cphbusiness

COPENHAGEN BUSINESS ACADEMY

Security

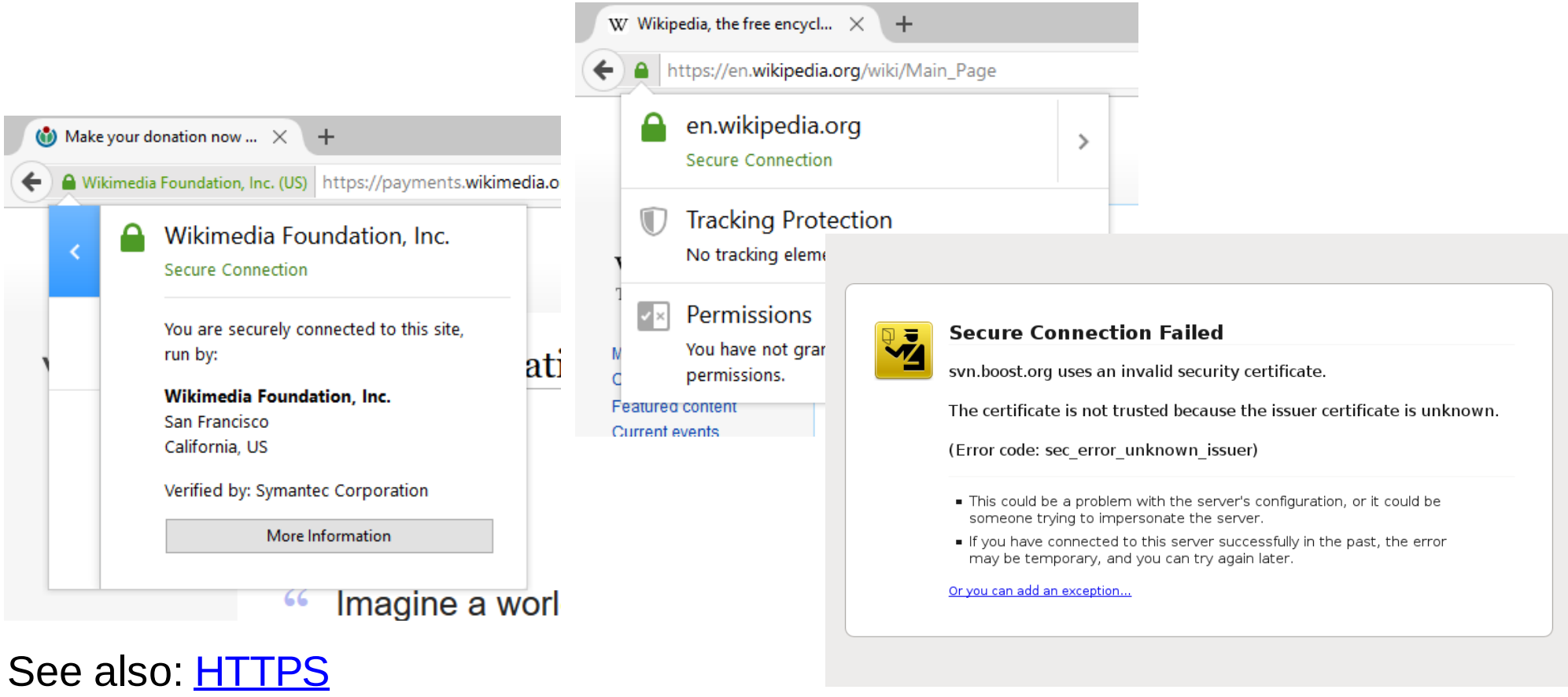
Lars Mortensen

Literature:

HTTPS

cphbusiness

- HTTP over TLS (on what port?)
- Simply HTTP inside a TLS tunnel



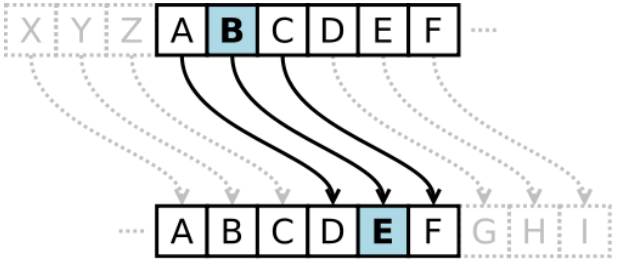
See also: HTTPS

Symmetric-Key Cryptography
Algorithms

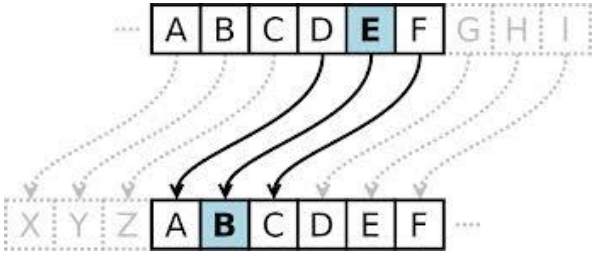
cphbusiness

The first recorded cipher text was used by Julius Caesar and is called the **Caesar Cipher**:

Encryption



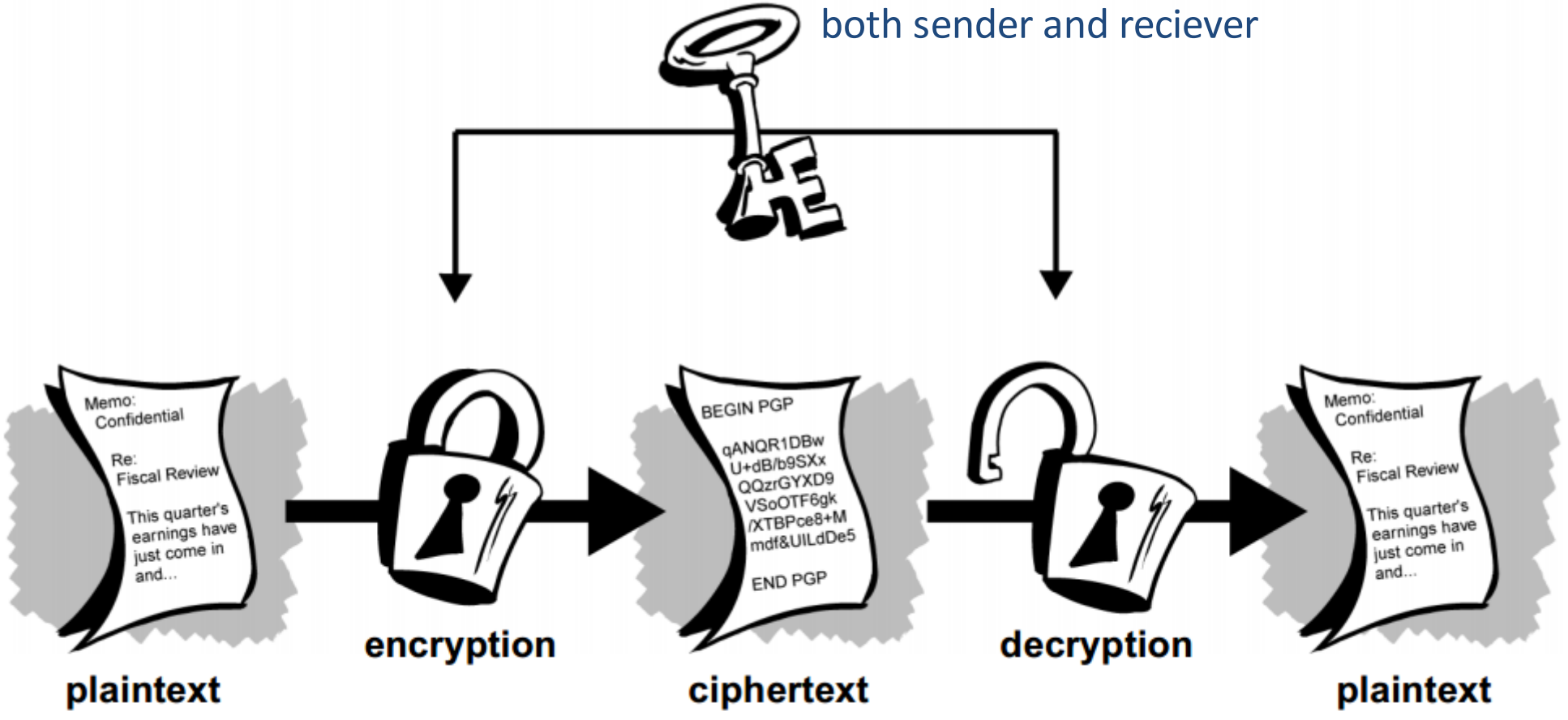
Decryption



Conventional Cryptography
Symmetric-Key Cryptography

cphbusiness

Same Shared Secret Key is used by both sender and reciever



Symmetric-Key Cryptography
Algorithms Used today ;-)

cphbusiness

In Cryptography, the encryption/decryption algorithms are public.
The keys are the secret

- DES Data Encryption Standard
  DES was approved as a US Federal Standard in November 1976, and published on 15 January 1977
  It is now obsolete (in 2008 hardware power had increased so that it could be broken in less than a day)
- 3DES triple-DES
- AES Advanced Encryption Standard
- …

http://en.wikipedia.org/wiki/Data_Encryption_Standard

Symmetric-Key Cryptography

cphbusiness

Symmetric-key encryption is very efficient (compared to public key encryption, up to 1000 times faster) and are often used for large messages.

What is the obvious drawback of this technology?

Public-Key Cryptography

cphbusiness

The problems of key distribution are (partly) solved by public key cryptography, which was introduced by Diffie and Hellman in 1975.

In this technology there are two keys, a public and a private key.

The Public key

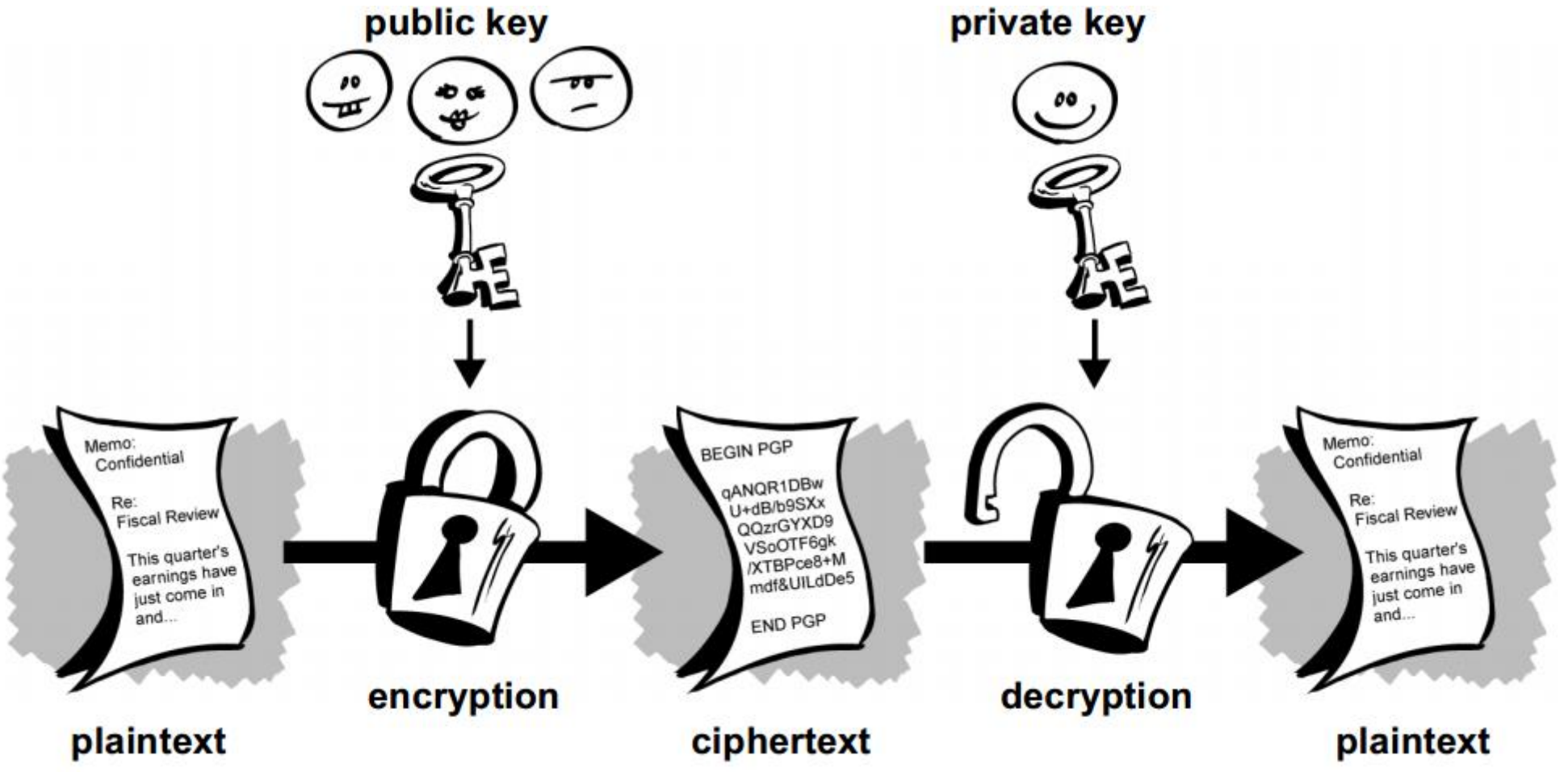
This key is available to anyone, so anyone can encrypt a message with this key.

The Private key

Only the private key can decrypt a message encoded with it's corresponding public key

Public-Key Cryptography

cphbusiness



Public-Key Cryptography
Algorithms

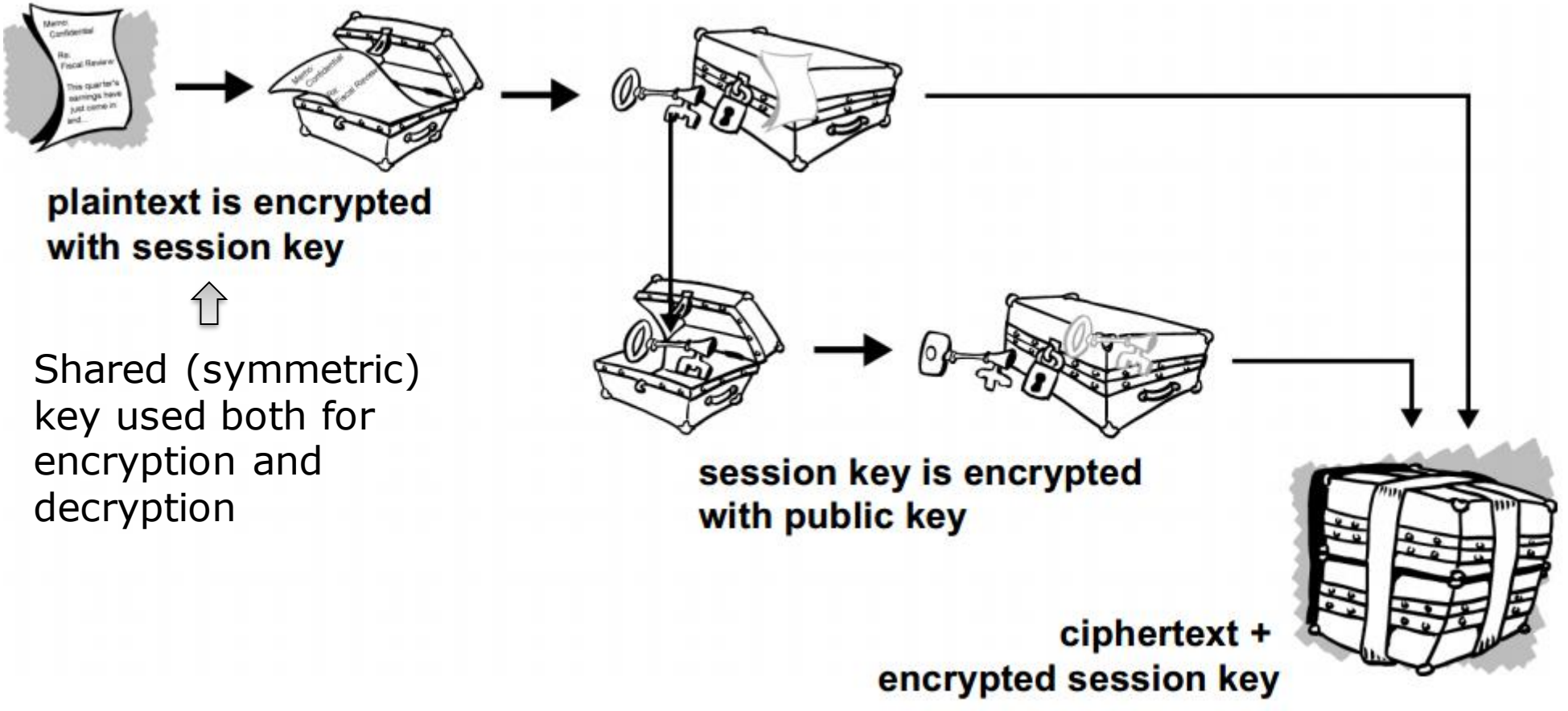
cphbusiness

- RSA (named after it inventors)
- Diffie-Hellman (named after its inventors, the inventors of Public-Key Cryptography)
- DSA (Digital Signature Algorithm)

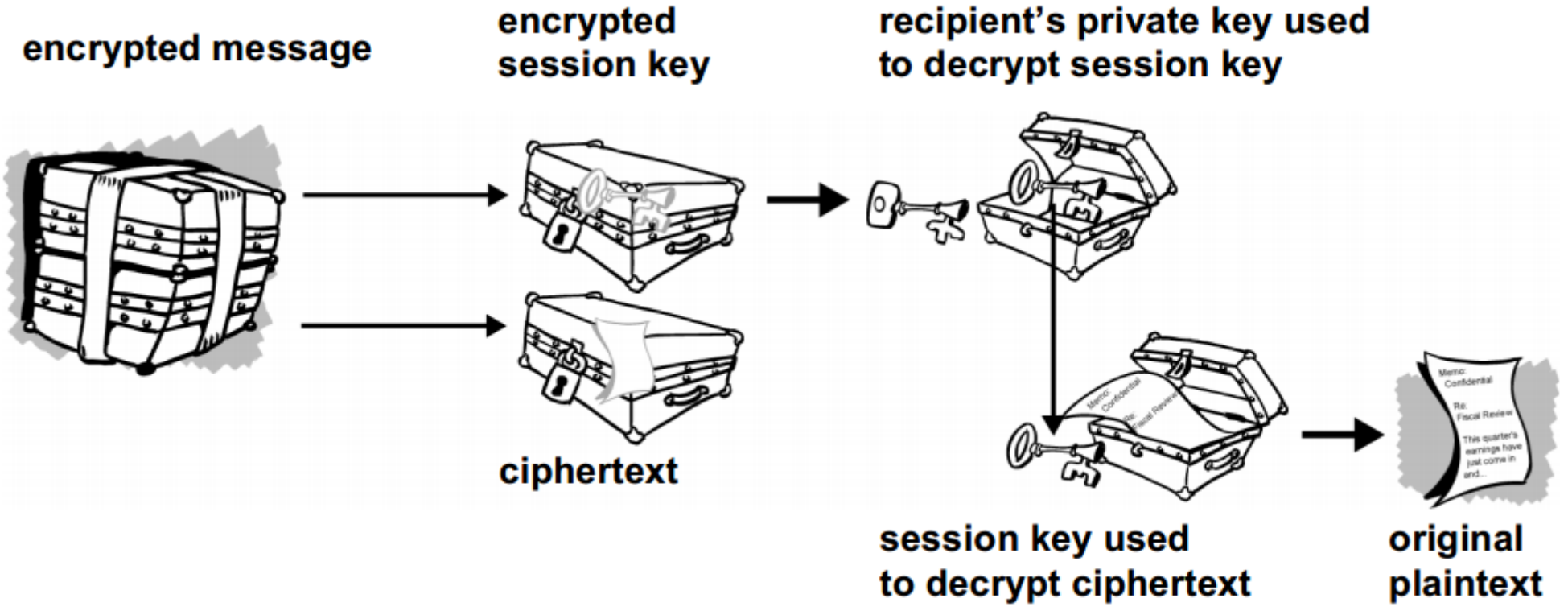
Public key algorithms is much less efficient than symmetric-key algorithms, partly because key length must me much larger (A conventional 128-bit key is roughly equivalent to a 3000-bit public key)

For that reason the two technologies are often uses together

How PGP Works
Encryption



How PGP Works
Decryption



Keys-1

cphbusiness

- A key is a value that works with a cryptographic algorithm to produce a specific cipher text.
- In public key cryptography, the bigger the key, the more secure the cipher text.
- Public key size and conventional cryptography's secret key size are totally unrelated.
  A conventional 128-bit key is equivalent to a 3000-bit public key.
- So comparing key sizes of conventional and public are like comparing apples to oranges.

Keys-2

cphbusiness

- Public and private keys are mathematically related, but it’s very difficult to derive the private key given only the public key.
- Very difficult yes, but deriving the private key is always possible given enough time and computing power.
- This makes it important to pick keys of the right size; large enough to be secure, but small enough to be applied fairly quickly.
- Larger keys will be cryptographically secure for a longer period of time.
- There was a time when a 56-bit symmetric key was considered extremely safe.

Digital Signatures

cphbusiness

A major benefit of public key cryptography is that it provides a method for employing digital signatures.

Authentication and Data Integrity

Digital signatures enable the recipient of information to verify the authenticity of the information's origin, and also verify that the information is intact.

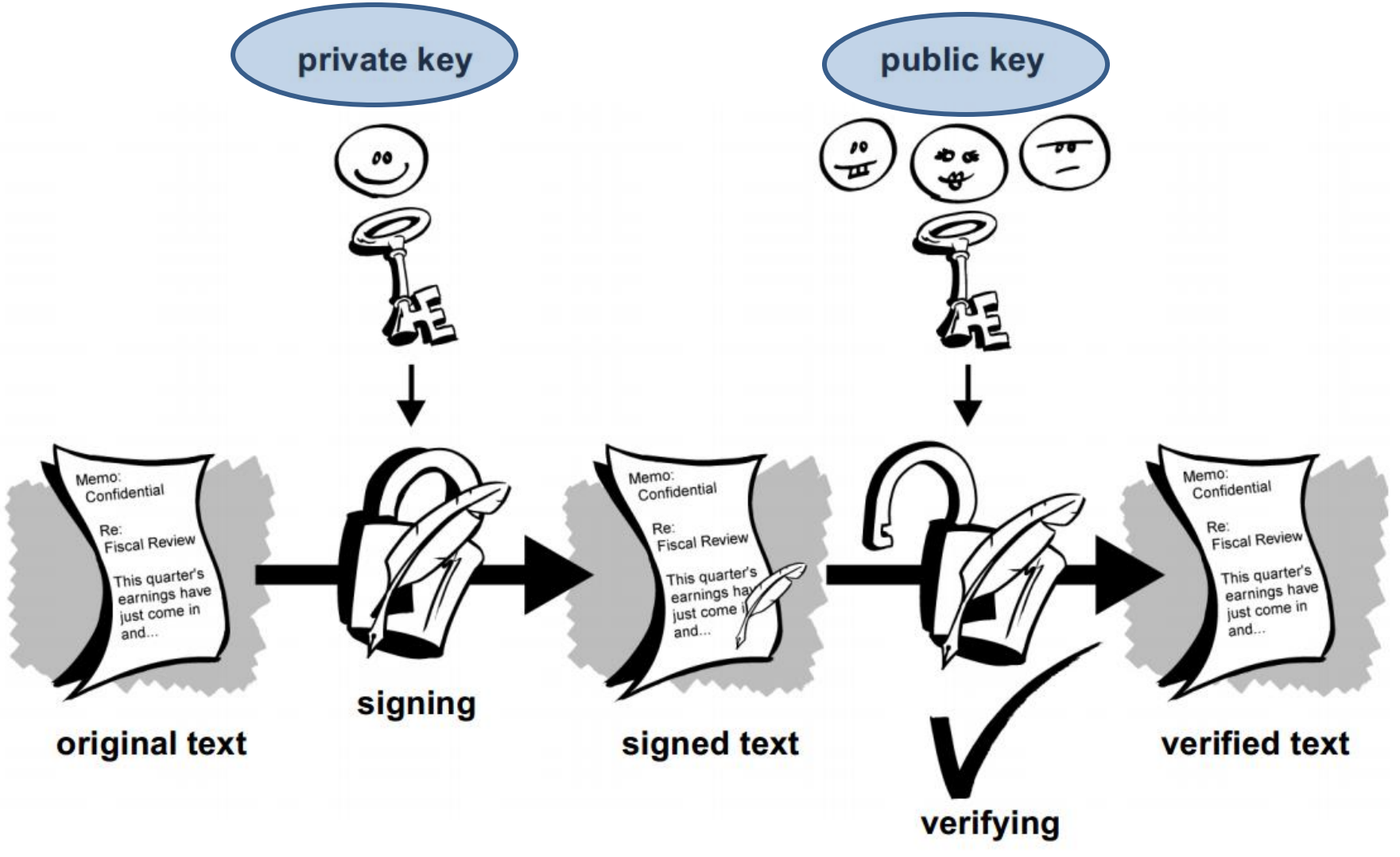
Non-repudiation

A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information

Digital Signatures

Signing the whole document

cphbusiness



Digital Signatures
Signing a Digest

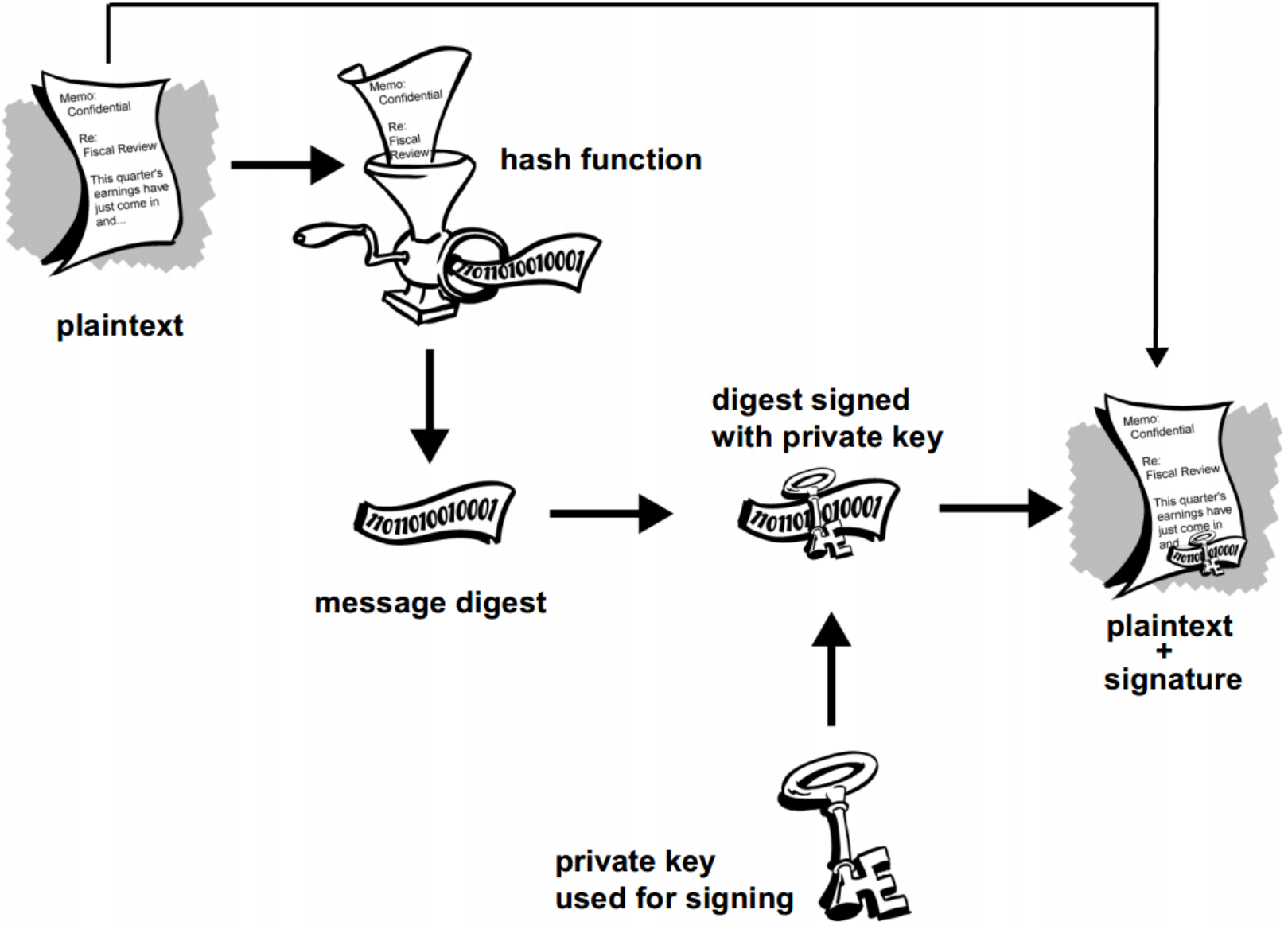
cphbusiness

Signing the whole document is slow, and produces an enormous volume of data—at least double the size of the original information.

- An improvement is to sign only a digest of the message using a one-way hash function in the process.
- A one-way hash function takes variable-length input—in this case, a message of any length, even thousands or millions of bits—and produces a fixed-length output; say, 160-bits.
- The hash function ensures that, if the information is changed in any way—even by just one bit—an entirely different output value is produced

Digital Signatures
Signing a Digest

cphbusiness



Digital Certificates

cphbusiness

A digital certificate is data that functions much like a physical certificate. A digital certificate is information included with a person's public key that helps others verify that a key is genuine or valid.

A digital certificate consists of three things:

- A public key.
- Certificate information. ("Identity" information about the user, such as name, user ID, and so on.)
- One or more digital signatures.

So, a certificate is basically a public key with one or two forms of ID attached, plus a hearty stamp of approval from some other trusted individual

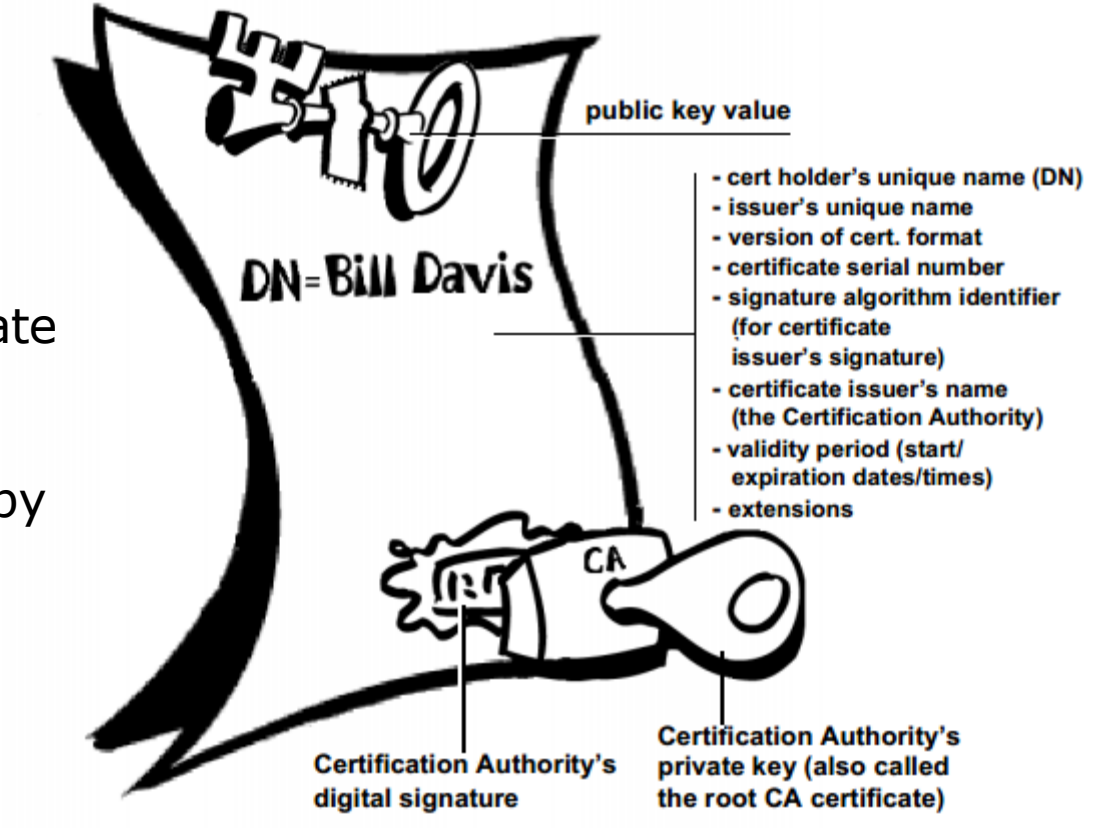
Certificate Formats

cphbusiness

Several kind of certificate formats exists including:

- PGP Certificates
- X.509 Certificates

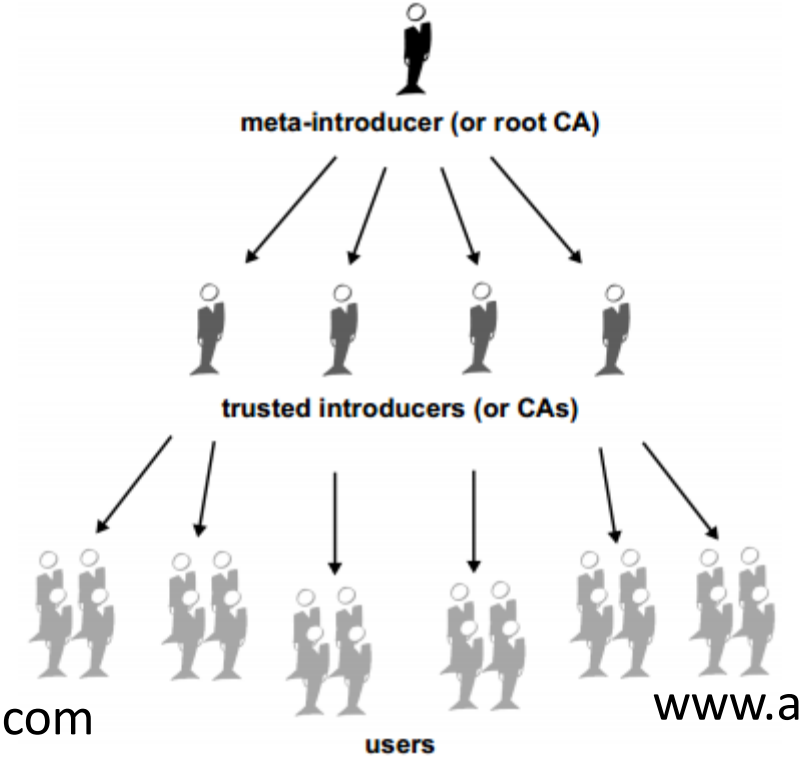
X.509 is published as ITU recommendation ITU-T X.509 which defines a standard certificate format for public key certificates and certification validation which more or less has been accepted by the internet.



Public key Infrastructure (PKI)
Hierarchical Trust

cphbusiness

In a hierarchical system, there are a number of "root" certificates from which trust extends. These certificates may certify certificates themselves, or they may certify certificates that certify still other certificates down some chain



Examples:

fronter.com

www.amacon.co.uk

*.danskebank.dk

View Installed Certificates on Windows

cphbusiness

To add the Certificates snap-in to an MMC for a user account

- Click **Start**
- type **mmc** in the **Search programs and files** box, and then press ENTER.
- On the **File** menu, click **Add/Remove Snap-in**.
- Under **Available snap-ins**, double-click **Certificates**, and then:

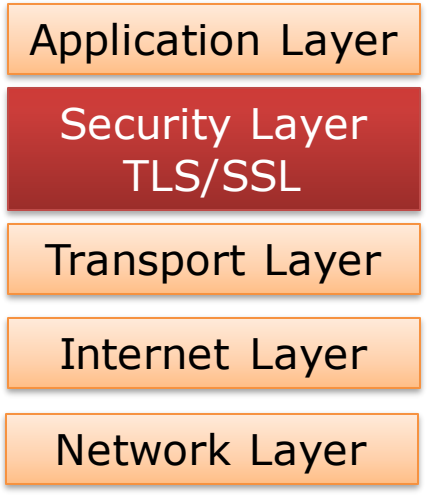
  If you are logged on as an administrator, click **My user account**, and then click **Finish**.

  If you are logged on as a user, the Certificates snap-in automatically opens.

Security on the Internet

cphbusiness

Security can be added at most of the layers in the TCP/IP stack, but at the IP-layer and Transport-layer this is complicated and beyond the scope of this introduction.



We will look at **TLS/SSL** which adds a new layer to the TCP/IP layers stack.

- As with all the other layers the TLS/SSL protocols are independent of the protocols above and below, but the layer "speaks the same language" as the same layer on the other side of the communications channel.
- This design not only ensures full compatibility with all the network technologies based on TCP/IP, but it also enables them to easily "switch" to their secure versions without having to reinvent them from the ground up.
- So, HTTP became HTTPS without having to modify its specifications, FTP became FTPS, and so on.

Security on the Internet
TLS/SSL

cphbusiness

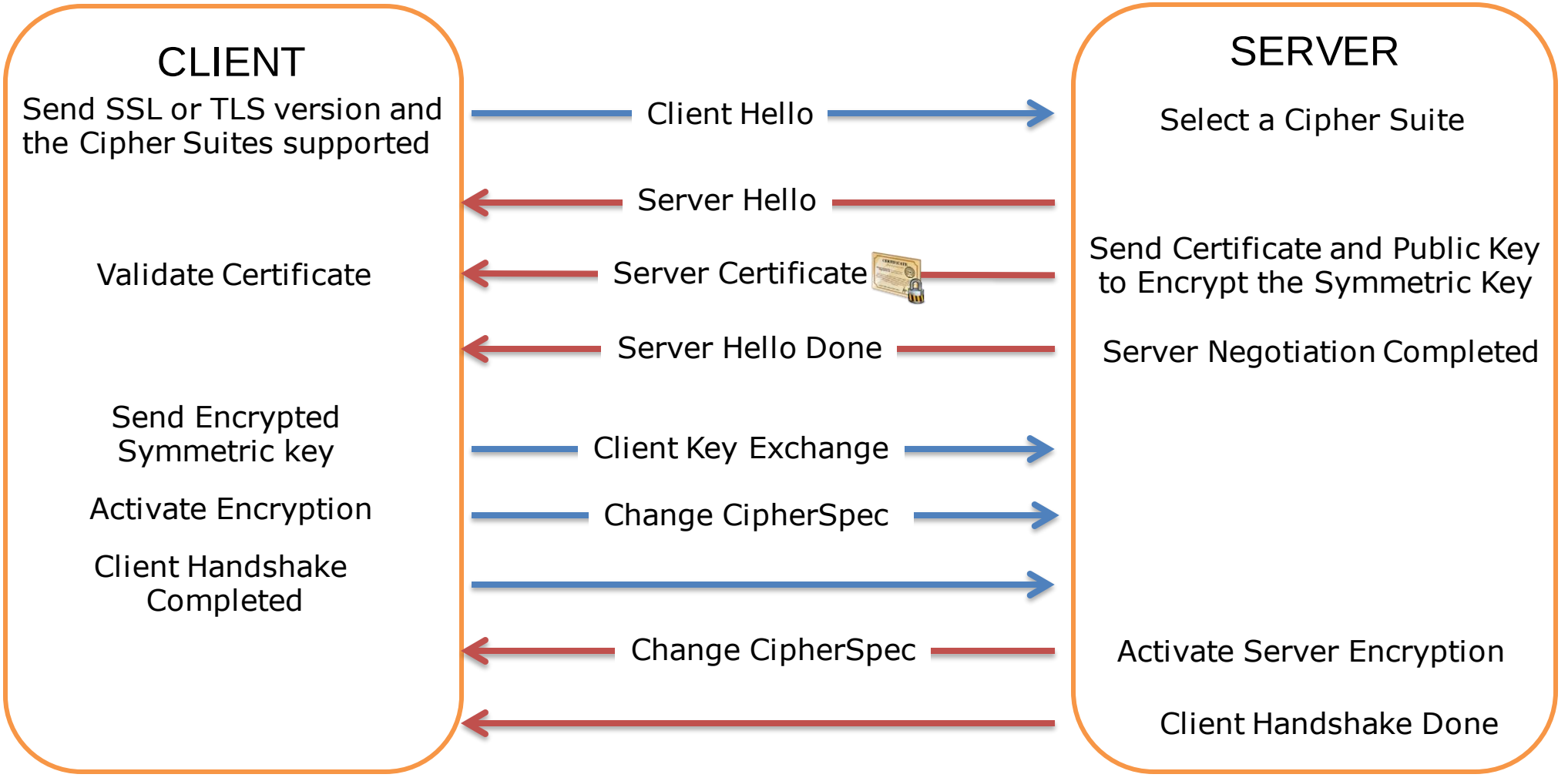
The SSL (Secure Socket Layer) and TLS (Transport Layer Security) protocols enable two parties to identify and authenticate each other and communicate with confidentiality and data integrity.
The TLS protocol evolved from the Netscape SSL 3.0 protocol but TLS and SSL do not interoperate.

The SSL and TLS protocols provide communications security over the internet, and allow client/server applications to communicate in a way that is confidential and reliable.

An SSL or TLS connection is initiated by an application, which becomes the SSL or TLS client. The application which receives the connection becomes the SSL or TLS server. Every new session begins with a handshake, as defined by the SSL or TLS protocols.

TLS

Handshake for Server-Only Authentication



For the duration of the session, the server and client can now exchange messages that are symmetrically encrypted with the shared secret key

What we Need to Host Secure Pages

cphbusiness

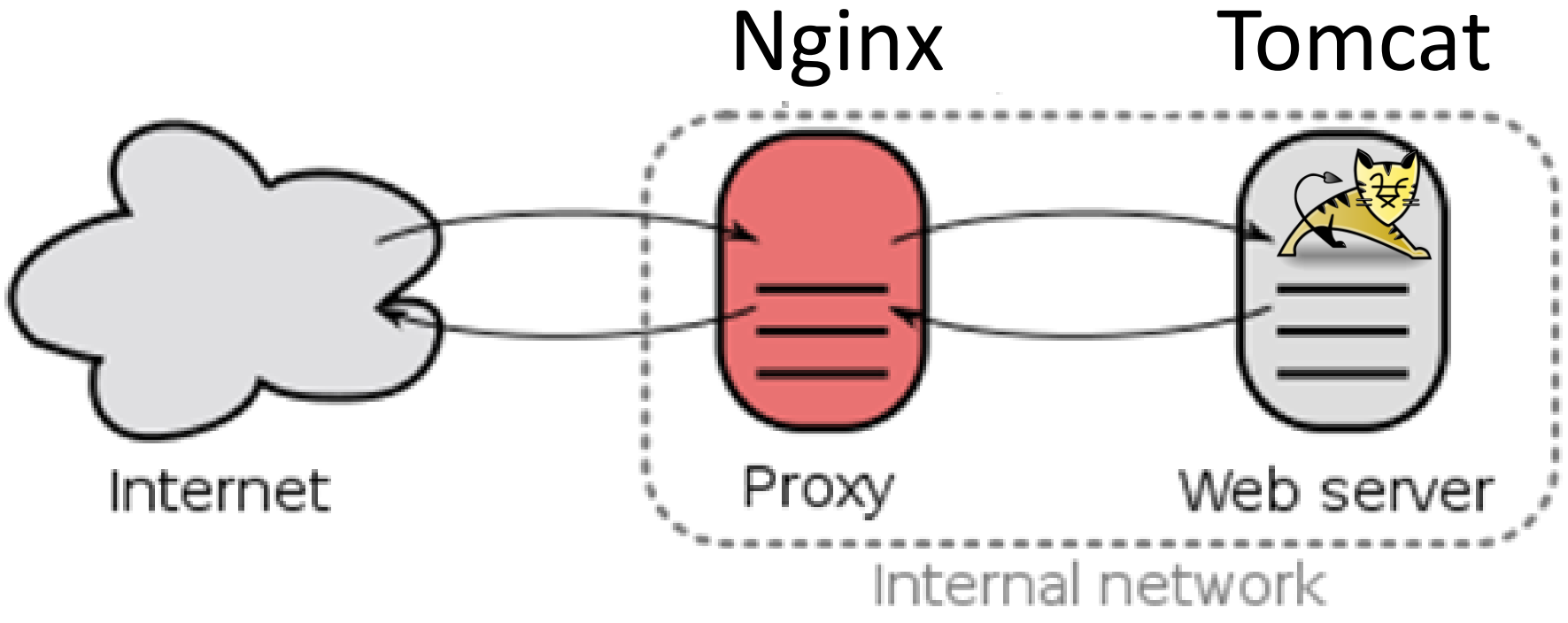
- A Web server such as Nginx (or Tomcat) that supports TLS/SSL encryption
- A Unique IP address + a Domain Name - this is one of the things the certificate providers uses to validate the secure certificate
- An SSL Certificate from an SSL certificate provider
- We will use Let's encrypt, because it's free ☺

`https://letsencrypt.org/`

We will use a gatekeeper

cphbusiness

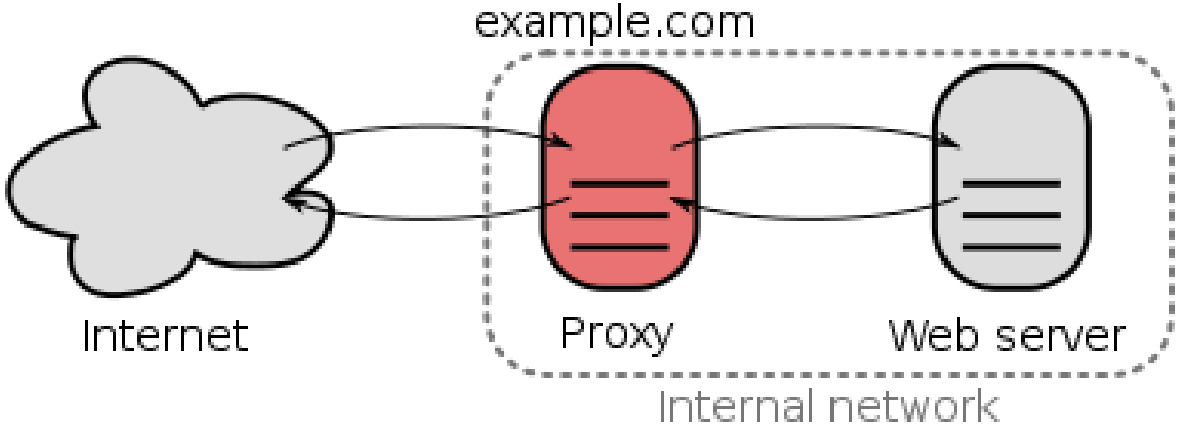
WHY?



The Reverse Proxy

cphbusiness

A reverse proxy taking requests from the Internet and forwarding them to servers in an internal network. Those making requests to the proxy may not be aware of the internal network.



- Reverse proxies can hide the existence and characteristics of an origin server or servers.
- Application firewall features can protect against common web-based attacks, like DoS or DDoS.
- In the case of **secure websites**, a web server may not perform SSL encryption itself, but instead offloads the task to a reverse proxy.
- A reverse proxy can distribute the load from incoming requests to several servers, with each server serving its own application area.
- A reverse proxy can reduce load on its origin servers by caching static content, as well as dynamic content - synonym: web acceleration.

https://en.wikipedia.org/wiki/Reverse_proxy

Nginx this semester

cphbusiness

Handle all SSL Traffic
Provide better front-end security than Tomcat.