Microsoft

Windows Server - Managing and Supporting Active Directory Certificate Services (ADCS)

Module 1: Introduction to PKI

Microsoft Services

Module Overview

- Introduction to Cryptography
- Symmetric Cryptography
- Asymmetric Cryptography
- Hybrid Cryptography
- Hash Functions and Digital Signatures
- Introduction to PKI

Introduction to Cryptography

When You’re Asked a Question About | **PKI**

Etymology of word Cryptography

- Word cryptography comes from Greek and means **to write a secret**:

  Kryptós - hidden, secret

  graphein **-** to write

- Today, Cryptography is more than just “writing secrets”
- It is secure communication in the presence of third parties

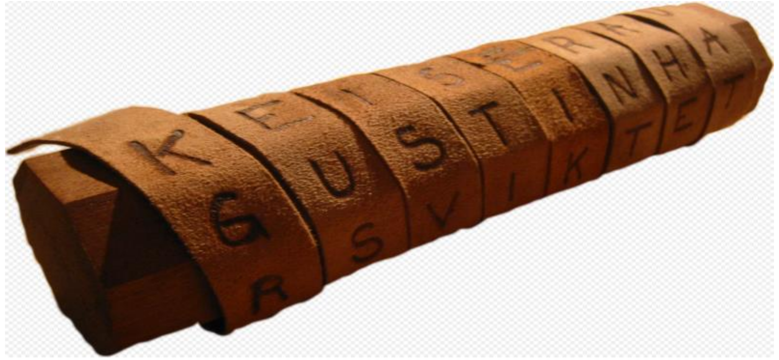
Milestones of Cryptography

3000 BC - Hieroglyphics

First known cryptographic method

Only few could read, therefore unintelligible to most people

400 BC – Scytale Cipher



Spartans wrapped papyrus around a rod to encrypt and decrypt a message

Used to convey military directives

Milestones of Cryptography

50 BC – Substitution (Caesar Cipher)

Based on the name of Julius Caesar.

One character is replaced with another character.
If only one alphabet is used for substitution it is an monoalphabetic substitution algorithm

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Milestones of Cryptography

World War II - Enigma

Enigma = **riddle** in lattin.

Rotor cipher machine that used polyalphabetic substitution.

Used in World War II to encrypt telegraphic communication.

Cracked by the famous Alan Turing

Goals of Cryptography

Data Integrity

Signed Email

Confidentiality

Online Purchase

Authentication

Smart Card

Non-Repudiation

Code Singing

Encryption and Decryption

- Encryption is the process of transforming plaintext into unreadable cipher-text.

- Decryption is the process of transforming unreadable cipher-text into plaintext.

- Encryption / Decryption requires an encryption method which is commonly called an algorithm

Symmetric Cryptography

Binary Mathematics - XOR

- Major function in modern cryptography
- Invented by Gilbert Vernam in 1917
- Symbolized by $\oplus$
- Binary mathematical operation (binary addition) that is applied to two bits

Binary Mathematics – XOR (continued)

- Based on only three rules:
  - If both bits are set to one, the result is zero (1 + 1 = 0)
  - If both bits are set to zero, the result is zero (0 + 0 = 0)
  - If the bits are different than each other, the result is one (1 + 0 = 1)

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Cipher text	**1111100**	**0001010**

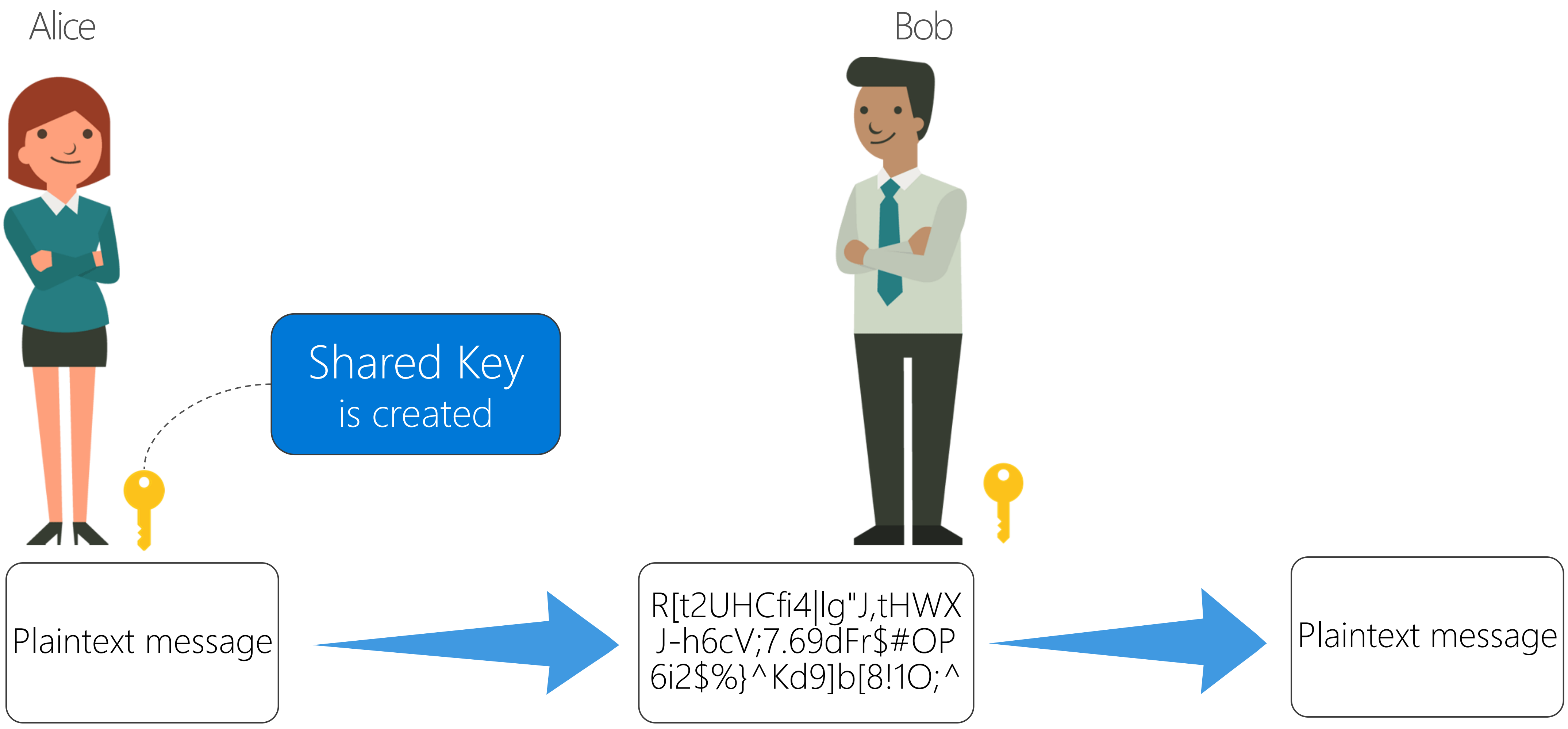
- This operation is easily reversible when you have the XOR key!

Symmetric Encryption

- With symmetric cryptography, the same key is used to encrypt and decrypt
- Problem/Challenge of Key Exchange

*Symmetric – **shared** key*

Symmetric Encryption



Alice

Bob

Shared Key
is created

Plaintext message

R[t2UHCfi4|lg"J,tHWX
J-h6cV;7.69dFr$#OP
6i2$%}^Kd9]b[8!1O;^

Plaintext message

SYMMETRIC:
Encrypted with a Shared key

SYMMETRIC:
Decrypted with the same Shared key

Symmetric Algorithms – Examples

- DES (Data Encryption Standard)
  56 Bit Key length, US standard.
  Can create 72 quadrillion possibilities (72,000,000,000,000,000)

- 3DES ("Triple DES")
  Triple encryption with a 56 Bit DES key, results in only 112 Bit safety instead of the calculated 168 Bit

- RC2, RC4, RC5 and RC6
  Developed by Ron Rivest Therefore, RC = "Rivest Cipher"

Advanced Encryption Standard (AES)

- **AES** or Rijndael Algorithm
- In the 1990's a "DES Cracker" machine was built that could **recover a DES key in a few hours**
- If a machine was built to recover a DES key in one second, it would take that system **149 trillion years to crack a 128-bit AES Key**
- AES is the U.S. official standard for sensitive but unclassified data encryption, effective as of May 26, 2002

Asymmetric Cryptography

Asymmetric Cryptography- Overview

- Asymmetric cryptography is accomplished by using two keys, also called ‘key pair’:

Public Key
Can and should be distributed

Private Key
Must remain secret

Asymmetric Cryptography- Overview

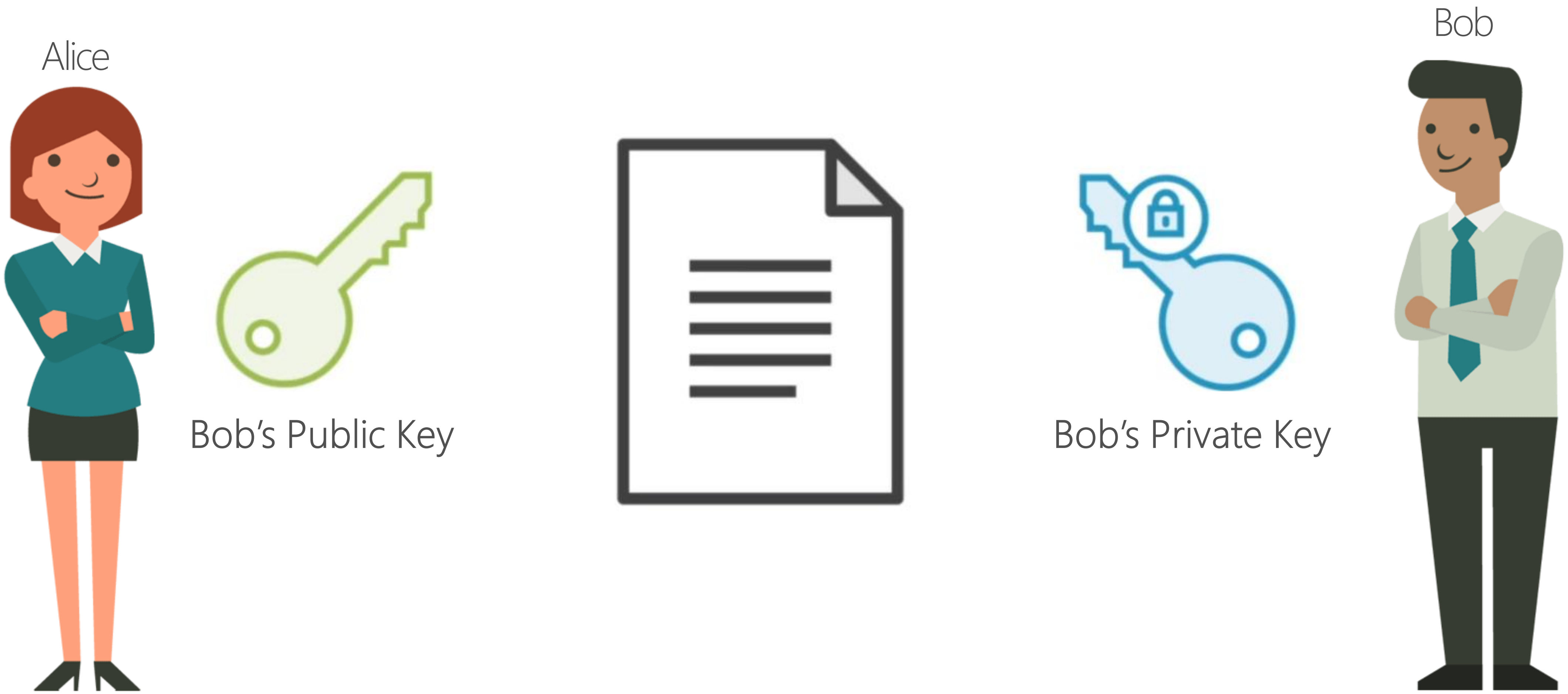
- The asymmetric keys are mathematically-related.

- If you asymmetrically encrypt something with a key, only the corresponding other key from the key pair can decrypt the information.

- Also called Public Key Encryption.

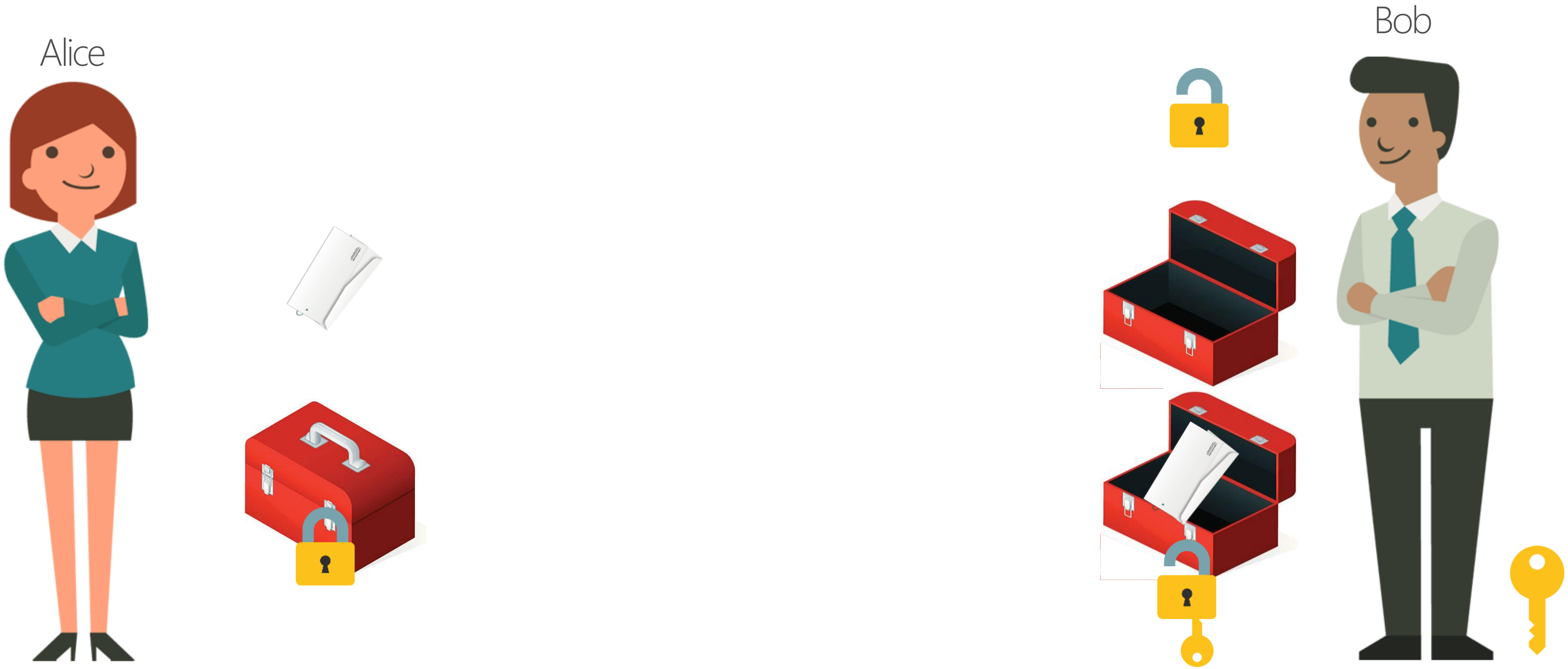
Asymmetric Encryption

Makes sure that the document, email or any other data I sent can view only by the receiver.

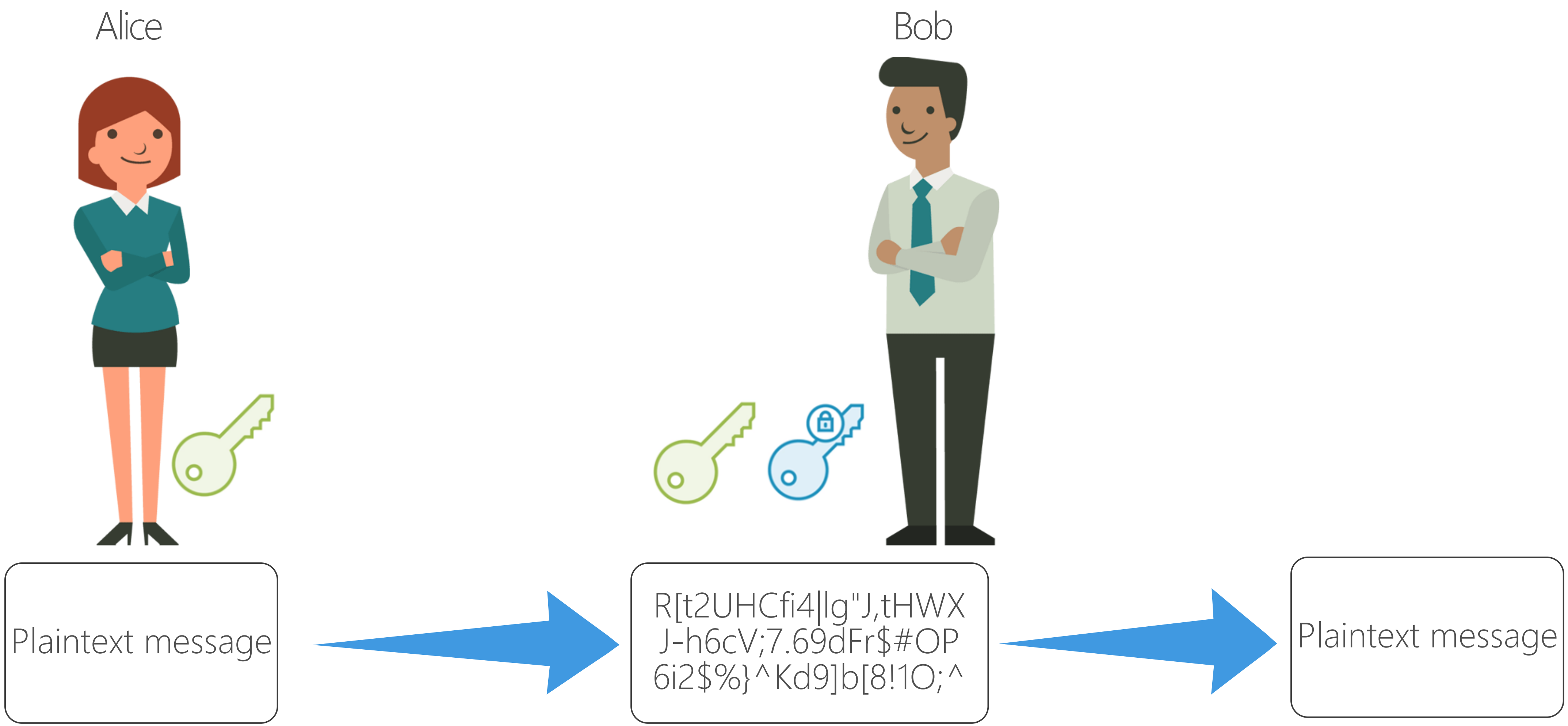


Asymmetric Encryption

Another example of asymmetric encryption process:



Asymmetric Encryption



Alice

Bob

Plaintext message

R[t2UHCfi4|lg"J,tHWX
J-h6cV;7.69dFr$#OP
6i2$%}^Kd9]b[8!1O;^

Plaintext message

ASYMMETRIC:
Encrypted with Bob's Public key

ASYMMETRIC:
Decrypted with Bob's associated Private key

Suite B Algorithms

- Created by National Security Agency (NSA) in 2005 and used to protect top-secret information of the U.S government.
- Suite B algorithms are:
    - AES with key sizes of 128 and 256 Bits – for symmetric encryption
    - Elliptic-Curve Digital Signature Algorithm (ECDSA) – for digital signatures
    - Elliptic-Curve Diffie-Hellman (ECDH) – for key agreement
    - Secure Hash Algorithm (SHA-256 and SHA-384) – for message digest
- Support for Suite B was added in Windows Vista SP1 and in Windows Server 2008 with the introduction of Cryptography Next Generation (CNG).

Commercial National Security Algorithm Suite

- In 2018, NSA (National Security Agency) replaced Suite B with the Commercial National Security Algorithm Suite (CNSA).
- CNSA algorithms are:
  - AES with key sizes 256 Bits – for symmetric encryption
  - Elliptic-Curve Digital Signature Algorithm (ECDSA) – for digital signatures
  - Elliptic-Curve Diffie-Hellman (ECDH) – for key agreement
  - Secure Hash Algorithm (SHA-384) – for message digest
  - RSA with a minimum modulus size of 3072 Bit

Asymmetric Algorithms

Diffie-Hellman (1976)

First implementation of an asymmetric algorithm

Based on calculating discrete logarithms in a finite field

RSA (1978)

Developed by Rivest, Shamir and Adleman

Strength in today's inefficiency to factorize into prime numbers

DSA (1991)

Developed by the National Security Agency (NSA)

Based on discrete logarithms in a finite field

Elliptic Curve Cryptosystem (ECC) (2005)

Suggested in 1985, but selected by the NSA to be included in "Suite B" algorithms

More efficient than other algorithms

Encryption Keys

Key type	Description
Symmetric	A shared Secret or key is used to encrypt and decrypt data between two communicating parties
Asymmetric	A key pair consists of a public key and a private key The private key is protected and kept secret, while the corresponding public key is widely distributed If the public key is used to encrypt data the corresponding private key is used to decrypt the data (& vice versa)

Symmetric vs. Asymmetric Algorithms

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities	One entity has a public key and the other entity has a private key
Key Exchange	Out-of-band (keys distributed outside of encryption process)	Symmetric key is encrypted and sent with message; thus, the key is distributed by in-bound means
Speed	Algorithm is less complex and faster (Up to 5000 times faster)	Algorithm is more complex and slower
Number of Keys	Grows as users grow	Does not grow uncontrollably
Usage	Bulk encryption	Key encryption and distributing keys
Security Service provided	Confidentiality	Confidentiality, integrity and non-repudiation

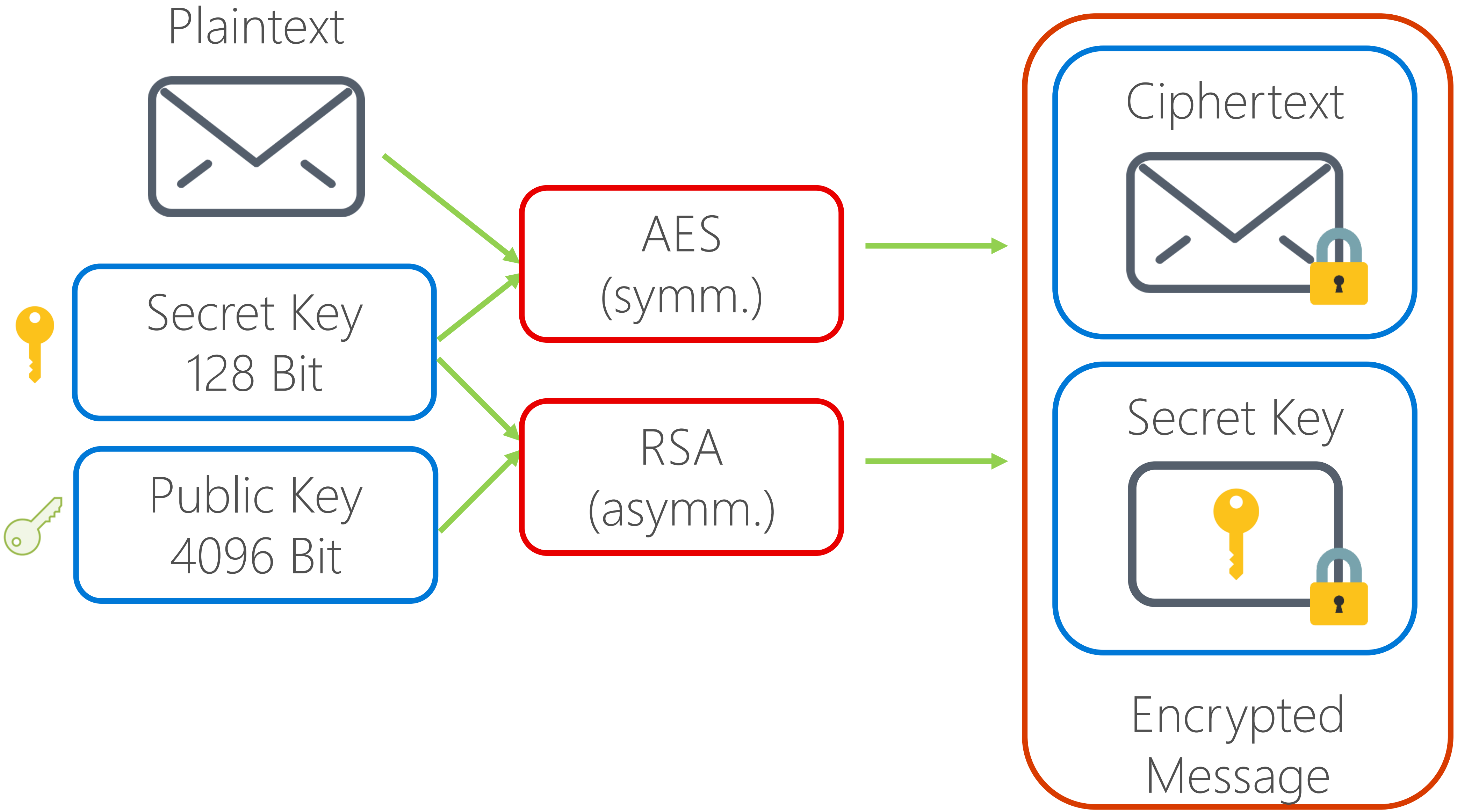
Hybrid Cryptography

Real World: Hybrid Encryption

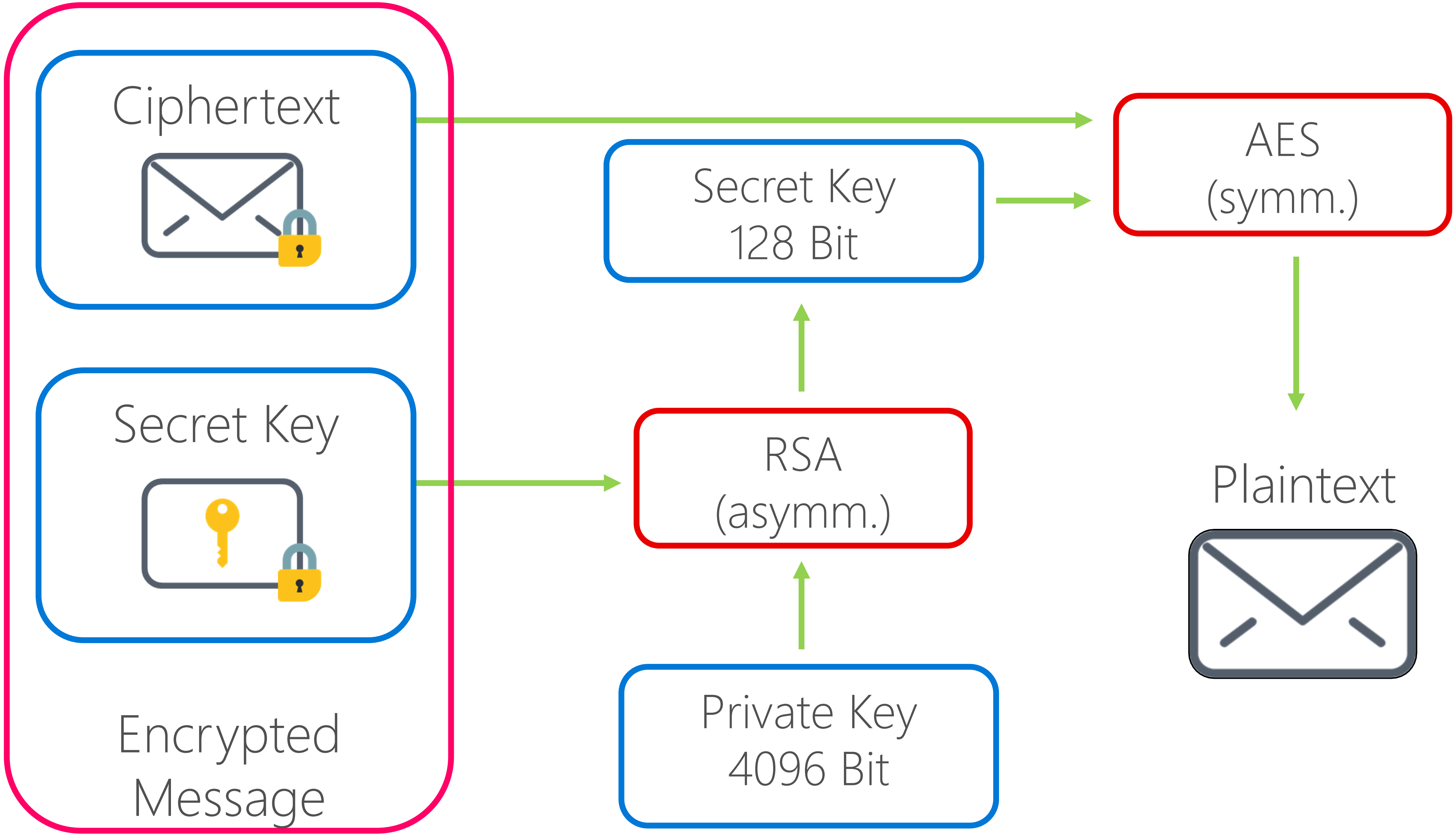
- **Asymmetric algorithm** is used for key exchange:
  One key is used to encrypt the symmetric key, the other one to decrypt it

- **Symmetric algorithm** is used to create a symmetric session key that encrypts the message/bulk data

Hybrid approach (encryption)



Hybrid approach (decryption)



Key Points of Hybrid Cryptohraphy

- Asymmetric algorithm performs encryption and decryption by using public and private keys
- Symmetric algorithm performs encryption and decryption by using one secret key
- A secret key is used to encrypt the actual message
- Public and private keys are used to encrypt/decrypt the secret key
- A secret key is synonymous to a symmetric key
- An asymmetric key refers to a public or private key

Lesson Review

Question 1:

What are the 4 goals of cryptography?

Data Integrity, Confidentiality, Authentication and Non-Repudiation.

Question 2:

Which algorithms belongs to CNSA-Suite group?

AES, ECDSA, ECDH, SHA-2 family, RSA.

Question 3:

How many keys will be used in hybrid encryption and decryption?

3 Keys - Secret key, private key and public key.

Hash Functions & Digital Signatures

Hash Algorithms - Overview

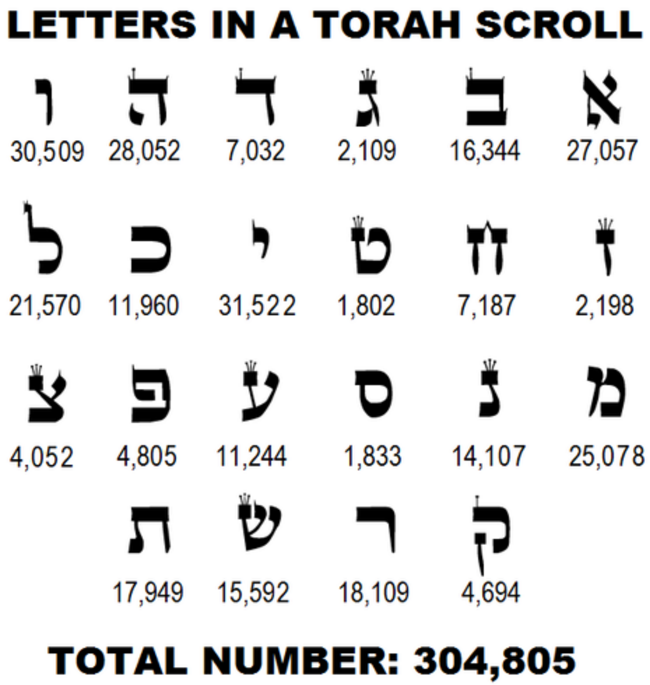
- A Hash algorithm takes a large chunk of data and compresses it into a fingerprint (or digest) of fixed length\size
- Trapdoor function, **one-way function**
- A Hash function returns a "**digest**" - usually 128 or 160 bits

Hash Algorithms - Overview

- It is practically infeasible to produce an original message that matches a digest
- Converts a changeable amount of information into a string of fixed length
- Hash is typically used to verify that a certain item has not been modified

Accuracy Checks in the Bible

- In generally it takes one year to write Sefer Torah.
- On average on each Sefer Torah we'll have 245 columns and 304,805 letters.
- For centuries, the content of the Sefer Torah, remain identical this is because of “hashing” technique.



LETTERS IN A TORAH SCROLL

א	27,057
ב	16,344
ג	2,109
ד	7,032
ה	28,052
ו	30,509
ז	2,198
ח	7,187
ט	1,802
י	31,522
כ	11,960
ל	21,570
מ	25,078
נ	14,107
ס	1,833
ע	11,244
פ	4,805
צ	4,052
ק	4,694
ר	18,109
ש	15,592
ת	17,949

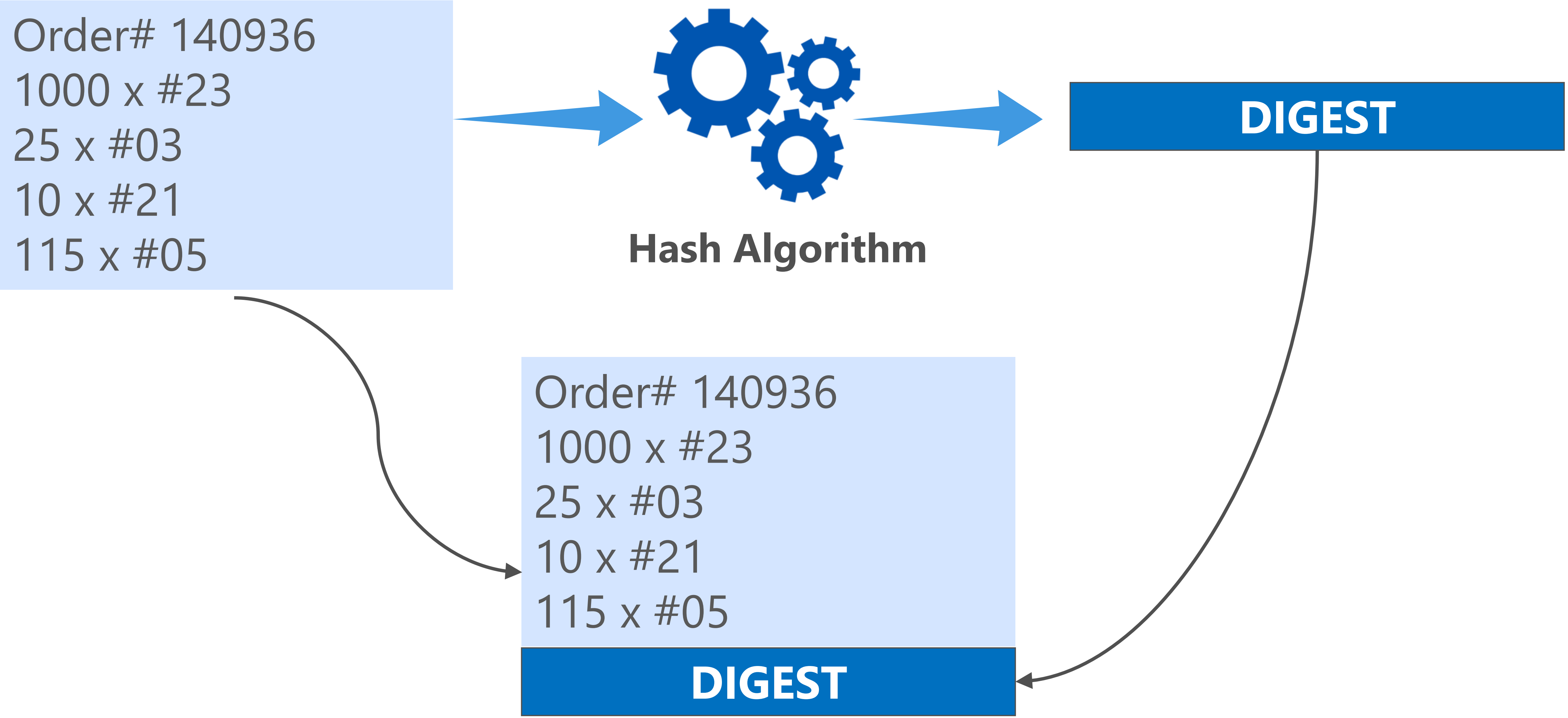
TOTAL NUMBER: 304,805

Digital Signature: Algorithms

Hashing Algorithms
MD5
SHA1
SHA256
SHA384
SHA512

- Some Hashing Algorithms such as MD5 and SHA1 have known weaknesses and should no longer be used:
  - MD5 - https://technet.microsoft.com/en-us/library/security/961509.aspx
  - SHA-1 - https://technet.microsoft.com/en-us/library/security/2880823.aspx
- Microsoft recommends using **SHA-2** hashing family

How hashing works…



Order# 140936
1000 x #23
25 x #03
10 x #21
115 x #05

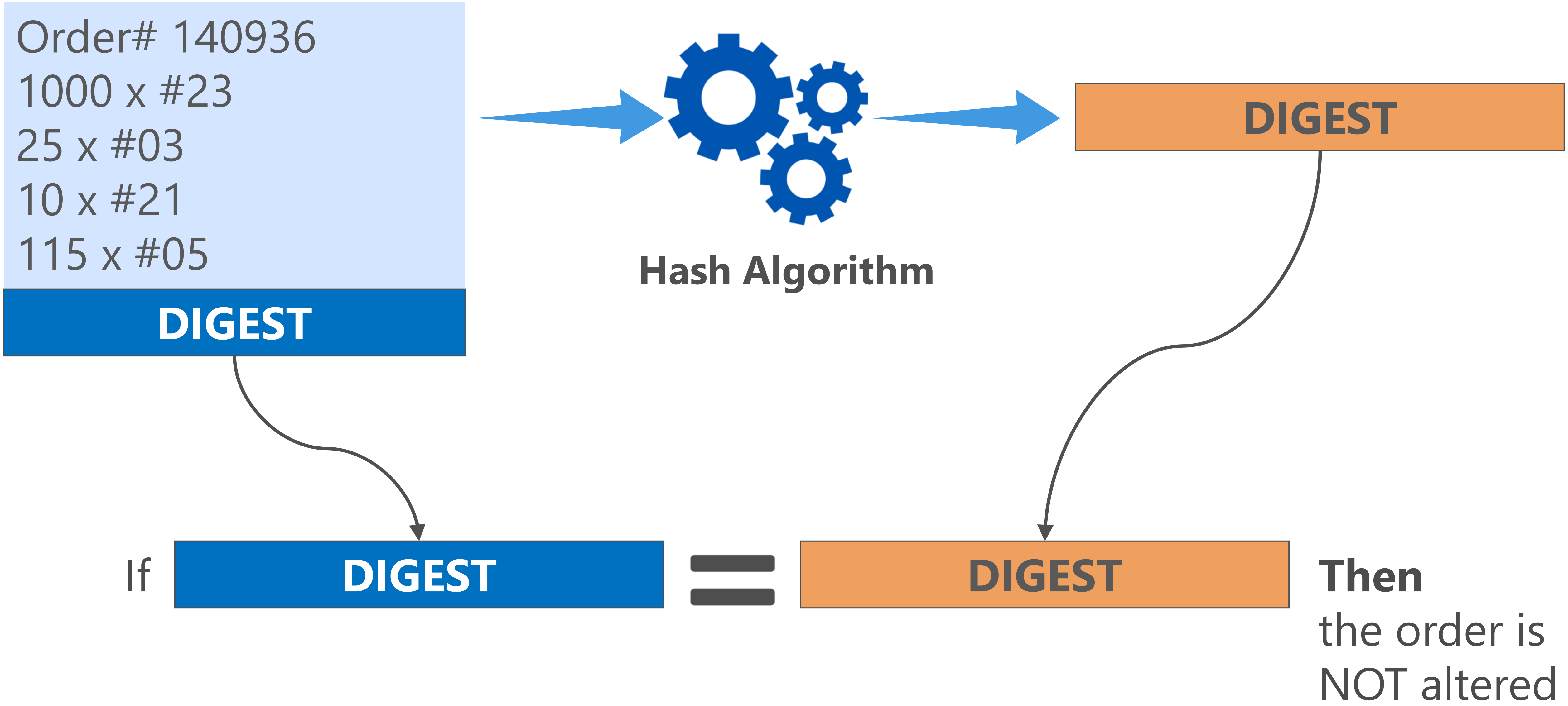
Hash Algorithm

DIGEST

Order# 140936
1000 x #23
25 x #03
10 x #21
115 x #05

DIGEST

How hashing works…



Order# 140936
1000 x #23
25 x #03
10 x #21
115 x #05

DIGEST

Hash Algorithm

DIGEST

If DIGEST = DIGEST

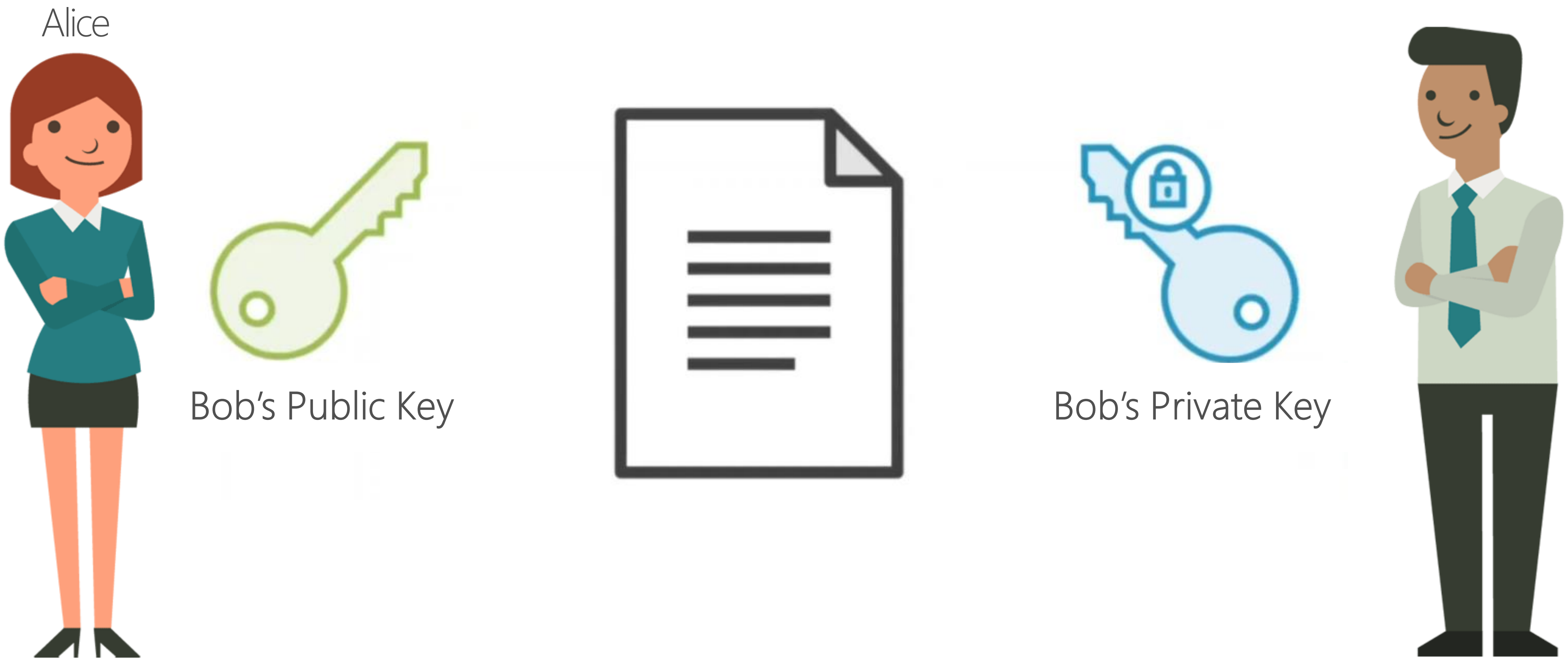
Then
the order is
NOT altered

Characteristics of Digital Signatures

- Identification
  The recipient of a signed message can be sure of who sent the message
- Integrity
  The recipient of a signed message can check it to make sure that the message was not tampered
- Reliability/non-Repudiation
  With a digital signature, there is no doubt that the sender truly sent the message

Signing Process

Proves that the owner of the private key is the one who sent the document, email or any other data.

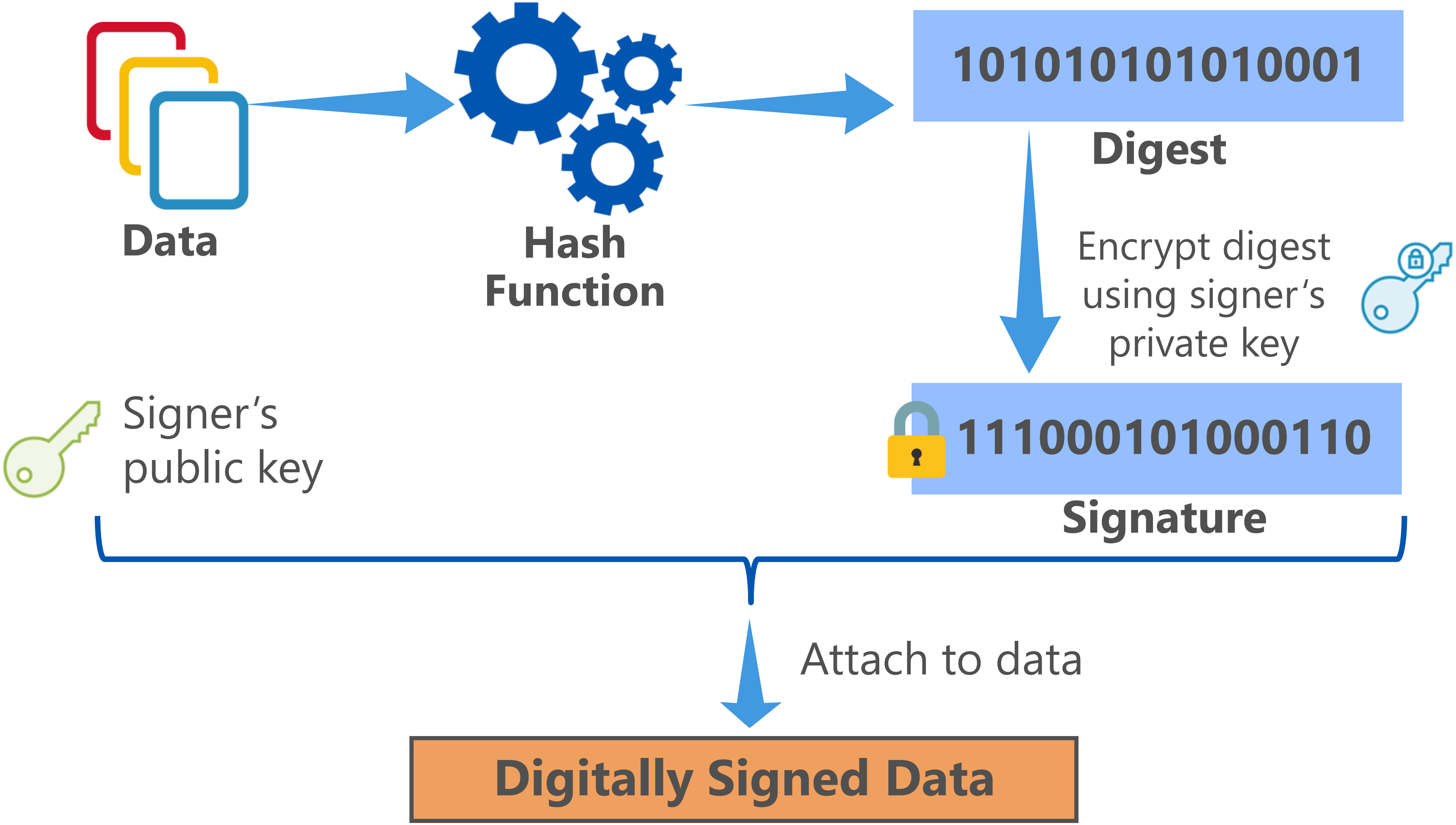


Alice

Bob’s Public Key

Bob’s Private Key

Signing Process



Data

Hash Function

101010101010001

Digest

Encrypt digest using signer's private key

Signer's public key

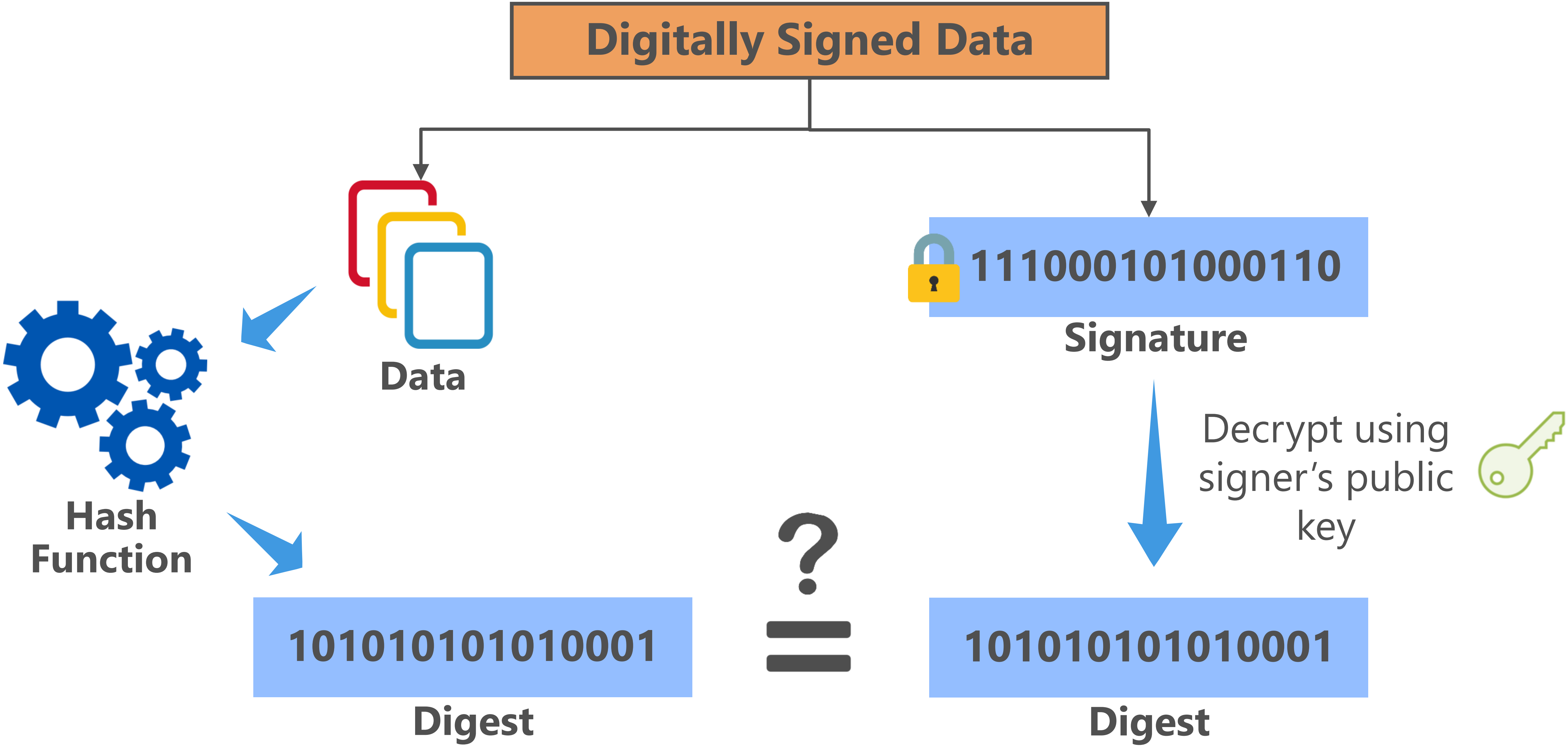
111000101000110

Signature

Attach to data

Digitally Signed Data

Verification Process



Digitally Signed Data

Data

Hash Function

1110001101000110

Signature

Decrypt using signer's public key

101010101010001

Digest

?

=

101010101010001

Digest

Lesson Review

Question 1:

Digest is another name for?

Hash.

Question 2:

Which key is used for encryption during the signing process?

The private key.

Question 3:

During document signing process, what do you have to do with the hash?

Encrypt the Hash.

Introduction to PKI

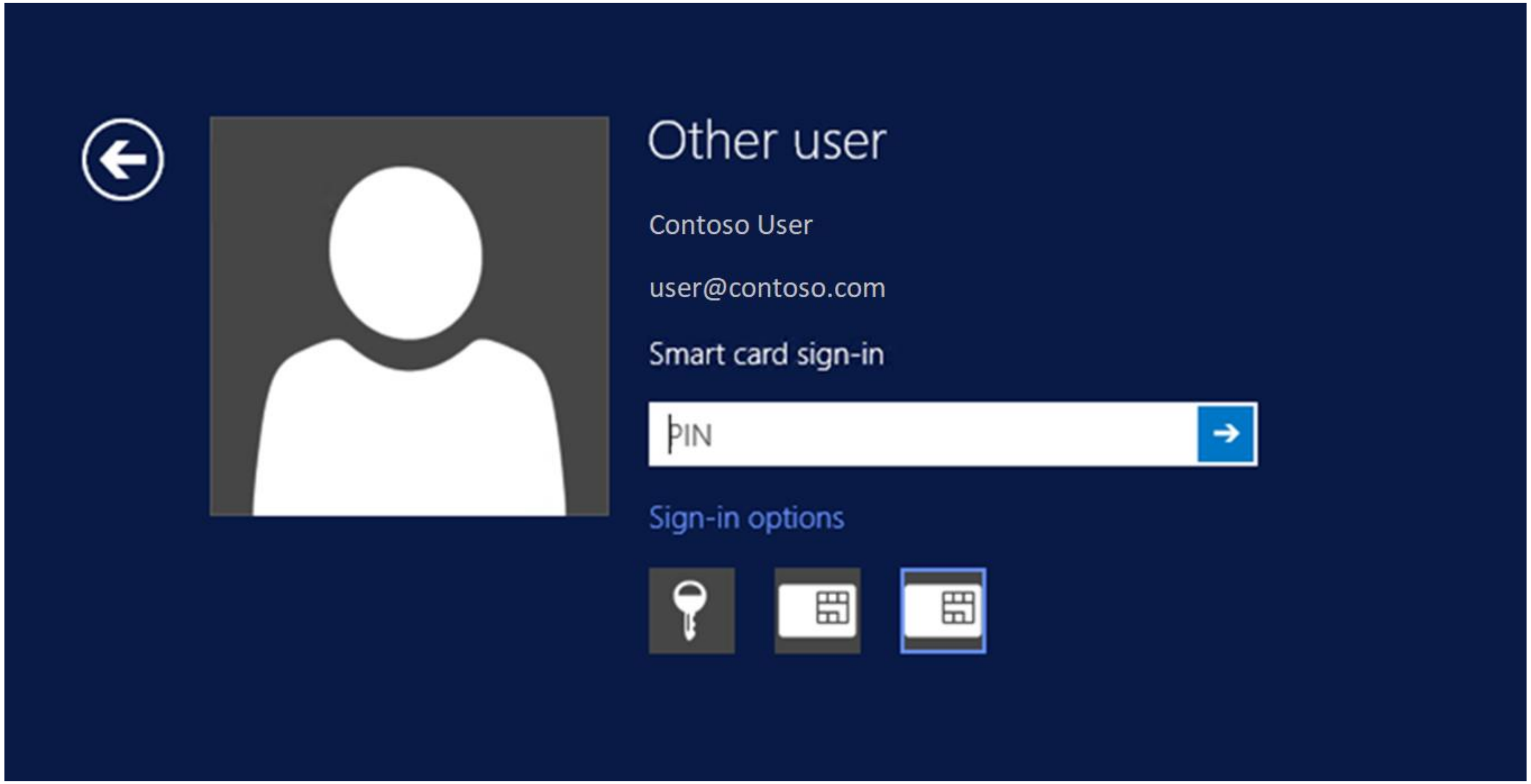
What is PKI?

- Public Key Infrastructure is a combination of:
  - Software
  - Hardware
  - Encryption technologies
  - Processes
  - Services
- Enables an organization to secure its communications and business transactions
- Goals of PKI: Confidentiality, Integrity, Authenticity, Non-repudiation

Common Uses of PKI

PKI can be used with many technologies like:

- Smart Card logon



Other user

Contoso User

user@contoso.com

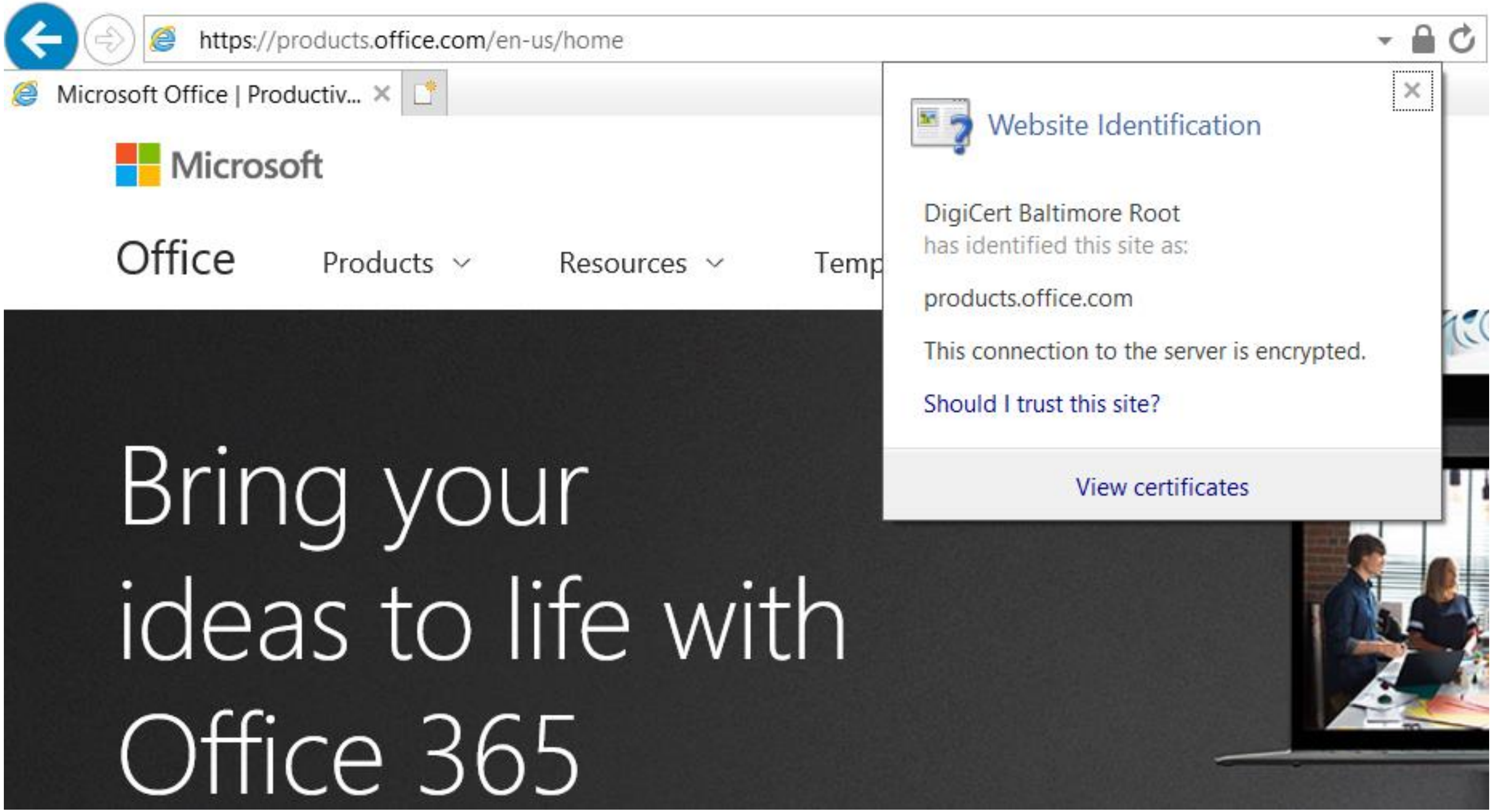
Smart card sign-in

PIN

Sign-in options

Common Uses of PKI (cont.)

- SSL/TLS for Websites



https://products.office.com/en-us/home

Microsoft Office | Productiv...
Microsoft
Office
Products
Resources
Temp
Bring your ideas to life with Office 365

Website Identification

DigiCert Baltimore Root has identified this site as:

products.office.com

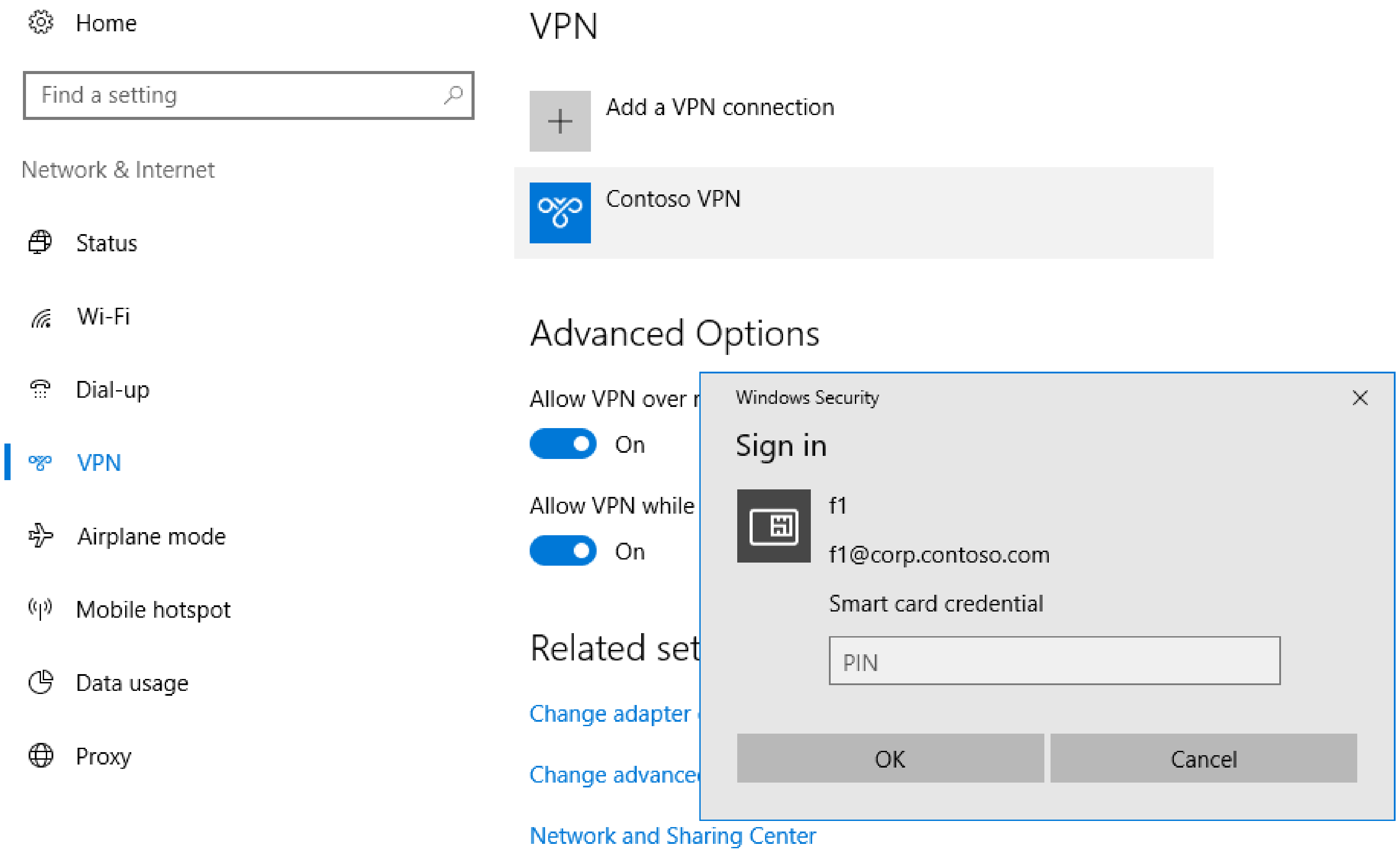
This connection to the server is encrypted.

Should I trust this site?

View certificates

Common Uses of PKI (cont.)

- VPN



Allow VPN over r
On

Allow VPN while
On

Windows Security

Sign in

f1

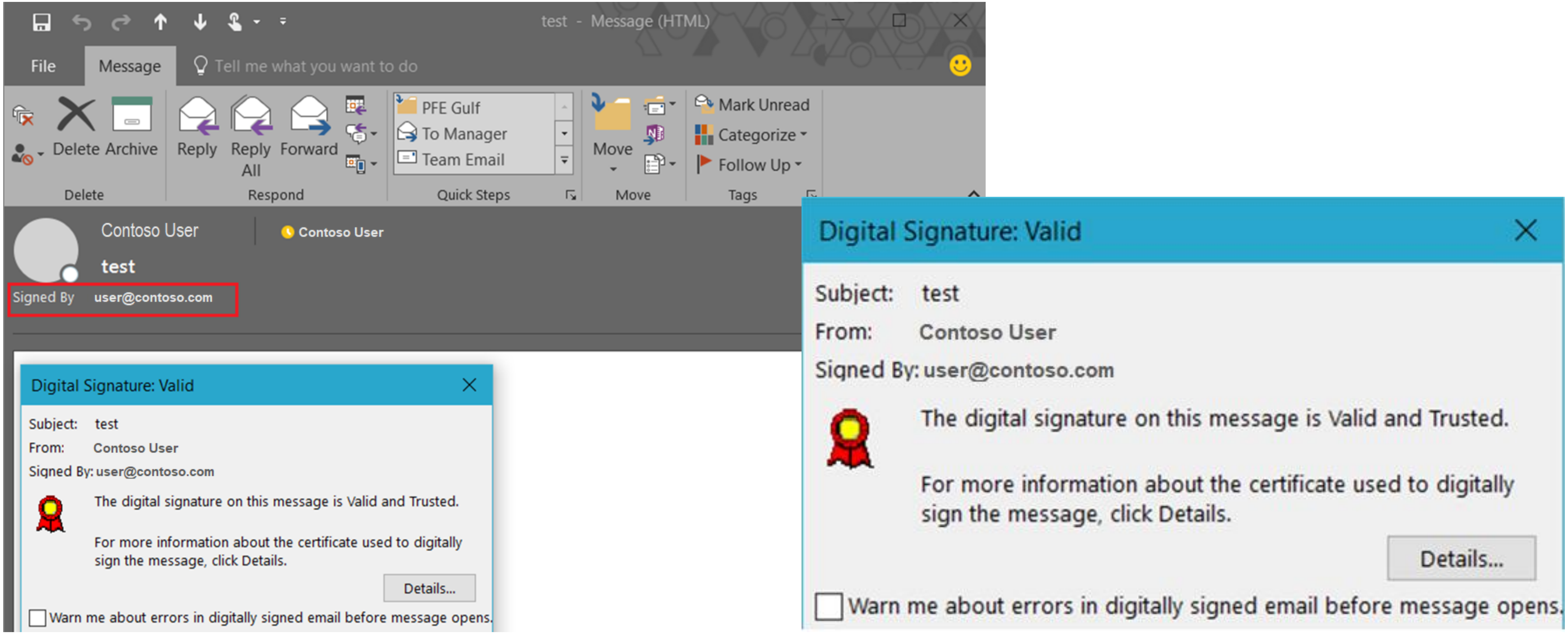
f1@corp.contoso.com

Smart card credential

PIN

Common Uses of PKI (cont.)

- Email signing and encryption



Signed By user@contoso.com

Digital Signature: Valid

Subject: test

From: Contoso User

Signed By: user@contoso.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 email before message opens.

Digital Signature: Valid

Subject: test

From: Contoso User

Signed By: user@contoso.com

The digital signature on this message is Valid and Trusted.

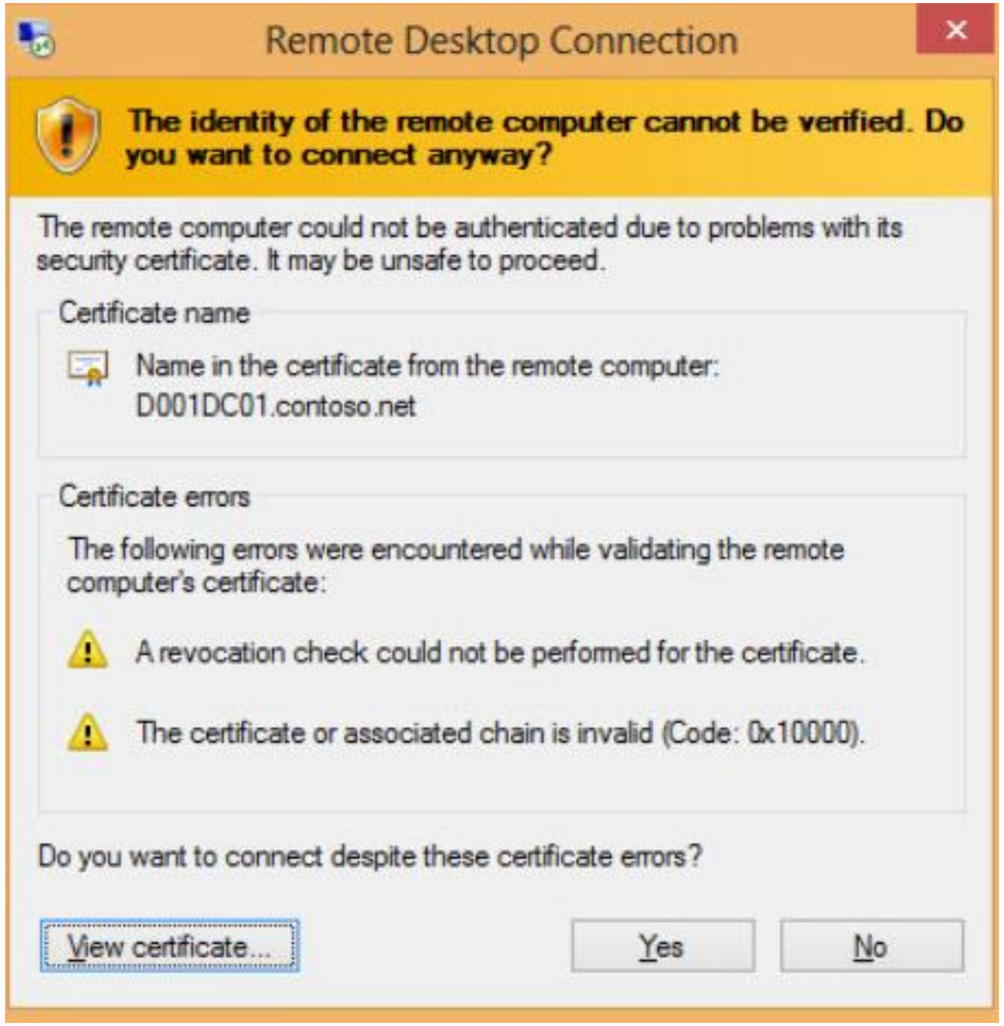
For more information about the certificate used to digitally sign the message, click Details.

Details...

□ Warn me about errors in digitally signed email before message opens.

Common Uses of PKI (cont.)

- RDP authentication



The identity of the remote computer cannot be verified. Do you want to connect anyway?

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
D001DC01.contoso.net

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

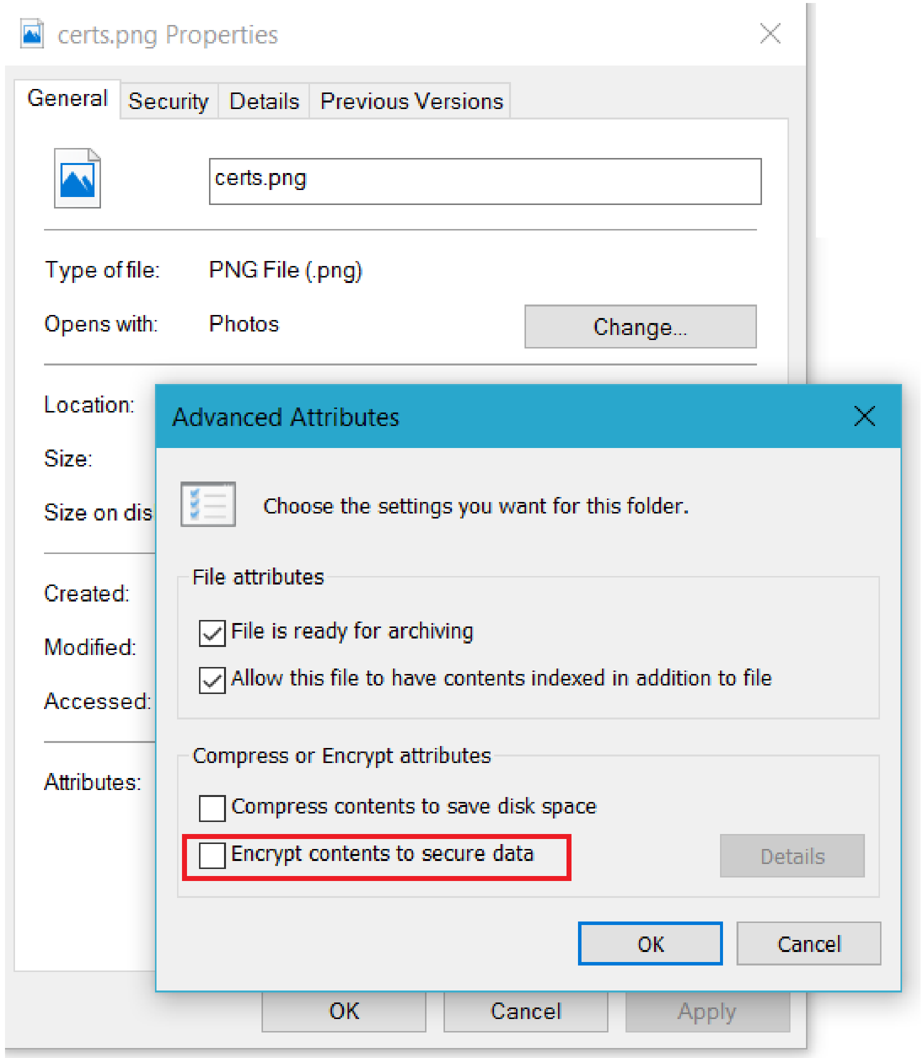
⚠ A revocation check could not be performed for the certificate.

⚠ The certificate or associated chain is invalid (Code: 0x10000).

Do you want to connect despite these certificate errors?

Common Uses of PKI (cont.)

- Encrypting File System



certs.png Properties

certs.png

Type of file: PNG File (.png)

Opens with: Photos

Location:

Size:

Size on dis

Created:

Modified:

Accessed:

Attributes:

Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

☑ Allow this file to have contents indexed in addition to file

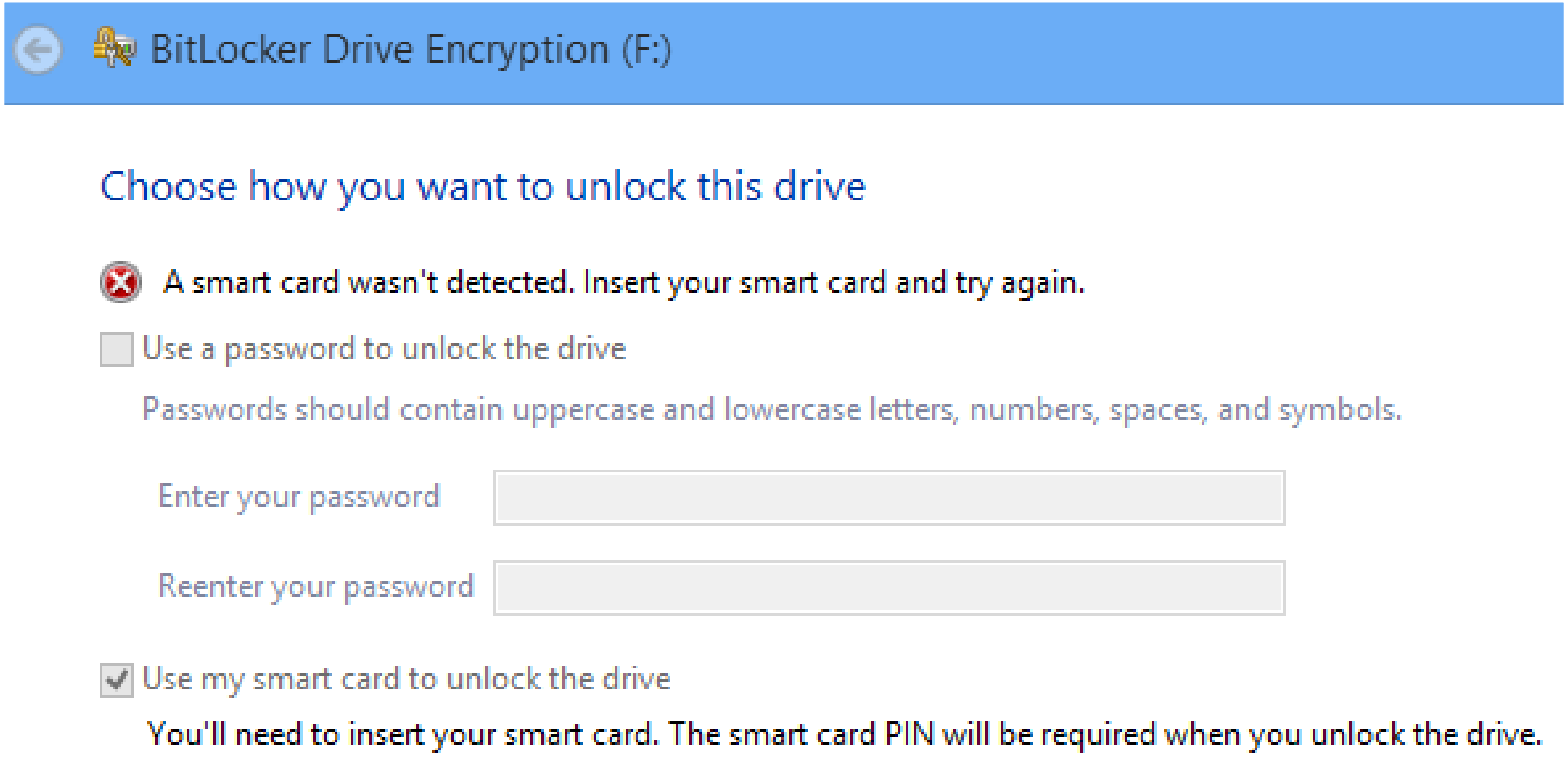
Compress or Encrypt attributes

□ Compress contents to save disk space

□ Encrypt contents to secure data

Common Uses of PKI (cont.)

- BitLocker



BitLocker Drive Encryption (F:)

Choose how you want to unlock this drive

☒ A smart card wasn't detected. Insert your smart card and try again.

□ Use a password to unlock the drive

Passwords should contain uppercase and lowercase letters, numbers, spaces, and symbols.

Enter your password

Reenter your password

☑ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Common Uses of PKI (cont.)

- Wired and wireless network authentication
- LDAPS (LDAP over SSL)
- TDE (Transparent Data Encryption for SQL)
- IPSec
- Virtual smart-cards
- Windows Hello for Business
- And much more..

PKI Components

- Software, hardware and processes comprise PKI components:
  - Digital certificates
  - Certification Authorities (CAs)
  - PKI enabled applications
  - Revocation of certificates
  - Certificate and CA management tools
  - Ancillary services: e.g. Online Certificate Status Protocol (OCSP), Network Device Enrollment Service (NDES) etc.
  - Hardware security devices (HSM, Smart Cards, etc.)
  - Processes

Digital Certificates

What is a Digital Certificate?

Digital credentials comparable to digital ID or digital passport.

Has purposes defined (Authentication, Encryption, Smart Card or Signing)

Can be issued for a user, a computer, network device or a service account

Securely binds a public key to the entity that holds the corresponding private key

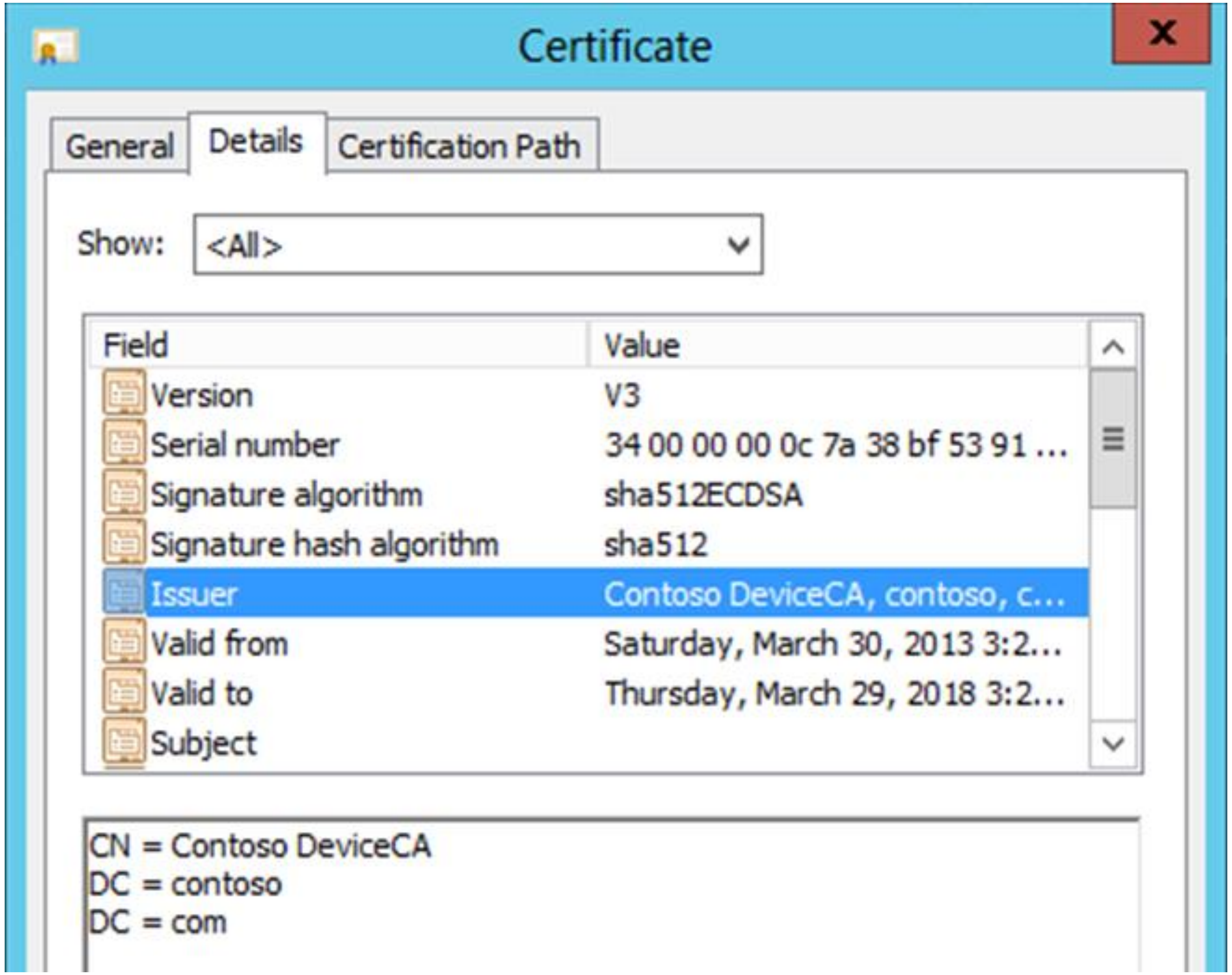
What is a Digital Certificate (cont.)?

Subject of the certificate contains name of the entity that receives the certificate, and holds the private key

Is digitally signed by an issuer (typically Certification Authority)

Current version of format: ITU-T X.509 version 3 international standards

Common Contents of a X.509v3 Certificate



Show: <All>

Field	Value
Version	V3
Serial number	34 00 00 00 0c 7a 38 bf 53 91 ...
Signature algorithm	sha512ECDSA
Signature hash algorithm	sha512
Issuer	Contoso DeviceCA, contoso, c...
Valid from	Saturday, March 30, 2013 3:2...
Valid to	Thursday, March 29, 2018 3:2...
Subject	

CN = Contoso DeviceCA
DC = contoso
DC = com

▤ - Version 1 fields

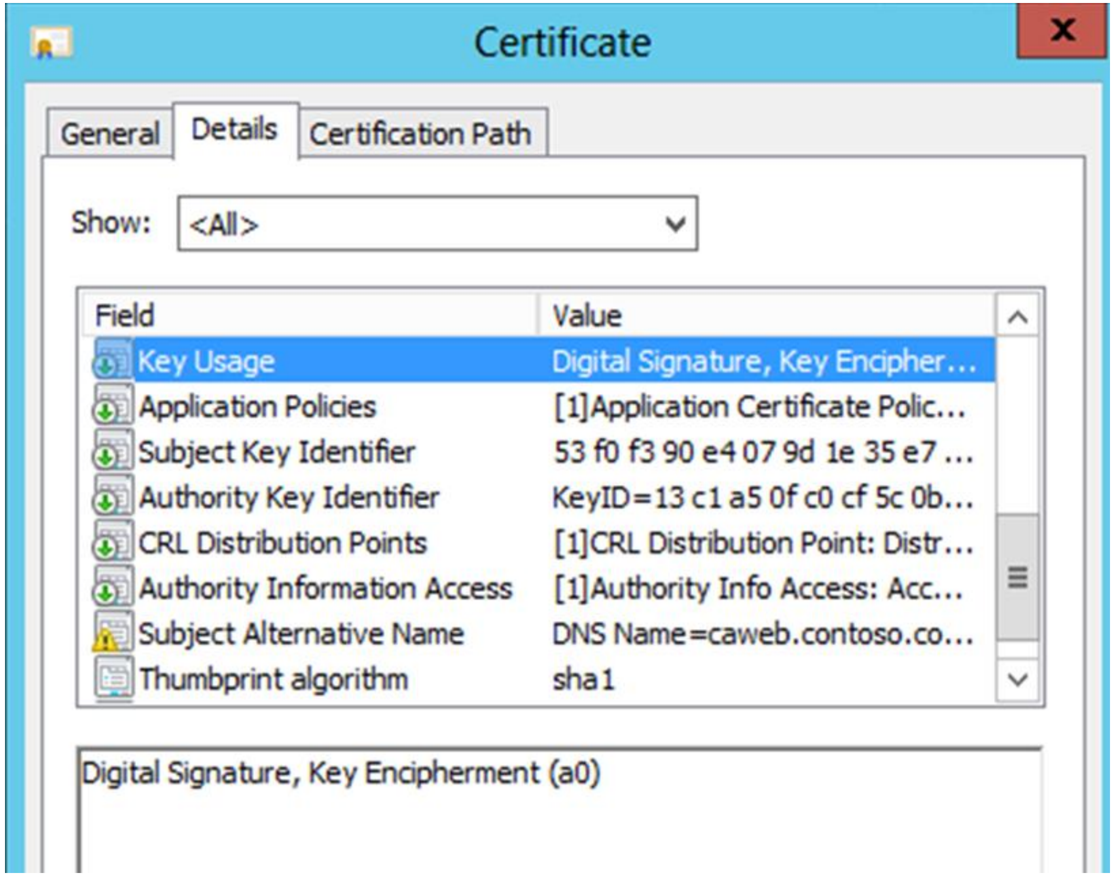
Certificate Attributes and Extensions

An extension provides additional information about the subject.

It is the responsibility of a security-enabled application to interpret the certificate or to use a sub-system like CryptoAPI to verify the status of a certificate.

The CryptoAPI engine and programming model puts the responsibility of parsing critical extensions on the calling application.

Certificate Extensions



Show: <All>

Field	Value
Key Usage	Digital Signature, Key Encipher...
Application Policies	[1]Application Certificate Polic...
Subject Key Identifier	53 f0 f3 90 e4 07 9d 1e 35 e7 ...
Authority Key Identifier	KeyID=13 c1 a5 0f c0 cf 5c 0b...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...
Subject Alternative Name	DNS Name=caweb.contoso.co...
Thumbprint algorithm	sha1

Digital Signature, Key Encipherment (a0)

- Non-critical extensions
- Critical extensions
- Properties

RFC 3280 compliant applications should reject a certificate if the certificate contains a critical extension not understood by the application (but it is still up to application)

Certificate Extensions (cont.)

- Authority Information Access (AIA)
  - Certificate extension used for verifying the trust status of a certificate
  - Potentially includes URLs where the issuing CA's certificate can be retrieved
  - The AIA extension can contain HTTP, FTP, LDAP or File URLs
- CRL Distribution Point (CDP)
  - Certificate extension that indicates where the certificate revocation list for a CA can be retrieved
  - This extension can contain multiple HTTP, FTP, File or LDAP URLs for the retrieval of the CRL.
- Extensions for AIA and CDP are not mandatory

CRL - Certificate Revocation List

- A CRL is a digitally signed list including information of all the certificates which have been revoked, issued by the CA that originally enrolled the certificates
- Applications or systems can perform CRL checking to determine a presented certificate's revocation status
- A CRL is typically generated and published periodically, following a clearly defined timeframe
- The CA can publish the CRL in a publicly accessible location and by default publishes it in the filesystem of the CA

Certification Authorities (CAs)

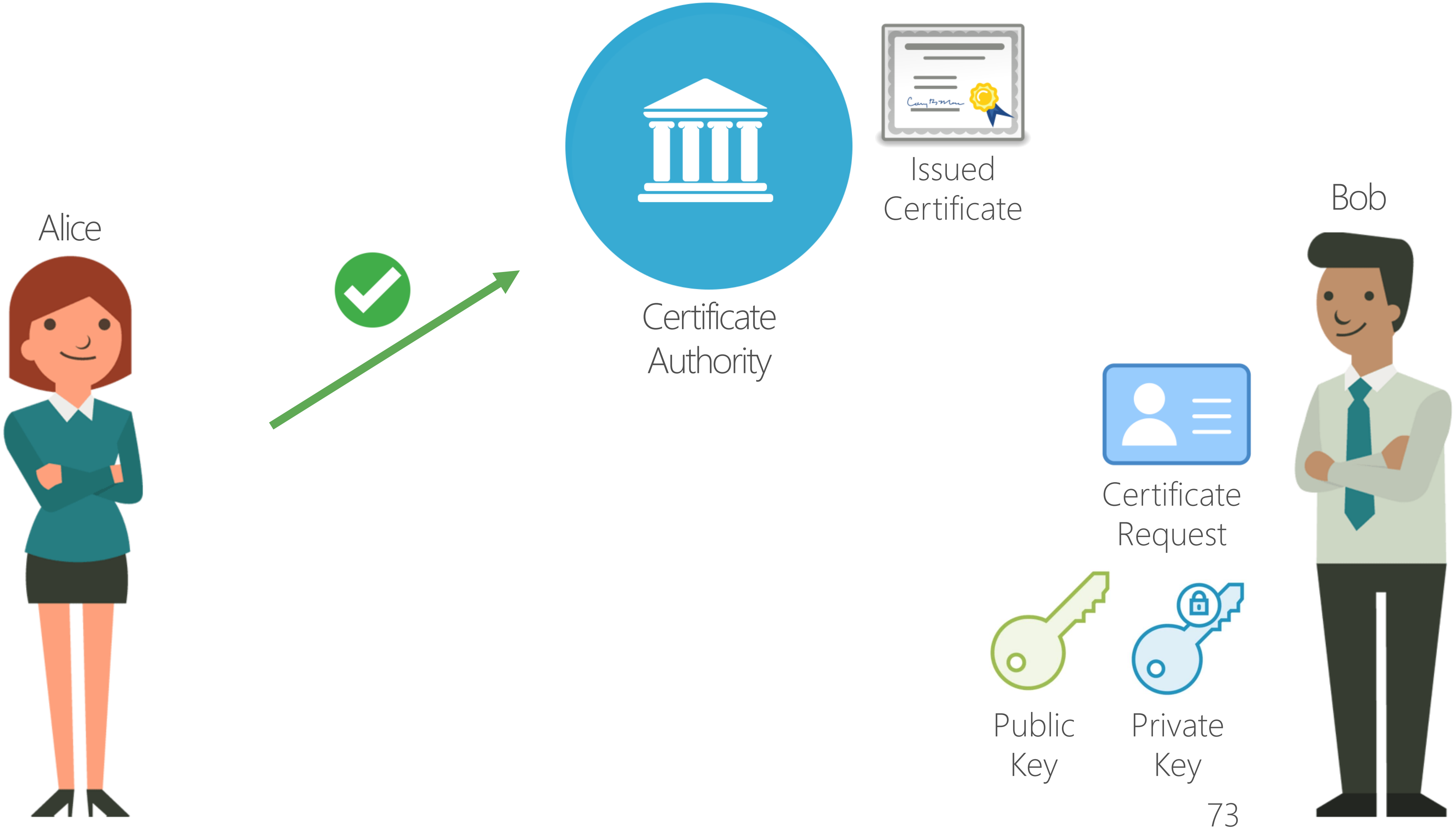
Certification Authority (CA)

- The CA is a machine which issues certificates to different entities (users, computers, network devices, service accounts, other CAs)

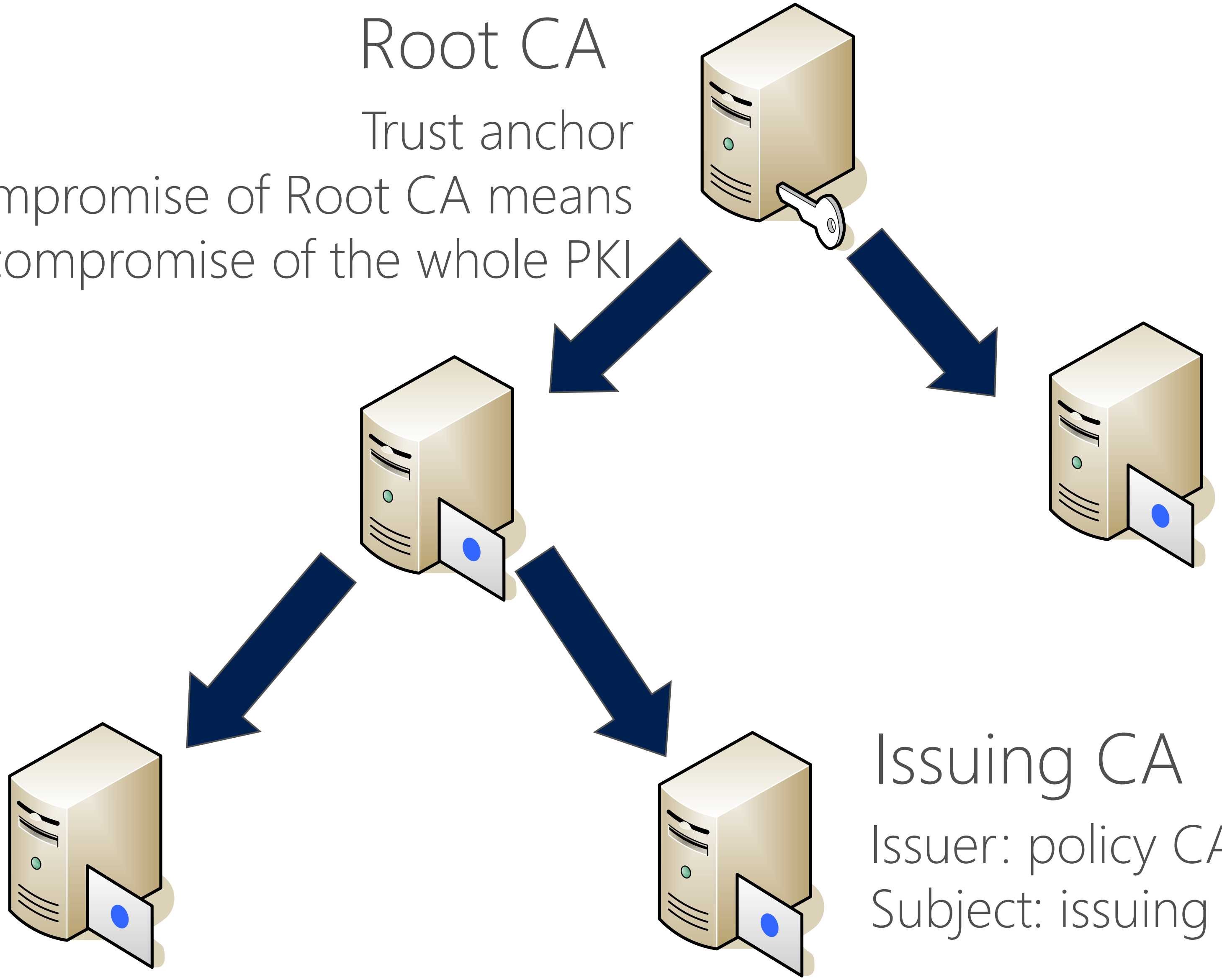
- The CA verifies the identity of a certificate requestor.
  The mode of identification depends on the:
  - Type of CA
  - Security policy
  - Request handling requirements

- The CA manages certificate revocation issuance
  - The CRL contains revoked certificate serial numbers
  - CRLs are updated manually or automatically

Trust Chains



Certificate Authority Hierarchy



Root CA

Trust anchor

Compromise of Root CA means compromise of the whole PKI

Policy CA

Issuer: root

Subject: policy CA

Issuing CA

Issuer: policy CA

Subject: issuing CA

Roles in CA Hierarchy

- Root CA
  - Highest CA in the hierarchy (Trust point for all certificates)
  - If a user, computer, or service trusts a root CA, they implicitly trust all certificates that are issued by all other CAs in the CA hierarchy
- Policy CA
  - Typically located on the second tier of a CA hierarchy (optional implementation)
  - Describes the policies and procedures that an organization implements to secure its PKI
  - Issues certificates only to other CAs
- Issuing CA
  - Typically located at the lowest tier of the hierarchy
  - Issues end-entity certificates

Reasons for Hierarchies

- Security
  - The Root CA is the trust anchor of the PKI
  - The Root CA certificate cannot be revoked because it is self-signed
- Mapping Trust
  - CAs may be operated by different entities (or divisions within an entity) and are configured to reflect the trust boundaries of their operators
- Manageability
  - Different departments are responsible for different levels of the PKI (“role separation”)
- Flexibility
  - A CA can be replaced easily instead of replacing the whole PKI

Deciding on the CA Hierarchy Depth

How many tiers of CAs should exist?

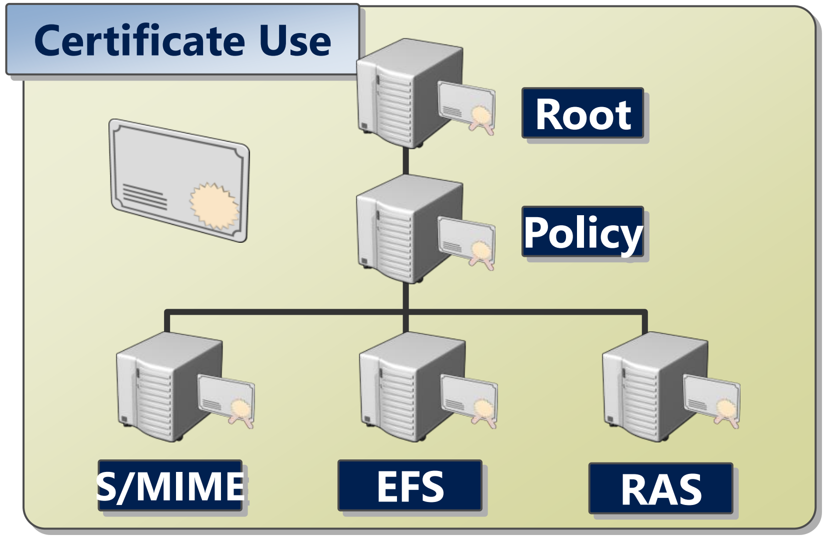
Two or three tiers is optimal

- Fewer tiers:
  - Decrease security
  - Cause operational difficulties (delegation)
- More tiers:
  - Provide little benefit for the isolation of issuance
  - Require more revocation checking (each level produces a logarithmic increase)
  - Bring about more variations in management groups and thus more-complex management processes

Two-Tier Hierarchy

- There are a minimum of two CAs in this model
- Root CA is offline and should never be connected to a network
- Strong key size recommended
- Issuing CA(s) is typically joined to a domain within a Microsoft environment
- Validity period is half of Root CA
- Most common type of hierarchy

Certification Authority Designs


Certificate Use

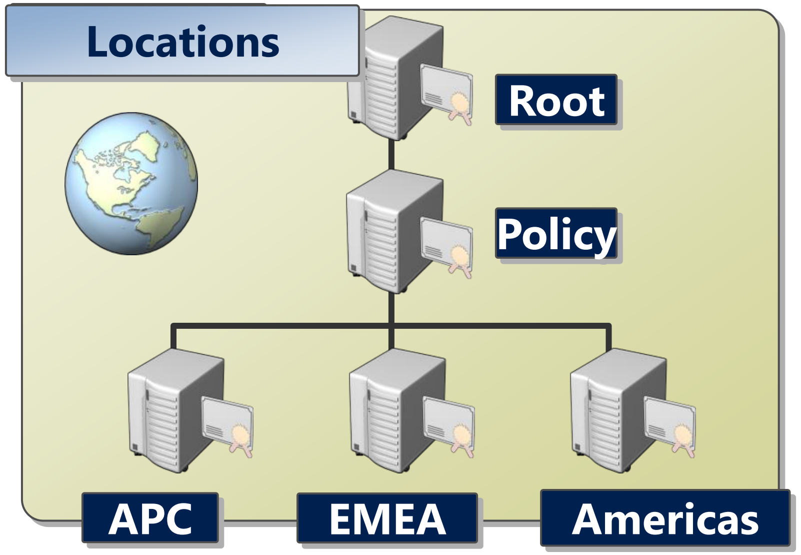
Root

Policy

S/MIME

EFS

RAS


Locations

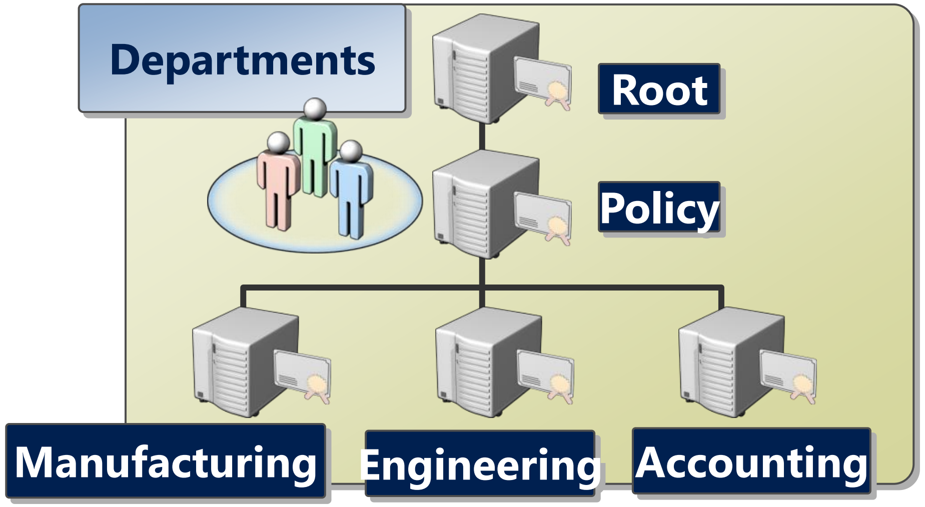
Root

Policy

APC

EMEA

Americas


Departments

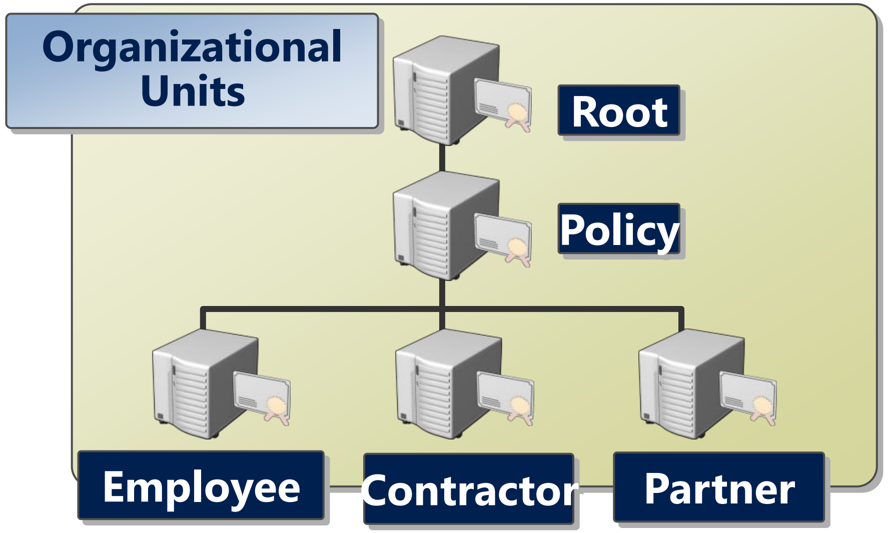
Root

Policy

Manufacturing

Engineering

Accounting


Organizational Units

Root

Policy

Employee

Contractor

Partner

Choosing Hash and Encryption Algorithms

- From the security perspective, use
  - For CA certificate: RSA 4096 bits, or 256 or 384 bits ECC
  - For End Entity certificate: RSA 2048 bits or 256 bits ECC
  - SHA-256 or SHA-384
- From the compatibility perspective
  - Many clients cannot understand ECC and/or the SHA-2 family anywhere in the chain
  - Some clients cannot use RSA certificates longer than 2048 bits

Lesson Review

Question 1:

What is a two-tier CA hierarchy?

A CA with a minimum of two servers (root CA and issuing CA).

Question 2:

List 3 practical uses for PKI:

Smart Card Authentication, Email Signing, Files Encryption.

Question 3:

What is a CRL and what does it used for?

CRL stands for Certificate Revocation List.
It can be used by clients to get certificate status and revocation information.

Module Summary

- Symmetric Cryptography vs. Asymmetric Cryptography
- The real world (Hybrid Cryptography)
- Hashing and digital signature
- PKI Basics – Certificates, CRL (Certificate Revocation List), CA trusts and hierarchy

Questions?

Microsoft