

**An Introduction to  
Cryptography and Public Key  
Infrastructure**

# Agenda

---



## Part One:

- Introduction
- Cryptography

## Part Two:

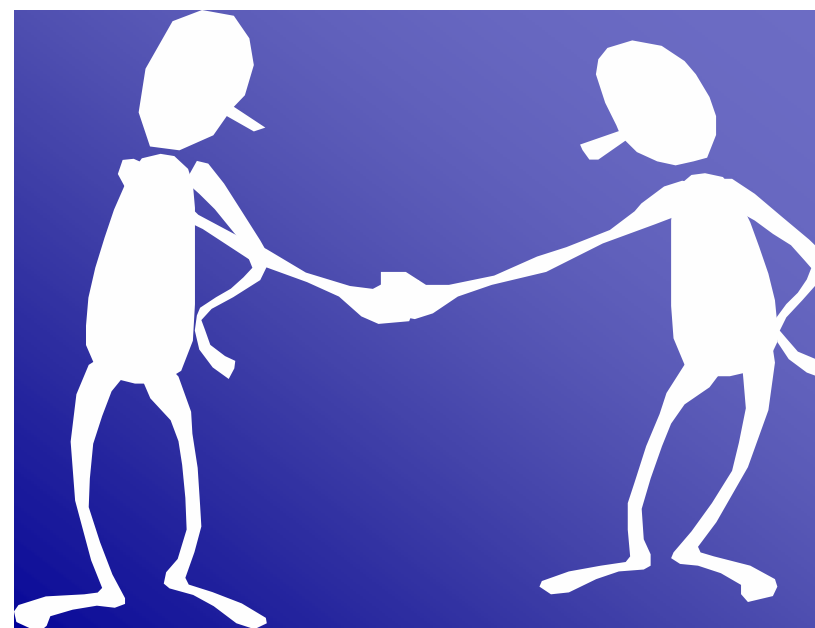
- Public Key Infrastructure
- Digital Certificates



BALTIMORE™  
www.baltimore.com

## Introduction: The problem

How to carry the trust which we have in the paper based world into the realm of electronic business?



[www.baltimore.com](http://www.baltimore.com) the global leader in e|security

## Paper based trust

---



### In the paper based society, we:

- Wrote a letter and signed it
- Perhaps a witness verified that our signature was authentic
- Put the letter in an envelope and sealed it
- Perhaps sent it by certified mail

## Paper based trust

---



### This gave the recipient confidence that:

- The contents had not been read by anyone else
- The contents of the envelope were intact
- The letter came from the person who claimed to have sent it
- The person who sent it could not easily deny having sent it



BALTIMORE™  
www.baltimore.com

## The 4 cornerstones

---

### Confidence . . .

- . . . in the identity of an individual or application  
**AUTHENTICATION**
- . . . that information can be kept private  
**CONFIDENTIALITY**
- . . . that information cannot be manipulated  
**INTEGRITY**
- . . . that information cannot be disowned  
**NON-REPUDIATION**

# Basic Cryptography - Agenda



BALTIMORE™  
www.baltimore.com

- Symmetric & Asymmetric Cryptography
- One way hashing
- How the 4 cornerstones of trust are achieved
- Algorithms and keys
- The need for certificates



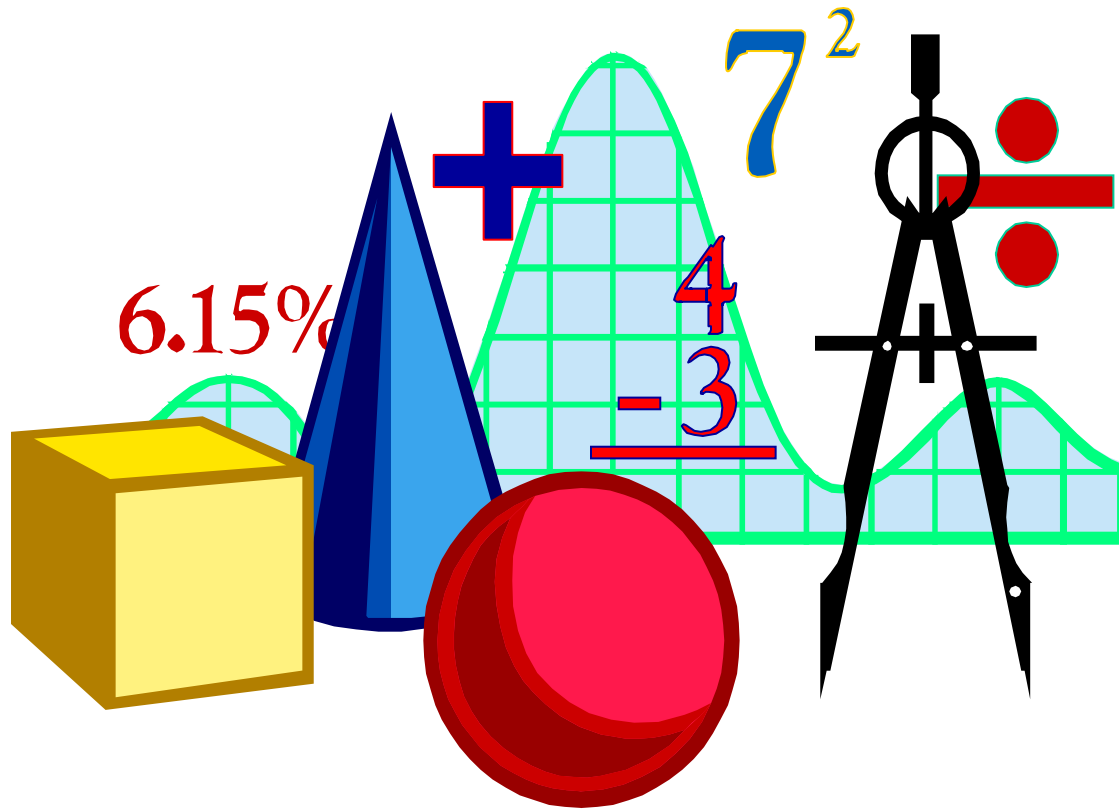
## Basic Encryption concepts

- **Encryption** is the process of turning **plaintext** into **ciphertext**
- **Decryption** is the process of turning **ciphertext** into **plaintext**
- **Encryption / decryption** requires:  
An **algorithm** and a **key**
- Two "cipher " types:  
**Symmetric** and **Asymmetric**



BALTIMORE™  
www.baltimore.com

## The Tools of the Trade



- Integer Mathematics
- Large Prime Numbers
- Pseudo-Random Numbers
- Modular Arithmetic
- Group Theory
- XOR
- Substitution tables



# Symmetric Cryptography

## Encrypting

A shared key



To: The Bank  
From: Tom Jones  
Date: 31 Dec 99  
  
Please transfer  
One Million Dollars  
from account 1234567  
to account 7654321,  
TomJones

+



+



\*> \*qI3\*UY  
#~00873/JDI  
c4(DH: IWB(883  
  
LKS9UI29as9eeasdoFi  
qw9vijhas9djerhp7goe.>  
(\*Y23k^wbvlqkwcYw83  
zqw-\_89237xGyjdc  
Biskdue di7@94

## Decrypting:

is required

\*> \*qI3\*UY  
#~00873/JDI  
c4(DH: IWB(883  
  
LKS9UI29as9eeasdoFi  
qw9vijhas9djerhp7goe.>  
(\*Y23k^wbvlqkwcYw83  
zqw-\_89237xGyjdc  
Biskdue di7@94

+



+



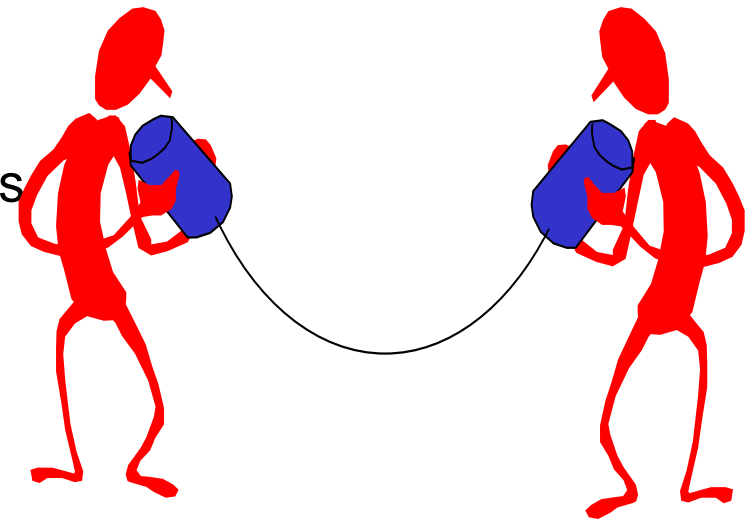
To: The Bank  
From: Tom Jones  
Date: 31 Dec 99  
  
Please transfer  
One Million Dollars  
from account 1234567  
to account 7654321,  
TomJones



# Symmetric Cryptography

## Characteristics

- **Performance:**  
Fast and safe  
provided the key is strong
- **Key Management:**  
Not practical for large numbers of users  
(shared key)
- **Useful for:**
  - Fast Encryption / Decryption
- **Examples:**
  - DES, IDEA, Red Pike, RC2,  
RC4





# Asymmetric Cryptography

No shared secret.

Two keys are created at the same time –

A public key



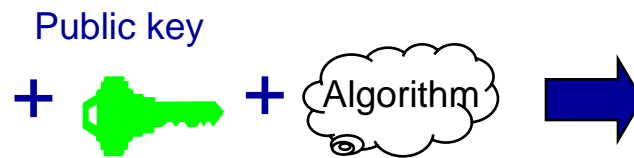
A private key



called a keypair

Encrypting:

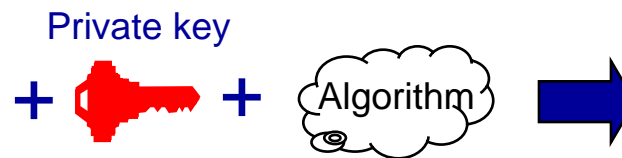
To: The Bank  
From: Tom Jones  
Date: 31 Dec 99  
  
Please transfer  
One Million Dollars  
from account 1234567  
to account 7654321,  
TomJones



\*> \*qI3\*UY  
#~00873/JDI  
c4(DH: IWB(883  
  
LKS9UI29as9eeasdoFi  
qw9vijhas9djerhp7goe.>  
(\*Y23k^wblqkwcYw83  
zqw-\_89237xGyjdc  
Biskdue di7@94

Decrypting:

\*> \*qI3\*UY  
#~00873/JDI  
c4(DH: IWB(883  
  
LKS9UI29as9eeasdoFi  
qw9vijhas9djerhp7goe.>  
(\*Y23k^wblqkwcYw83  
zqw-\_89237xGyjdc  
Biskdue di7@94



To: The Bank  
From: Tom Jones  
Date: 31 Dec 99  
  
Please transfer  
One Million Dollars  
from account 1234567  
to account 7654321,  
TomJones



# Asymmetric Cryptography

Asymmetric cryptography is also known as **Public Key Cryptography**

- Public key is made public
- Private key is kept private (usually never leaves the place where it was generated)
- If private key is used to encrypt then **only** public key can decrypt
- If public key is used to encrypt then **only** private key can decrypt

# Asymmetric Cryptography

---



## About the keypair:

- Mathematically related
- Derived from very, very, very large prime numbers
- Infeasible to determine one knowing the other
- Keys come in different strengths

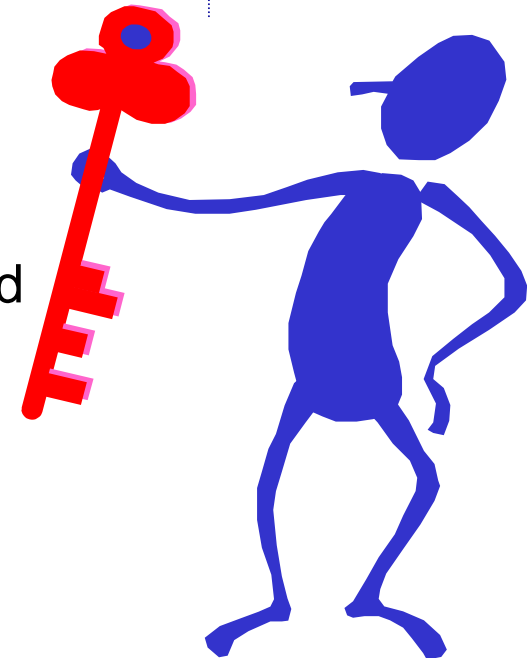


BALTIMORE™  
www.baltimore.com

# Asymmetric Cryptography

## Characteristics

- **Performance:**  
Slower - not practical for bulk encryption
- **Key Management:**  
Public key can be widely and openly distributed
- **Useful for:**
  - Encryption
  - Signing/Verifying
  - Key Exchange
- **Examples:**
  - RSA, ECC, Diffie-Hellman, DSA



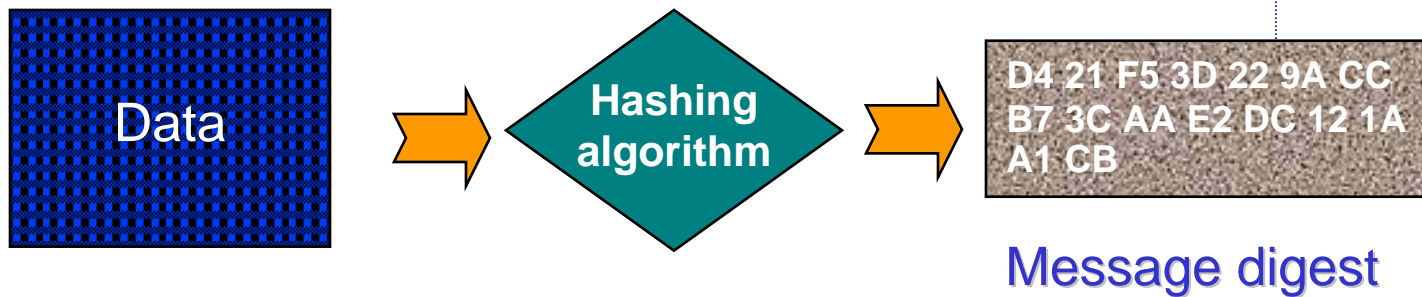


## One Way Hash

---

- A **hash** is produced by putting data through a **hashing algorithm**
- The result is a fixed length “**fingerprint**” of the data, usually 128 or 160 bits. Same size output for any size input.
- Like a CRC, but much more sophisticated
- Used to determine if data has changed - possibly maliciously
- Infeasible to produce a document which matches a digest
- A one-bit change in the message affects at least half the bits in the digest

# A One Way Hash



## Characteristics

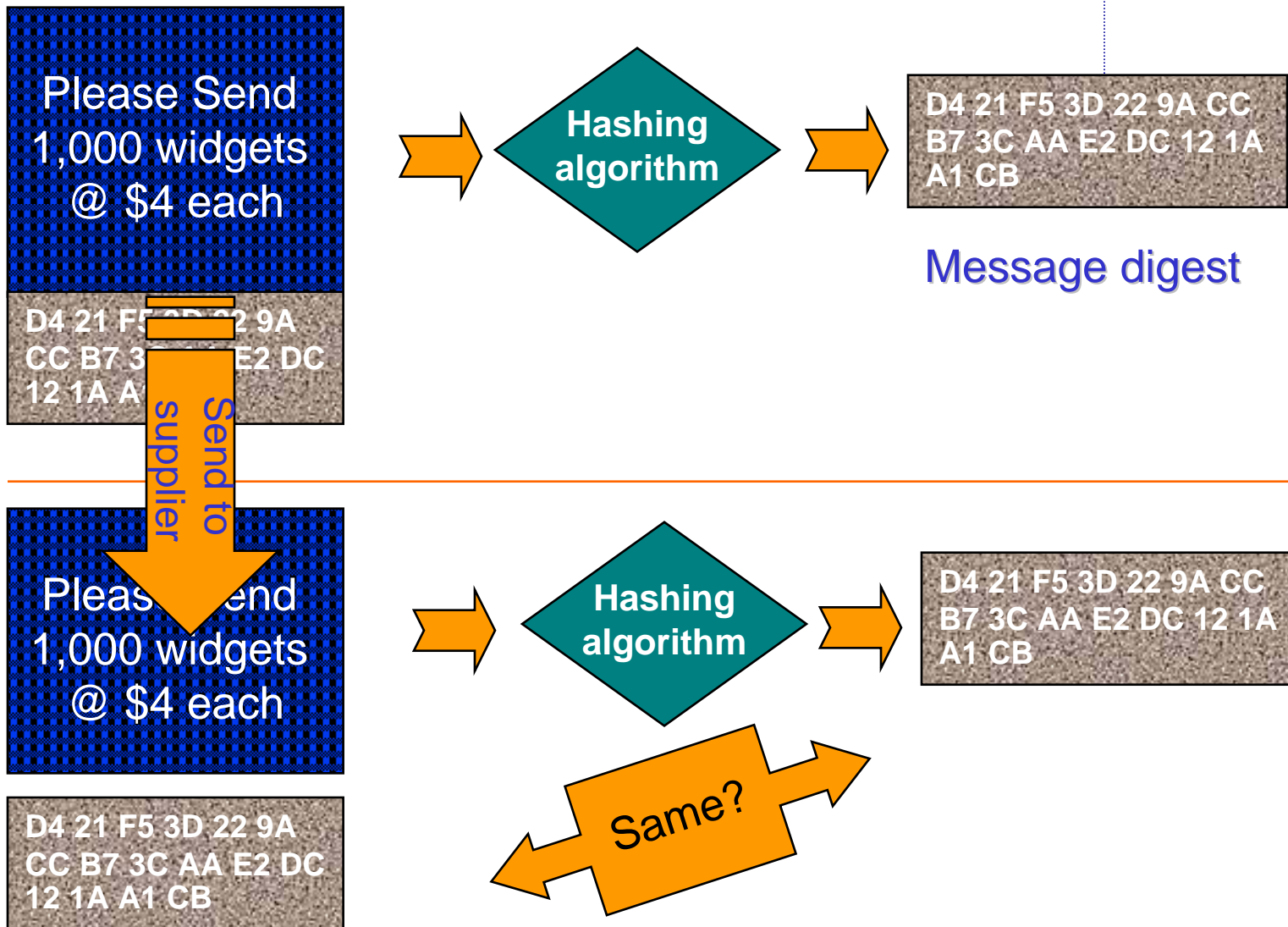
- No Key
- Irreversible
- Examples:
  - MD5, SHA-1

## Public Key cryptography uses hashes (digests)

- To do integrity checks
- To produce digital signatures

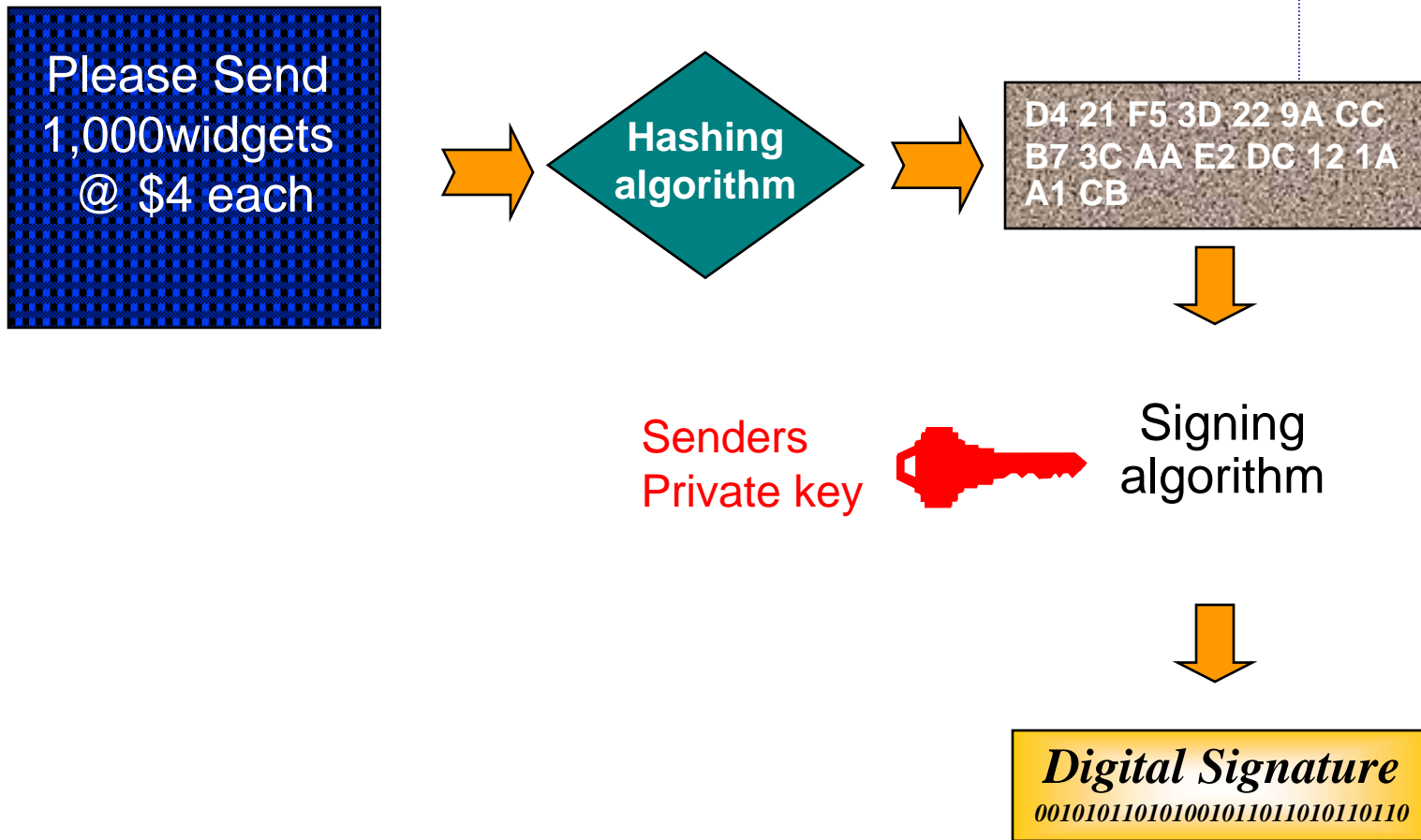


# One Way Hash - Integrity





# One Way Hash - Digital signature



Alice



Public key



Private key



Bob's Public key



Randomly Generated Symmetric Key (seed + PRNG)

Bob



Public key



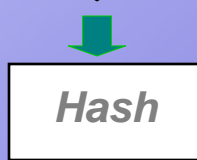
Private key



Alice's Public key

# Securing a message

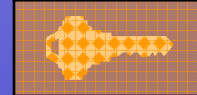
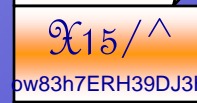
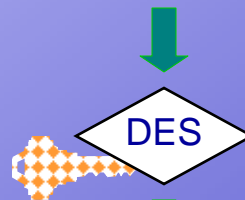
Signing the message:



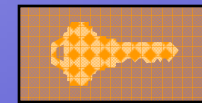
Alice's Digital Signature



Encrypting the message:



Encrypting the session key:



Alice



Public key



Private key



Bob's Public key



Randomly Generated Symmetric Key (seed + PRNG)

Bob



Public key



Private key



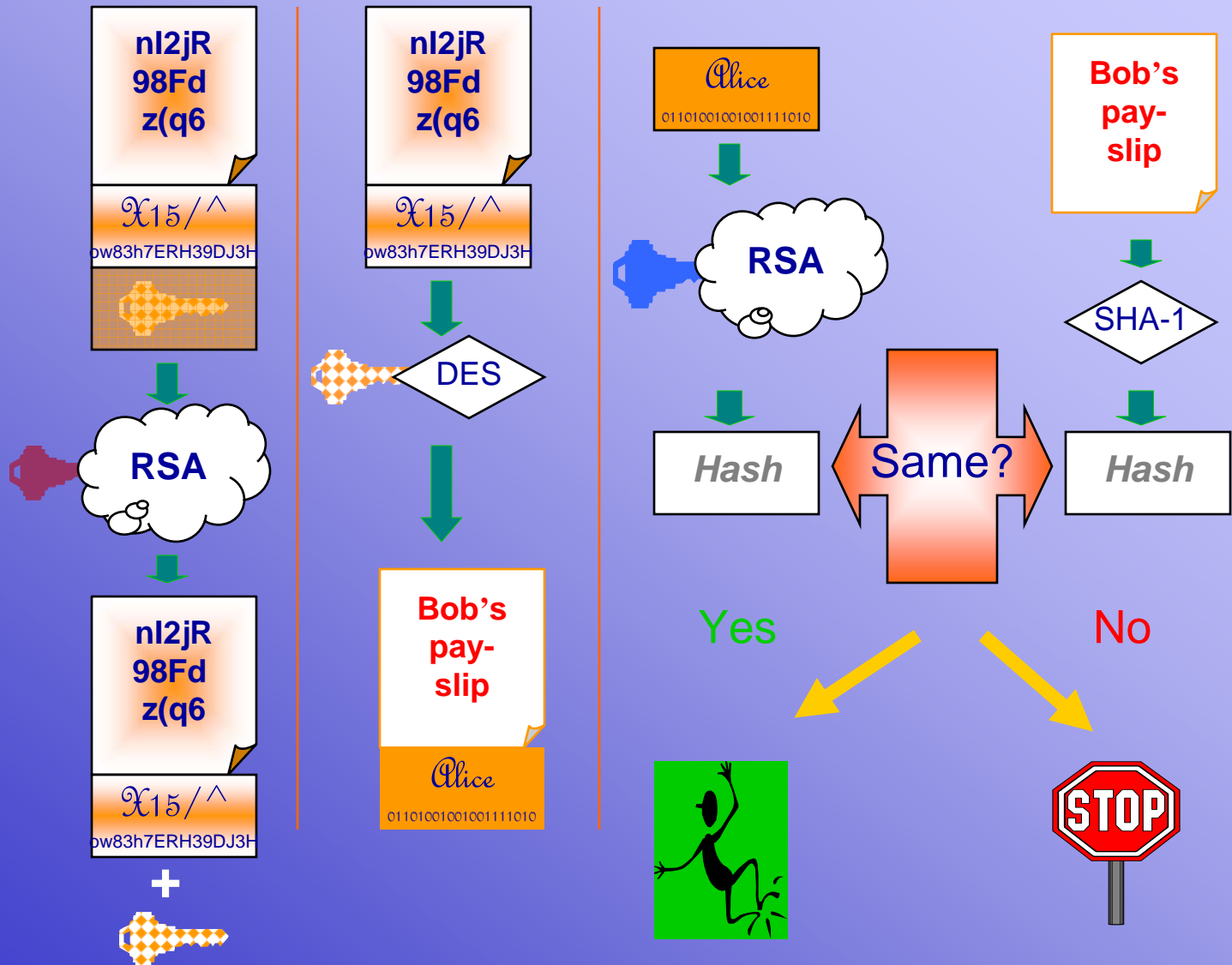
Alice's Public key

# Desecuring a message

Decrypting the session key:

Decrypting the message:

Verifying signature and message integrity:



## Four simple rules

---

- Sign First, then Encrypt
- Compress before Encrypting
- Sign using your Private Key
- Encrypt using Receiver's Public Key

# Algorithms

---



- **Symmetric key algorithms:**
  - **DES**
  - Triple-DES
  - IDEA
  - RC2, RC4
- **Asymmetric key algorithms:**
  - RSA
  - DSA
  - ECC Elliptic Curve Crypto Signing algorithms
  - Diffie-Hellman

# Hash algorithms & RNGs

---

- **Common hash algorithms:**
  - MD5 (128-bit digest)
  - SHA-1 (160-bit digest)
  - RIPE-MD (128-bit and 160-bit Versions)
- **Random number generators:**  
**Blum-Blum-Shub**



**BALTIMORE**  
www.baltimore.com

## Key size is vital

**Key Size = Strength**

	1995	2000	2005
40 bits	<b>68 seconds</b>	<b>8.6 seconds</b>	<b>1.07 seconds</b>
56 bits	<b>7.4 weeks</b>	<b>6.5 days</b>	<b>19 hours</b>
64 bits	<b>36.7 years</b>	<b>6.9 years</b>	<b>4.6 years</b>
128 bits	<b>6.7e 17 millenia</b>	<b>8.4e 16 millenia</b>	<b>1.1e 16 millenia</b>



## Secure storage of Private Keys



- File based storage:  
Using passphrase-based encryption
- Smartcard storage
- Hardware Security Module (HSM) storage

# Cryptography: Further Reading



BALTIMORE™  
www.baltimore.com

<i>Publication</i>	<i>Author/Source</i>
• <i>Applied Cryptography.</i>	Bruce Schneier. Wiley Press.
• <i>Answers to Frequently Asked Questions about Today's Cryptography.</i>	RSA. Version 4 Available at WWW.RSA.COM
• <i>Crypto Law Survey</i>	KOOPS : <a href="http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm">http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm</a>
• <i>Architecture for Public Key Infrastructure</i>	The Open Group
• <i>Cryptography &amp; Network Security Principles &amp; Practice (2<sup>nd</sup> Edition)</i>	William Stallings: Prentice Hall

One more problem to solve:



Q. How do we know who the public key belongs to?

A. Digital Certificates!

# Digital Certificates & Public Key Infrastructure

---



## About Certificates

---

- A **Certificate** binds a public key to an owner
- It is the ‘**envelope**’ in which the public key is distributed
- It is usually **signed by a third party**, which has first verified that it contains a valid key and that the owner is who he or she say they are.

# About Certificates

---



## A certificate contains:

- Details about Bob
- Details about the certificate issuer
- Bob's public key
- Validity and Expiration dates
- A digest of the certificate contents. The certificate digest is signed by the CA

# Certificates - Issuing

---



## How Bob gets a certificate:

- Bob's Registration Agent (RA) - or end user software - generates public / private key pair
- Bob's Registration Agent checks Bob's ID
- The Registration Agent sends a certificate request (which contains the public key) to the CA
- CA issues certificate and signs it, then returns it to Bob and publishes his certificate
- Bob's software stores certificate



BALTIMORE™  
www.baltimore.com

## Certificates - Validation

---

**To ensure that Bob's certificate is valid (and hence his public key is valid):**

- Alice gets Bob's certificate
- Alice's software performs the following:
  - Gets certificate of CA that signed his certificate
  - Decrypts Bob's certificate digest using the CA's public key
  - Takes a digest of Bob's certificate
  - Compares the digests
  - Checks the expiration dates in Bob's certificate



BALTIMORE™  
www.baltimore.com

## Certificates - Revocation

---

- **Reasons:**
  - CA Compromise
  - Key Compromise
  - Change of Status
  - Suspension
  - Other
- Certificate Revocation Lists (CRLs) are issued and signed by the CA
- Upon receipt of a Certificate, check the CA's CRL



BALTIMORE™  
www.baltimore.com

## Public Key Cryptography

....but public key cryptography, on its own, is not enough if we are to truly re-create the conditions for traditional paper-based commerce in an electronic world. We also need:

- Security policies to define the rules under which the cryptographic systems should operate
- Products to generate, store and manage the keys
- Procedures to dictate how the keys and certificates should be generated, distributed and used



BALTIMORE™  
www.baltimore.com

## The Components of a PKI

- A **Public Key Infrastructure** is a combination of hardware and software products, policies and procedures.
- It provides the security required to carry out electronic business so that users who do not know each other can communicate securely through a chain of trust.
- **PKI** is based on digital IDs known as “**digital certificates**” which act like “electronic passports”, and bind the user’s digital signature to his or her public key.

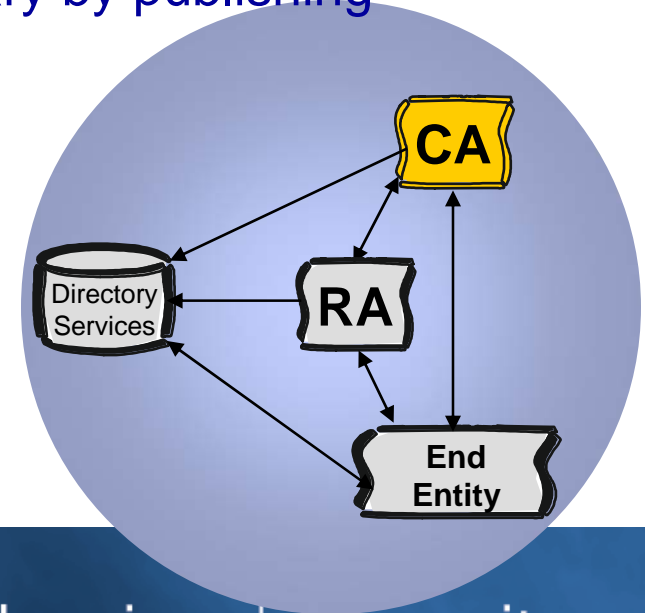


# Certification Authorities

The CA system is the trust basis of a PKI, as it manages public key certificates for their whole life cycle. The CA will:

- Issue certificates by binding the identity of a user or system to a public key with a digital signature
- Schedule expiry dates for certificates
- Ensure certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs)

When implementing a PKI, an organisation can either operate its own CA system, or use the CA service of a **Trusted Third Party**.

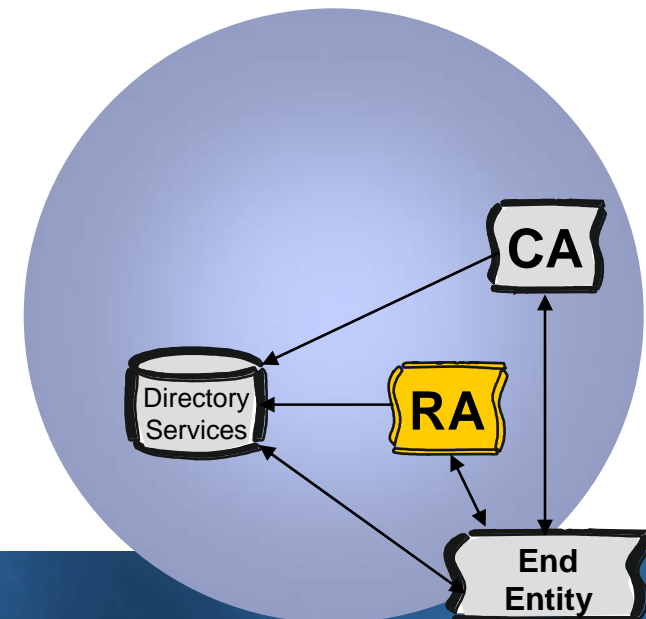




**BALTIMORE**<sup>™</sup>  
www.baltimore.com

## RA- Registration Authorities

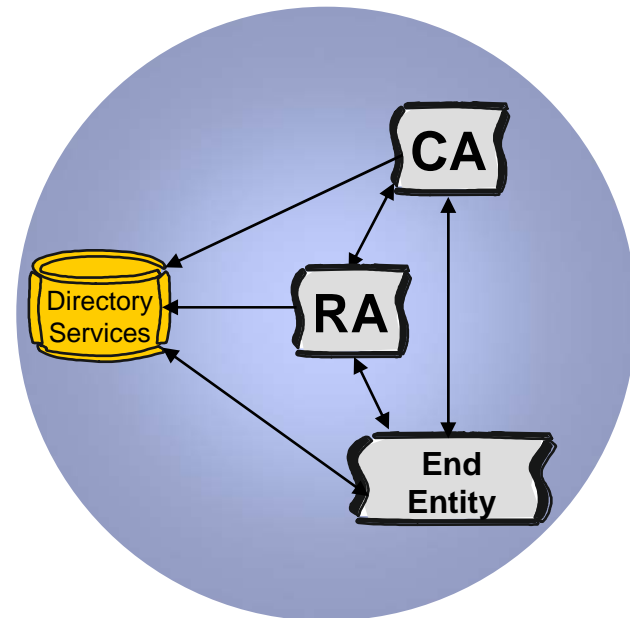
- Interface between CA and end entities
- Identifies end entity
- The quality of this authentication process determines the level of trust that can be placed in the certificates.
- Keep records of end entities





## Directories

- Provide distribution points for certificates and certificate revocation lists
- Can be distributed over networks
- X.500 standard
- (May also be repositories for other information)



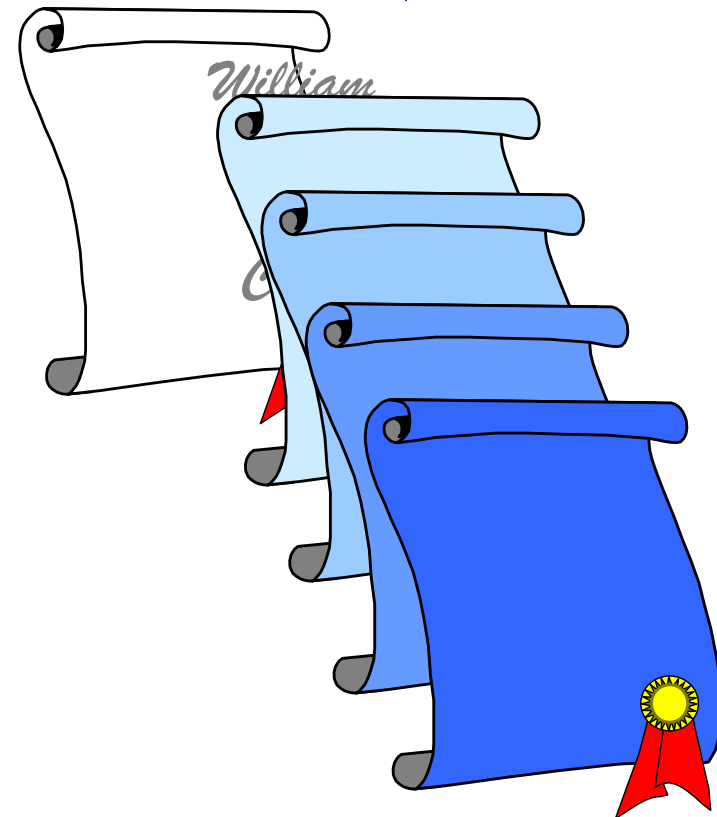
# Certificate Chain

---



BALTIMORE™  
www.baltimore.com

- Your Cert is signed by your CA
- Your CA's Cert is signed by its CA
- ...and so on
- “Chain of Certificates”
- Last certificate is self-signed by Root CA
- Not usually this long!



## Current trends in PKI

---



- Government controls & CA regulation
- Digital signature legislation
- Key escrow

# Emerging Government Controls on Cryptography

---



- Relaxation of export controls over stronger cryptography
- Move towards more commercially acceptable arrangements
- Voluntary licensing of Certification Authorities
- Access to keys under warrant for Law enforcement  
OR enforced decryption of cipher text



## Key Escrow

---

- Use of strong cryptography is a concern for both Law Enforcement Agencies and National Security Agencies
- These agencies are promoting the concept of key escrow:
  - Involves the back-up of encryption keys with Trusted Third Parties
  - Keys released to government agencies upon obtaining a warrant



BALTIMORE™  
www.baltimore.com

## Key Escrow Vs. Key Archive

- **Key Escrow** originally favoured by governments as means of:
  - controlling use of stronger cryptography
  - enabling, under warrant, decryption of cipher text
- **Key Archive** is a business requirement enabling organisations primarily to recover from:
  - loss of keys
  - forgetting passwords
  - departure of key individuals

## BTW - Separate keypairs

---



- **The problem:**
  - Backing up private keys without losing non-repudiation
- **The answer:**
  - Separate keypairs for encryption and signing
  - Archive the encryption private key, but never the signing private key.

# Conclusion

---



- **Symmetric cryptographic** systems are secure provided the key is sufficiently long and secure
- The future of electronic commerce depends upon the ability to create **trust** between people that don't know each other
- **Asymmetric cryptographic** systems provide a range of services which will enable secured electronic commerce
- Once implemented, and operated correctly, **PKIs** will provide enterprises with security services needed to exploit technology securely

“

*Given the growing importance of public key cryptography to many applications from e-mail to electronic commerce, a PKI is probably the most critical information security investment a company will make in the next three years.*

”

Ira Machefsky, Giga Group