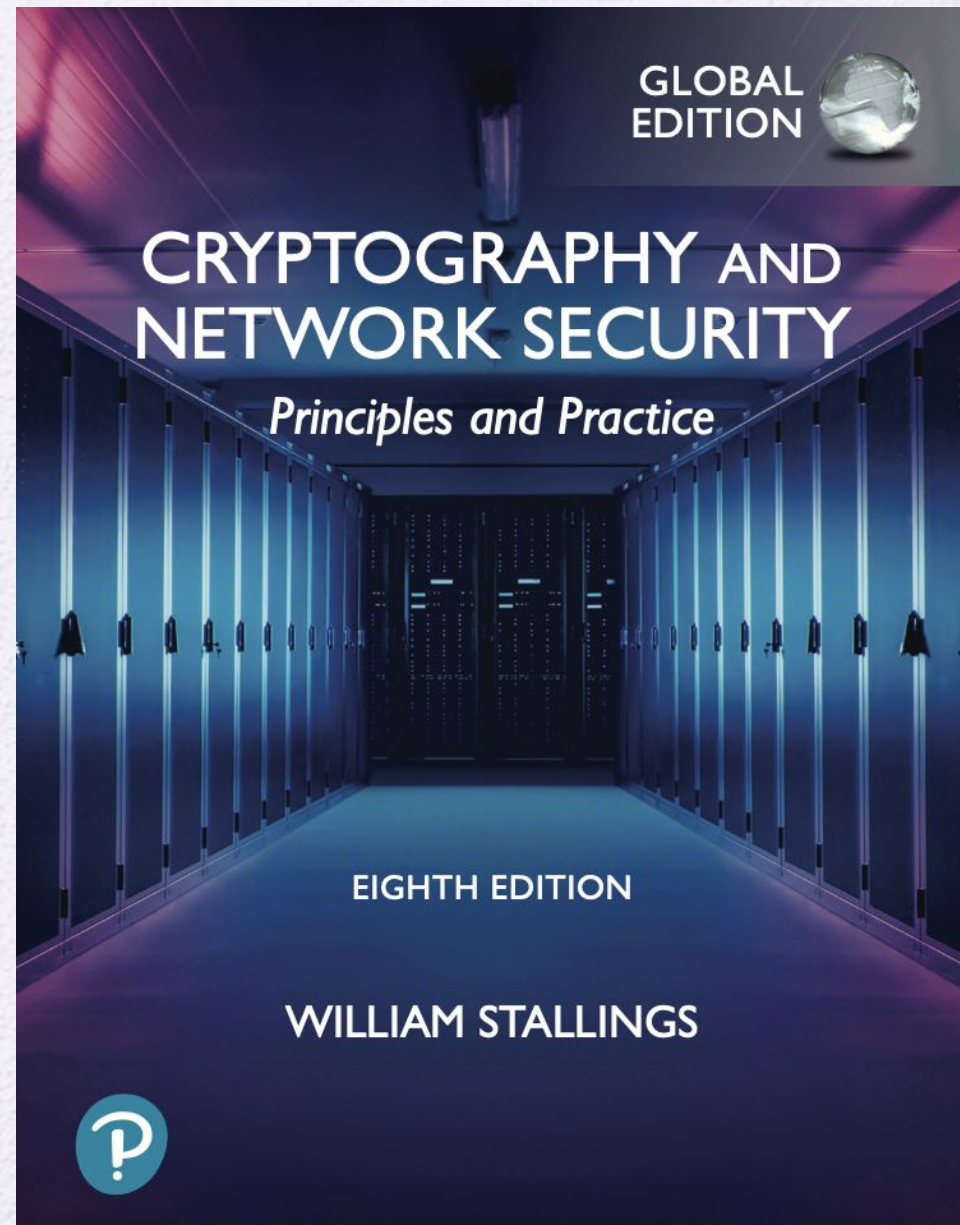


University of Nevada – Reno
Computer Science & Engineering
Department

CS454/654 Reliability and Security
of Computing Systems - Fall 2024

Lecture 16

Dr. Batyr Charyyev
bcharyyev.com



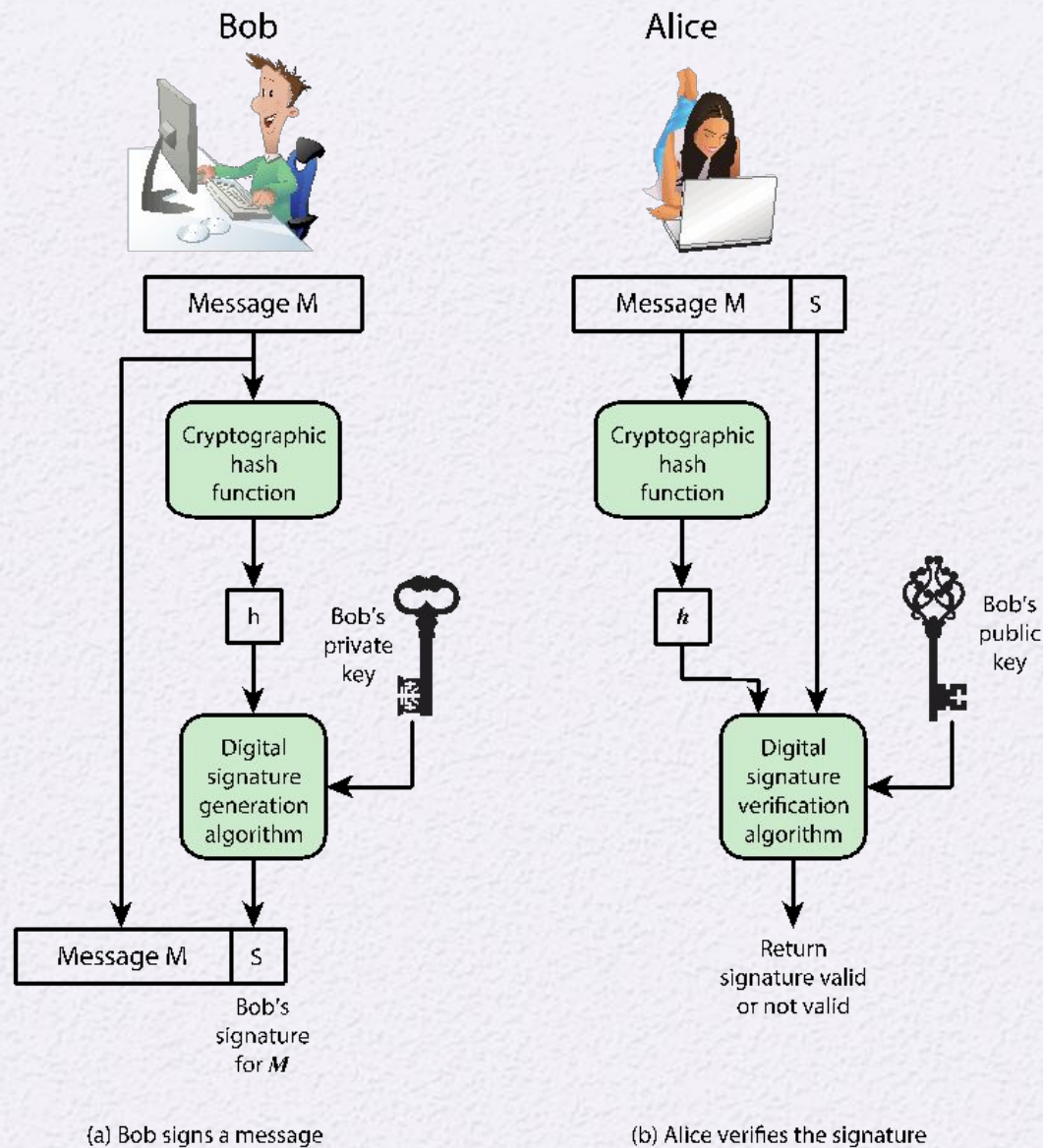
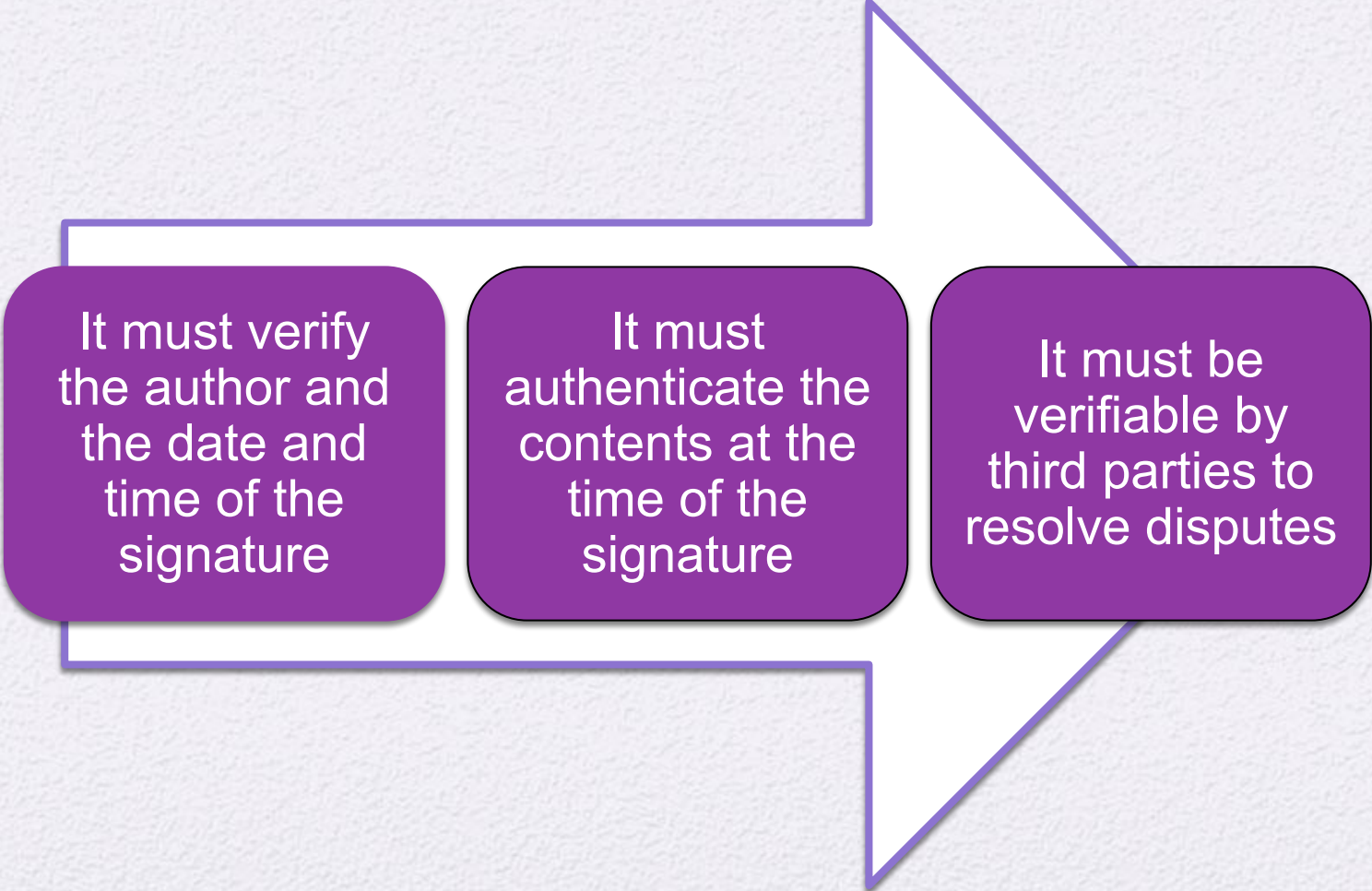


Figure 13.1 Simplified Depiction of Essential Elements of Digital Signature Process

Digital Signature Properties

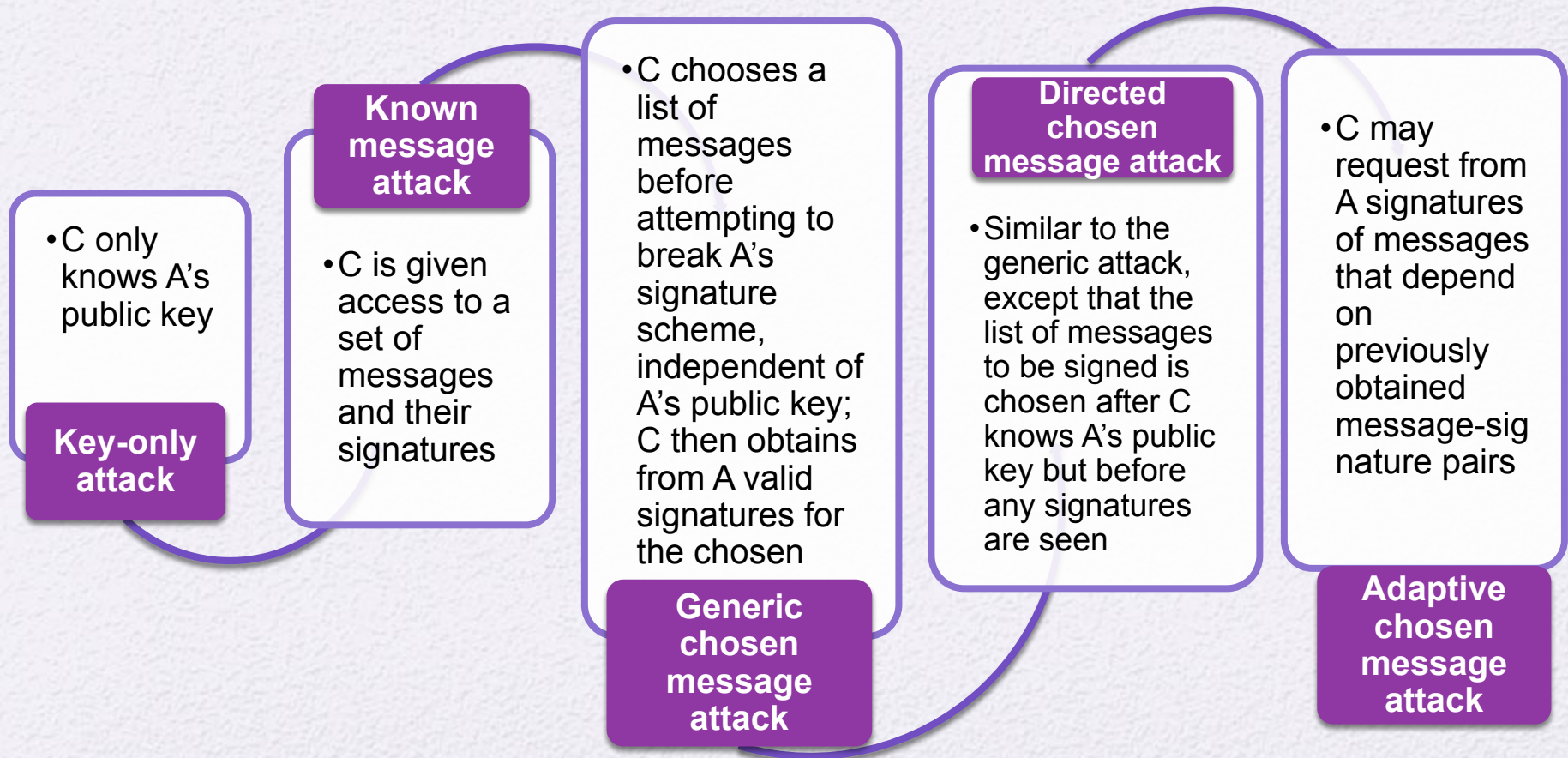


It must verify
the author and
the date and
time of the
signature

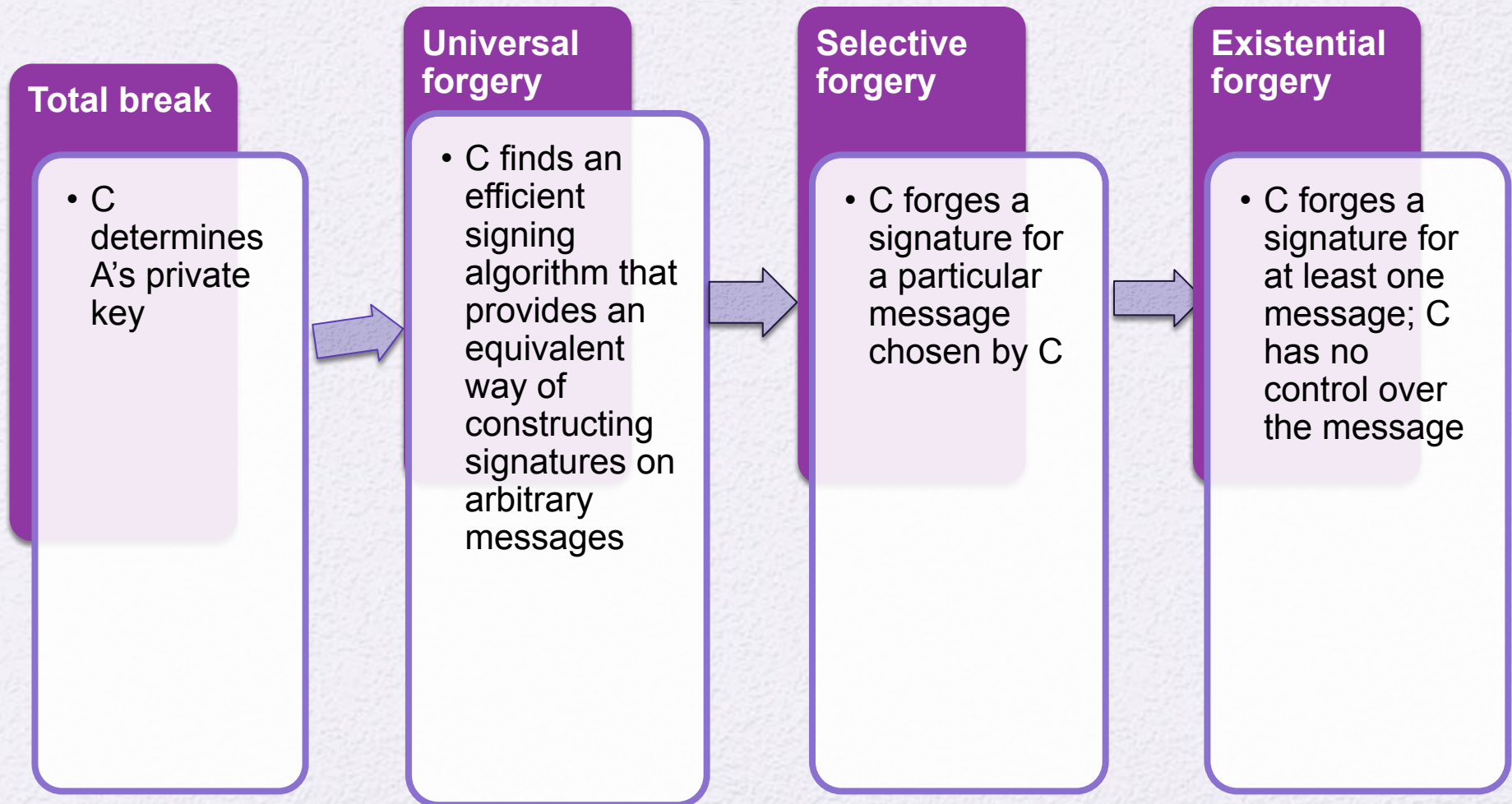
It must
authenticate the
contents at the
time of the
signature

It must be
verifiable by
third parties to
resolve disputes

Attacks



Forgeries



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

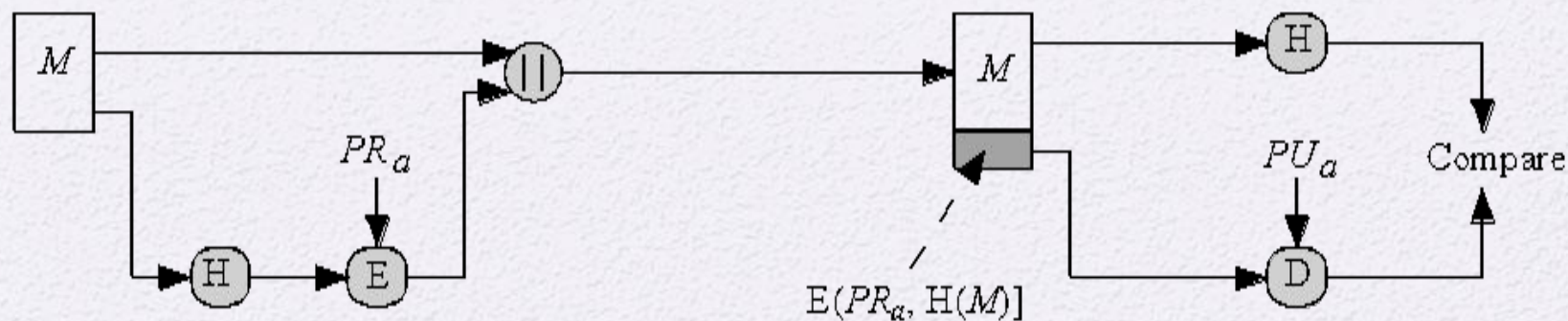
ElGamal Digital Signature

- 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: $y_A = a^{x_A} \bmod q$

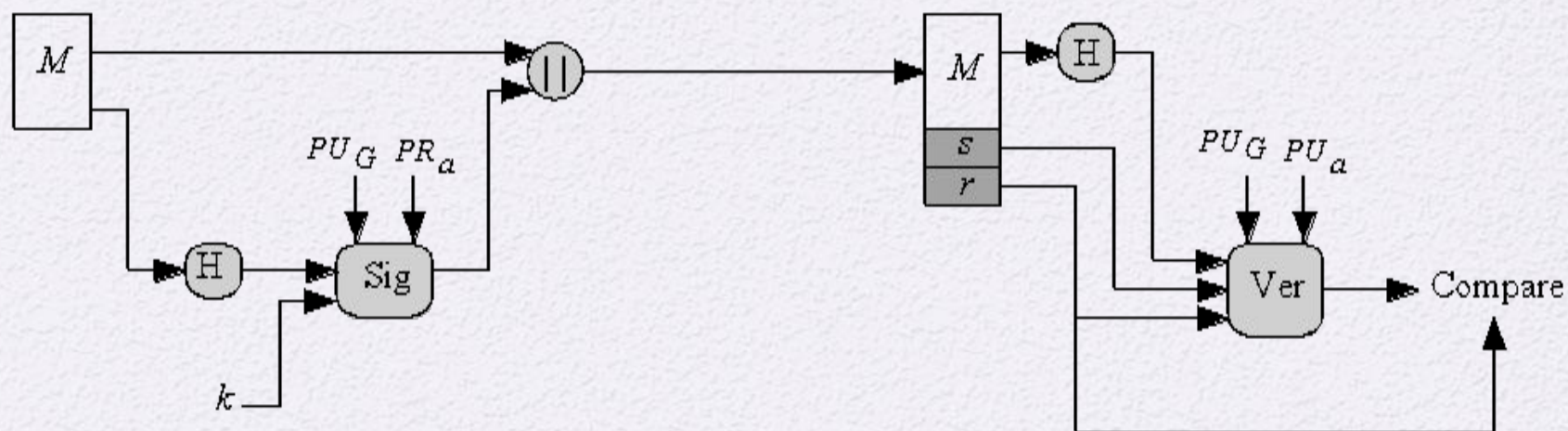
NIST Digital Signature Algorithm

- 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





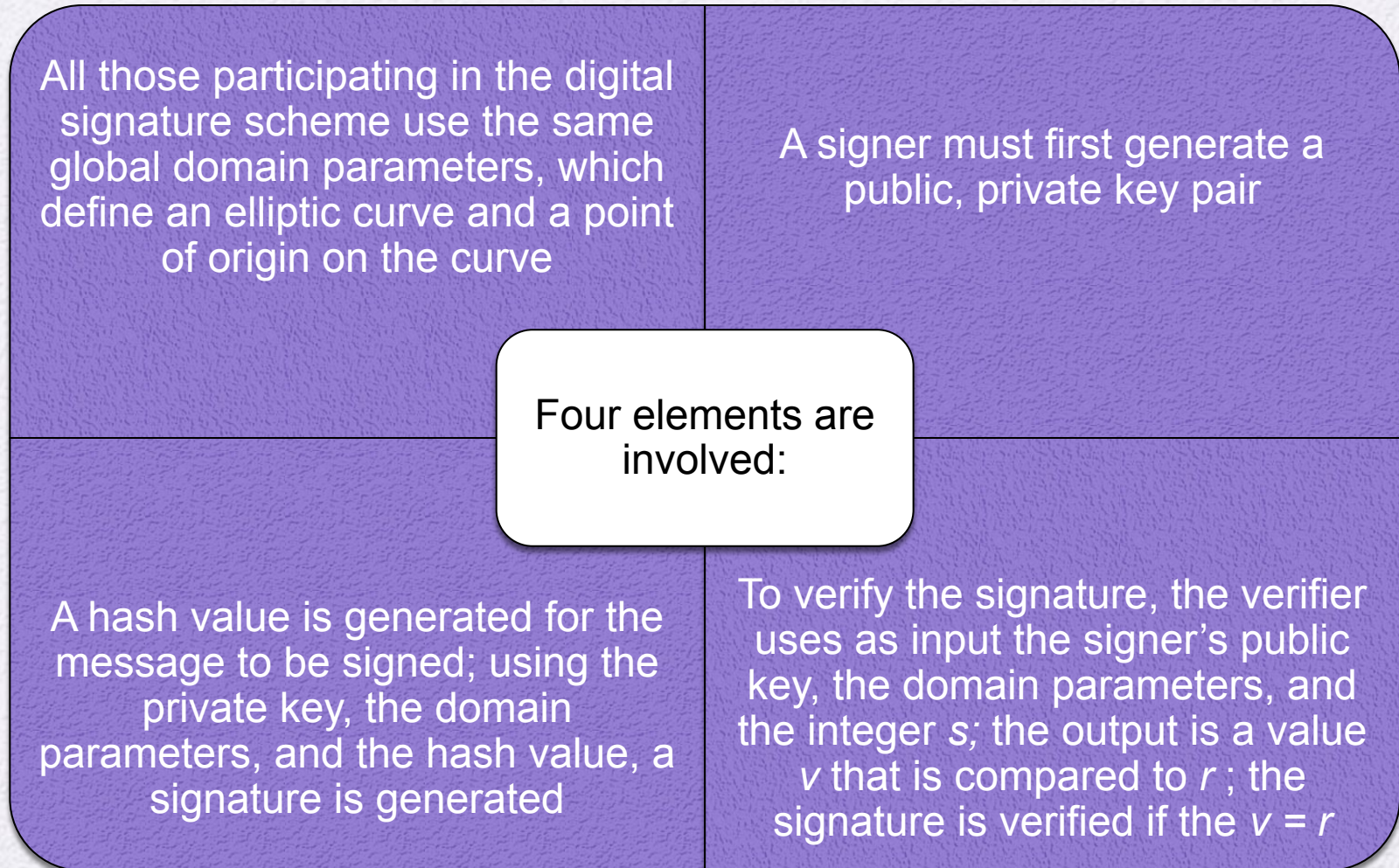
(a) RSA Approach



(b) DSA Approach

Figure 13.2 Two Approaches to Digital Signatures

Elliptic Curve Digital Signature Algorithm (ECDSA)



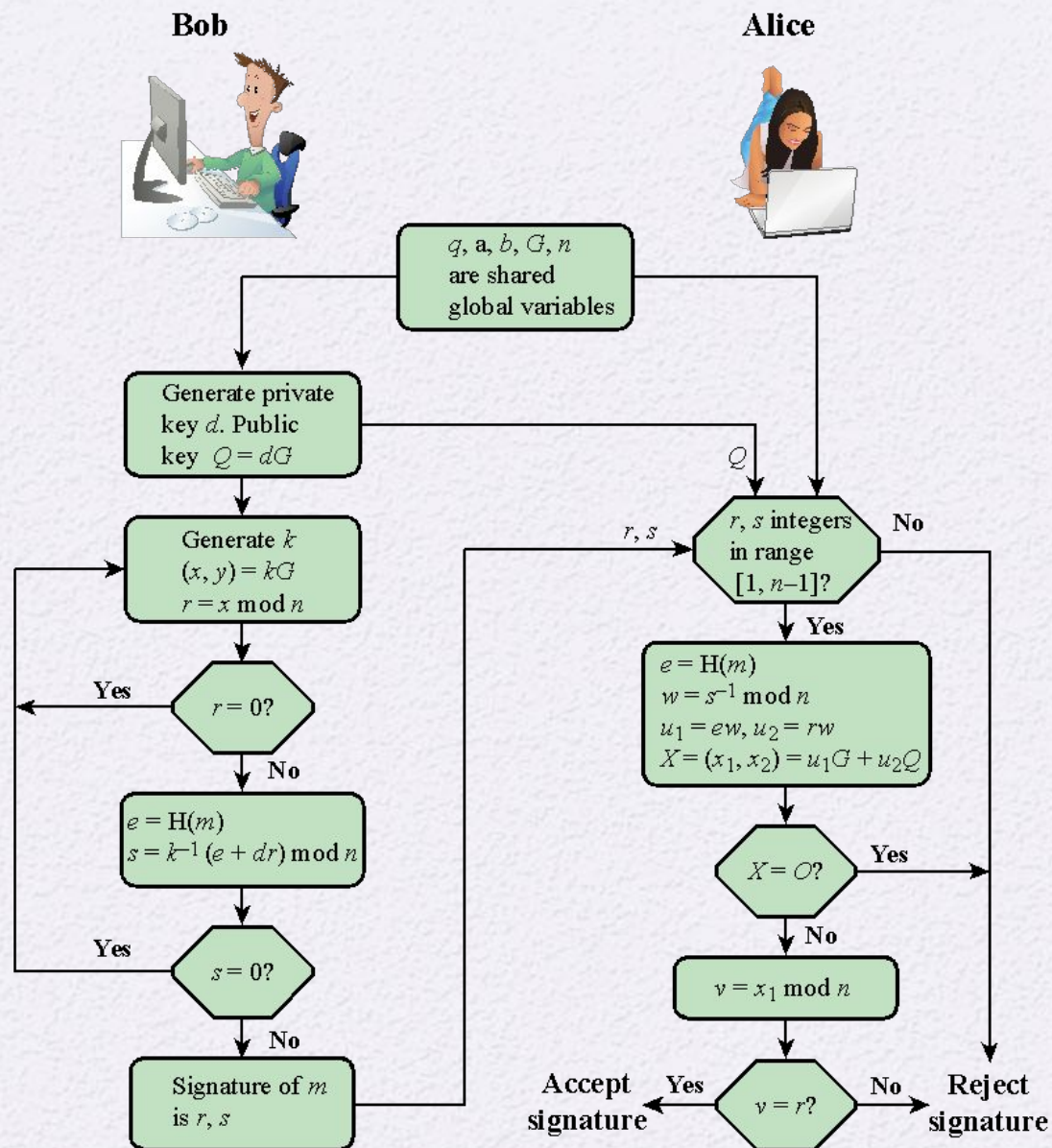


Figure 13.5 ECDSA Signing and Verifying

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

Mask Generation Function (MGF)

- Typically based on a secure cryptographic hash function such as SHA-1
 - Is intended to be a cryptographically secure way of generating a message digest, or hash, of variable length based on an underlying cryptographic hash function that produces a fixed-length output

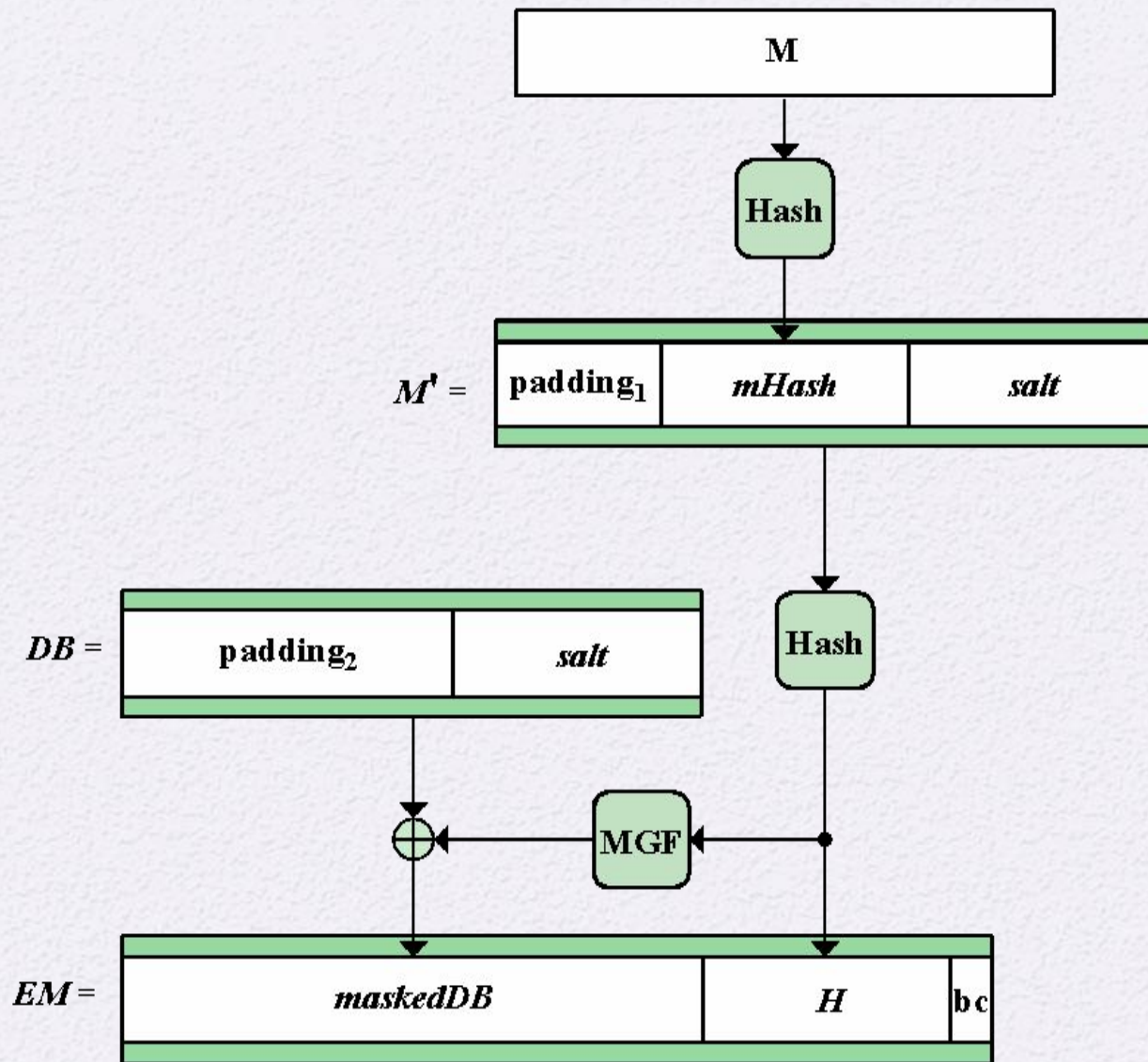


Figure 13.6 RSA-PSS Encoding

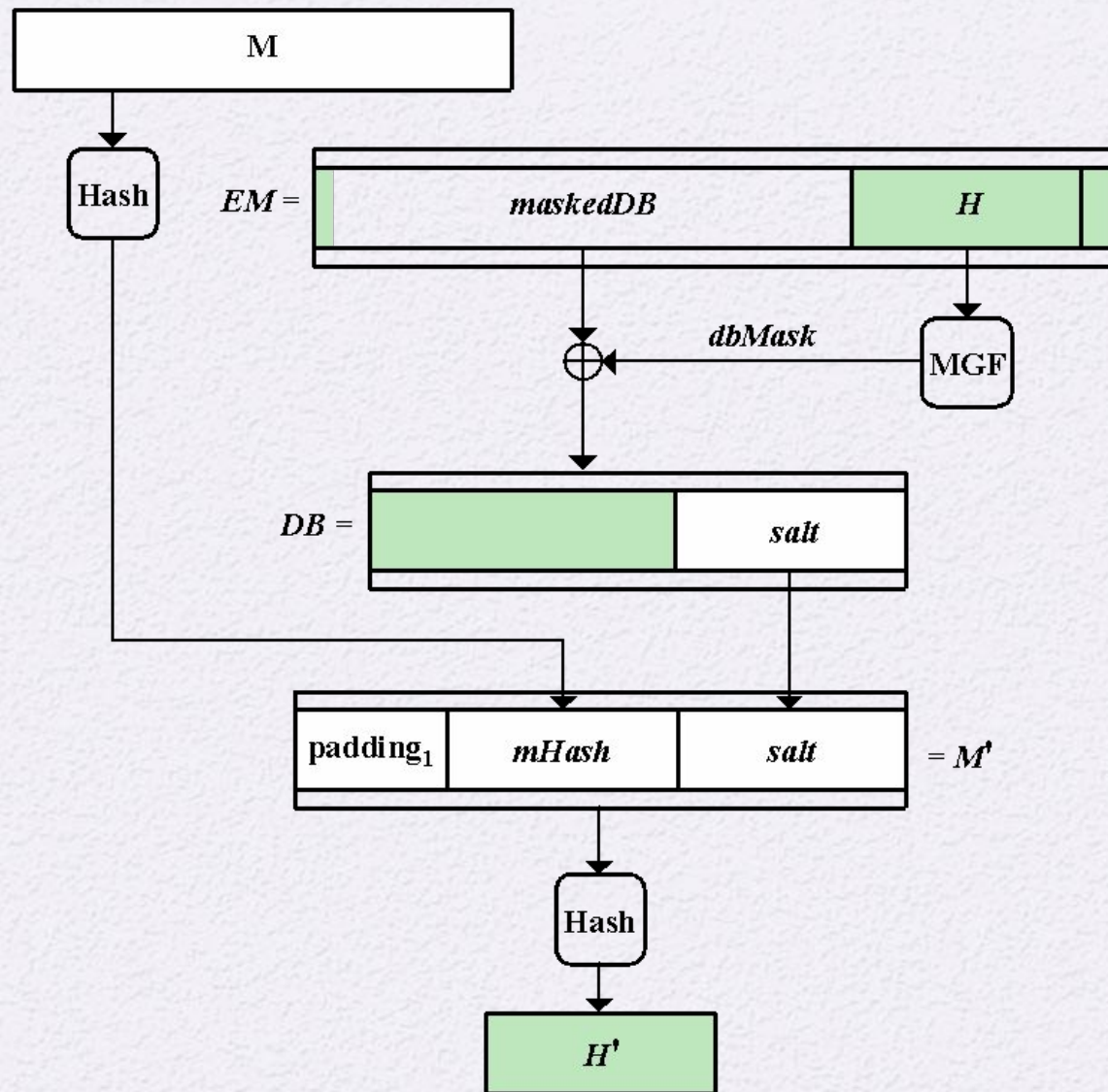


Figure 13.7 RSA-PSS EM Verification

HW3

Implement RSA from Scratch

Summary

- Present an overview of the digital signature process
- Understand the ElGamal digital signature scheme
- Understand the Schnorr digital signature scheme
- Understand the NIST digital signature scheme
- Compare and contrast the NIST digital signature scheme with the ElGamal and Schnorr digital signature schemes
- Understand the elliptic curve digital signature scheme
- Understand the RSA-PSS digital signature scheme

