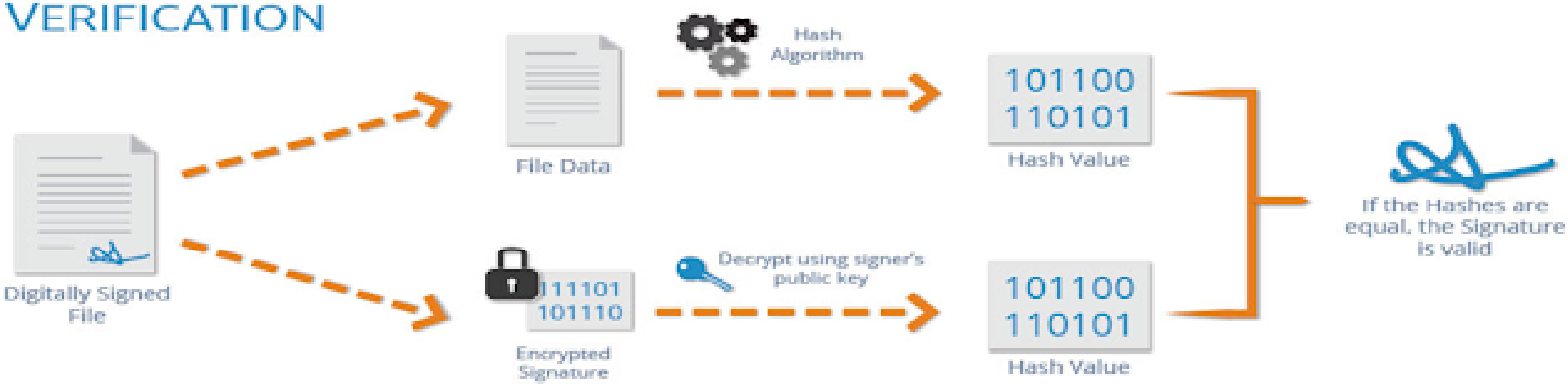
Process of Digital Signature

- Hash value of a message when encrypted with the private key of a user is, his digital signature on that e-Document. Digital signature is an example of asymmetric key cryptography which uses three different algorithms to complete the process.
  1. Step – 1: Key generation algorithm: which generates private key and a corresponding public key.
  2. Step – 2: Signing algorithm: which selects sending message and a private key generated in step 1, to produce a signature.
  3. Step – 3: Signature verifying algorithm: which verifies the authenticity of sending message and public key.

SIGNING



VERIFICATION



Properties of Digital Signature

1. It must verify the author and the date and time of the signature.
2. It must authenticate the contents at the time of the signature.
3. It must be verifiable by third parties, to resolve disputes.

Thus, the digital signature function includes the authentication function.

- Advantages
  1. Authentication: Identification of person that signs.
  2. Integrity of data: Every change will be detected.
  3. Non repudiation: Author cannot be denied of his work.
  4. Imposter prevention: Elimination of possibility of committing fraud by an imposter.
- Disadvantages
  1. Expiry: In this era of fast technology, many of these tech products have a short life.
  2. Certificates: In order to effectively use of digital signatures, both senders and receivers may have to buy digital certificates.
  3. Software: To work with digital certificates/digital signatures, senders and receivers have to buy verification software or pay to third party for verification.

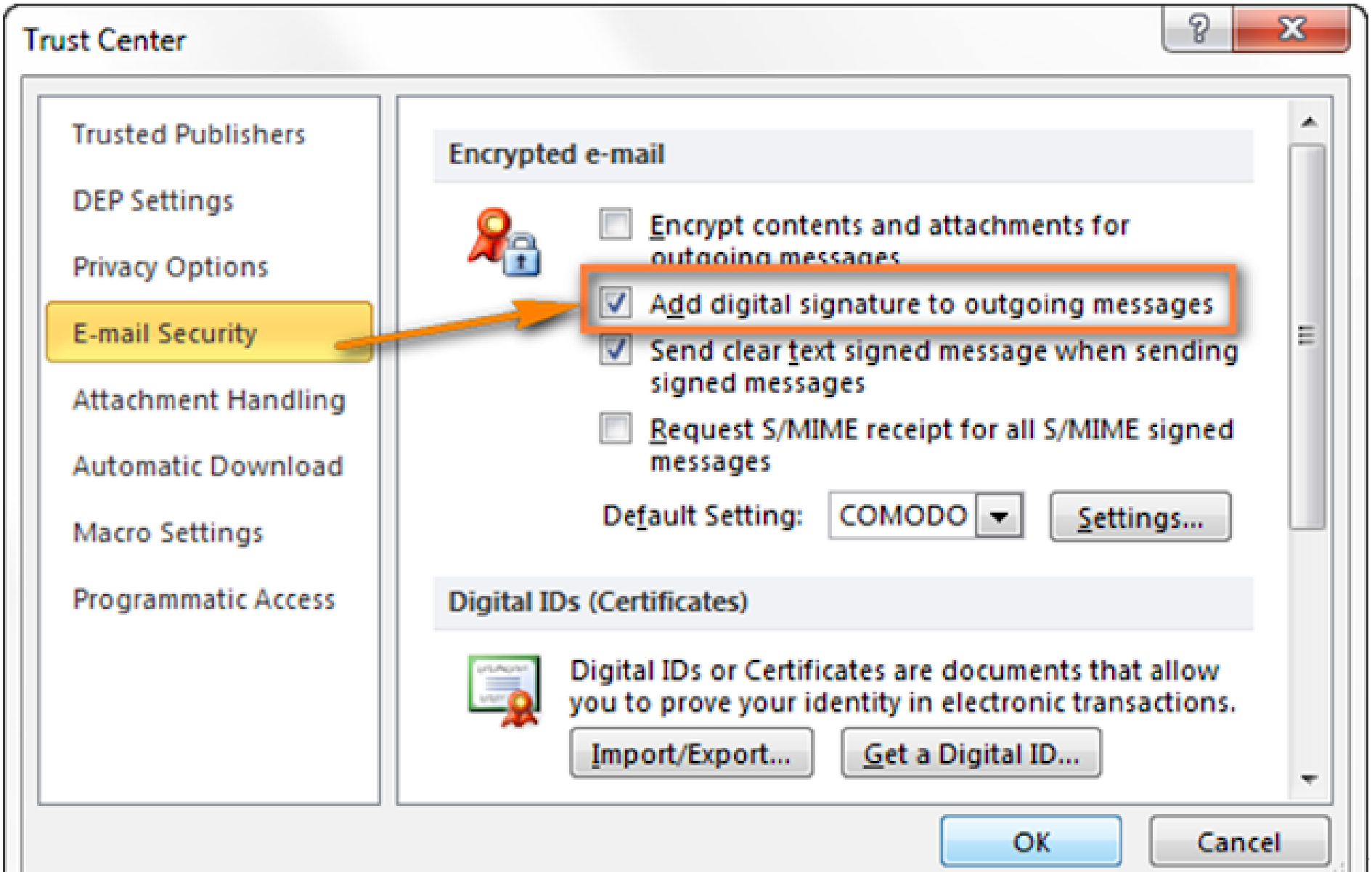
Digital Signature Requirement

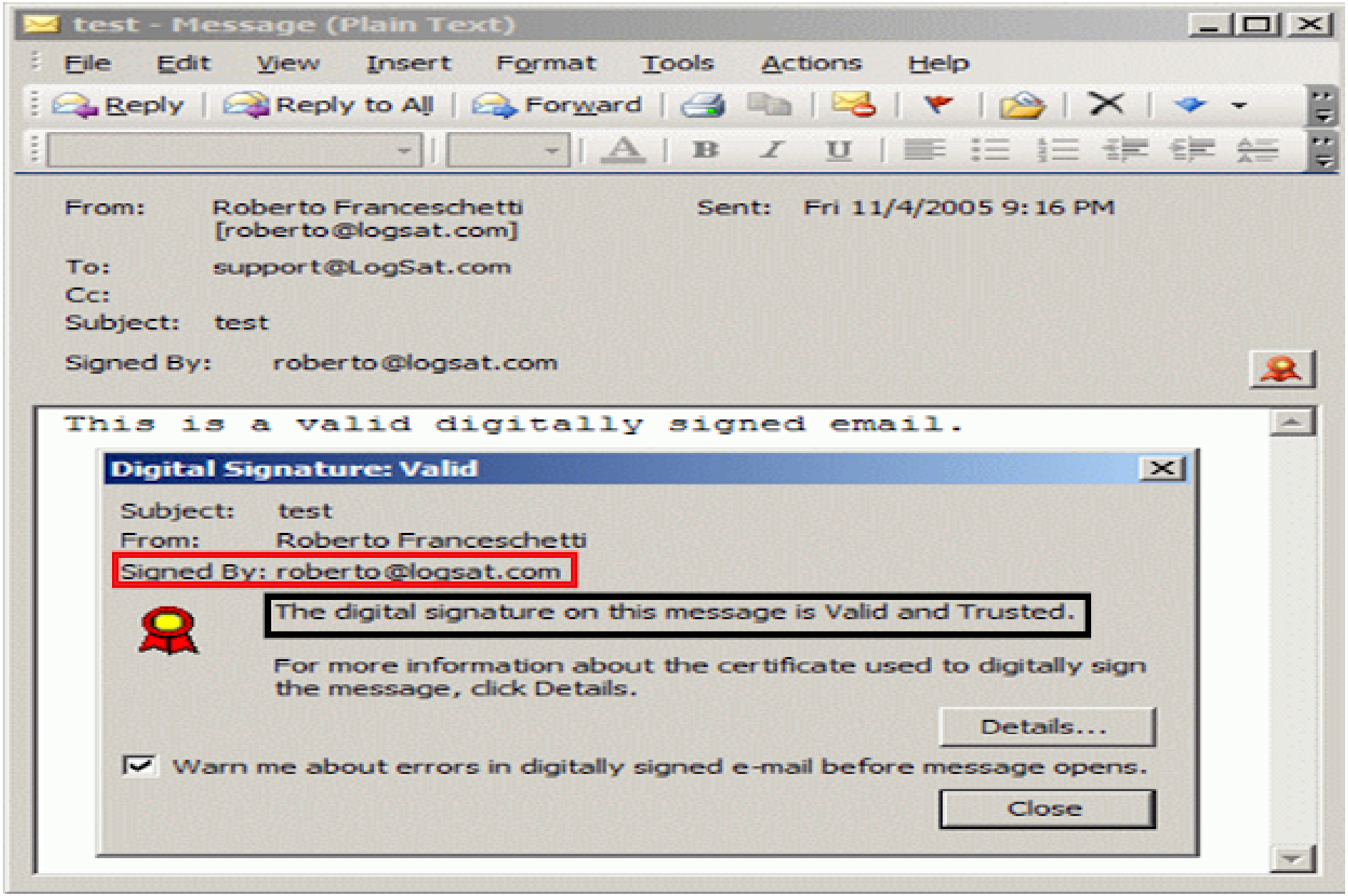
- The signature must be a bit pattern that depends on the message being signed.
- The signature must use some unique information of the sender to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital 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 fraud digital signature for a given message.

Security

- Message Authentication: A digital signature technique can provide message authentication. Digital signature is used to establish proof of identities and ensure that the origin of an electronic message is correctly identified.
- Message Integrity: Digital signature are used to detect unauthorized modification to data which assures that the contents of message are not changed after sender sends but before it reaches to intended receiver.
- Non-Repudiation: There are situation where a user sends a message and alter on refuses that he had sent that message. That is known as non-repudiation because the person who signed the document cannot repudiate the signature at a later time.
  We can prevent man in the middle attack, Replay attack, Masquerade, Impersonation attack

Realtime usage of digital signature



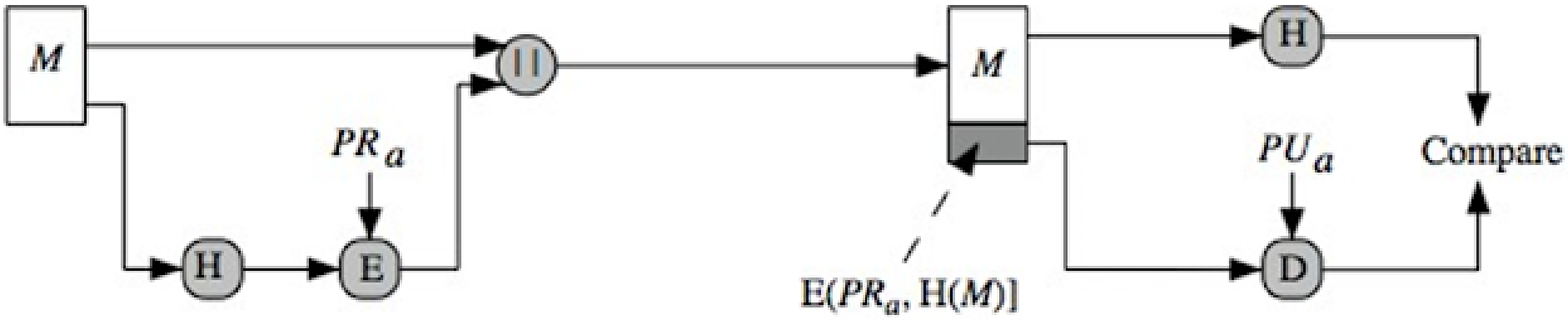

test - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: Roberto Franceschetti [roberto@logsat.com]
Sent: Fri 11/4/2005 9:16 PM
To: support@LogSat.com
Cc:
Subject: test
Signed By: roberto@logsat.com
This is a valid digitally signed email.
Digital Signature: Valid
Subject: test
From: Roberto Franceschetti
Signed By: roberto@logsat.com
The digital signature on this message is Valid and Trusted.
For more information about the certificate used to digitally sign the message, click Details.
Details...
Warn me about errors in digitally signed e-mail before message opens.
Close

Digital Signature Algorithm & Digital Signature Standards

- The National Institute of Standards and Technology (NIST) has published Federal Information Processing Standard FIPS 186, known as the Digital Signature Standard (DSS).
- The DSS makes use of the SHA and presents a new digital signature technique, the Digital Signature Algorithm (DSA).
- Latest version also incorporates digital signature algorithms based on RSA and on elliptic curve cryptography

The RSA Approach

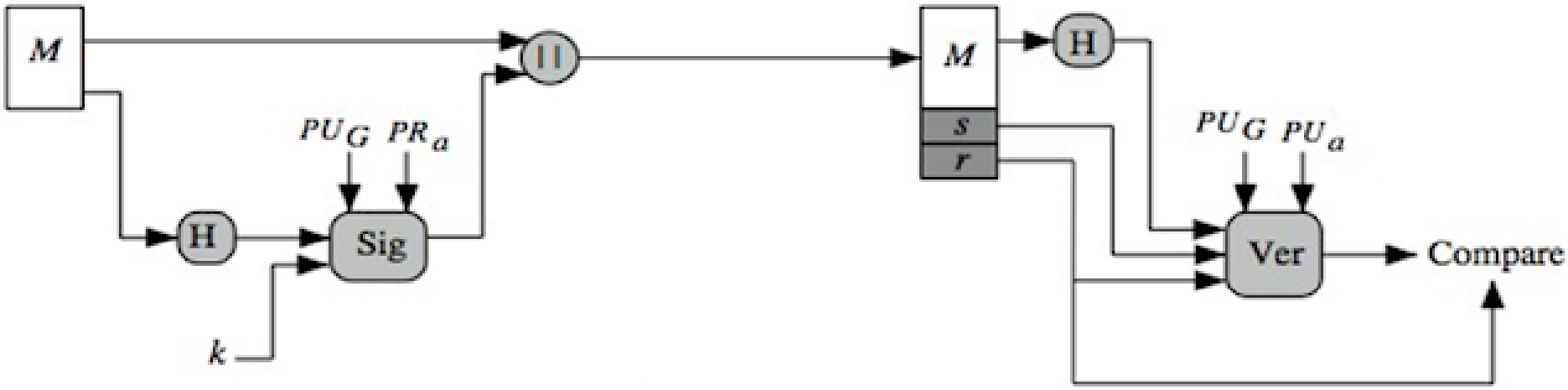
- In the RSA approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length.
- This hash code is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted.
- The recipient takes the message and produces a hash code.
- The recipient also decrypts the signature using the sender's public key.
- If the calculated hash code matches the decrypted signature, the signature is accepted as valid.



DSS Approach

- The DSS approach also makes use of a hash function.
- The hash code is provided as input to a signature function along with a random number k, generated for this particular signature.
- The signature function also depends on the sender's private key (PRa), and a set of parameters known to a group of communicating principle.
- We can consider this set to constitute a global public key (PU_G).
- The result is a signature consisting of two components, labelled s and r.
- At the receiving end, the hash code of the incoming message is generated.
- The signature is input to a verification function.
- The verification function also depends on the global public key as well as the sender's public key (PUa), which is paired with the sender's private key.

- The output of the verification function is a value that is equal to the signature component r, if the signature is valid.
- The signature function is such that only the sender, with knowledge of the private key, could have produced the valid signature.



Digital Signature Algorithm-Key Generation Process

Global Public-Key Components

p prime number where $2^{L-1} < p < 2^L$ for $512 \leq L \leq 1024$ and L a multiple of 64; i.e., bit length of between 512 and 1024 bits in increments of 64 bits

q prime divisor of $(p-1)$, where $2^{159} < q < 2^{160}$; i.e., bit length of 160 bits

g $= h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < (p-1)$ such that $h^{(p-1)/q} \bmod p > 1$

User's Private Key

x random or pseudorandom integer with $0 < x < q$

User's Public Key

$y = g^x \bmod p$

User's Per-Message Secret Number

k = random or pseudorandom integer with $0 < k < q$

Signing

$r = (g^k \bmod p) \bmod q$

$s = [k^{-1}(\mathrm{H}(M) + xr)] \bmod q$

Signature $= (r, s)$

Verifying

$w = (s')^{-1} \bmod q$

$u_1 = [\mathrm{H}(M')w] \bmod q$

$u_2 = (r')w \bmod q$

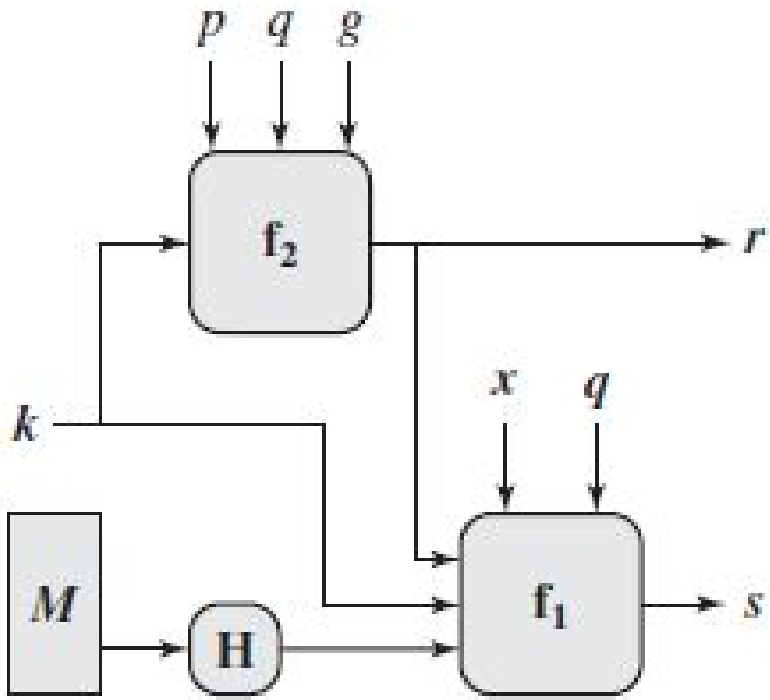
$v = [(g^{u1} y^{u2}) \bmod p] \bmod q$

TEST: $v = r'$

M = message to be signed

$\mathrm{H}(M)$ = hash of M using SHA-1

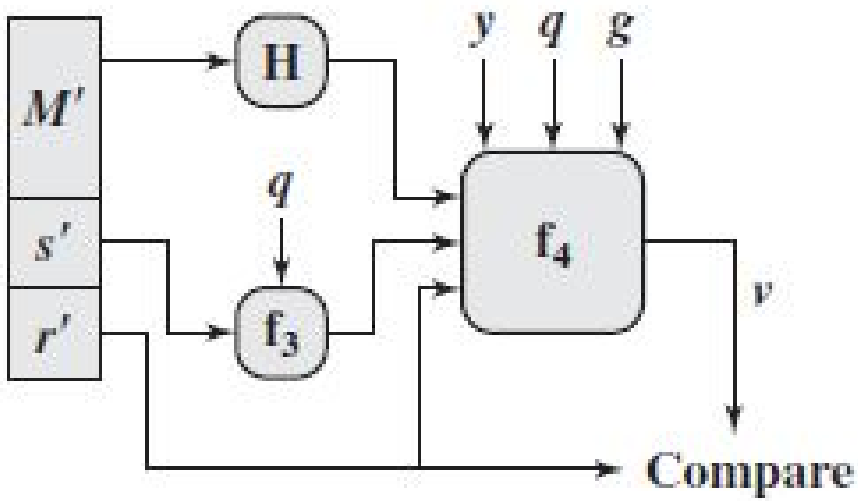
M', r', s' = received versions of M, r, s



$s = f_1(H(M), k, x, r, q) = (k^{-1} (H(M) + xr)) \bmod q$

$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$

(a) Signing



$w = f_3(s', q) = (s')^{-1} \bmod q$

$v = f_4(y, q, g, H(M'), w, r')$

$= ((g^{(H(M')w) \bmod q} y^{r'w \bmod q}) \bmod p) \bmod q$

(b) Verifying

Figure 13.5 DSS Signing and Verifying