Institute of Information Technology

Jahangirnagar University

জাহাঙ্গীরনগর বিশ্ববিদ্যালয়

IT-4259: Computer Network Security

for

4th Year 2nd Semester of B.Sc (Honors) in IT (5th Batch)

Lecture: 07

Digital Signature

Prepared by:

K M Akkas Ali

akkas_khan@yahoo.com, akkas@juniv.edu

Associate Professor

Institute of Information Technology (IIT)

Jahangirnagar University, Dhaka-1342

Lecture-07: Digital Signature

Objectives of this Lecture:

- To define a digital signature
- To define security services provided by a digital signature
- To define attacks on digital signatures
- To discuss some digital signature schemes:
  - RSA
  - ElGamal
- To describe some applications of digital signatures

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

What is Digital Signature?

- Digital signature, first proposed in 1976 by Whitfield Diffie of Stanford University, is a digital code (encrypted message digest) that can be attached to an electronically transmitted message that uniquely identifies the sender.
- Typically the signature is formed by taking the hash of the message (called message digest) and encrypting the digest with the creator's private key. The encrypted message digest is known as a digital signature. The signature guarantees the source and integrity of the message.
- Like a written signature on a document, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. It is linked to the data in such a manner that if the data is changed, the digital signature is invalidated.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Digital Signature Process

- In digital signature, a block of data or a sample of the message (called a message digest) represents a private key. When this message digest is encrypted with the owner's private key, then a digital signature is created.
- This digital signature is then added at the end of each message that is to be sent to the recipient.
- The recipient decrypts the message using the owner's public key and thus verifies that the message digest is correct and the message has come from the genuine sender.
- The process of digital signature is outlined below:
    1. Sender generates a message.
    2. Sender creates a "digest" of the message.
    3. Sender encrypts the message digest with his/her private key for authentication. This encrypted message digest is called digital signature.
    4. Sender attaches the digital signature to the end of the message that is to be sent.
    5. Sender encrypts both the message and signature with the recipient's public key.
    6. The recipient decrypts the entire message with his/her private key.
    7. Thus, the recipient verifies the digest for accuracy.

Digital Signature Process

Illustration of digital signature process:

- **Sender Site (Alice):**
  - Suppose, Alice generates a message digest using cryptographic hash function for her message to Bob.
  - She encrypts the message digest with her private key, and sends that digital signature along with the plaintext message to Bob.
- **Receiver Site (Bob):**
  - Bob uses Alice's public key to decrypt the digital signature and receives a copy of the message digest that Alice encoded.
  - Because Alice's public key decrypted her digital signature, Bob is certain that the message was from Alice. This authenticates the sender as genuine.
  - Bob then uses the same hash function (known to him and to Alice in advance) to encode his own message digest of Alice's plaintext message. If the encoded message digest turns out the same as the one Alice sent, the digital signature is considered authentic and the message has not been tempered.
  - The process is illustrated in the figure below:

Digital Signature Process

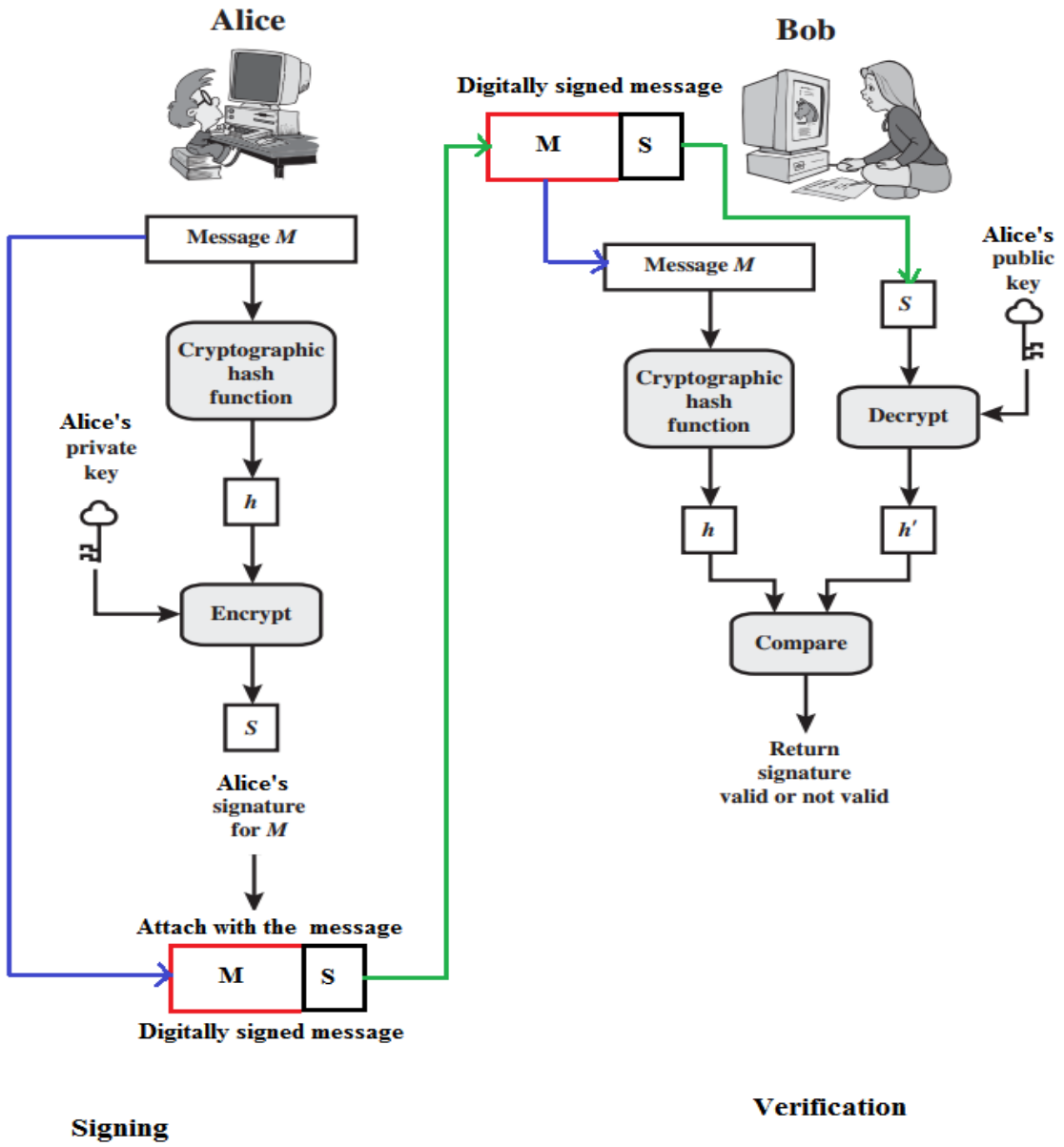

Figure: Illustration of digital signature process:

Digital Signature Vs. Conventional Signature

Key-point	Conventional Signature	Digital Signature
Inclusion	a conventional signature is included in the document; it is part of the document. E.g., when we write a check, the signature is on the check; it is not a separate document.	But, when we sign a document digitally, we send the signature as a separate document.; a digital signature is a separate document. The sender sends two documents- the message and the signature. The recipient receives both documents and verifies that the signature belongs to the supposed sender. If this is proven, the message is kept; otherwise, it is rejected.
Verification method	A conventional signature on a document is verified by comparing the signature on it with the signature on file.	For a digital signature, the recipient receives the message and the signature. The recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

Digital Signature Vs. Conventional Signature

Key-point	Conventional Signature	Digital Signature
Relationship	For a conventional signature, there is normally a one-to-many relationship between a signature and documents. A person uses the same signature to sign many documents.	For a digital signature, there is a one-to-one relationship between a signature and a message. Each message has its own signature. The signature on one message can not be used in another message. For example, if Bob receives two messages, one after another, from Alice, he can not use the signature of the first message to verify the second. Each message needs a new signature.
Duplicity	In conventional signature, a copy of the signed document can be distinguished from the original one on file.	In digital signature, there is no such distinction unless there is a factor of time (such as a timestamp) on the document. For example, suppose Alice sends a document instructing Bob to pay Eve. If the intercepts the documents and the signature, she can replay it later to get money again from Bob.

Services Provided by Digital Signature

- A digital signature servers three important purposes:
    1. Provides authentication of the sender
    2. Verifies data integrity
    3. Provides non-repudiation

Services Provided by Digital Signature

Message Authentication:

- A digital signature's main function is to verify that a message or document, in fact, comes from the claimed sender. That is, to provide authentication is the main function of digital signature.

Message Integrity:

- The integrity of the message is preserved even if we sign the whole message because we cannot get the same signature if the message is changed. Therefore, digital signature provides the integrity of the message.

Non-repudiation:

- Attaching a digital signature with message prevents repudiation. This ensures that the sender should not be able to later deny that he/she sent a message. Non-repudiation prevents sender and vendor in a transaction or communication activity from later falsely denying that the transaction occurred.

N.B. As contrast to encryption scheme, digital signature does not provides the confidentiality of the message.

Attacks and Forgeries on Digital Signature

- In order of increasing severity, following types of attacks are discussed.
- Here, ***A*** denotes the user whose signature method is being attacked, and ***C*** denotes the attacker.

- **Key-only attack:**
  - C only knows A's public key.
- **Known message attack:**
  - C is given access to a set of messages and their signatures.
- **Generic chosen message attack:**
  - C chooses a list of messages before attempting to breaks A's signature scheme, independent of A's public key. C then obtains from A valid signatures for the chosen messages. The attack is generic, because it does not depend on A's public key; the same attack is used against everyone.
- **Directed chosen message attack:**
  - Similar to the generic attack, except that the list of messages to be signed is chosen after C knows A's public key but before any signatures are seen.
- **Adaptive chosen message attack:**
  - C is allowed to use A as an "oracle." This means the A may request signatures of messages that depend on previously obtained message–signature pairs.

Digital Signature Requirements

- On the basis of the properties and attacks , we can formulate the following 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 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 fraudulent digital signature for a given message.
  - It must be practical to retain a copy of the digital signature in storage.
- A secure hash function, embedded in a digital signature scheme (such as that of Figure 13.2) provides a basis for satisfying these requirements. However, care must be taken in the design of the details of the scheme.

Digital Signature Schemes

- Several digital signature schemes have evolved during the last few decades. Some of them have been implemented.
  - RSA Digital Signature Scheme
  - ElGamal Digital Signature Scheme
  - Schnorr Digital Signature Scheme
  - Elliptic Curve Digital Signature Scheme

Prepared by: K M Akkas Ali, Associate Professor, IIT, JU

RSA Digital Signature Scheme:

- The idea behind RSA can be used for signing and verifying a message. In this case, it is called the RSA digital signature scheme.
- The digital signature scheme changes the roles of the private and public keys:
  - First, the private and public key of the sender (not the receiver) are used:
  - Second, the sender uses her own private key to sign the document; the receiver uses the sender's public key to verify it.
- Alice can not use Bob's public key to sign the message because then any other person could do the same.

RSA Digital Signature Scheme: General Idea

- Figure below shows the general idea behind the RSA digital signature scheme.

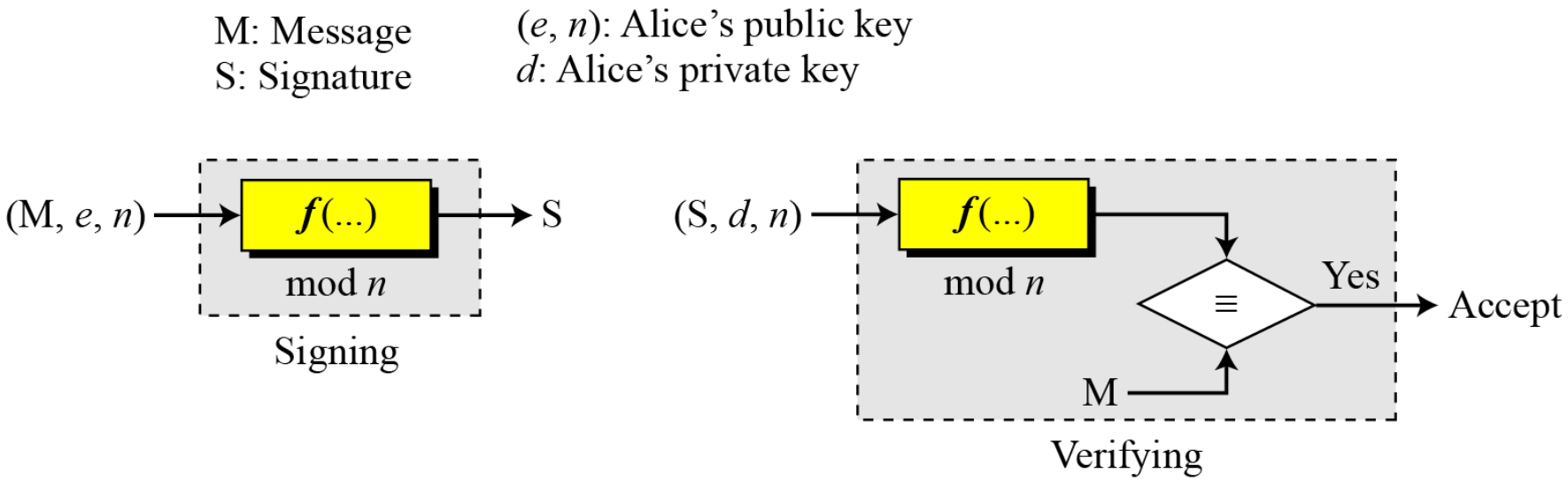

Figure: General idea behind the RSA digital signature scheme

RSA Digital Signature Scheme: Key Generation

- Key generation in the RSA digital signature scheme is exactly the same as key generation in the RSA cryptosystem.
- In the RSA digital signature scheme, d is private; e and n are public.

RSA Digital Signature Scheme: Signing and Verifying

Signing:

- Alice creates a signature S out of the message M using her private exponent d with this formula, $S = M^d \bmod n$. She then sends the message and the signature to Bob

Verifying:

- Bob receives M and S. He applies Alice's public exponent e to the signature to create a copy of the message M` using this formula, $M` = S^e \bmod n$. Bob compares the value of M` with the value of M. If the two values are congruent, Bob accepts the message.

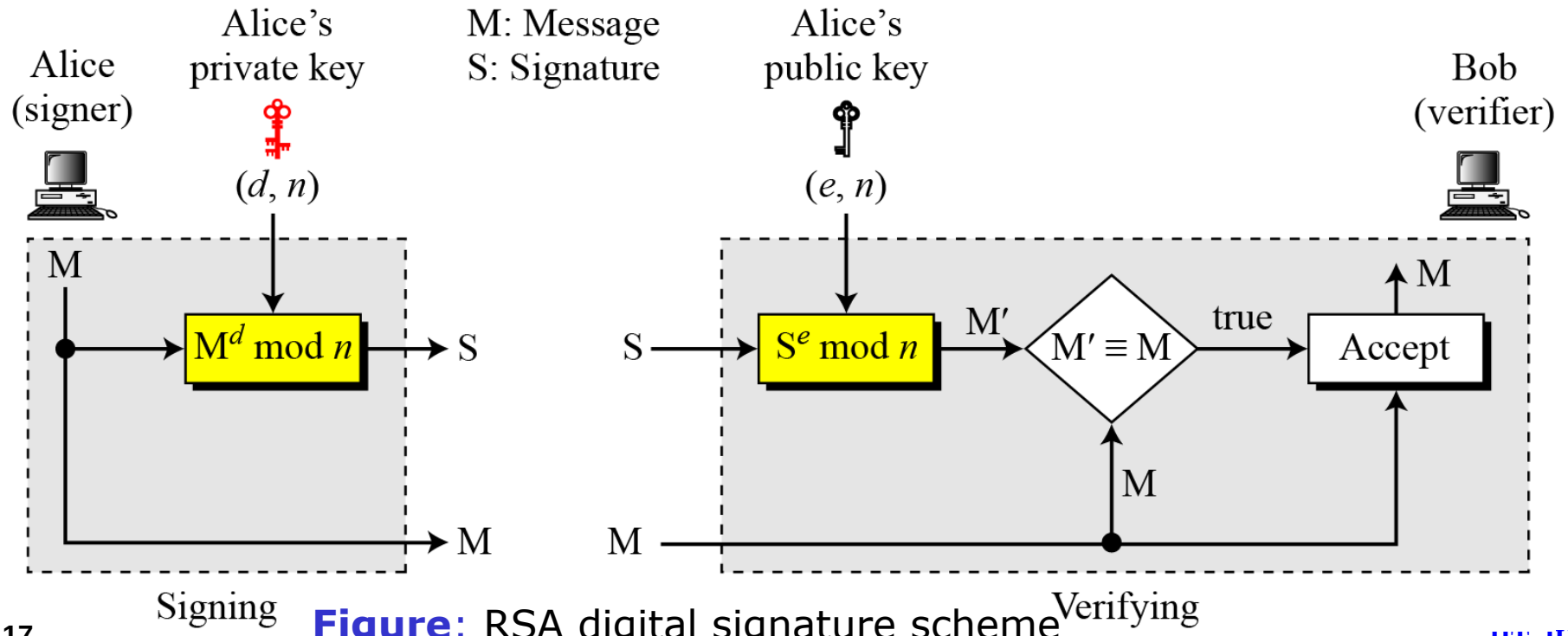

Figure: RSA digital signature scheme

ElGamal Digital Signature Scheme:

- The ElGamal encryption scheme is designed to enable encryption by a user's public key with decryption by the user's private key.
- The ElGamal signature scheme involves the use of the private key for encryption and the public key for decryption.

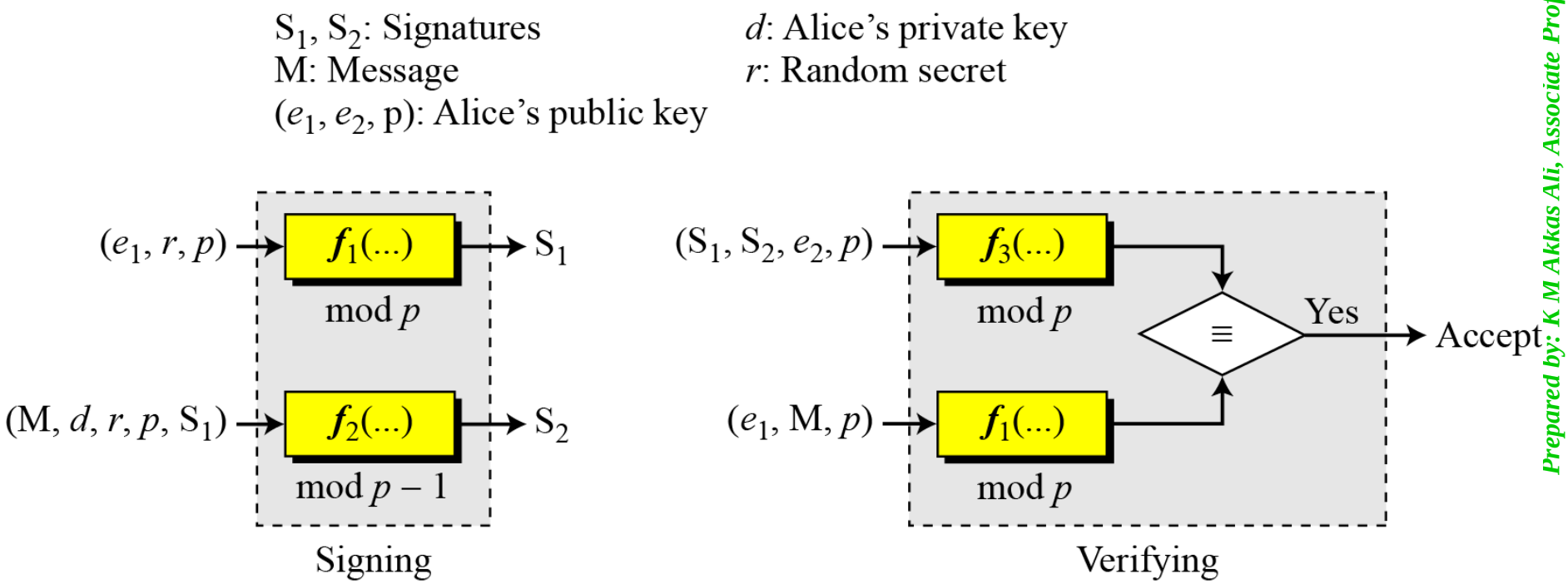

Figure: General idea behind the ElGamal digital signature scheme

ElGamal Digital Signature Scheme:

- As with ElGamal encryption, the global elements of ElGamal digital signature are a prime number q and α, which is a primitive root of q. User A generates a private/public key pair as follows.
- 1. Generate a random integer X_A, such that $1<X_A<q-1$.
- 2. Compute $Y_A= \alpha^{X_A} \bmod q$.
- 3. A's private key is X_A; A's pubic key is $\{q, \alpha, Y_A\}$.
- To sign a message M, user A first computes the hash m=H(M), such that m is an integer in the range $0<=m<=q-1$. A then forms a digital signature as follows.
- 1. Choose a random integer K such that and $1<=K<=q-1$ and gcd(K,q-1)=1. That is, K is relatively prime to q-1.
- 2. Compute $S_1= \alpha^K \bmod q$. Note that this is the same as the computation of C_1 for ElGamal encryption.
- 3. Compute $K^{-1} \bmod (q-1)$. That is, compute the inverse of K modulo q-1 .
- 4. Compute $S_2=K^{-1}(m - X_A S_1) \bmod (q-1)$.
- 5. The signature consists of the pair S_1, S_2.
- Any user B can verify the signature as follows.
- 1. Compute $V_1= \alpha^m \bmod q$.
- 2. Compute $V_2=(Y_A)^{S_1} (S_1)^{S_2} \bmod q$.
- The signature is valid if $V_1=V_2$.

ElGamal Digital Signature Scheme:

- To sign a message M, user A first computes the hash m=H(M), such that m is an integer in the range 0<=m<=q-1. A then forms a digital signature as follows.
- 1. Choose a random integer K such that and 1<=K<=q-1 and gcd(K,q-1)=1. That is, K is relatively prime to q-1.
- 2. Compute $S_1 = \alpha^K \bmod q$. Note that this is the same as the computation of C_1 for ElGamal encryption.
- 3. Compute $K^{-1} \bmod (q-1)$. That is, compute the inverse of K modulo q-1 .
- 4. Compute $S_2 = K^{-1}(m - X_A S_1) \bmod (q-1)$.
- 5. The signature consists of the pair S_1, S_2.
- Any user B can verify the signature as follows.
- 1. Compute $V_1 = \alpha^m \bmod q$.
- 2. Compute $V_2 = (Y_A)^{S_1} (S_1)^{S_2} \bmod q$.
- The signature is valid if $V_1 = V_2$.

RSA Digital Signature Scheme Vs. RSA Cryptosystem

- The idea behind the RSA digital signature scheme is the same as the RSA cryptosystem, but the roles of the private and public keys are changed.
  - First, the private and public keys of the sender, not the receiver, are used.
  - Second, the sender uses her own private key to sign the document; the receiver uses the sender's public key to verify it.

Digital Signature Vs. Cryptosystem

- A digital signature needs a asymmetric-key cryptosystem. The signer signs the message with her private key; the verifier verifies it with the signer's public key.
- A cryptosystem uses the private and public keys of the receiver. On the other hand, a digital signature uses the private and public keys of the sender.
- A digital signature does not provide confidential communication. But a cryptosystem can provide the confidentiality of a message.
- A cryptosystem can not provide the authenticity of the message originator, but a digital signature can.

Message Authentication Code (MAC) Vs. Digital Signature

Is a message digest the same as a message authentication code?

- A message authentication code (MAC) is a short piece of information used to authenticate a message.
  - A MAC algorithm accepts as input a secret key and a message to be authenticated.
  - It outputs a MAC, which is sometimes called a tag.
- The MAC value protects both a message's integrity as well as its authenticity by allowing verifiers (who also possess the same secret key) to detect any changes to the message content.
- A message authentication code is different than a digital signature.
  - MAC values are both generated and verified using the same secret key.
    - While using MAC, sender and receiver of a message must agree on keys before initiating communications. As is the case with private key encryption.
  - A message authentication code does not provide the property of non-repudiation offered by digital signature.