Web Server Management: Securing Access to Web Servers

Jon Warbrick
University of Cambridge Computing Service

Introduction

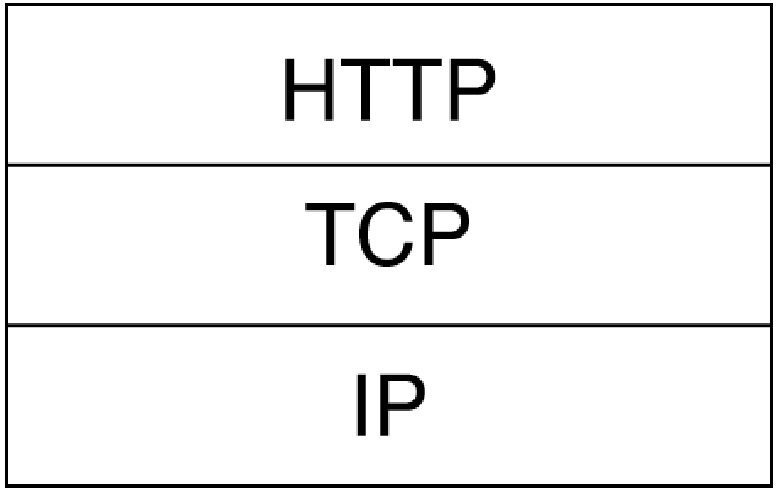
- Course Outline

Introduction

- Course Outline
- What is HTTPS?

Introduction

- Course Outline
- What is HTTPS?



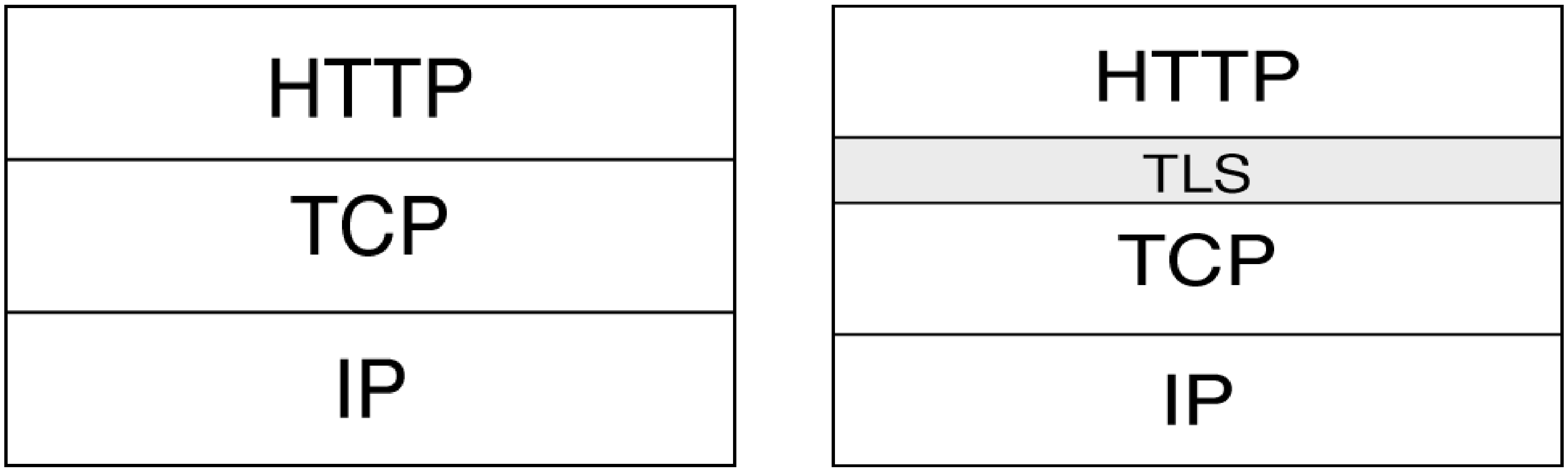
HTTP

TCP

IP

Introduction

- Course Outline
- What is HTTPS?



What does HTTPS give you?

- Client-server, end-to-end encrypted traffic

What does HTTPS give you?

- Client-server, end-to-end encrypted traffic
- Message Integrity

What does HTTPS give you?

- Client-server, end-to-end encrypted traffic
- Message Integrity
- Authentication of the server

What does HTTPS give you?

- Client-server, end-to-end encrypted traffic
- Message Integrity
- Authentication of the server
- *(optional)* Authentication of the browser user

A warning about security

- "Security is a process, not a product"

A warning about security

- "Security is a process, not a product"
- TLS protects data in transmission

A warning about security

- "Security is a process, not a product"
- TLS protects data in transmission
  - What happens after it's received?

A warning about security

- "Security is a process, not a product"
- TLS protects data in transmission
  - What happens after it's received?
  - .. or before it's sent?

A warning about security

- "Security is a process, not a product"
- TLS protects data in transmission
  - What happens after it's received?
  - .. or before it's sent?
  - Is the webserver secure from attack?

A warning about security

- "Security is a process, not a product"
- TLS protects data in transmission
  - What happens after it's received?
  - .. or before it's sent?
  - Is the webserver secure from attack?
  - Is the webserver physically secure?

A warning about security

- "Security is a process, not a product"
- TLS protects data in transmission
  - What happens after it's received?
  - .. or before it's sent?
  - Is the webserver secure from attack?
  - Is the webserver physically secure?
- Legal requirements (DPA, RIPA)

Politics

- Patents

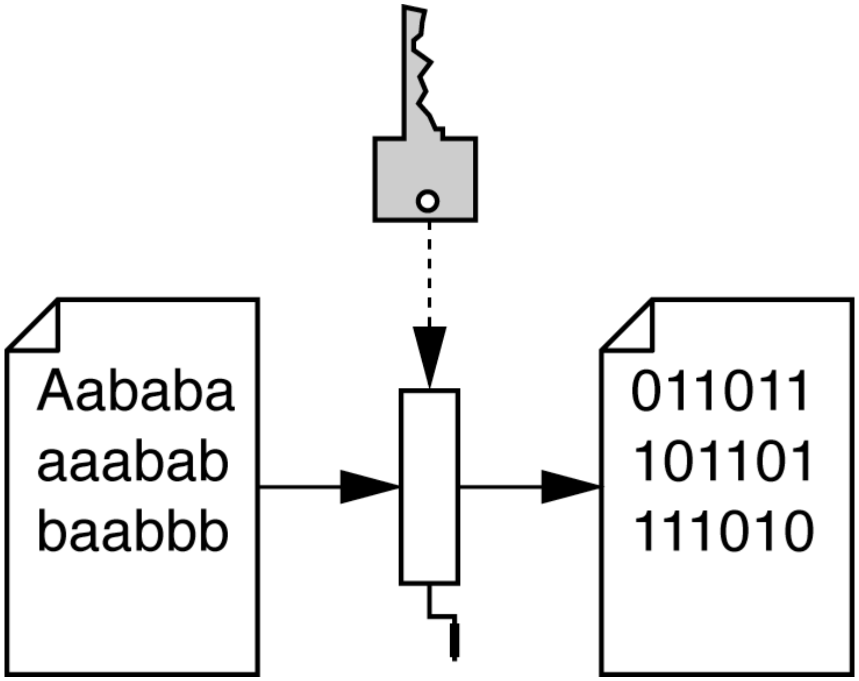
Politics

- Patents
- Munitions

A Crash Course in Cryptography

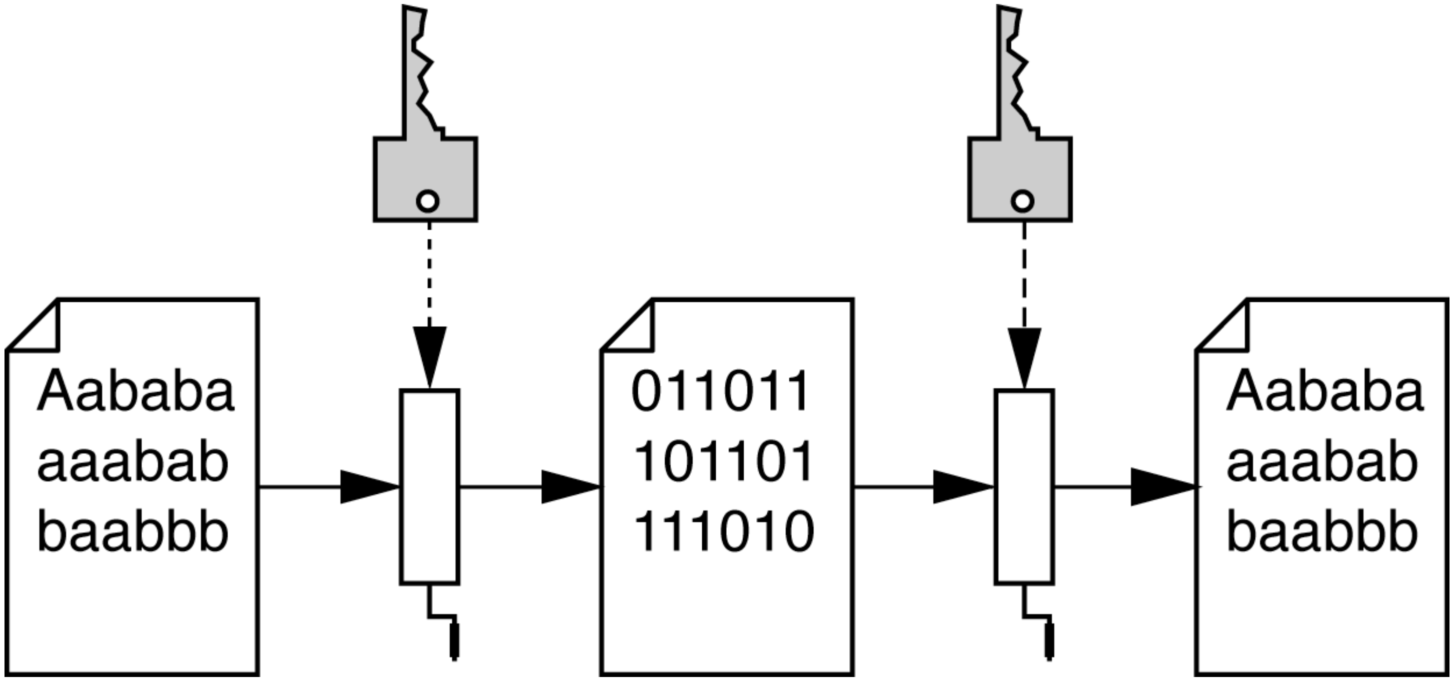
A Crash Course in Cryptography

- Symmetric ciphers



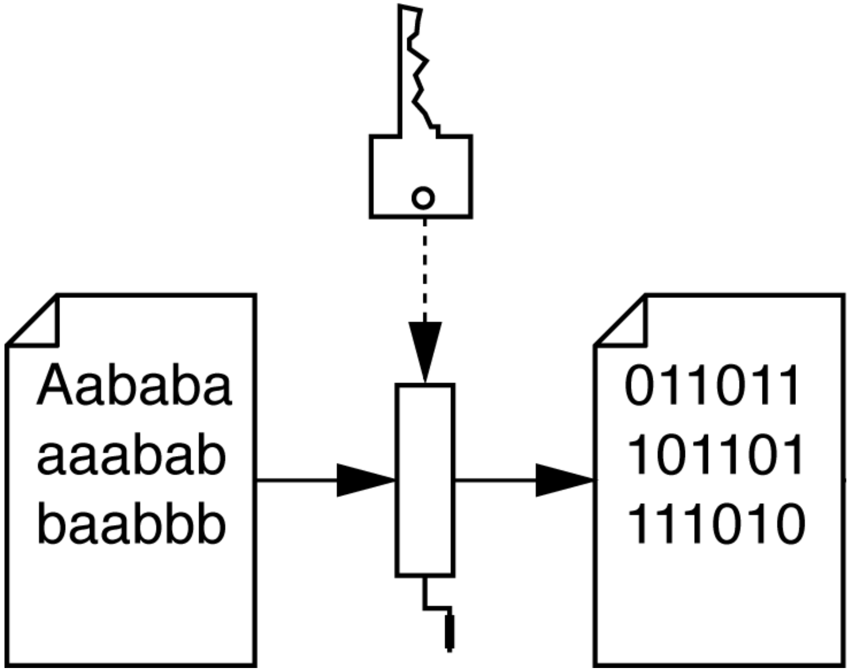
A Crash Course in Cryptography

- Symmetric ciphers



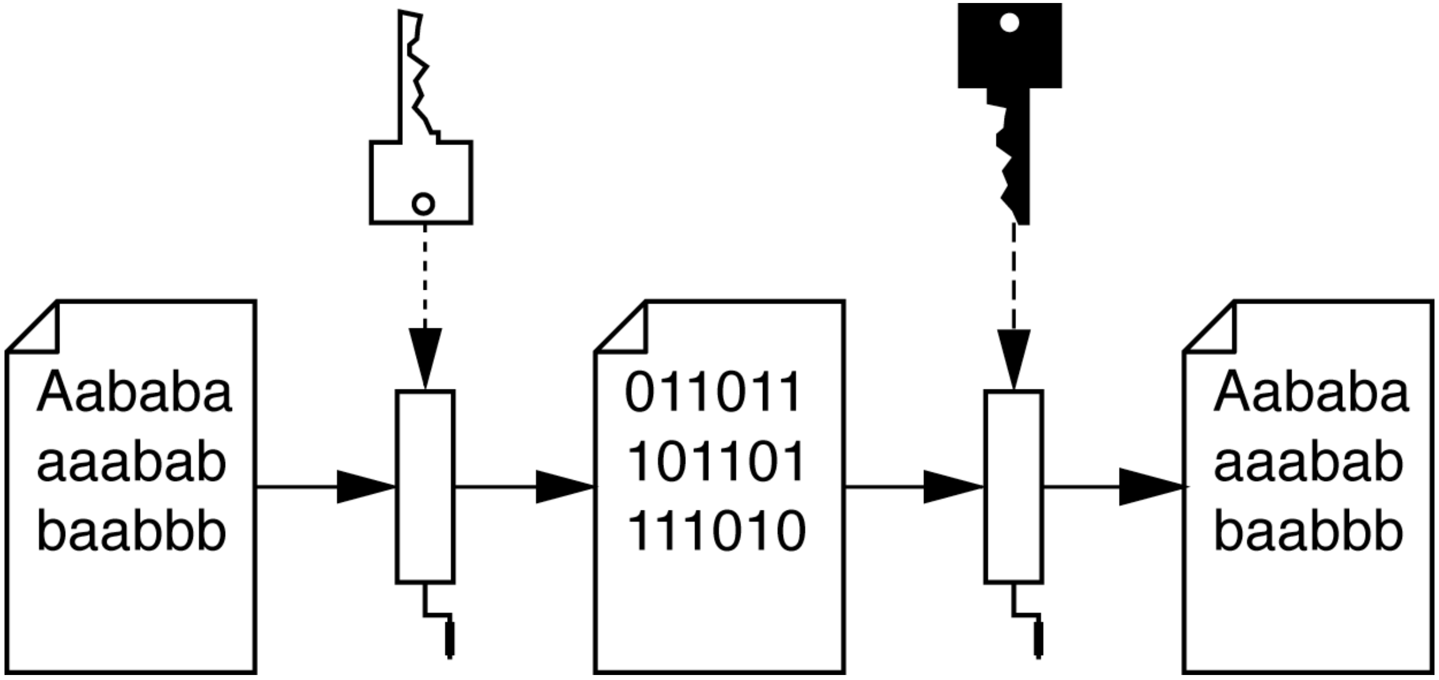
A Crash Course in Cryptography (2)

- Public-key ciphers



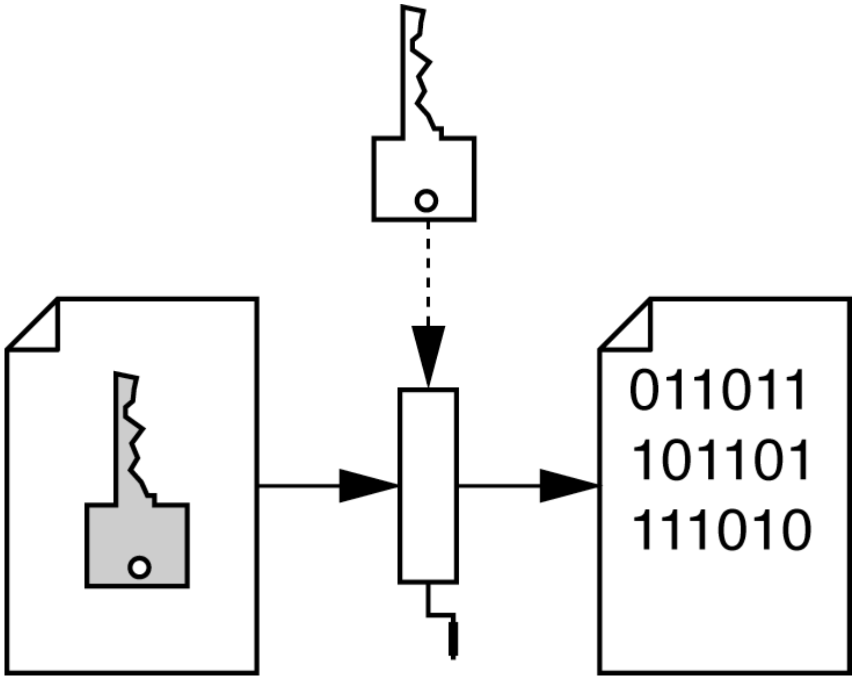
A Crash Course in Cryptography (2)

- Public-key ciphers



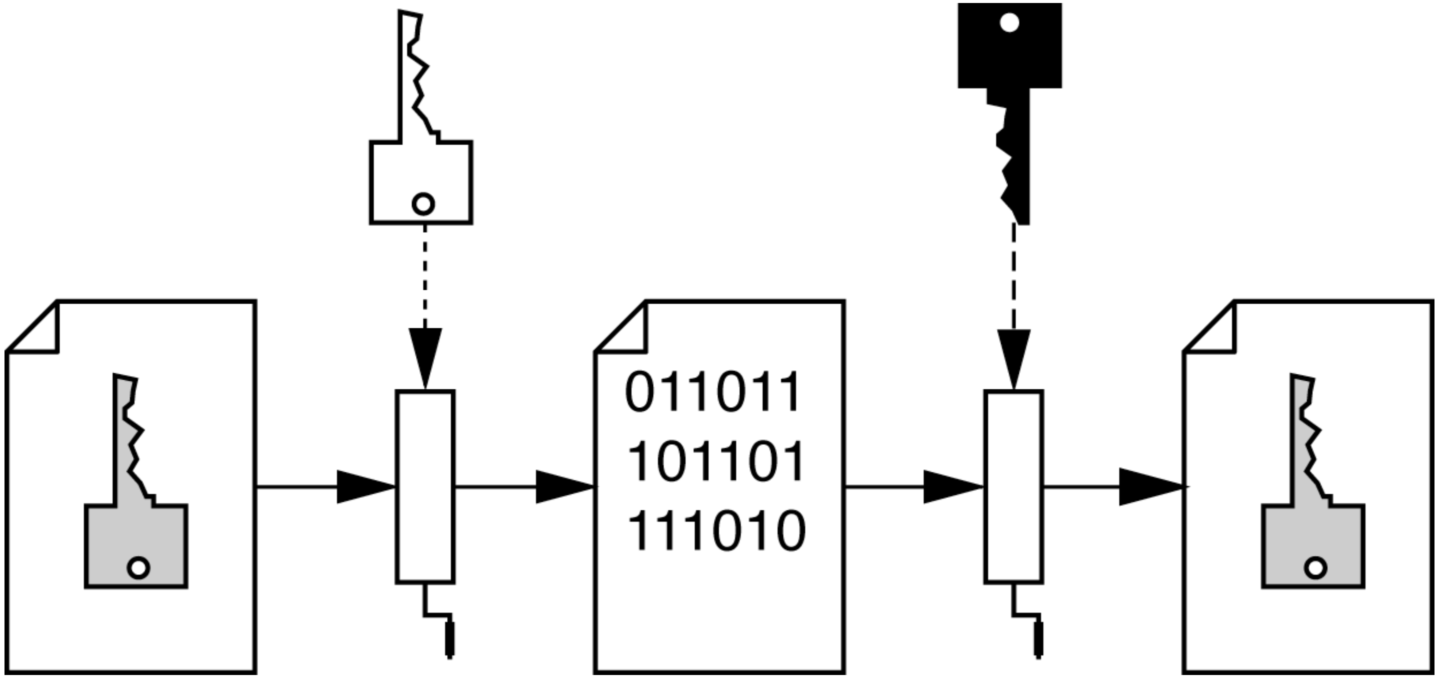
A Crash Course in Cryptography (3)

- Key Exchange



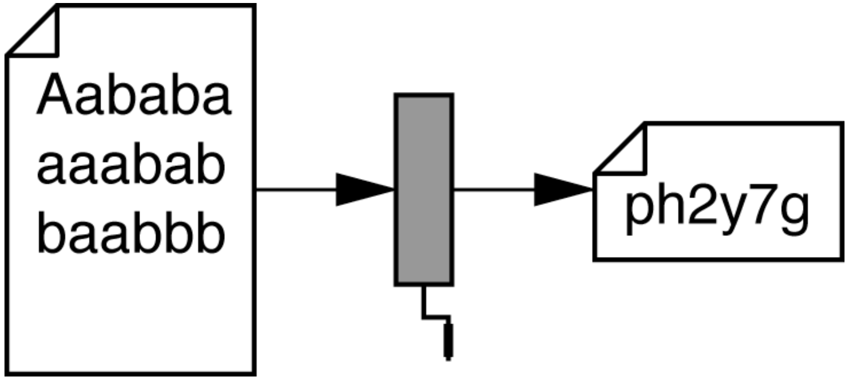
A Crash Course in Cryptography (3)

- Key Exchange



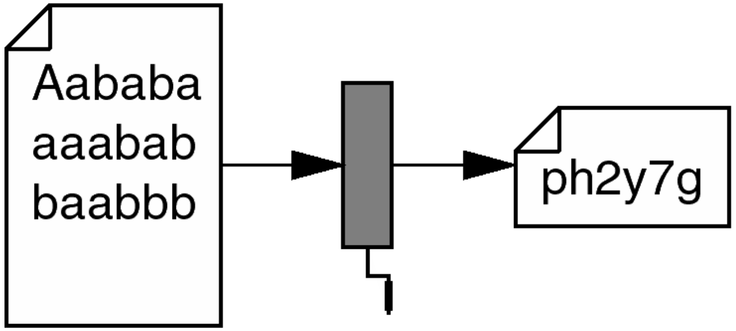
A Crash Course in Cryptography (4)

- Message digests



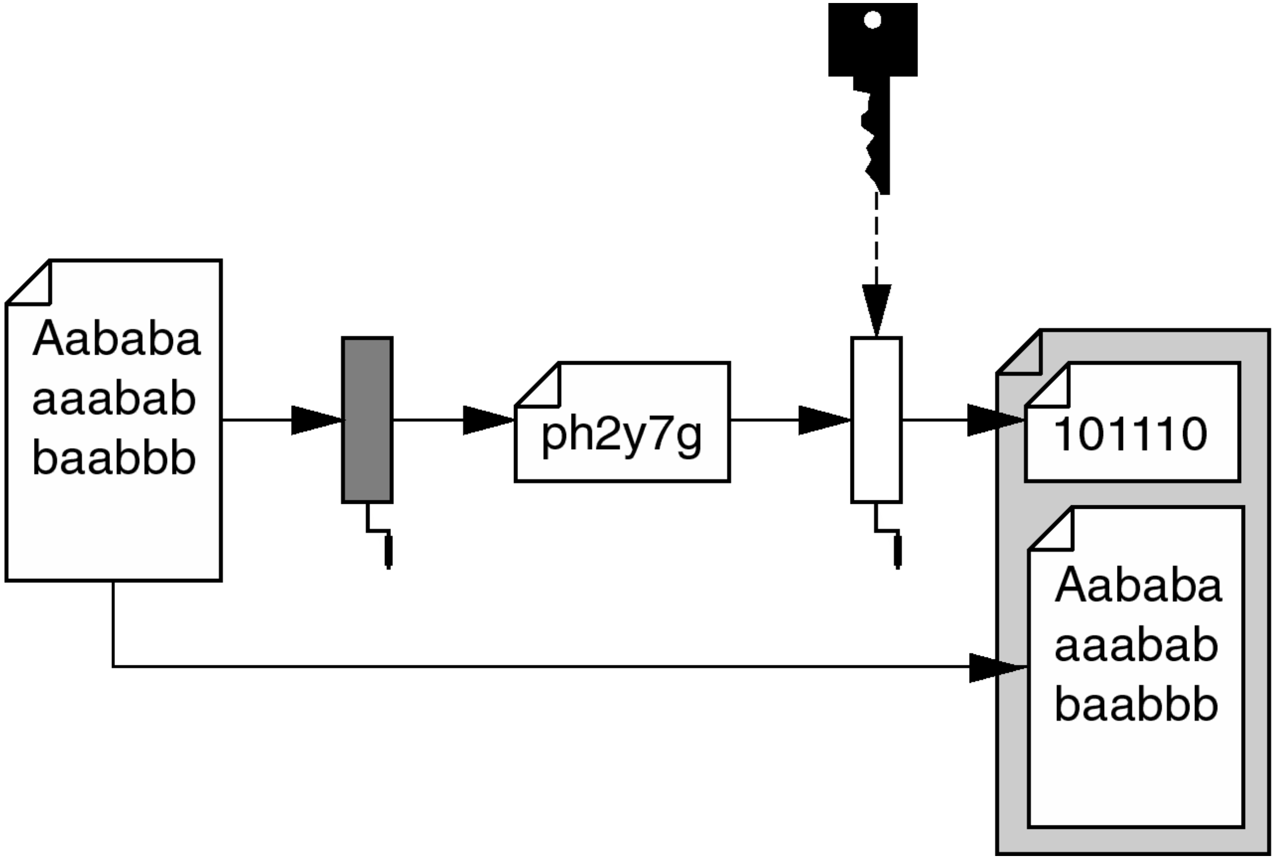
A Crash Course in Cryptography (5)

- Digital signatures



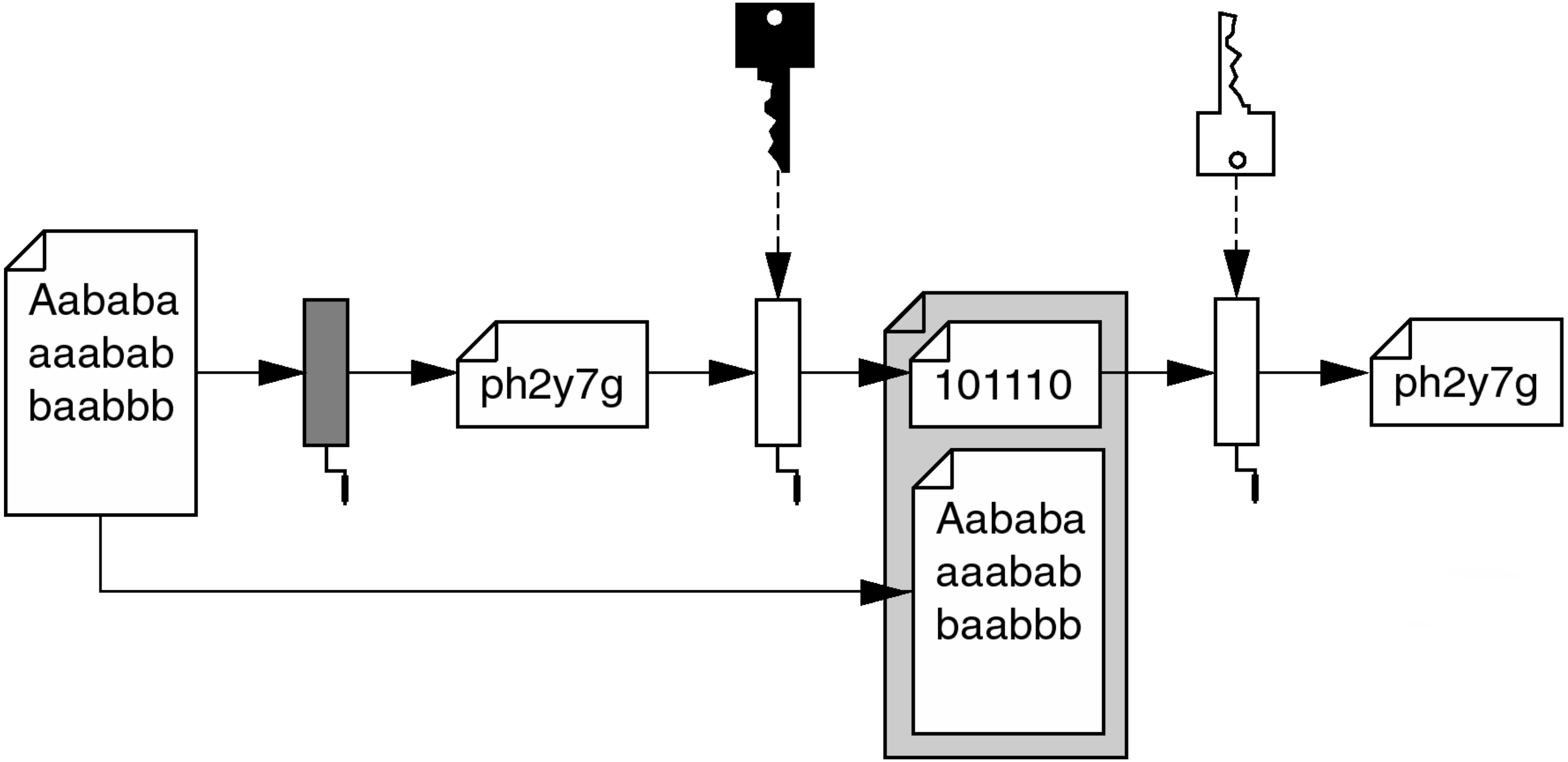
A Crash Course in Cryptography (5)

- Digital signatures



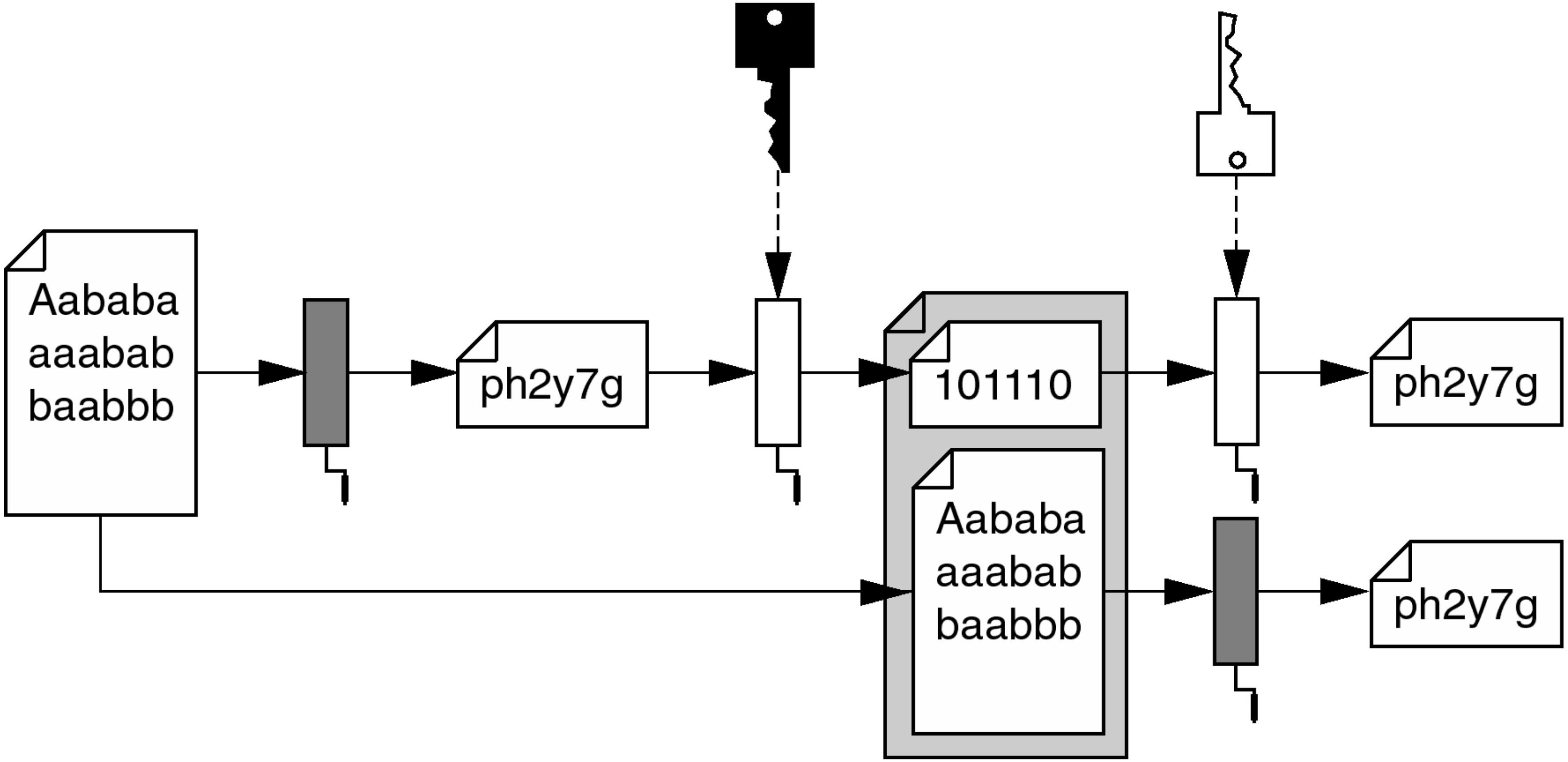
A Crash Course in Cryptography (5)

- Digital signatures



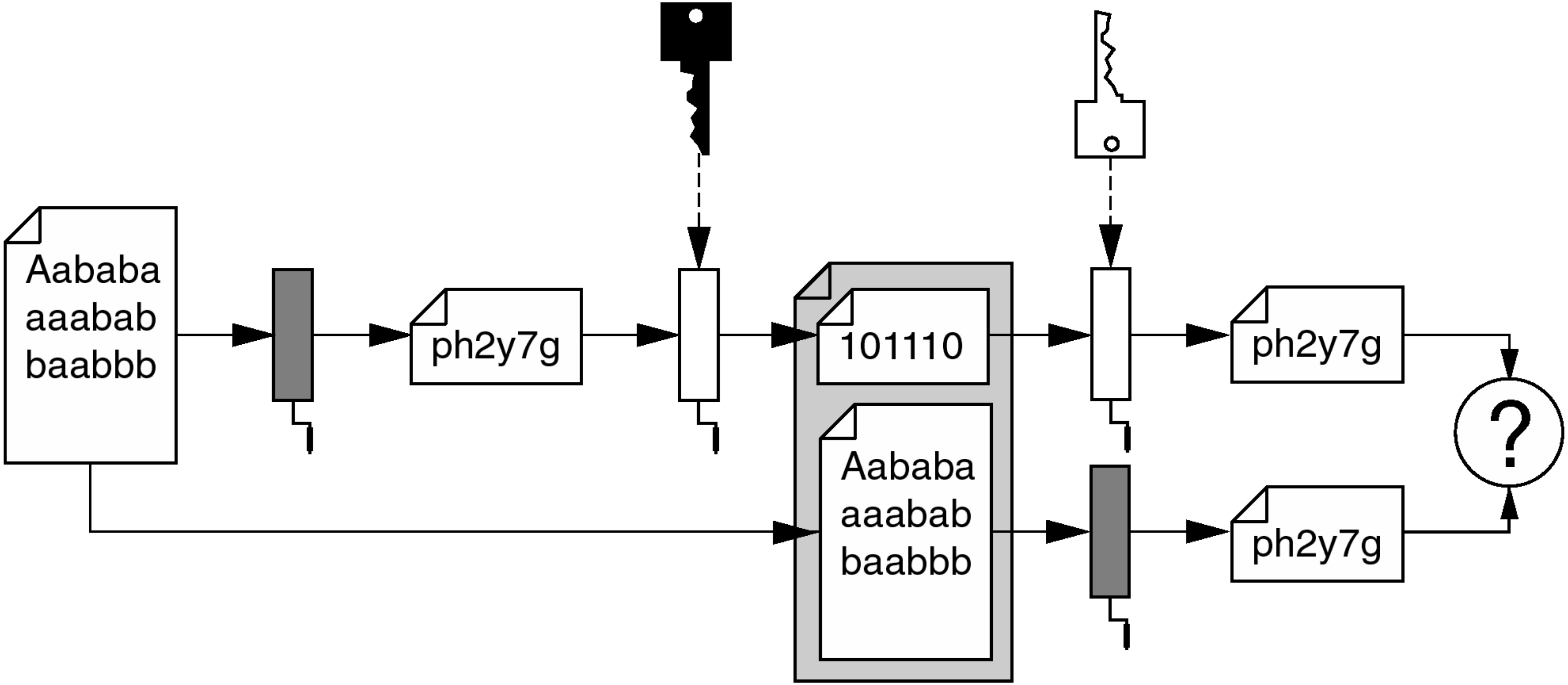
A Crash Course in Cryptography (5)

- Digital signatures



A Crash Course in Cryptography (5)

- Digital signatures



A Crash Course in Cryptography (6)

- Public key certificates

A Crash Course in Cryptography (6)

- Public key certificates
- Certification authorities

A Crash Course in Cryptography (6)

- Public key certificates
- Certification authorities
  - UCS Certificate scheme

A Crash Course in Cryptography (6)

- Public key certificates
- Certification authorities
  - UCS Certificate scheme
- PKI

The SSL Process

- Browser contacts server

The SSL Process

- Browser contacts server
- Client & server agree ciphers, protocols, etc.

The SSL Process

- Browser contacts server
- Client & server agree ciphers, protocols, etc.
- Server sends its certificate to the client

The SSL Process

- Browser contacts server
- Client & server agree ciphers, protocols, etc.
- Server sends its certificate to the client
- Client verifies the server's certificate

The SSL Process

- Browser contacts server
- Client & server agree ciphers, protocols, etc.
- Server sends its certificate to the client
- Client verifies the server's certificate
- Client sends a secret using server's public key

The SSL Process (2)

- Client & server create symmetric keys

The SSL Process (2)

- Client & server create symmetric keys
- Client & server switch to the agreed cipher

The SSL Process (2)

- Client & server create symmetric keys
- Client & server switch to the agreed cipher
- Sequence numbers and hashes protect against tampering

The downside of using HTTPS

- No caching of documents

The downside of using HTTPS

- No caching of documents
- Overheads on client and server

The downside of using HTTPS

- No caching of documents
- Overheads on client and server
- Firewalls may not allow HTTPS traffic

The downside of using HTTPS

- No caching of documents
- Overheads on client and server
- Firewalls may not allow HTTPS traffic
- £££ Cost

The downside of using HTTPS

- No caching of documents
- Overheads on client and server
- Firewalls may not allow HTTPS traffic
- £££ Cost
- Search Engines

Creating Keys and Certificates

OpenSSL

- Used by most Unix and some Windows systems

OpenSSL

- Used by most Unix and some Windows systems
  - Cryptographic library

OpenSSL

- Used by most Unix and some Windows systems
  - Cryptographic library
  - Command-line utilities

OpenSSL

- Used by most Unix and some Windows systems
  - Cryptographic library
  - Command-line utilities
- Pre-built packages for RedHat, Fedora, SuSE, Debian, Solaris. Windows executables can be found

OpenSSL

- Used by most Unix and some Windows systems
  - Cryptographic library
  - Command-line utilities
- Pre-built packages for RedHat, Fedora, SuSE, Debian, Solaris. Windows executables can be found
- ... or build your own

OpenSSL

- Used by most Unix and some Windows systems
  - Cryptographic library
  - Command-line utilities
- Pre-built packages for RedHat, Fedora, SuSE, Debian, Solaris. Windows executables can be found
- ... or build your own
- Command-line arguments confusing

Configuring Apache

Getting or building SSL Apache

- Apache V.1 with mod_ssl (*or* Apache-SSL)

Getting or building SSL Apache

- Apache V.1 with mod_ssl (*or* Apache-SSL)
- Apache V.2

Getting or building SSL Apache

- Apache V.1 with mod_ssl (*or* Apache-SSL)
- Apache V.2
- RedHat/Debian/Fedora/SuSE have pre-built packages

Getting or building SSL Apache

- Apache V.1 with mod_ssl (*or* Apache-SSL)
- Apache V.2
- RedHat/Debian/Fedora/SuSE have pre-built packages
- Pre-compiled Windows available

Getting or building SSL Apache

- Apache V.1 with mod_ssl (*or* Apache-SSL)
- Apache V.2
- RedHat/Debian/Fedora/SuSE have pre-built packages
- Pre-compiled Windows available
- ... or build your own

Other Issues

- Additional Directives

Other Issues

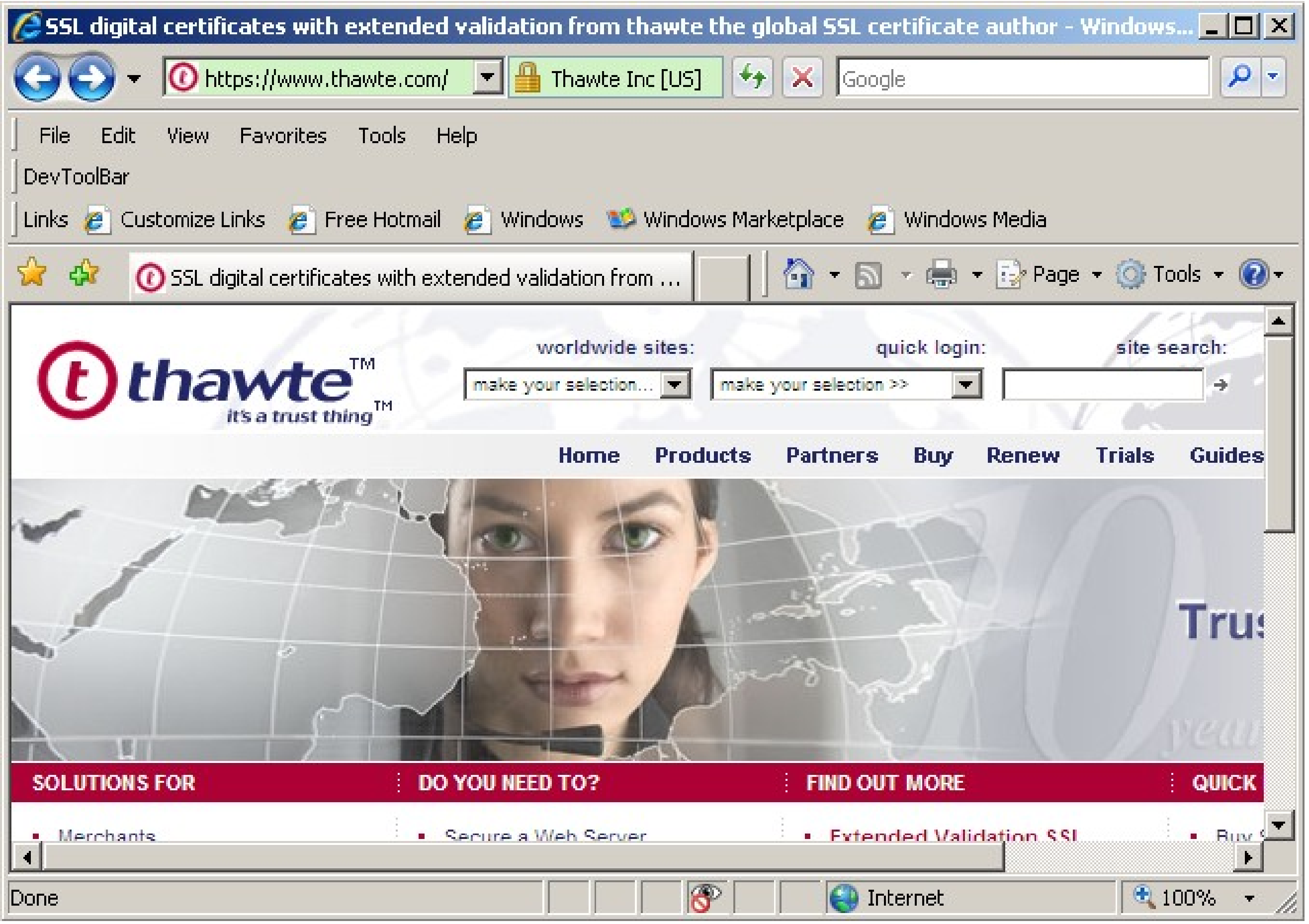
- Additional Directives
- Proxying HTTPS

Other Issues

- Additional Directives
- Proxying HTTPS
- Extended Validation

Other Issues

- Addit
- Proxy
- Exter



Other Issues

- Additional Directives
- Proxying HTTPS
- Extended Validation
- Server Gated Cryptography

Further Material

- http://www-uxsup.csx.cam.ac.uk/~jw35/courses/using_https/
- web-support@ucs.cam.ac.uk