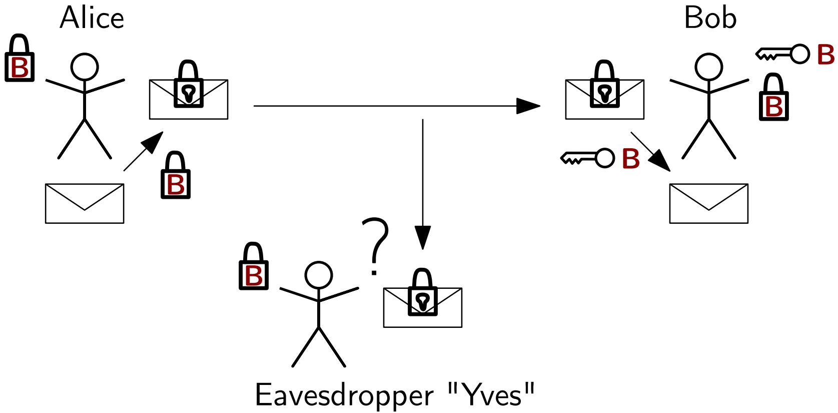
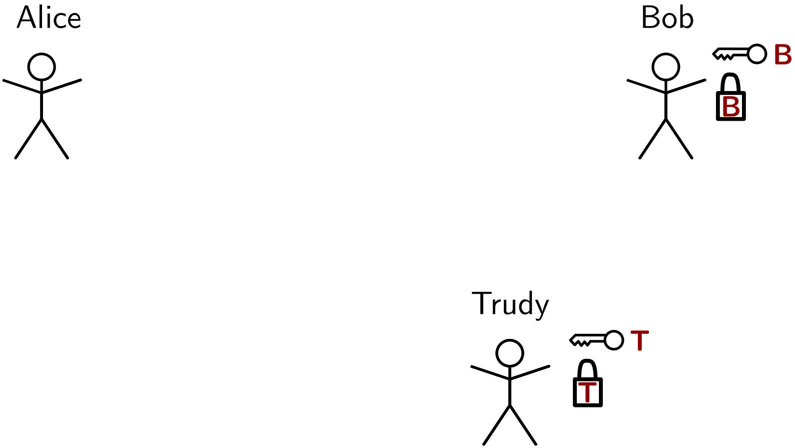
Asymmetric Cryptography



Man-in-the-Middle Attack



Alice

Bob

B

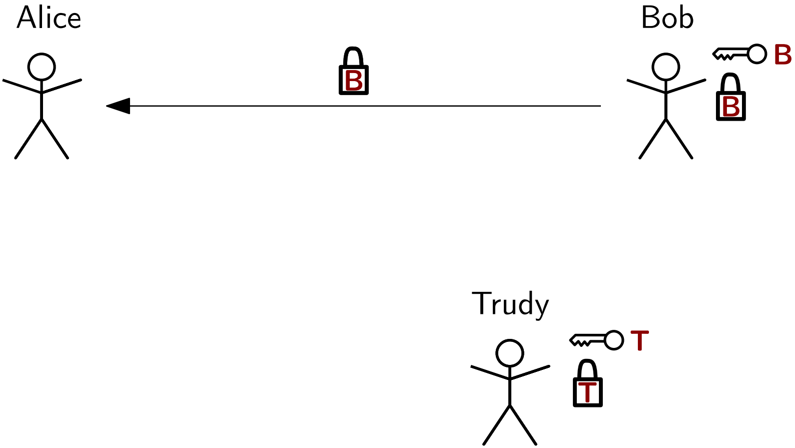
B

Trudy

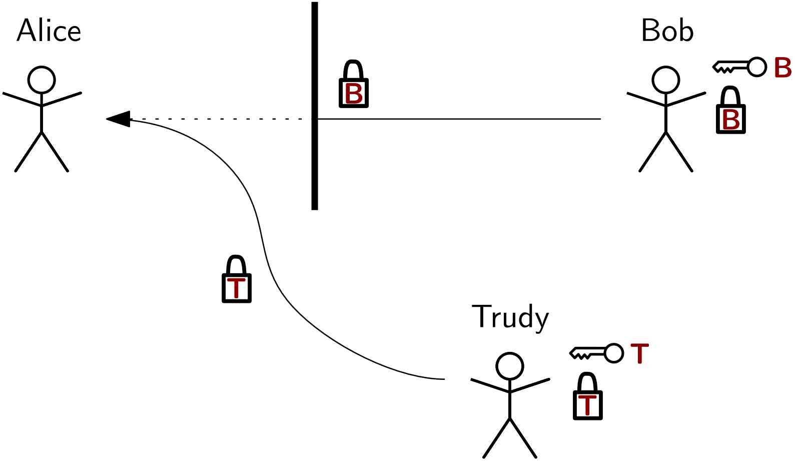
T

T

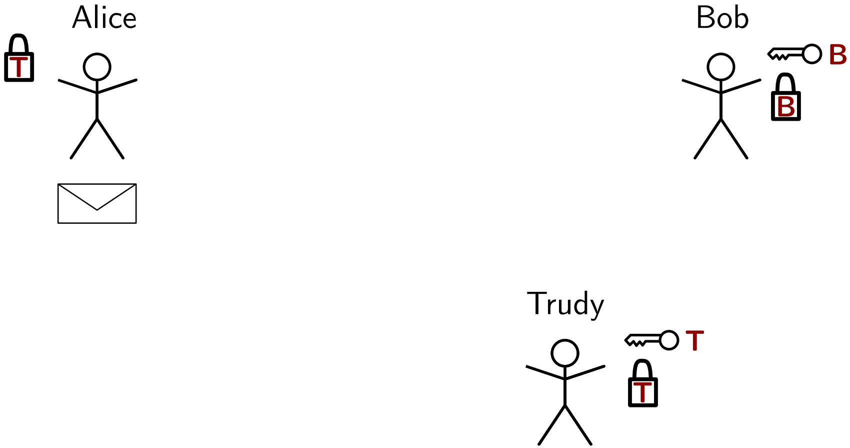
Man-in-the-Middle Attack



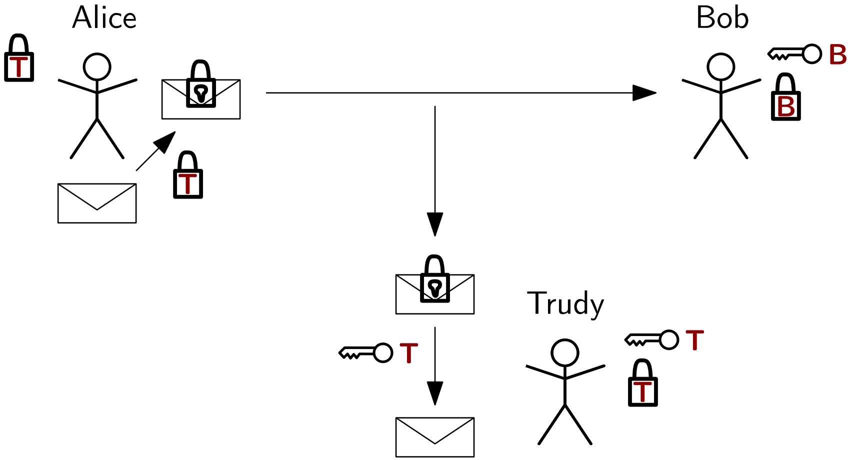
Man-in-the-Middle Attack



Man-in-the-Middle Attack



Man-in-the-Middle Attack



Authentication

- To prevent Man-in-the-Middle attacks, Alice must verify that the message sender is Bob

Authentication

- To prevent Man-in-the-Middle attacks, Alice must verify that the message sender is Bob
- Use of “Digital Signatures”

Authentication

- To prevent Man-in-the-Middle attacks, Alice must verify that the message sender is Bob
- Use of “Digital Signatures”

Digital Signature

Like Public Key Encryption, but the other way round:

Authentication

- To prevent Man-in-the-Middle attacks, Alice must verify that the message sender is Bob
- Use of “Digital Signatures”

Digital Signature

Like Public Key Encryption, but the other way round:

- Using the Private Key, one can create a signature

Authentication

- To prevent Man-in-the-Middle attacks, Alice must verify that the message sender is Bob
- Use of “Digital Signatures”

Digital Signature

Like Public Key Encryption, but the other way round:

- Using the Private Key, one can create a signature
- Using the Public Key, one can verify a signature

Certification Authorities

Digital Signature

Like Public Key Encryption, but the other way round:

- Using the Private Key, one can create a signature
- Using the Public Key, one can verify a signature

Certification Authorities

Digital Signature

Like Public Key Encryption, but the other way round:

- Using the Private Key, one can create a signature
- Using the Public Key, one can verify a signature

To verify Bob's signature, Alice still needs his public key!

Certification Authorities

Digital Signature

Like Public Key Encryption, but the other way round:

- Using the Private Key, one can create a signature
- Using the Public Key, one can verify a signature

To verify Bob's signature, Alice still needs his public key!

- Instead use a Certification Authority that certifies that Bob's Public Key belongs to Bob

Certification Authorities

Digital Signature

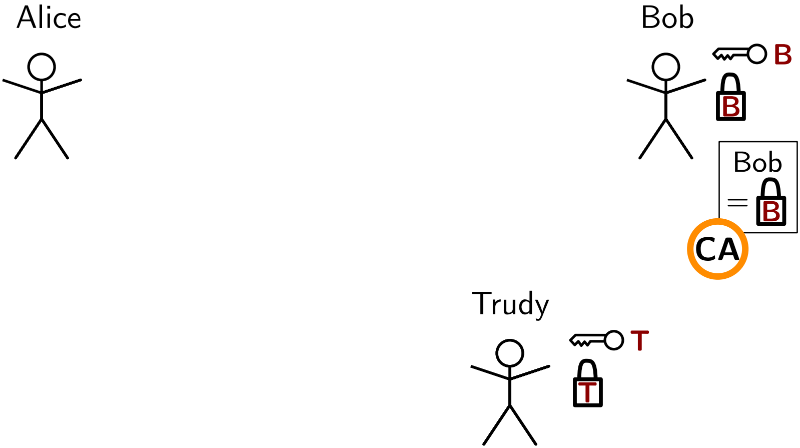
Like Public Key Encryption, but the other way round:

- Using the Private Key, one can create a signature
- Using the Public Key, one can verify a signature

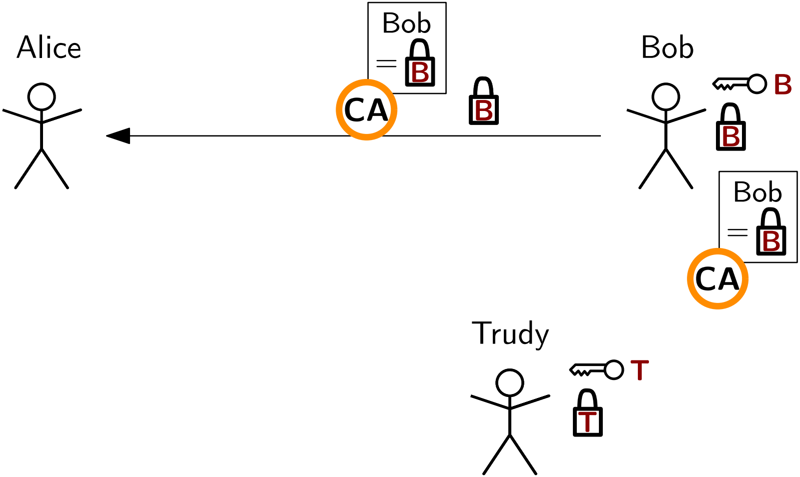
To verify Bob's signature, Alice still needs his public key!

- Instead use a Certification Authority that certifies that Bob's Public Key belongs to Bob
- Everyone "knows" the Public Keys of the Certification Authorities

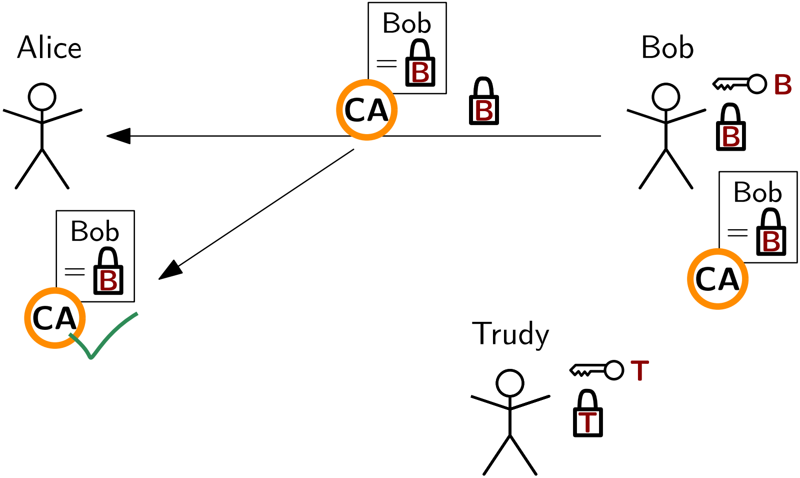
Certification Authorities



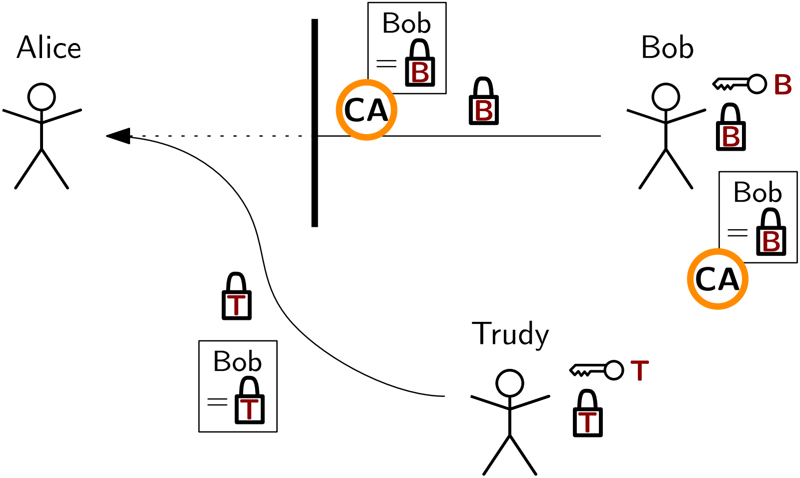
Certification Authorities



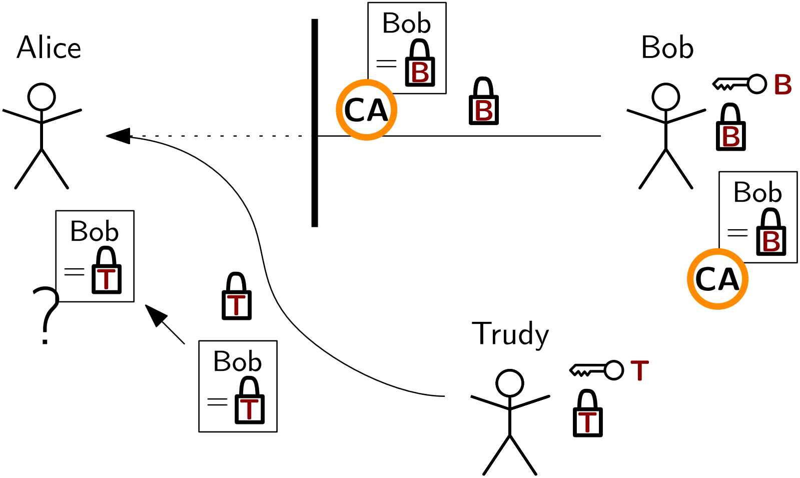
Certification Authorities



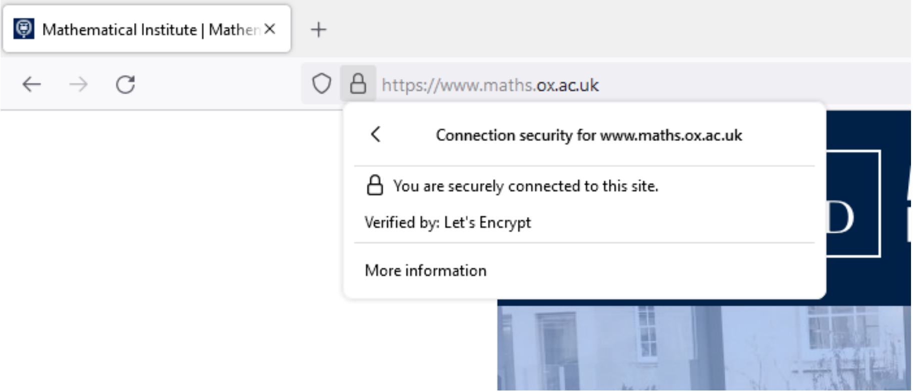
Certification Authorities



Certification Authorities



Certification Authorities



Mathematical Institute | Mathen

https://www.maths.ox.ac.uk

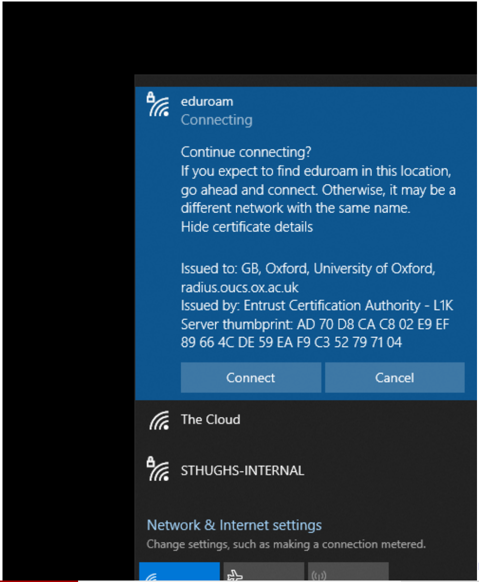
Connection security for www.maths.ox.ac.uk

You are securely connected to this site.

Verified by: Let's Encrypt

More information

Certification Authorities



eduroam
Connecting

Continue connecting?
If you expect to find eduroam in this location, go ahead and connect. Otherwise, it may be a different network with the same name.
Hide certificate details

Issued to: GB, Oxford, University of Oxford, radius.oucs.ox.ac.uk
Issued by: Entrust Certification Authority - L1K
Server thumbprint: AD 70 D8 CA C8 02 E9 EF 89 66 4C DE 59 EA F9 C3 52 79 71 04

Connect
Cancel
The Cloud
STHUGHS-INTERNAL
Network & Internet settings
Change settings, such as making a connection metered.

Thank you for listening!

HOW TO USE PGP TO VERIFY THAT AN EMAIL IS AUTHENTIC:
LOOK FOR THIS TEXT AT THE TOP.
PLANS
INBOX
REPLY
-----BEGIN PGP SIGNED MESSAGE-----
HASH: SHA256
HEY,
FIRST OF ALL, THANKS FOR TAKING CARE OF
IF IT'S THERE, THE EMAIL IS PROBABLY FINE.

Source: www.xkcd.com