Security in Informatics and in the Organizations (2018/2019)

Practical Class (#6):

Public Key Infrastructure (PKI)

Vitor Cunha (vitorcunha@ua.pt)

Recap – Asymmetric ciphers *(RSA n-bits)*

"Plain" RSA encryption

N, e

c

$(N, e, d) \leftarrow \text{RSAGen}(1^n)$

$pk = (N, e)$

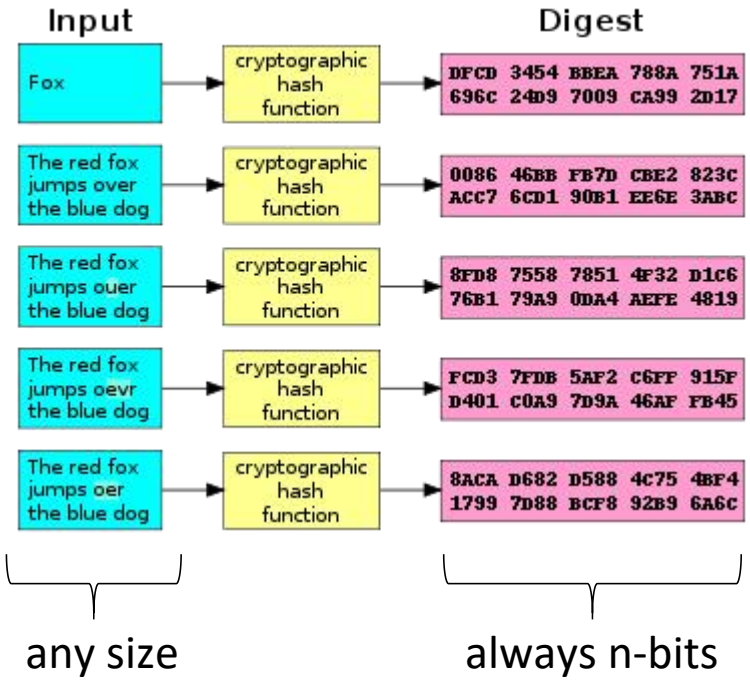
$sk = d$

$m = [c^d \bmod N]$

$c = [m^e \bmod N]$

Source: *J. Katz, UMD – in Coursera*

Recap – Digest Function (aka “Hash”)



1 - Pre-image resistance

Given a hash value h it should be difficult to find any message m such that h = hash(m). This concept is related to that of a one-way function. Functions that lack this property are vulnerable to preimage attacks.

2 - Second pre-image resistance

Given an input m1, it should be difficult to find a different input m2 such that hash(m1) = hash(m2). Functions that lack this property are vulnerable to second-preimage attacks.

3 - Collision resistance

It should be difficult to find two different messages m1 and m2 such that hash(m1) = hash(m2). Such a pair is called a cryptographic hash collision. This property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as that required for pre-image resistance; otherwise collisions may be found by a birthday attack.

Recap – Practical Use

- Confidentiality (eg. File Encryption)
  - Encrypt data with ***public key***
  - Decrypt with ***private key***
  - Source is not authenticated!

- Authenticity (eg. Digital Signatures, Authentication)
  - Encrypt challenge/identifier with ***private key***
  - Decrypt with ***public key***
  - Source is now authenticated!

How Trust works

Trust is transitive:

$$\text{Trust}(A, B) \wedge \text{Trust}(B, C) \Rightarrow \text{Trust}(A, C)$$

I *trust* my Bank **and** my Bank *trusts* the Bank Clerk **, therefore** I *trust* the Bank Clerk

But does <u>not *always*</u> work the other way around:

$$\text{Trust}(A, C) \not\Rightarrow \text{Trust}(A, B) \wedge \text{Trust}(B, C)$$

(it may be true in some cases, but not always!)

I *trust* my Bank **, therefore** I *trust* some Criminal **and** the Criminal *trusts* my Bank

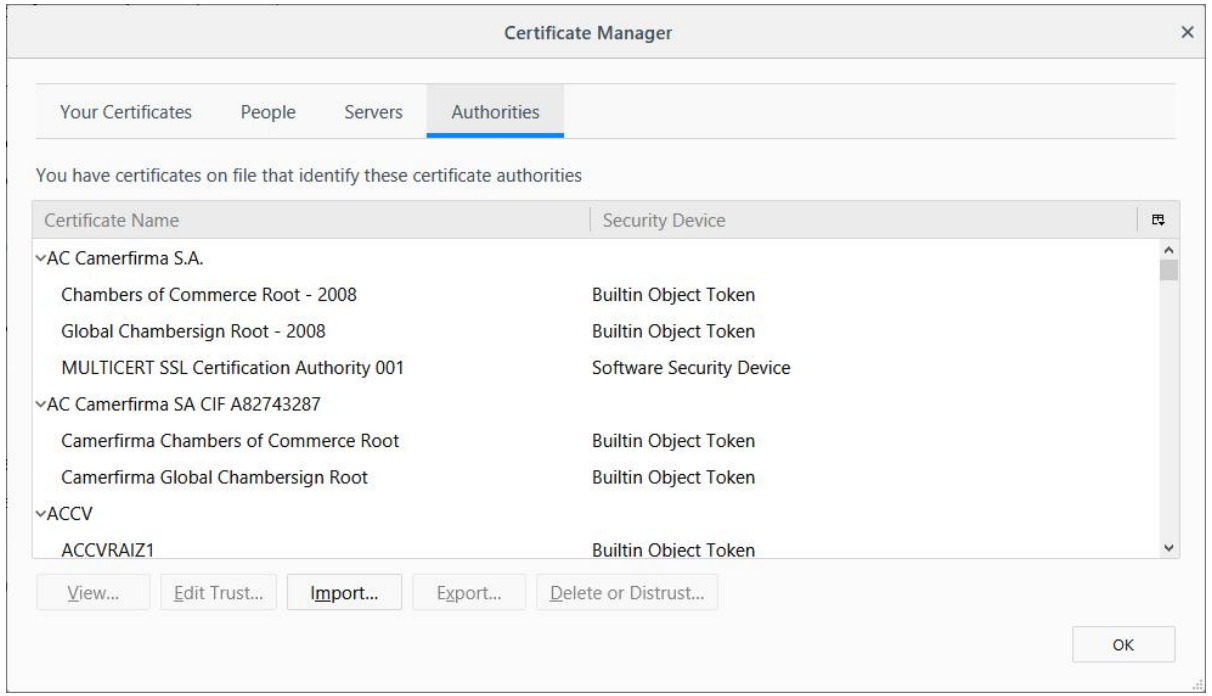
Trusted Roots

ORDEM DOS ADVOGADOS

IMT INSTITUTO DA MOBILIDADE E DOS TRANSPORTES, I.P.

instituto dos registos e do notariado

ORDEM DOS ENGENHEIROS



Public Key Certificates (X.509)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10:e6:fc:62:b7:41:8a:d5:00:5e:45:b6
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign Organization Validation CA - SHA256 - G2
        Validity
            Not Before: Nov 21 08:00:00 2016 GMT
            Not After : Nov 22 07:59:59 2017 GMT
        Subject: C=US, ST=California, L=San Francisco, O=Wikimedia Foundation, Inc., CN=*.wikipedia.org
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:c9:22:69:31:8a:d6:6c:ea:da:c3:7f:2c:ac:a5:
                    af:c0:02:ea:81:cb:65:b9:fd:0c:6d:46:5b:c9:1e:
                    ed:b2:ac:2a:1b:4a:ec:80:7b:e7:1a:51:e0:df:f7:
                    c7:4a:20:7b:91:4b:20:07:21:ce:cf:68:65:8c:c6:
                    9d:3b:ef:d5:c1
                ASN1 OID: prime256v1
                NIST CURVE: P-256
```

Public Key Certificates (X.509)

X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Key Agreement
Authority Information Access:
CA Issuers - URI:http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
OCSP - URI:http://ocsp2.globalsign.com/gsorganizationvalsha2g2

X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.4146.1.20
CPS: https://www.globalsign.com/repository/
Policy: 2.23.140.1.2.2

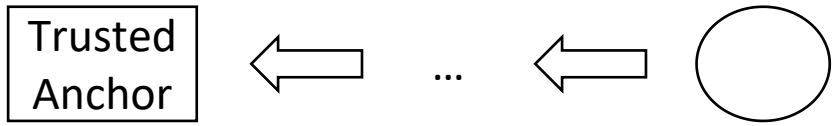
X509v3 Basic Constraints:
CA:FALSE
X509v3 CRL Distribution Points:
Full Name:
URI:http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl

X509v3 Subject Alternative Name:
DNS:*.wikipedia.org, DNS:*.m.mediawiki.org, …, DNS:wikipedia.org
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Subject Key Identifier:
28:2A:26:2A:57:8B:3B:CE:B4:D6:AB:54:EF:D7:38:21:2C:49:5C:36
X509v3 Authority Key Identifier:
keyid:96:DE:61:F1:BD:1C:16:29:53:1C:C0:CC:7D:3B:83:00:40:E6:1A:7C

Public Key Certificates (X.509)

Signature Algorithm: sha256WithRSAEncryption
8b:c3:ed:d1:9d:39:6f:af:40:72:bd:1e:18:5e:30:54:23:35:
...

Validation:



Public Key Certificates (X.509)

X509v3 extensions:

X509v3 Key Usage: critical

Digital Signature, Key Agreement

Authority Information Access:

CA Issuers - URI:http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt

OCSP - URI:http://ocsp2.globalsign.com/gsorganizationvalsha2g2

X509v3 Certificate Policies:

Policy: 1.3.6.1.4.1.4146.1.20

CPS: https://www.globalsign.com/repository/

Policy: 2.23.140.1.2.2

X509v3 Basic Constraints:

CA:FALSE

X509v3 CRL Distribution Points:

Full Name:

URI:http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl

X509v3 Subject Alternative Name:

DNS:*.wikipedia.org, DNS:*.m.mediawiki.org, …, DNS:wikipedia.org

X509v3 Extended Key Usage:

TLS Web Server Authentication, TLS Web Client Authentication

X509v3 Subject Key Identifier:

28:2A:26:2A:57:8B:3B:CE:B4:D6:AB:54:EF:D7:38:21:2C:49:5C:36

X509v3 Authority Key Identifier:

keyid:96:DE:61:F1:BD:1C:16:29:53:1C:C0:CC:7D:3B:83:00:40:E6:1A:7C

Practical stuff

(switch to other window)