Information Security

Digital Signatures and PKI

Learning Objectives

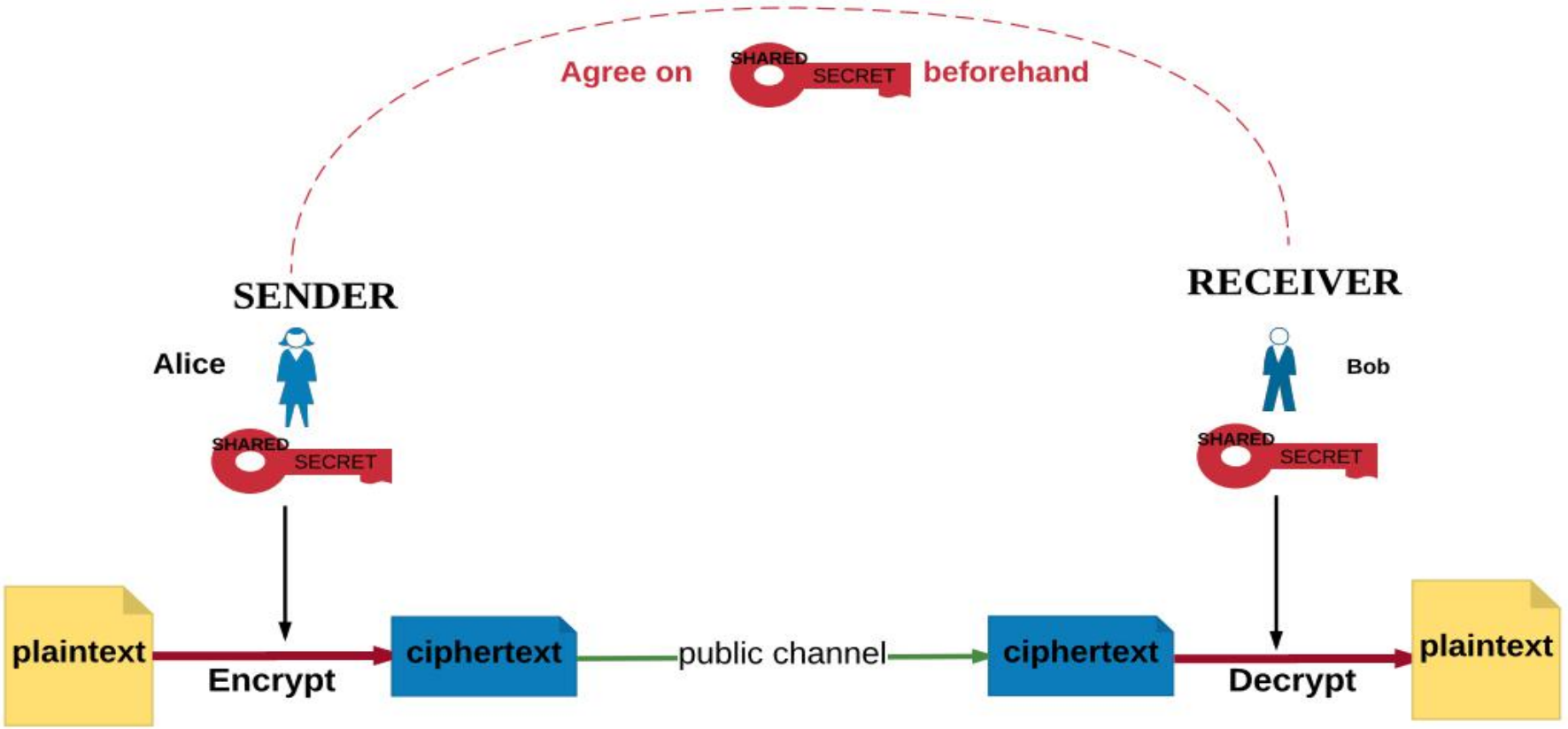
Upon completion of this unit:

- Students will be able to explain the mechanisms used for digital signatures.
- Students will be able to explain the role of digital certificates and certificate authorities in secure communications.
- Students will be able to illustrate how digital signatures work using software such as Kryptos.

Recall: Cryptography and the Main Tenets of Information Security

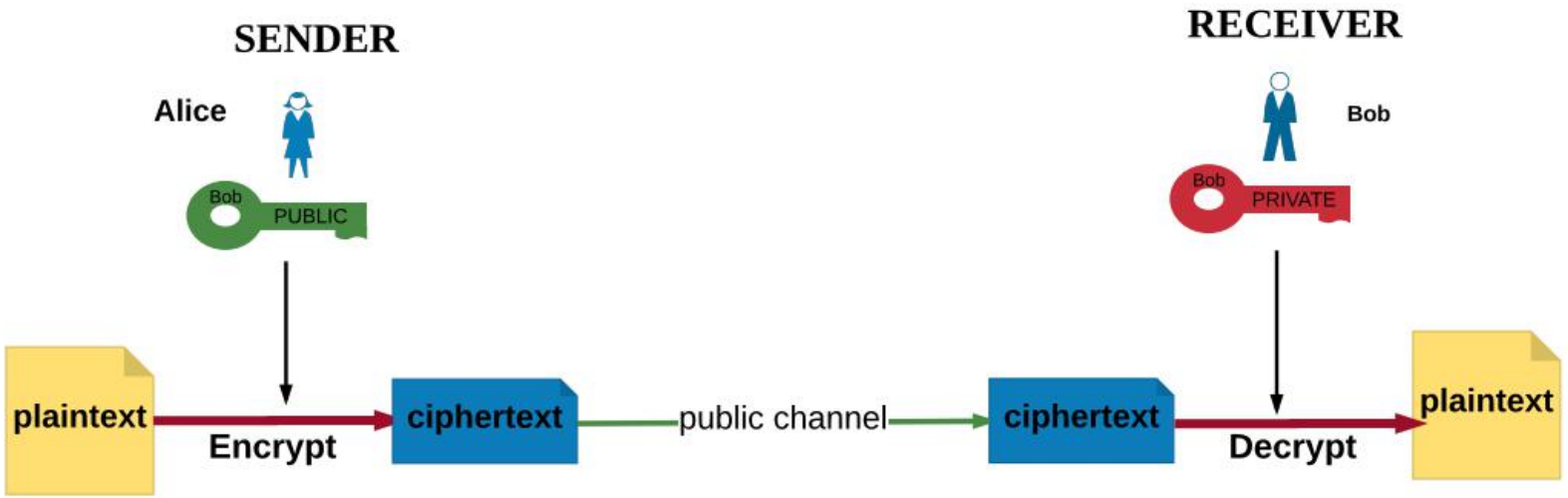
- Confidentiality
  - Encryption algorithms
- Integrity
  - Hash functions
- Authenticity
  - Digital signatures, digital certificates
- Non-repudiation
  - Digital signatures, digital certificates

Recall: Symmetric Key Cryptography



"Symmetric Encryption" by Yesem Kurt-Peker licensed under CC BY 4.0

Recall: Asymmetric Encryption



Note that no communication is necessary beforehand to agree on a shared secret key.

Recall: Advantages of Asymmetric Encryption

- With asymmetric encryption, users do not have to share a secret value that they have to communicate or agree on beforehand or over a public channel.
- Public keys are published and available to everyone in the system.
- **Note:** Private keys should NOT be shared!

Recall: Problem of Authentication

- How does Bob know that the message is indeed from Alice?
- Someone else might have used Bob's public key, sent him the message, and claimed he/she was Alice!
- Solution: Digital signatures and certificates

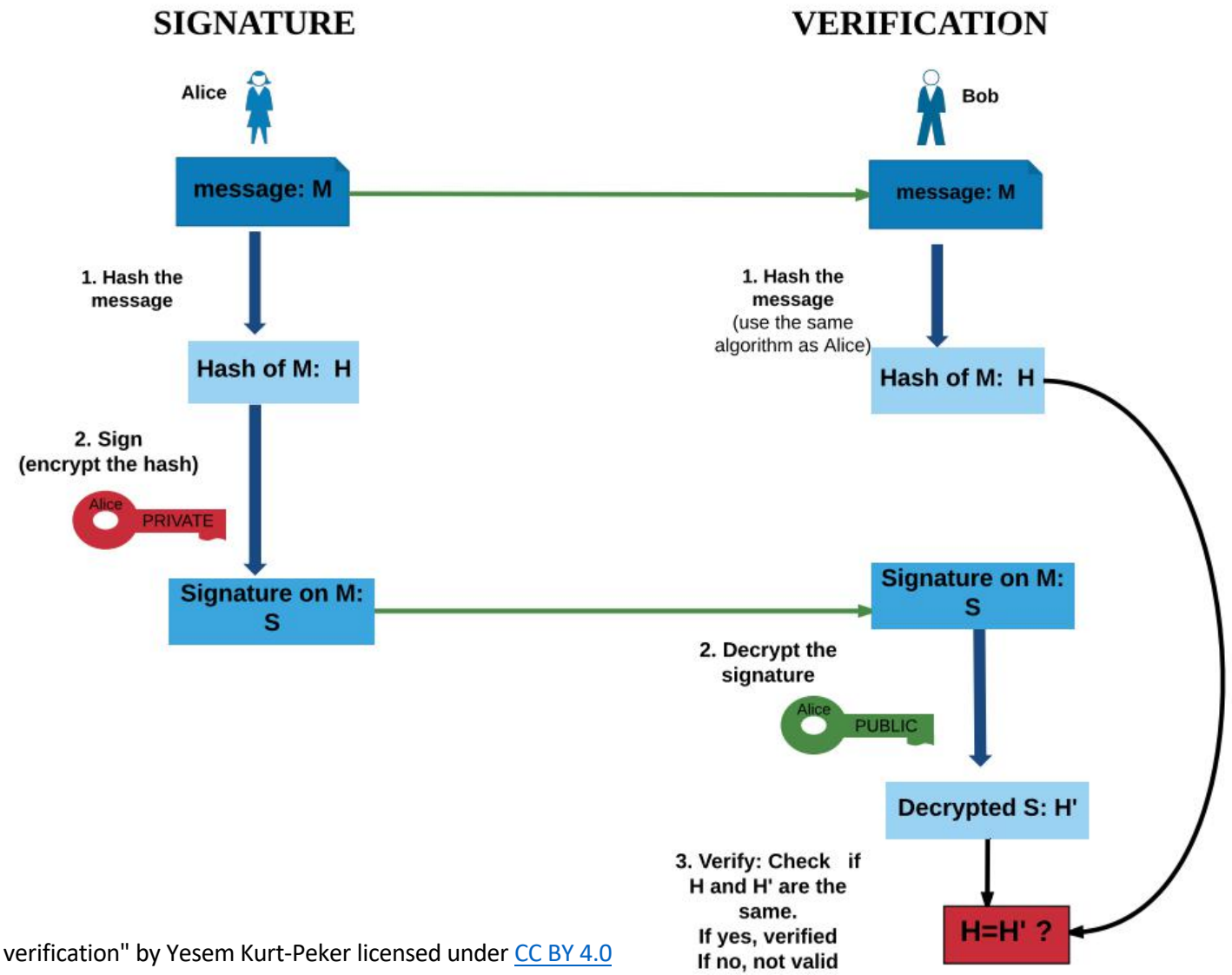
Digital Signatures

- In public key cryptography there are schemes that allow the private key to be used for encryption and the public key to be used for decryption. (Contrast this with the use of keys in asymmetric encryption for confidential communication.)
- Why would we want to do that?

Digital Signatures and Authentication

- If encrypted with a private key, the successful decryption of a ciphertext with the corresponding public key indicates that the message was indeed encrypted with the private key that corresponds to the public key used for decrypting it.
- So if we consider the ciphertext of the message as a signature, then a successful decryption indicates the verification of the signature.
- In practice, the hash value of the message is encrypted to get the signature, **not** the message itself. (Recall that a message can be arbitrarily large but the hash value has a fixed length.)

Signature Creation and Verification



Digital Signatures and Integrity

- If Alice's signature on a message does not verify, one of two things might have happened:

  1. It wasn't Alice's private key that was used to sign the message

  OR

  2. The message was altered, so the hash of the message does not match the signature.

- If Alice signed the message, then the digital signature detects the alteration in the message; hence the signature indicates the integrity of the message.

Digital Signatures and Non-repudiation

- Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- In the scenario for digital signatures, because the private key is known only to the owner, if a signature verifies on a message, it is highly unlikely that it was signed by someone else!

Digital Signatures and Hash Functions

- Unlike paper equivalents, digital signatures are unique to each document.
- That is, the same person's digital signature on one message is different from his/her signature on a different message.
- Because a message can get arbitrarily large and public key encryption algorithms require the length of messages to be under a certain maximum, instead of the message itself being signed, the **hash** of the message is signed. (Recall that a message can be arbitrarily large but the hash value has a fixed length.)

Examples of Digital Signature Algorithms

- RSA (Rivest Shamir Adleman) signatures
- Elliptic Curve Signatures
- DSA: Digital Signature Algorithm

Still a Problem: Authenticity

- Even though Bob can verify that the signature on a message is signed by the private key corresponding to the public key he used, how does he know that it is indeed Alice who is associated with that public key?

- **Solution:** PKI and digital certificates

PKI – Public Key Infrastructure

- The set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke **digital certificates** based on asymmetric cryptography.

- Provides key distribution and key management

Digital Certificates

- A digital certificate is an electronic document that binds a public key with an entity (person, organization).
- It includes
  - The owner (subject) name/id
  - The public key of the owner
  - The digital signature (seal) of the issuing entity (authority)
  - Validity period of the certificate
  - Algorithms used

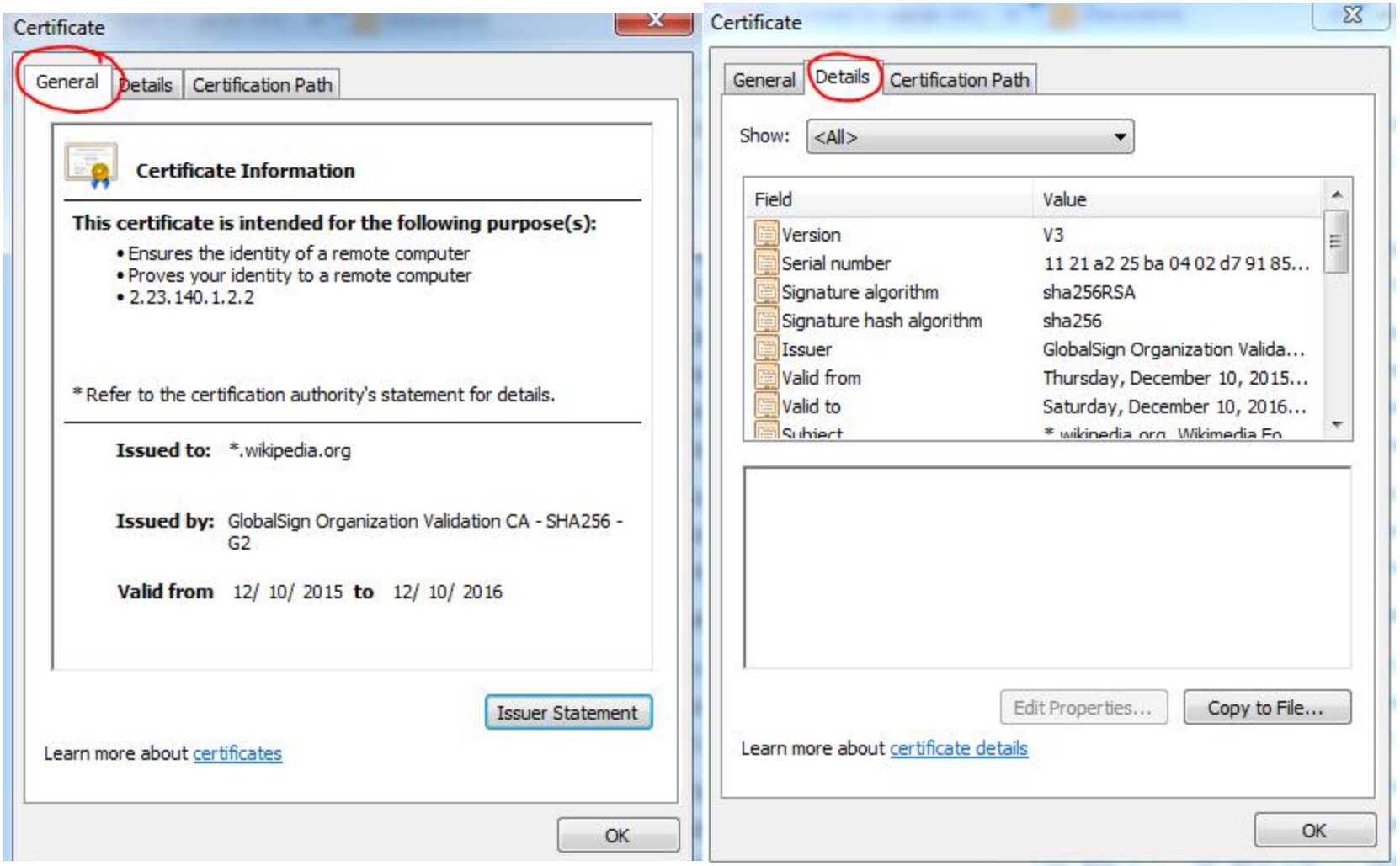
    and more …

Digital Certificates

© 2006 M/C Journal

"Figure 3: Example of a new digital certificate presentation". (June 2005). Vicky Liu. *Seal Culture Still Remains in Electronic Commerce*. M/C Journal. vol. 8, no. 2.

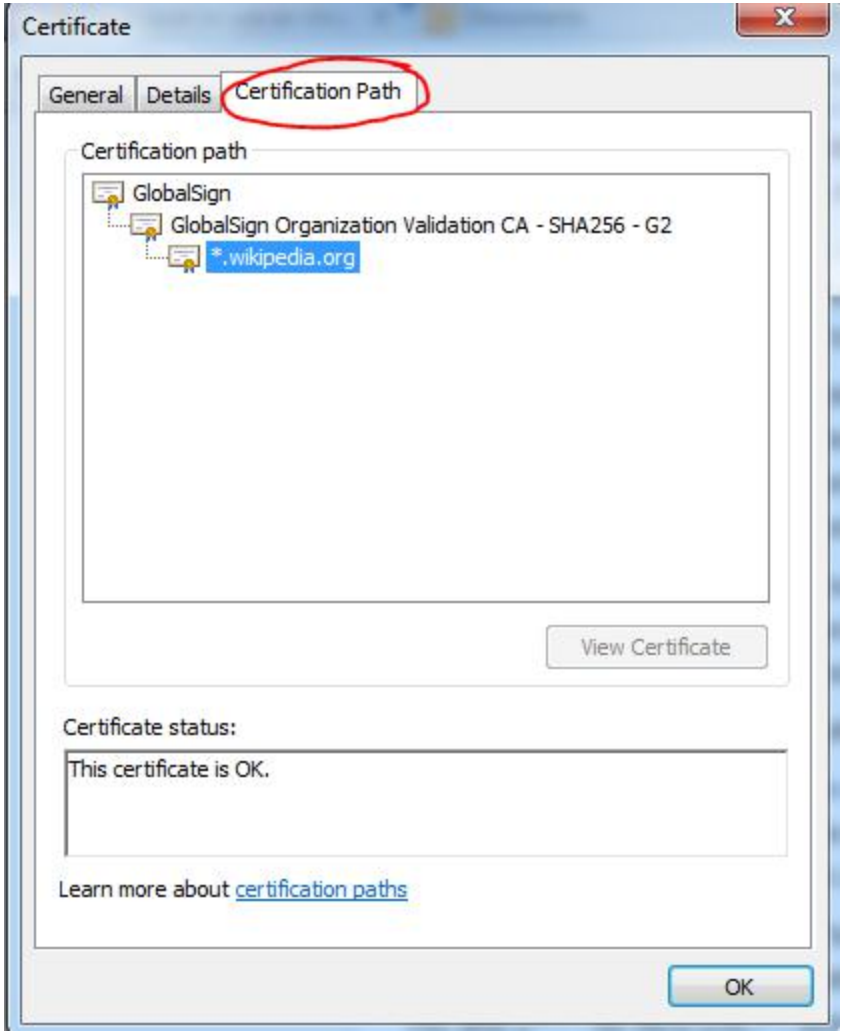
A Digital Certificate



Certificate Authority (CA)

- A trusted entity that issues electronic documents and digital certificates that verify a digital entity's identity on the Internet.
- Signs these certificates using its private key; its public key is made available to all interested parties in a self-signed CA certificate.
- CAs use the trusted root certificate to create a "chain of trust."
- Many root certificates are embedded in web browsers so they have built-in trust of those CAs.
- Web servers, email clients, smartphones, and many other types of hardware and software also support PKI and contain trusted root certificates from the major CAs.

Certification Path and Chain of Trust



Elements of PKI

- A trusted party, called a *certificate authority* (CA), acts as the root of trust and provides services that authenticate the identity of individuals, computers and other entities
- A *registration authority*, often called a *subordinate CA*, is certified by a root CA to issue certificates for specific uses permitted by the root.
- A *certificate database*, which stores certificate requests and issues and revokes certificates.
- A *certificate store*, which resides on a local computer as a place to store issued certificates and private keys.

Some Applications in Which Cryptography Is Used

- SSH
- SSL/TLS
- IPSec
- VPN
- PGP
- Bluetooth Pairing and Communication Protocols

Hands-on: Examine Digital Certificates

- Open a Chrome browser and go to gmail.com.
- Note that the url starts with https. This means that this is a secure communication.
- Notice also the lock by the url. (Visit https://support.google.com/chrome/answer/95617?hl=en)
- Click on the lock and the details.
- View the certificate for the site and answer these questions:
  - Who is the certificate authority on this certificate?
  - Who is the certificate issued to?
  - What is the associated public key?
  - When does the certificate expire?

Hands-on: Find the Certification Path

- Look at the path of the certification. Click on the immediate parent of google.com, Google Internet Authority G2.
  - View the certificate for Google Internet Authority G2 and answer these questions:
    - Who is the certificate authority on this certificate?
    - Who is the certificate issued to?
    - What is the associated public key?
    - When does the certificate expire?
- Proceed with this until you view the certificates of all intermediate authorities and the root authority.
- Try a different website!

Catalyzing Computing and Cybersecurity in Community Colleges

is funded by a National Science Foundation grant and
is located at Whatcom Community College

237 West Kellogg Road
Bellingham, WA 98226

www.C5colleges.org