Digital Signatures

ITC 3093 Principles of Computer Security

Based on
Cryptography and Network Security by William Stallings
and Lecture slides by Lawrie Brown

and
Introduction to Cryptography and Security Mechanisms by Dr Keith Martin

Digital Signatures

- Informally, a digital signature is a technique for establishing the origin of a particular message in order to settle later disputes about what message (if any) was sent.
- The purpose of a digital signature is thus for **an entity to bind its identity to a message**.
- Common terminology:
  - **Signer** - an entity who creates a digital signature
  - **Verifier** - an entity who receives a signed message and attempts to check whether the digital signature is "correct" or not

Electronic signatures

- The European Community Directive on electronic signatures refers to the concept of an *electronic signature* as:
    - ***data in electronic form attached to, or logically connected with, other electronic data and which serves as a method of authentication***

Advanced electronic signatures

- The European Community Directive on electronic signatures also refers to the concept of an *advanced electronic signature* as:
- an electronic signature that is:
    1. uniquely linked to the signatory
    2. capable of identifying the signatory
    3. created using means under the sole control of the signatory
    4. linked to data to which it relates in such a way that subsequent changes in the data is detectable

Security requirements

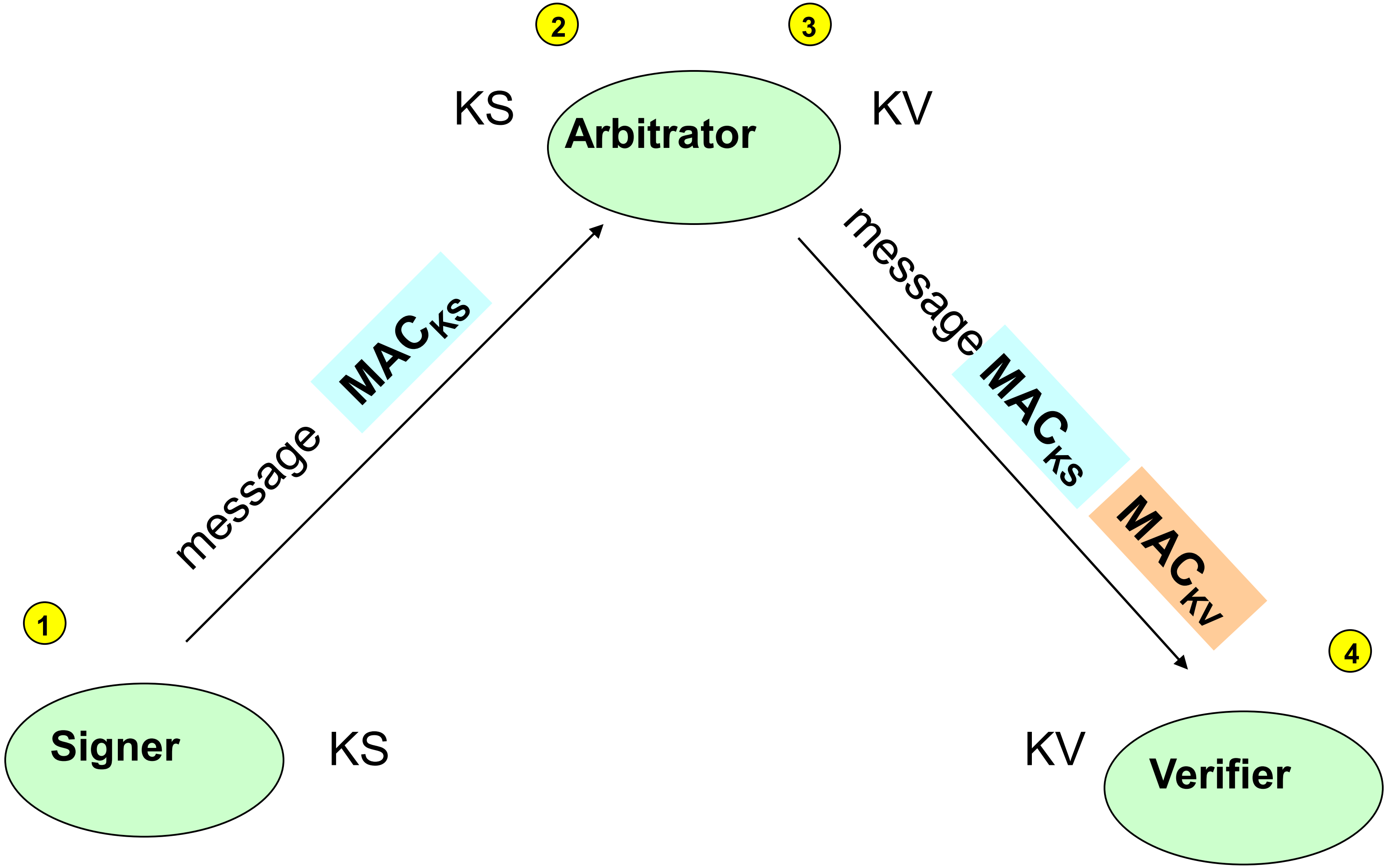
- We will define a **digital signature** on a message to be some data that provides:

1. Data origin authentication of the signer
    - A digital signature validates the message in the sense that assurance is provided about the integrity of the message and of the identity of the entity that signed the message.
2. Non-repudiation
    - A digital signature can be stored by anyone who receives the signed message as evidence that the message was sent and of who sent it. This evidence could later be presented to a third party who could use the evidence to resolve any dispute that relates to the contents and/or origin of the message.

Input to a digital signature

- The message
    - Since a digital signature needs to offer data origin authentication (and non-repudiation) it is clear that the digital signature itself must be a piece of data that depends on the message, and cannot be a completely separate identifier.
    - It may be sent as a separate piece of data to the message, but its computation must involve the message.
- A secret parameter known only by the signer
    - Since a digital signature needs to offer non-repudiation, its calculation must involve a secret parameter that is known only by the signer.
    - The only possible exception to this rule is if the other entity is totally trusted by all parties involved in the signing and verifying of digital signatures.

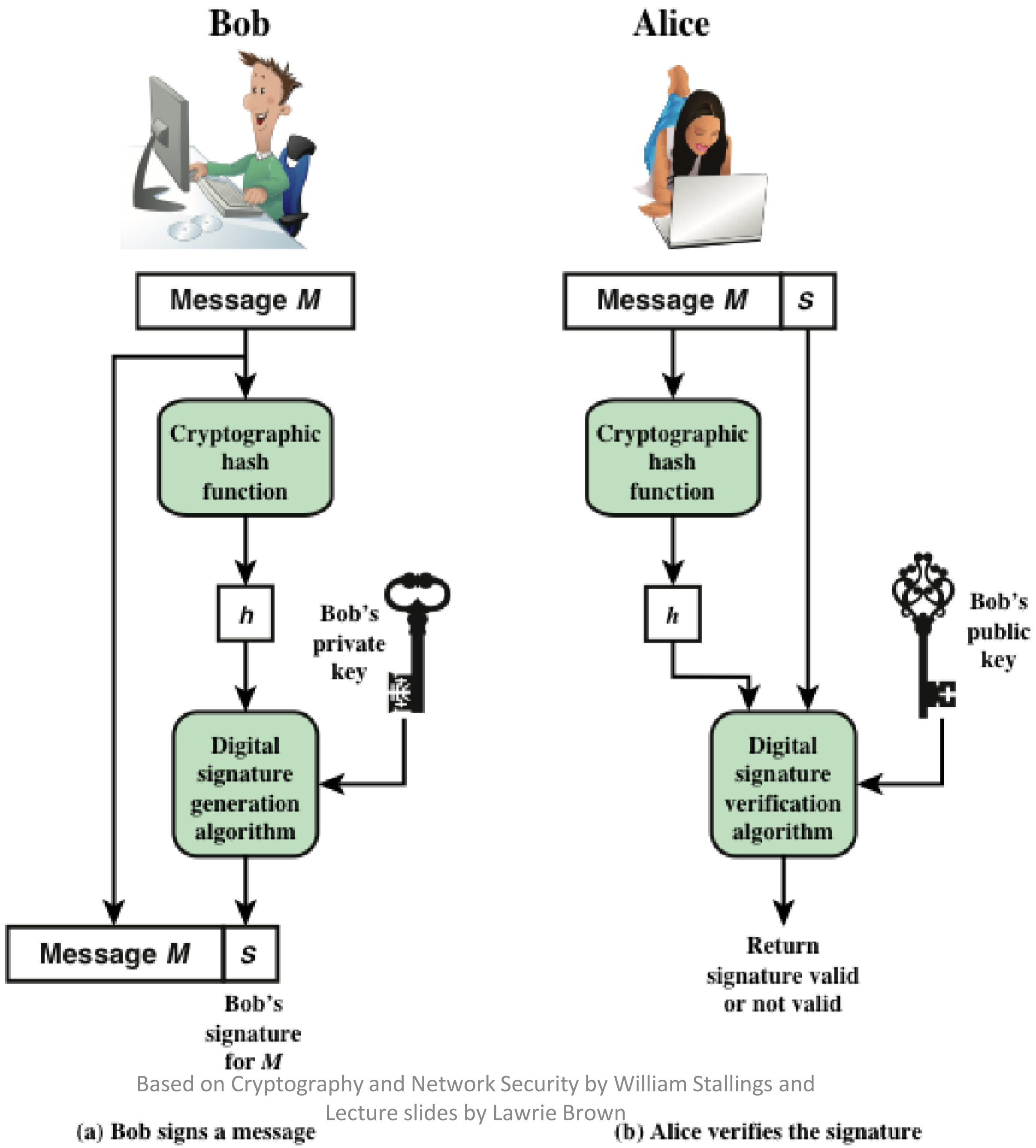
Arbitrated digital signatures



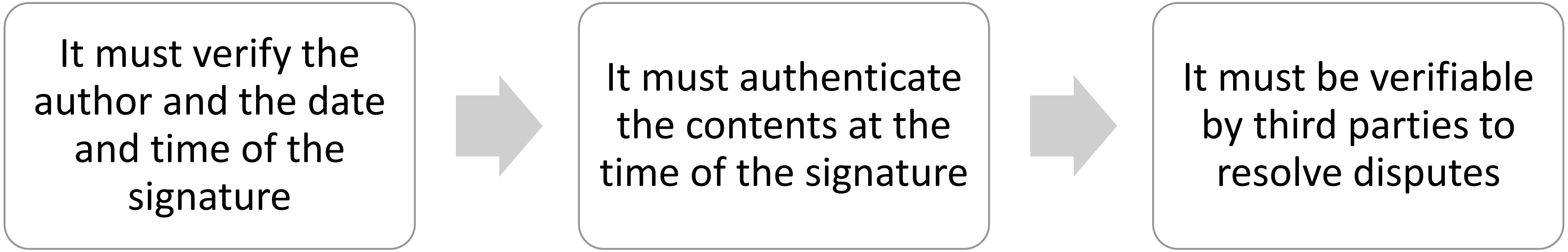
True digital signatures

- The vast majority of digital signature techniques do not involve having to communicate through a trusted arbitrator.
- A *true digital signature* is one that can be sent directly from the signer to the verifier. For the rest of this unit when we say “digital signature” we mean “true digital signature”.

True digital signature requirements	Public key encryption requirements
Only the holder of some secret data can sign a message	“Anyone” can encrypt a message
“Anyone” can verify that a signature is valid	Only the holder of some secret data can decrypt a message


Bob
Alice
Message M
Message M
S
Cryptographic hash function
Cryptographic hash function
h
h
Bob's private key
Bob's public key
Digital signature generation algorithm
Digital signature verification algorithm
Message M
S
Bob's signature for M
Return signature valid or not valid
(a) Bob signs a message
(b) Alice verifies the signature

Digital Signature Properties



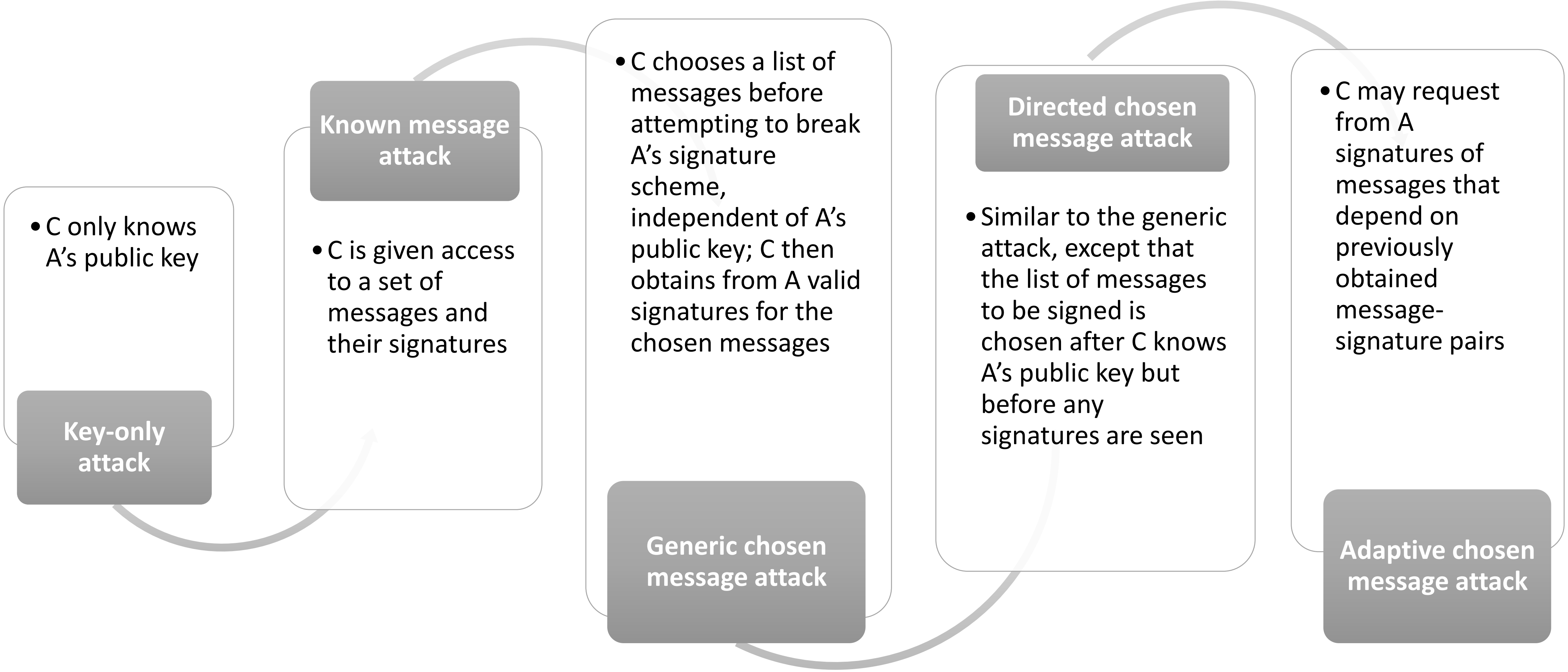
It must verify the author and the date and time of the signature

It must authenticate the contents at the time of the signature

It must be verifiable by third parties to resolve disputes

Based on Cryptography and Network Security by William Stallings and
Lecture slides by Lawrie Brown

Attacks



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 break A's signature scheme, independent of A's public key; C then obtains from A valid signatures for the chosen messages

Directed chosen message attack

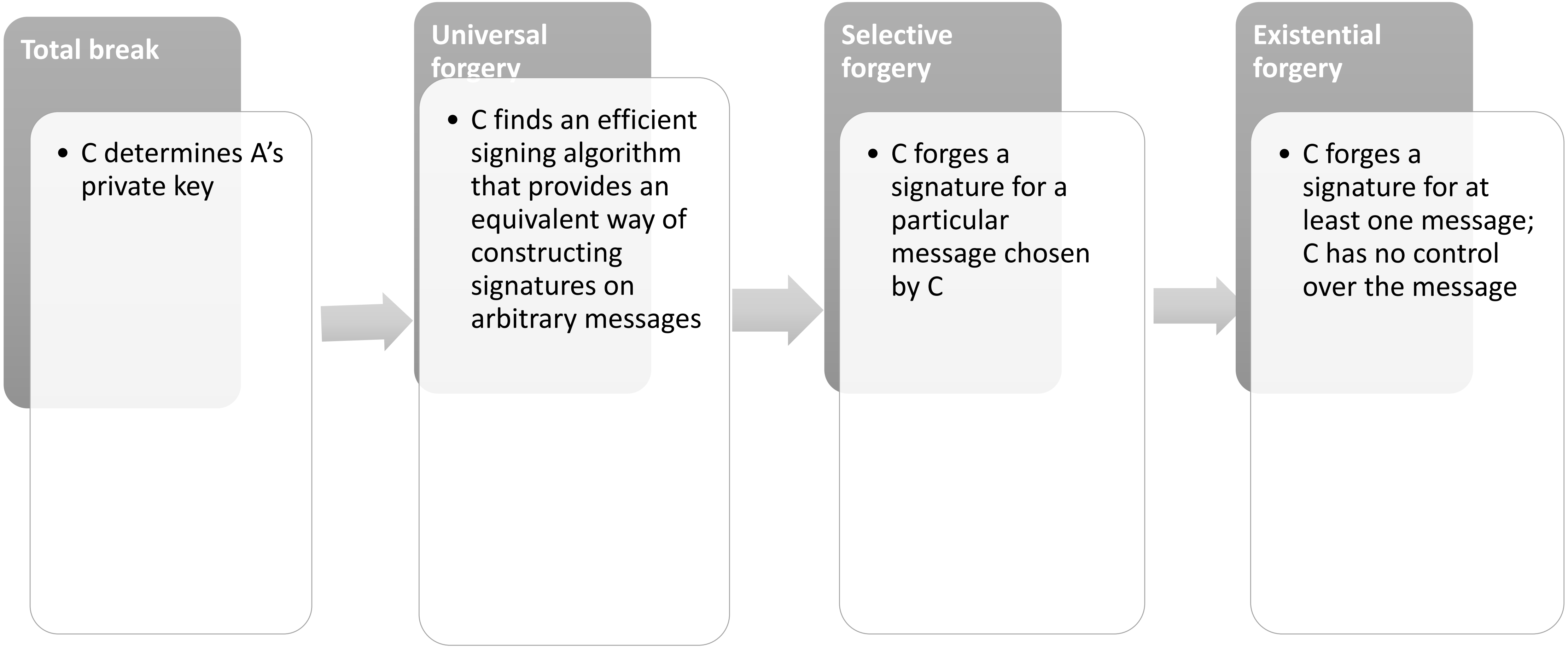
- Similar to the generic attack, except that the list of messages to be signed is chosen after C knows A's public key but before any signatures are seen

Adaptive chosen message attack

- C may request from A signatures of messages that depend on previously obtained message-signature pairs

Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

Forgeries



Total break

- C determines A’s private key

Universal forgery

- C finds an efficient signing algorithm that provides an equivalent way of constructing signatures on arbitrary messages

Selective forgery

- C forges a signature for a particular message chosen by C

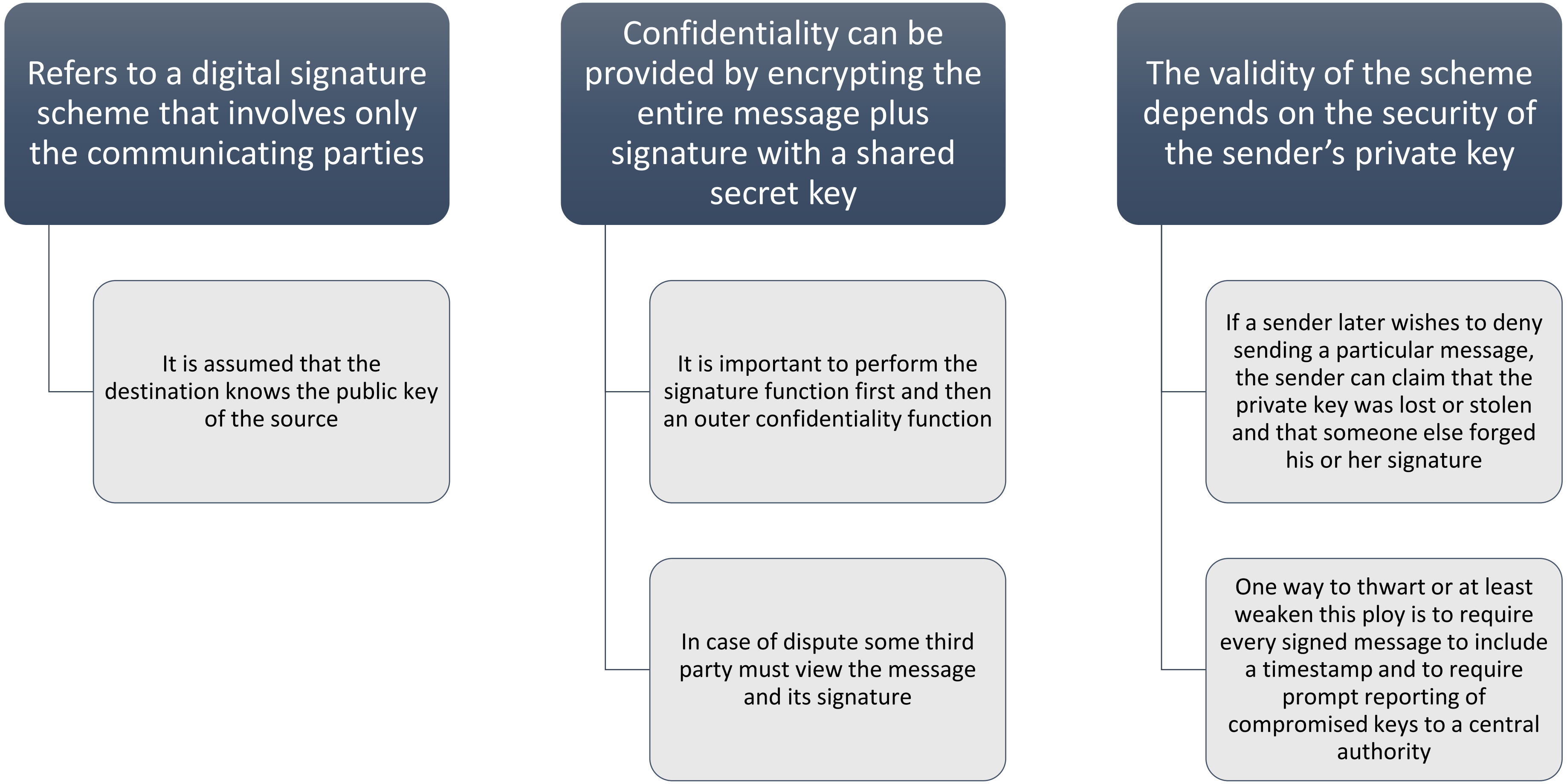
Existential forgery

- C forges a signature for at least one message; C has no control over the message

Digital Signature Requirements

- 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

Direct Digital Signature



Refers to a digital signature scheme that involves only the communicating parties

- It is assumed that the destination knows the public key of the source

Confidentiality can be provided by encrypting the entire message plus signature with a shared secret key

- It is important to perform the signature function first and then an outer confidentiality function
- In case of dispute some third party must view the message and its signature

The validity of the scheme depends on the security of the sender’s private key

- If a sender later wishes to deny sending a particular message, the sender can claim that the private key was lost or stolen and that someone else forged his or her signature
- One way to thwart or at least weaken this ploy is to require every signed message to include a timestamp and to require prompt reporting of compromised keys to a central authority

Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

ElGamal Digital Signature

- Scheme involves the use of the private key for encryption and the public key for decryption
- Global elements are a prime number *q* and a, which is a primitive root of *q*
- Use private key for encryption (signing)
- Uses public key for decryption (verification)
- Each user generates their key
  - Chooses a secret key (number): $1 < x_A < q-1$
  - Compute their public key: $y_A = a^{xA} \bmod q$

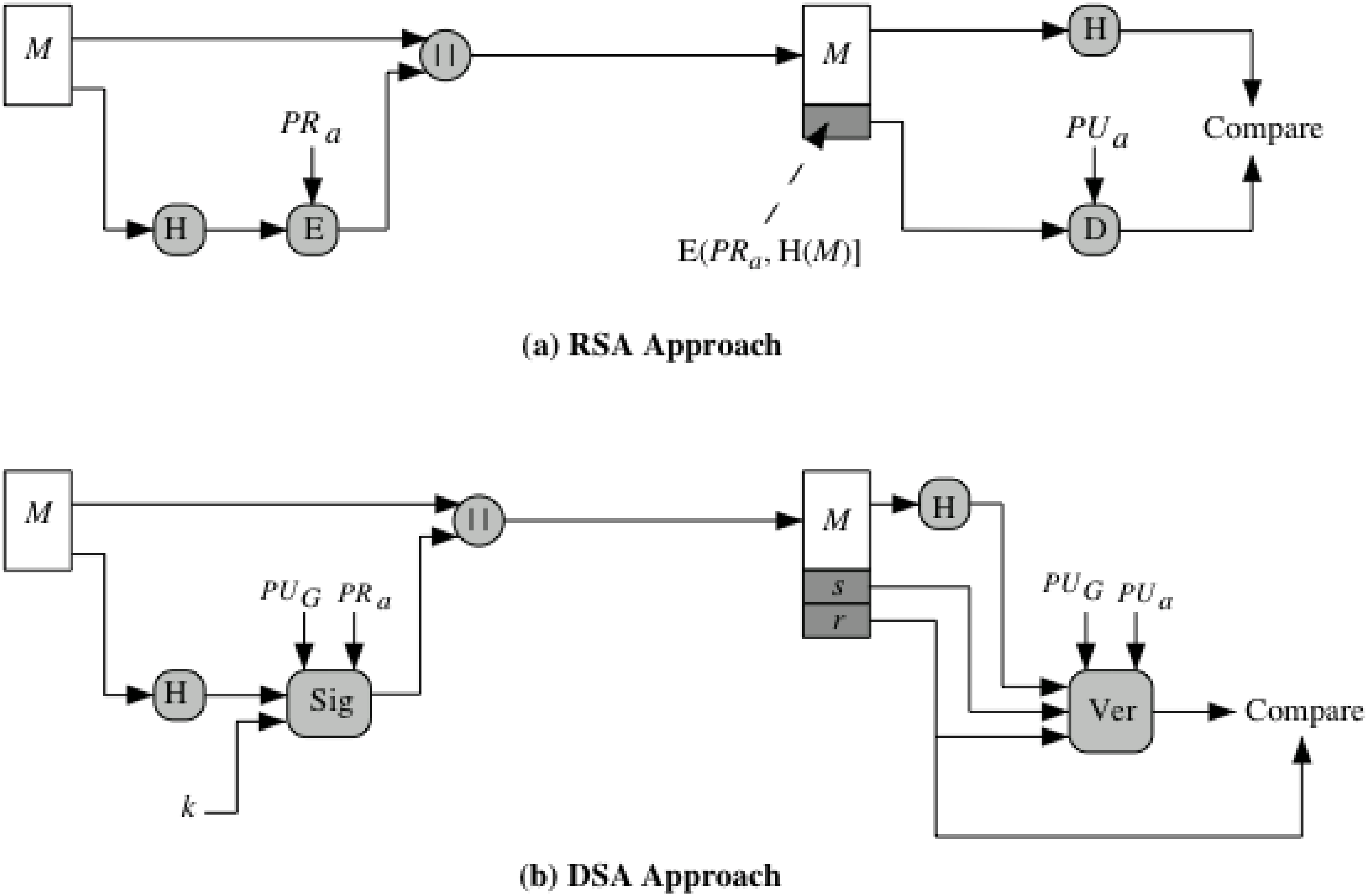
Based on Cryptography and Network Security by William Stallings and Lecture slides by Lawrie Brown

NIST Digital Signature Algorithm

- Published by NIST as Federal Information Processing Standard FIPS 186
- Makes use of the Secure Hash Algorithm (SHA)
- The latest version, FIPS 186-3, also incorporates digital signature algorithms based on RSA and on elliptic curve cryptography

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 (PR_a) to form the signature.

In the DSA approach, the signature function also depends on the sender’s private key (PR_a) and a set of parameters known to a group of communicating principals. We can consider this set to constitute a global public key (PU_G).



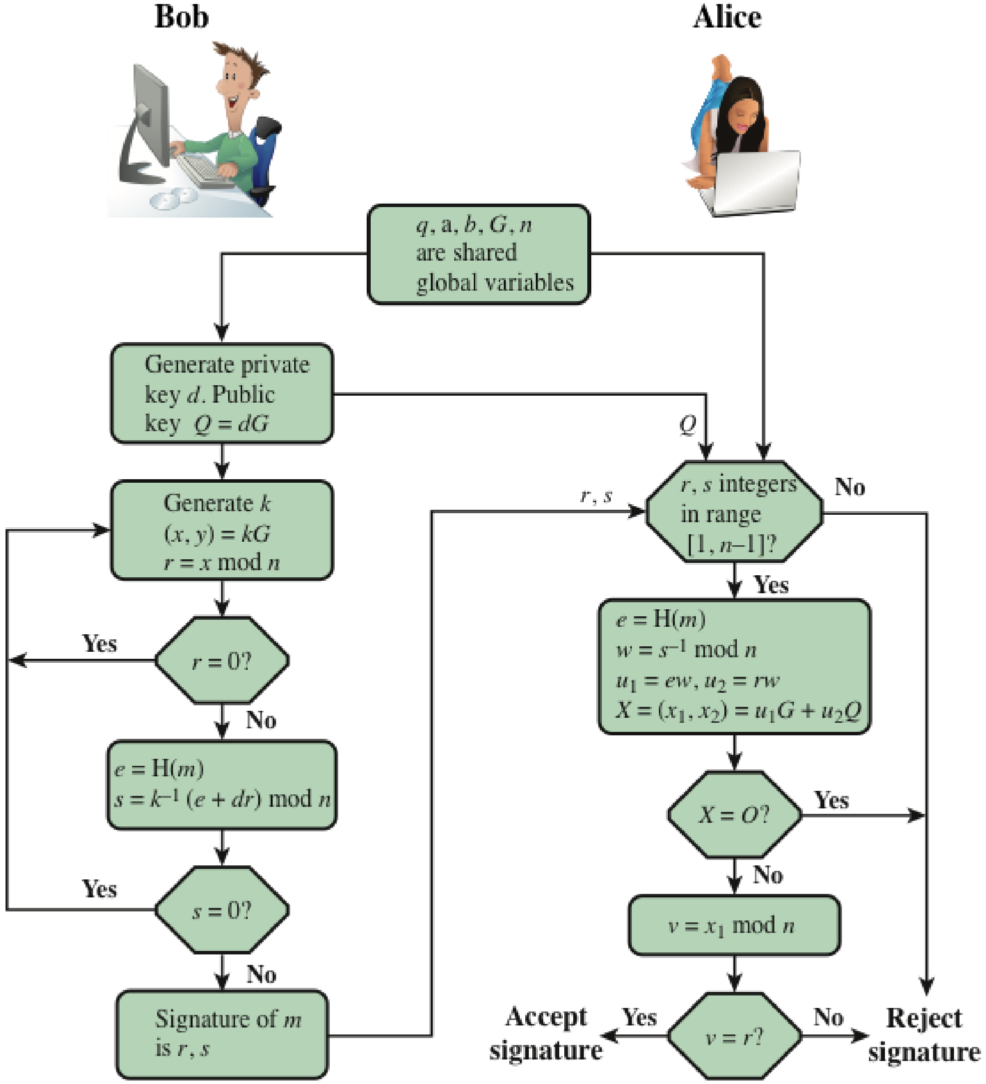
(a) RSA Approach

(b) DSA Approach

Figure 13.2 Two Approaches to Digital Signatures

Elliptic Curve Digital Signature Algorithm (ECDSA)

- Four elements are involved:
  - All those participating in the digital signature scheme use the same global domain parameters, which define an elliptic curve and a point of origin on the curve
  - A signer must first generate a public, private key pair
  - A hash value is generated for the message to be signed; using the private key, the domain parameters, and the hash value, a signature is generated
  - To verify the signature, the verifier uses as input the signer's public key, the domain parameters, and the integer *s;* the output is a value *v* that is compared to *r* ; the signature is verified if the *v = r*



Bob
Alice
q, a, b, G, n are shared global variables
Generate private key d. Public key $Q = dG$
Q
Generate k $(x, y) = kG$ $r = x \bmod n$
$r = 0?$
Yes
No
$e = H(m)$ $s = k^{-1}(e + dr) \bmod n$
$s = 0?$
Yes
No
Signature of m is r, s
r, s
r, s integers in range $[1, n-1]$?
No
Yes
$e = H(m)$ $w = s^{-1} \bmod n$ $u_1 = ew, u_2 = rw$ $X = (x_1, x_2) = u_1G + u_2Q$
$X = O?$
Yes
No
$v = x_1 \bmod n$
$v = r?$
Yes
No
Accept signature
Reject signature

Figure 13.5 ECDSA Signing and Verifying

RSA-PSS

- RSA Probabilistic Signature Scheme
- Included in the 2009 version of FIPS 186
- Latest of the RSA schemes and the one that RSA Laboratories recommends as the most secure of the RSA schemes
- For all schemes developed prior to PSS it has not been possible to develop a mathematical proof that the signature scheme is as secure as the underlying RSA encryption/decryption primitive
- The PSS approach was first proposed by Bellare and Rogaway
- This approach, unlike the other RSA-based schemes, introduces a randomization process that enables the security of the method to be shown to be closely related to the security of the RSA algorithm itself

Summary

- Digital signatures
  - Properties
  - Attacks and forgeries
  - Digital signature requirements
  - Direct digital signature
- Elgamal digital signature scheme
- NIST digital signature algorithm
- Elliptic curve digital signature algorithm
- RSA-PSS Digital Signature Algorithm