

COMPUTER SECURITY

PUBLIC KEY CRYPTOGRAPHY RSA, Digital Signatures, PKI

Willy Sudiarto Raharjo

Teknik Informatika
Universitas Kristen Duta Wacana

RSA

- Developed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977
- Uses a large pair of prime numbers so that factoring the product is beyond all computing capabilities
 - ◆ Testing for primes is easy
 - ◆ Factoring the product is very difficult
- Unbreakable (for now)



Ronald L. Rivest, Adi Shamir, and Leonard Adleman

RSA

- Choose two prime numbers p and q
- Calculate modulus $n = pq$
- Calculate $(p-1)(q-1)$
- Chose $e > 1$ that is coprime to $((p-1)(q-1))$
 - ◆ *Choosing a prime number for e leaves you with a single check: that e is not a divisor of $((p-1)(q-1))$*
- Compute d such that $de = 1 \pmod{((p-1)(q-1))}$
- Public key: $\{e, n\}$, Private key: $\{d\}$
- It's currently virtually impossible to obtain private key (d) from the public key (n and e)

Example

- $p = 5, q = 11$
- $n = p \times q = 55$
- $(p-1)(q-1) = 40$
- $e = 3$ (because 40 can't be divided by 3 and it's a prime)
- $d = 27$ because $27 * 3 = 81$ and $81 \bmod 40 = 1$
- Public key = $(n = 55, e = 3)$
- Private key = $(d = 27)$

Encryption/Decryption

- Encryption

$$C = M^e \bmod n$$

- To encrypt M (message) = 5

$$C = 5^3 \bmod 55$$

$$125 \bmod 55 = 15$$

- Decryption

$$M = C^d \bmod n$$

- To decrypt C (ciphertext) = 15

$$M = 15^{27} \bmod 55 = 5$$

Practice

- $p = 17$
- $q = 11$
- $M = 88$
- What is the C ?
- Show the process to convert $C \rightarrow M$

Answers

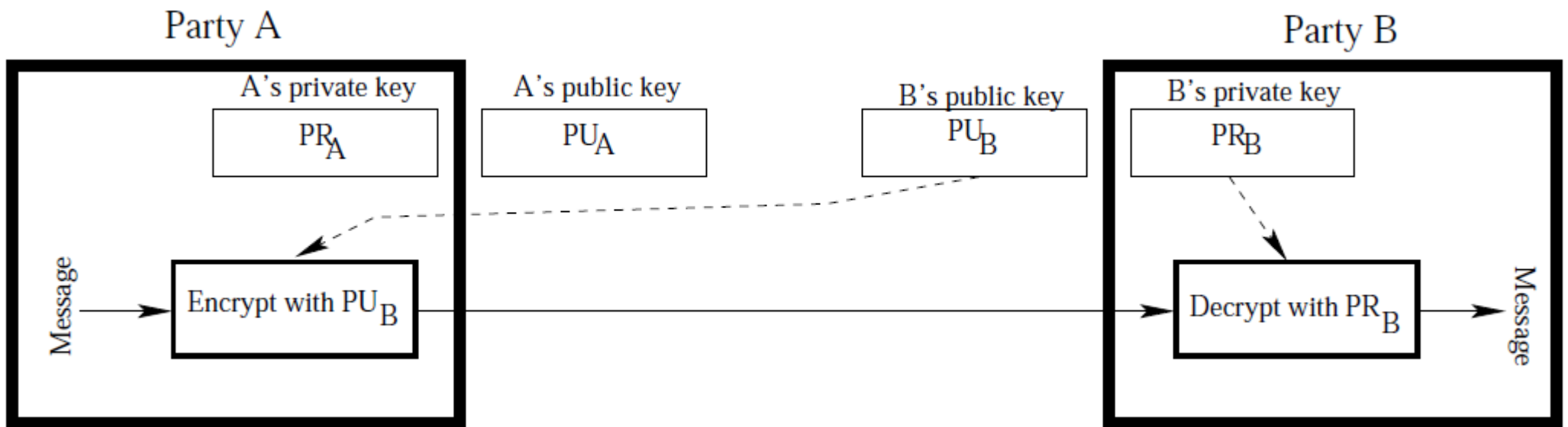
- Select primes: $p=17$ & $q=11$
- Compute $n = pq = 17 \times 11 = 187$
- Compute $\Phi(n) = (p-1)(q-1) = 16 \times 10 = 160$
- Select e : $\gcd(e, 160) = 1$; choose $e=7$
- Determine d : $de = 1 \pmod{160}$ and $d < 160$ Value is $d=23$ since $23 \times 7 = 161 = 10 \times 160 + 1$
- Publish public key $P = \{7, 187\}$
- Keep secret private key $S = \{23, 17, 11\}$
 - ◆ 17, 11 (p dan q)

- given message $M = 88$
- Encryption (using public key):
$$C = 88^7 \bmod 187 = 11$$
- Decryption (using private key):
$$M = 11^{23} \bmod 187 = 88$$

Public-Key Cryptography

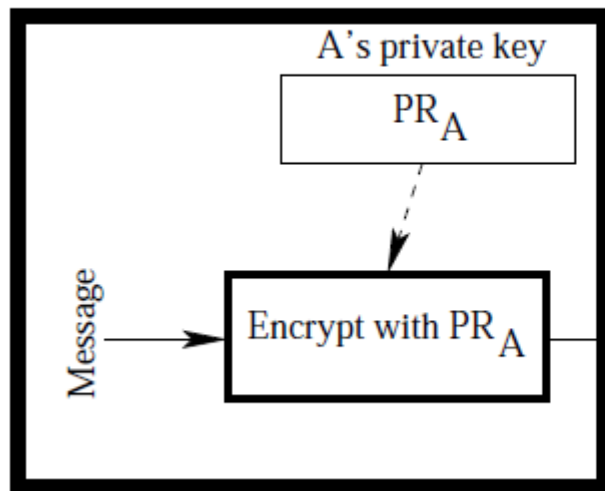
- Public key cryptography can provides
 - ◆ Confidentiality (plus integrity)
 - ◆ Authenticity
 - ◆ Confidentiality + Authenticity

Confidentiality + Integrity

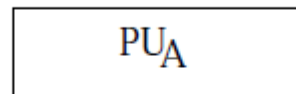


Authenticity

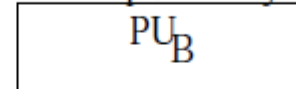
Party A



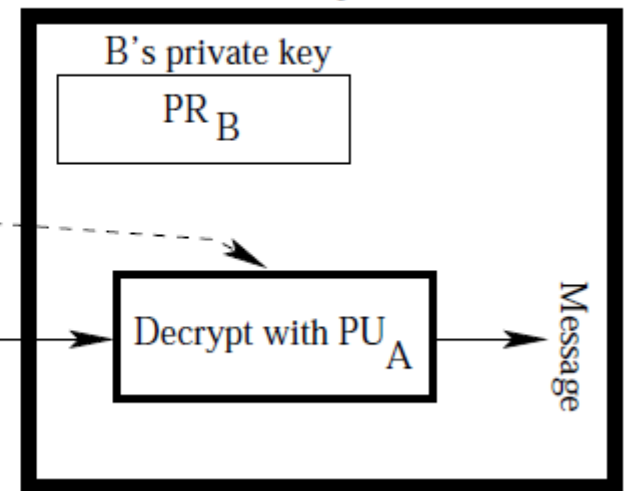
A's public key



B's public key

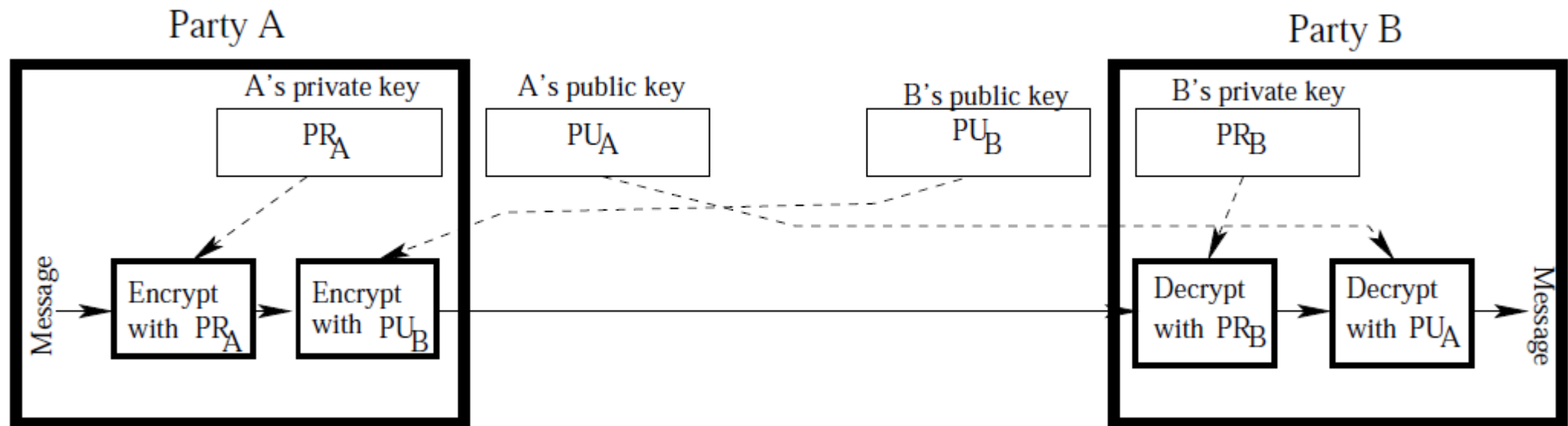


Party B



Public key signatures also provides **Non Repudiation**

Confidentiality, Integrity and Authenticity



Issues on RSA

- Encryption and Decryption
 - ◆ The efficiency of exponentiation computation
- Key generation
 - ◆ Determining two prime numbers p and q
 - ◆ Selecting either e or d and calculating the other
- Key distribution
 - ◆ Public key can be intercepted (MiTM attack)
 - ◆ Solution: use key server to distribute the public key

Speeding Up RSA

- To speed up RSA → use the same e for all users
 - ◆ As long as p and q are different for each user, d (private keys) will be different also
 - ◆ Common value for $e = 3$
- Private key operation remains expensive
- Don't use same d for all users → symmetric key



Search For Keys

Search

Enter a name, email address, or key ID

[advanced](#)

The PGP Global Directory is a free service designed to make it easier to find and trust the universe of PGP keys. Publish your key today and allow others to start sending you secure email.



Publish Your Key

Upload your PGP public key to make it searchable by the PGP community.



Remove Your Key

Remove your key from the searchable directory.

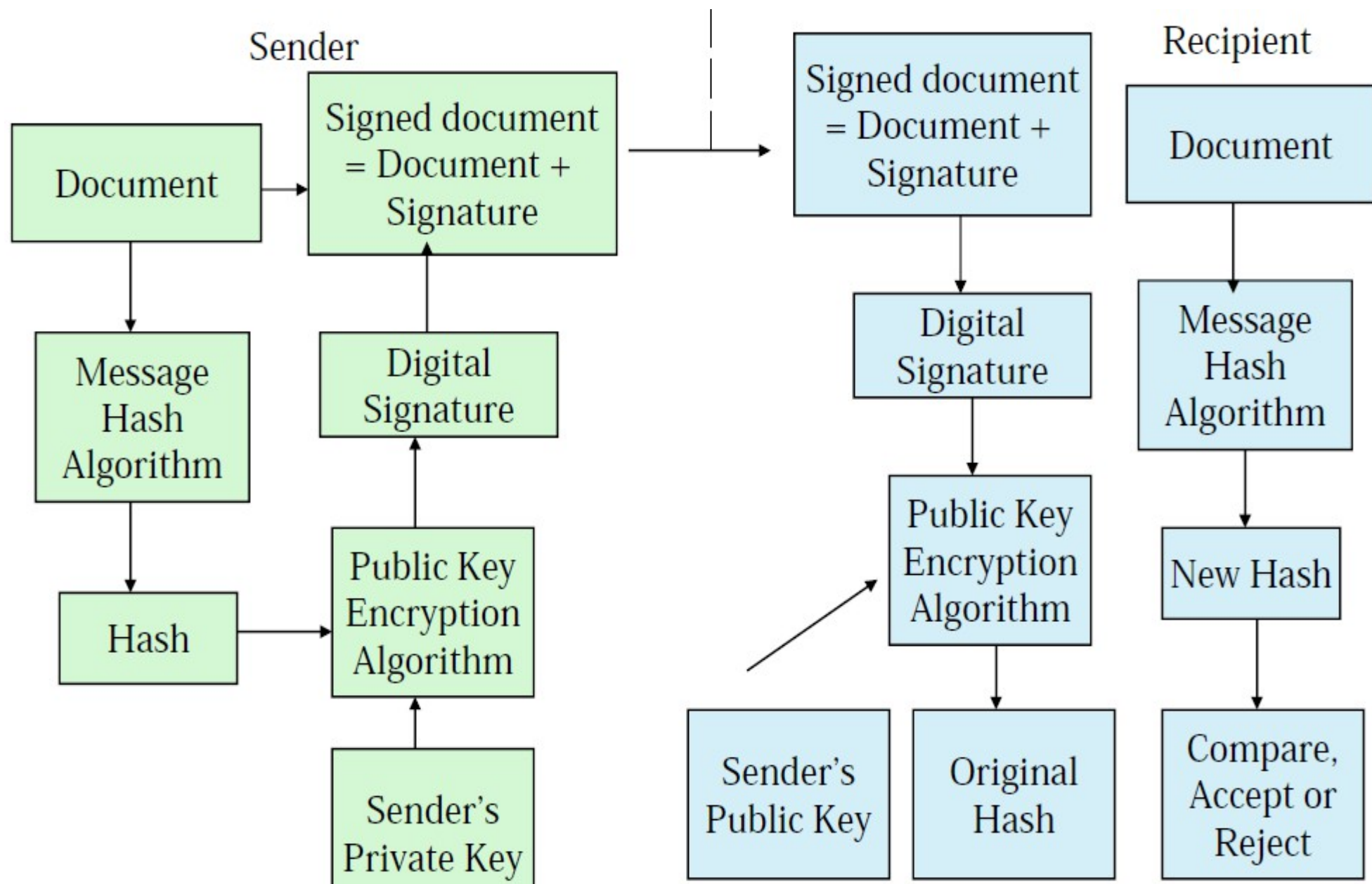
Digital Signature

Digital Signature is a type of asymmetric cryptography used to simulate the security properties of a signature in digital, rather than written form

Digital signature schemes normally give two algorithms; one for signing which involves the user's secret or private key, and one for verifying signatures which involves the user's public key

The output of the signature process is called the "digital signature"





Scenario

- Alice create digital signature s

$$s = m^d \bmod n$$

- Alice send s and m to Bob
- To verify, Bob use Alice's public key

$$m = s^e \bmod n$$

Example

- Public key = $(n = 55, e = 3)$
- Private key = $(d = 27)$
- $M = 5$
- Count for s and m

Components of Digital Signature:

Public key

Name and E-mail of sender

Key expiry date

Company name that sends the information

Serial number of Digital Signature

Digital signature of certification authority



Digital Signatures are used to check:

Identity of the sender

Dependability of the message

Whether message sent is genuine

For risk of frauds

Whether message is illegally reproduced

Fulfillment of lawful requirements

For security of open systems



Digital Certificates

Digital Certificates verify the uniqueness of the principles and entities over networks as electronic documents

Unique identity to the owner of the digital certificate is defined by both public key and private keys

Widely accepted format for digital certificates is defined by the ITU-T X.509 international standard

Digital certificate includes a variety of information such as:

- Name of the subject
- Subject's public key
- Certification authority's name
- Serial number
- Lifetime period of the digital certificate right from the start date



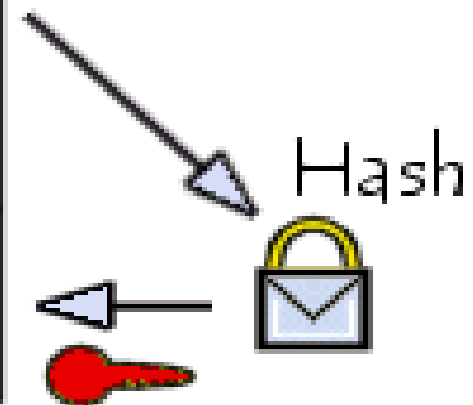
Certificate

Data

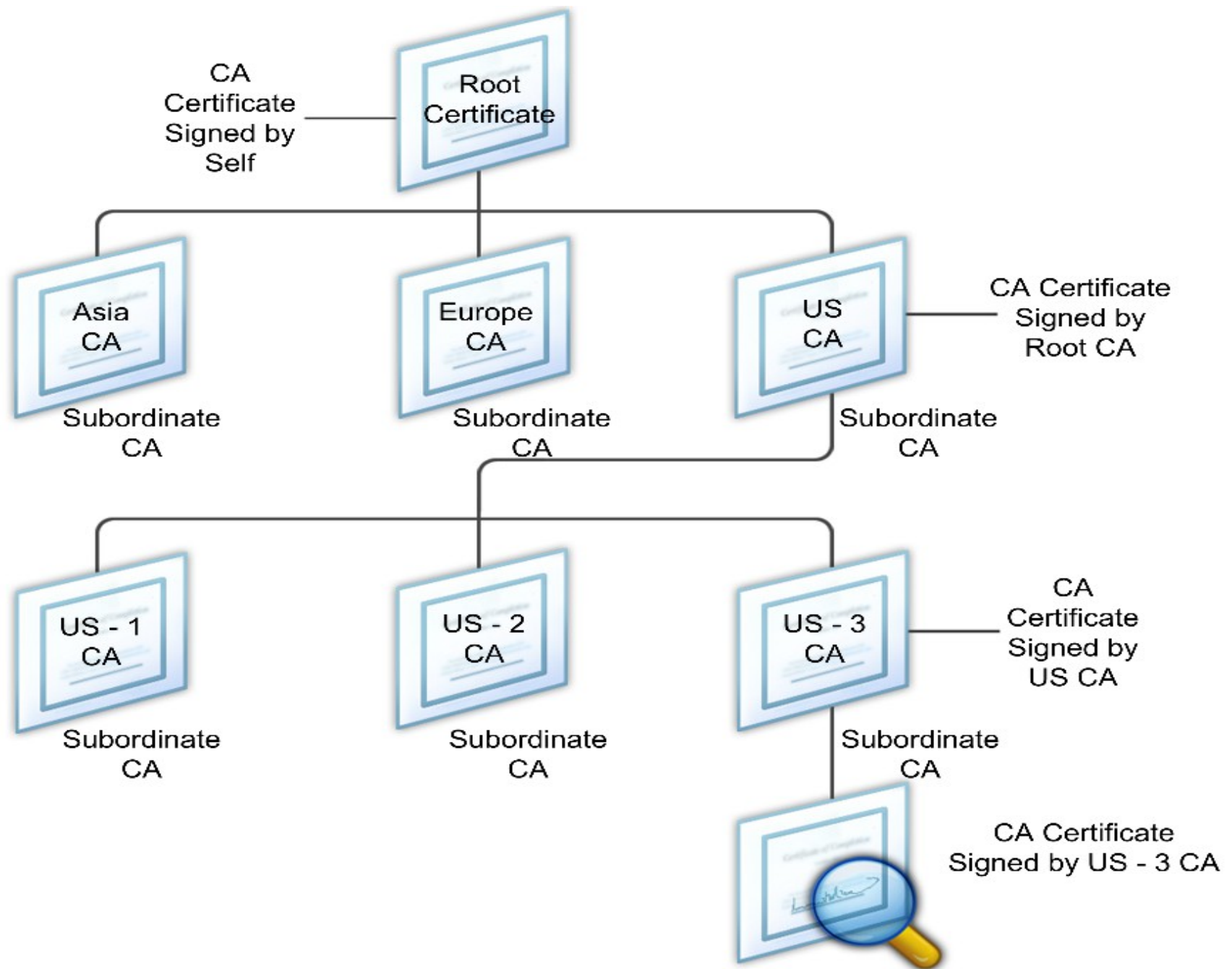
- Certificate Authority: Verisign
- Owner name: jeff PILLOU
- Email: webmaster@commentcamarche.net
- Validity: 04/10/2001 to 04/10/2002
- Public key: 1a:5b:c3:a5:32:4c:d6:df:42
- Algorithm: RC5

Signature

3b:c5:cF:d6:9a:Bd:e3:c6







Verifying Certificates

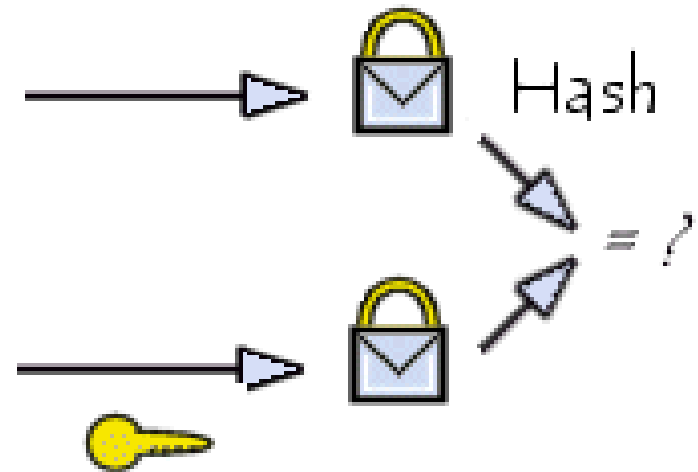
Certificate

Data

- Certificate Authority: Verisign
- Owner name: jeff PILLOU
- Email: webmaster@commentcamarche.net
- Validity: 04/10/2001 to 04/10/2002
- Public key: 1a:5b:c3:a5:32:4c:d6:df:42
- Algorithm: RC5

Signature

3b:c5:cF:d6:9a:8d:e3:c6



Decoding with the
certificate authority
public key

Report of incident on 15-MAR-2011

An RA suffered an attack that resulted in a breach of one user account of that specific RA.

This RA account was then used fraudulently to issue 9 certificates (across 7 different domains).

All of these certificates were revoked immediately on discovery.

Monitoring of OCSP responder traffic has not detected any attempted use of these certificates after their revocation.

Fraudulently issued certificates

9 certificates were issued as follows:

Domain: mail.google.com [NOT seen live on the internet]

Serial: 047ECBE9FCA55F7BD09EAE36E10CAE1E

Domain: www.google.com [NOT seen live on the internet]

Serial: 00F5C86AF36162F13A64F54F6DC9587C06

Domain: login.yahoo.com [Seen live on the internet]

Serial: 00D7558FDAF5F1105BB213282B707729A3

Domain: login.yahoo.com [NOT seen live on the internet]

Serial: 392A434F0E07DF1F8AA305DE34E0C229

Domain: login.yahoo.com [NOT seen live on the internet]

Serial: 3E75CED46B693021218830AE86A82A71

<http://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html>

Public Key Infrastructure (PKI)

