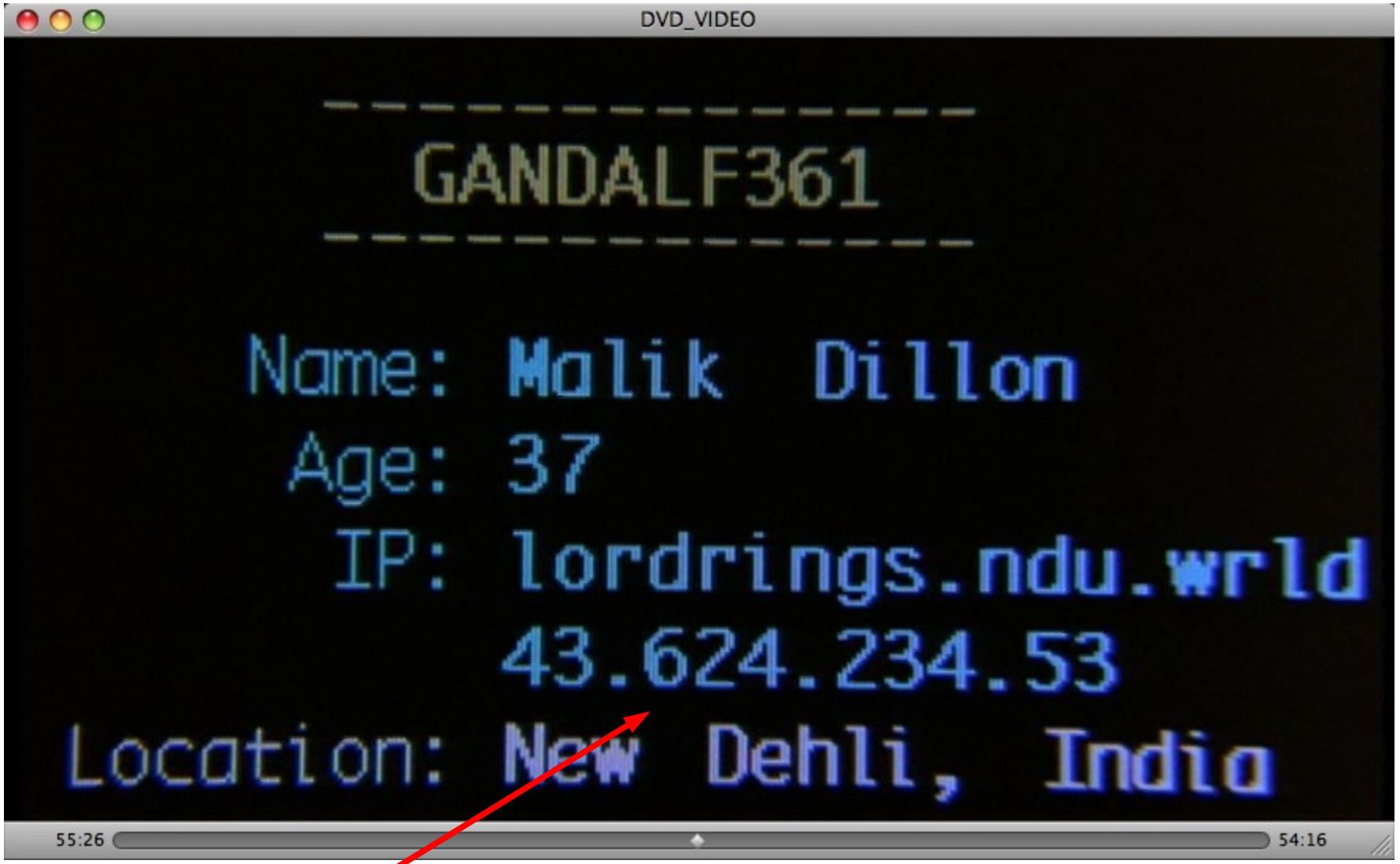
Grundlagen

Hier könnte ein reißerischer Text stehen

Internet

- Verwendet das Internet Protocol „IP“
- Jeder Teilnehmer benötigt eine eindeutige Adresse: Die IP Adresse.
- Beispiel: 87.32.63.27
- Jede der vier Zahlen kann zwischen 0 und 255 sein

Hollywood sieht das anders



Mööööp

Ansonsten kann man sich „Das Netz“ aber ruhig mal wieder ansehen.

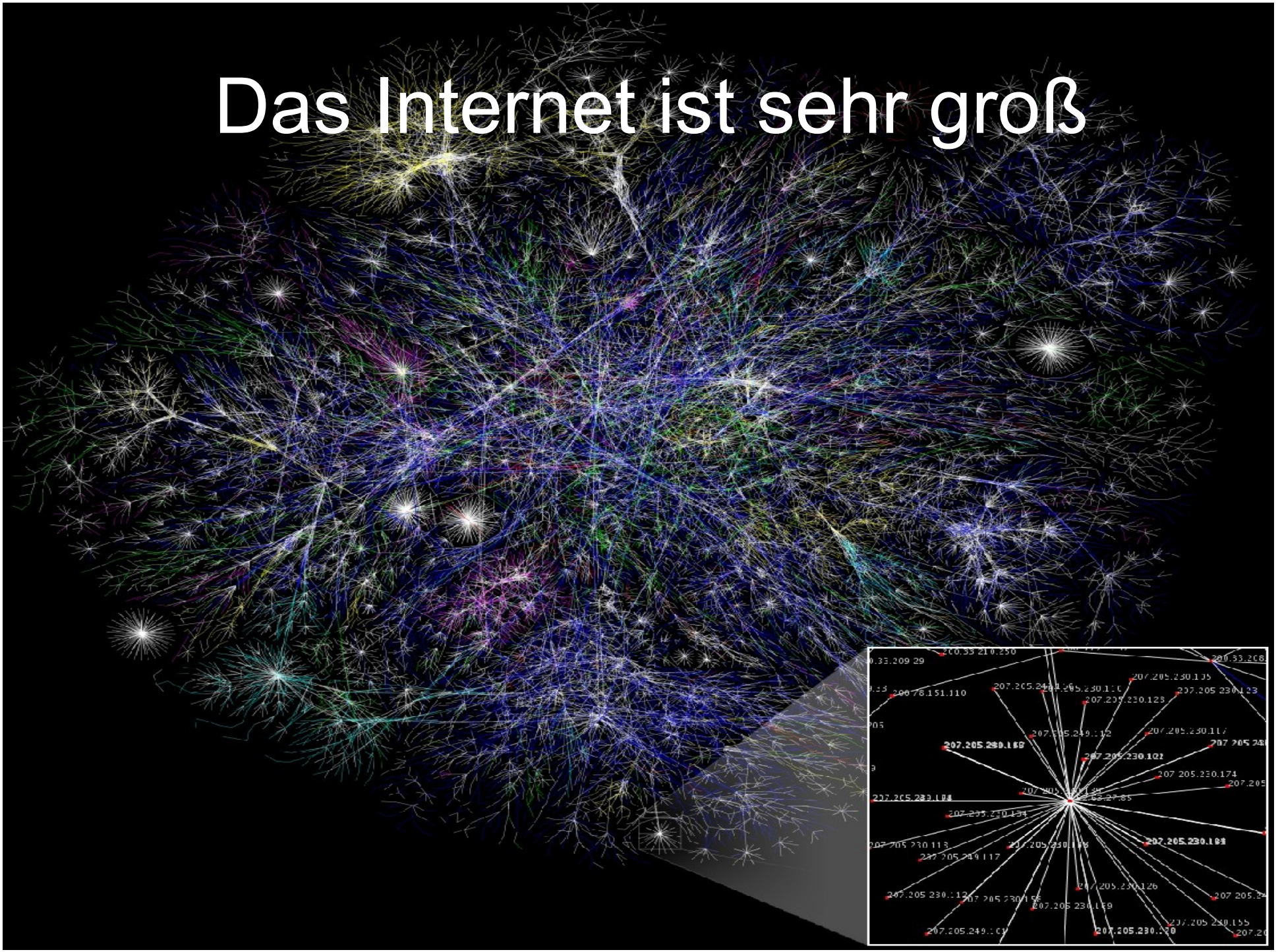
Eine Datenverbindung

- Um Daten durch das Internet zu transportieren werden die IP Adressen des Empfängers und des Absenders benötigt.
- Zur Datenübertragung werden die Daten in kleine Pakete zerteilt und einzeln zum Ziel Transportiert
  - E-Mail
  - Webseiten
  - Alles Mögliche

Ein IP-Paket

Beispiel:

Das Internet ist sehr groß



http://de.wikipedia.org/wiki/Bild:Internet_map_1024.jpg

Zu groß

- Niemand hat 1969 damit gerechnet, dass das Internet so groß wird, wie es heute ist. Und es wächst immer noch.
- Es gibt „nur“ 2 hoch 32 = 4.294.967.296 Adressen

Tricks um den Adressbedarf zu reduzieren

- (Ganze Netzwerke verwenden nur eine einzige Adresse, um mit dem Internet verbunden zu werden)
- Adressen werden nur temporär einem Teilnehmer zugewiesen. Nur während er mit dem Netz verbunden ist.

Dynamisch zugewiesene Adressen

- Teilnehmer „wählt sich ins Internet ein“
  - Modem über Telefonleitung
  - DSL
  - Handy (GPRS, UMTS)
- ... Und bekommt dabei temporär eine IP Adresse zugewiesen

Begrenzte Anonymität

- Anders, als bei einer Telefonnummer ist einer IP Adresse nicht eindeutig einem Teilnehmer zuzuordnen, denn:
- Wenn er die Verbindung zum Internet trennt, wird seine Adresse wieder freigegeben und dem nächsten Teilnehmer zugewiesen
- Der Provider merkt sich aber, wann er welchem Kunden eine Adresse zugewiesen hatte
  - Wie lange er sich das merken soll ist ein Streitpunkt

Transporteure

- Mein Computer
- Mein Netzwerk. Kabel oder WLAN (Funknetz)
- Mein Modem / DSL-Router
- Mein Internet Zugangs Provider
- Internet Knoten
- Noch ein Internet Knoten
- Noch viel mehr Internet Knoten
- Am Ende: Das Ziel

Abhörgefahr

- An jedem Punkt der Strecke können die Pakete mitgelesen werden
- Sie können sogar verändert werden
- Es ist für den Anwender nicht nachvollziehbar, welche Knoten genau verwendet werden

Wir wollen

- Vertraulichkeit
  - Nur der Empfänger soll die Daten lesen können
- Unveränderte Daten
  - Niemand soll die Daten unbemerkt verändern können
- Echtheit
  - Ich möchte Sicher sein, dass ich wirklich mit der Person oder dem Server „spreche“, mit dem ich glaube zu sprechen.

Kryptografie

- Kann das leisten
- Ist bei der Erfindung des Internets nicht nötig gewesen, weil das Netz sehr klein und die Teilnehmer bekannt waren (Wissenschaftler an Universitäten)
- Muss daher jetzt nachträglich eingebaut werden

Die Stars

Alice. Sie möchte Bob eine vertrauliche Nachricht senden.

Bob. Er möchte eine vertrauliche Nachricht von Alice empfangen.

http://en.wikipedia.org/wiki/Image:Crypto_clipart1.svg

Symetrische Verschlüsselung

- Alice und Bob vereinbaren ein Kennwort (und ein Verschlüsselungsverfahren)
- Alice verschlüsselt die Nachricht mit dem Kennwort
- Die Nachricht ist im Netz sicher. Sie kann nicht gelesen werden und wer sie verändert zerstört sie.
- Bob verwendet *dasselbe* Kennwort um die Nachricht zu entschlüsseln.

Aber...

- Alice ist in Göttingen, Bob in San-Francisco.
  - Wie sollen die beiden ein Kennwort vereinbaren, ohne dass jemand mithören kann?
- Bob ist vielleicht gar keine Person, sondern ein Webserver.
  - Wie vereinbart man mit einer Maschine ein Kennwort? Über das Internet? Ohne dass abgehört werden kann?

Die Idee: Asymmetrische Kryptografie

Wir teilen die Ver- und Entschlüsselung auf zwei Schlüssel auf:

Öffentlicher Schlüssel
- Kann verschlüsseln

Privater Schlüssel
- Kann entschlüsseln, was der öffentliche Schlüssel verschlüsselt hat.

Die beiden Schlüssel gehören zusammen. Der Private kann nur Nachrichten seines Kollegen entschlüsseln.

Die Idee: Asymmetrische Kryptografie

Wir teilen die Ver- und Entschlüsselung auf zwei Schlüssel auf:

Öffentlicher Schlüssel
- Kann verschlüsseln

Andere Namen:
- Public Key
- Zertifikat (wozu aber noch mehr gehört)

Privater Schlüssel
- Kann entschlüsseln, was der öffentliche Schlüssel verschlüsselt hat.

Andere Namen:
- Private Key
- Secret Key
- Key

Die beiden Schlüssel gehören zusammen. Der Private kann nur Nachrichten seines Kollegen entschlüsseln.

Asymmetrische Kryptografie

Wir Teilen die Ver- und Entschlüsselungs auf zwei Schlüssel auf:

Öffentlicher Schlüssel
- Kann Verschlüsseln

Kopien dieses Schlüssels an alle meine Freunde verteilen, damit Sie mir damit Nachrichten verschlüsseln

Privater Schlüssel
- Kann Entschlüsseln, was der öffentliche Schlüssel verschlüsselt hat.

Die beiden Schlüssel gehören zusammen. Der Private kann nur Nachrichten seines Kollegen entschlüsseln.

Asymmetrische Kryptografie

Wir Teilen die Ver- und Entschlüsselungs auf zwei Schlüssel auf:

Öffentlicher Schlüssel
- Kann Verschlüsseln

Privater Schlüssel
- Kann Entschlüsseln, was der öffentliche Schlüssel verschlüsselt hat.

Diesen Schlüssel NIEMANDEM geben. Wer ihn mir klaut, kann Nachrichten, die für mich sind entschlüsseln.

Die beiden Schlüssel gehören zusammen. Der Private kann nur Nachrichten seines Kollegen entschlüsseln.

Super GAU

Wenn mein Privater Schlüssel geklaut wird, gibt es keine Sicherheit mehr. Nur ich darf diesen Schlüssel haben.

Super GAU

Wenn mein Privater Schlüssel geklaut wird, gibt es keine Sicherheit mehr. Nur ich darf diesen Schlüssel haben.

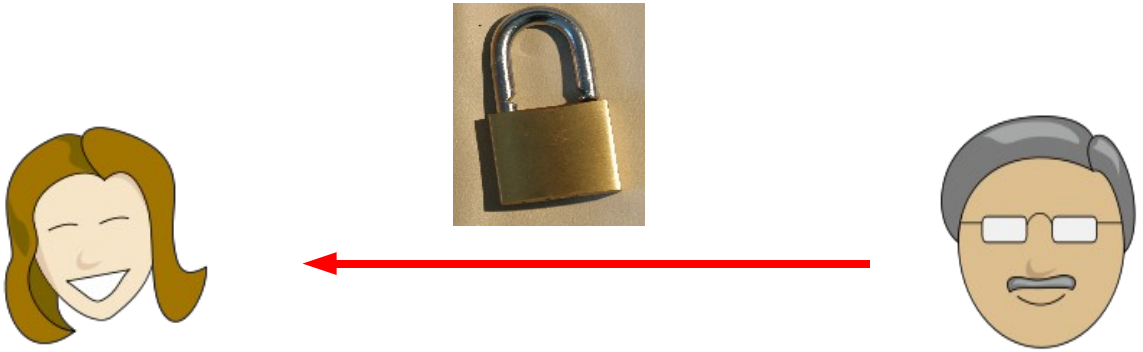
Deshalb wird dieser Schlüssel (der in Wirklichkeit ja eine Datei ist) selbst verschlüsselt gespeichert und nur bei Bedarf entschlüsselt.

Besonders wichtige Private Schlüssel werden nicht mal auf Festplatte gespeichert, sondern in externen Geräten gelagert, auf die der PC keinen vollen Zugriff hat.

Wie geht das nun?

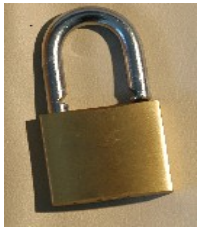
Alice möchte Bob eine Nachricht schicken...

1. Schlüsselübergabe

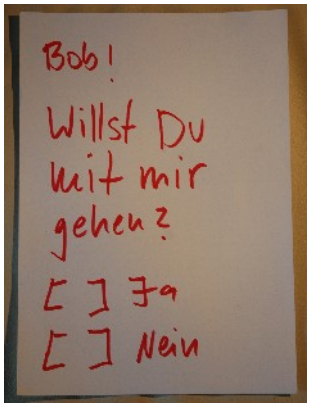


1.Bob schickt Alice seinen öffentlichen Schlüssel

2. Verschlüsseln



+



=

2.Alice verschlüsselt ihre Nachricht mit Bobs öffentlichem Schlüssel

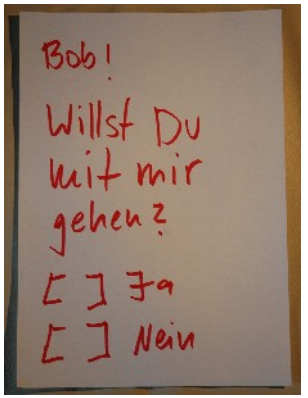
3. Nachricht verschicken

3. Alice schickt Bob die verschlüsselte Nachricht

4. Entschlüsseln

+

=



4. Bob kann die Nachricht entschlüsseln. Nur er kann das. Denn nur er hat den passenden privaten Schlüssel dazu.

Problem gelöst!

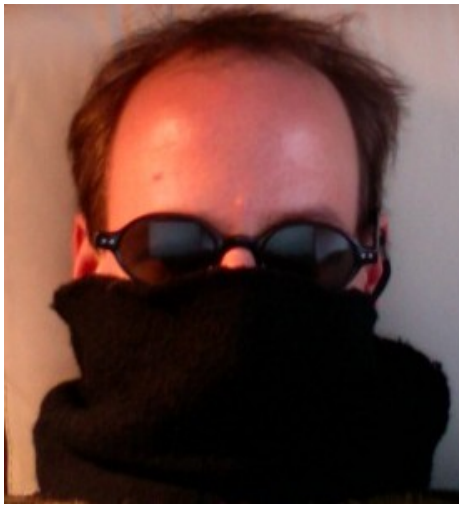
Die Digitale Welt ist in Ordnung.

Oder doch nicht?...

Mallory (Archivfoto)

Nachbar von Bob. Hat sich an dessen Netzwerk angeschlossen und kann dort alle Daten sehen und verändern.

Oder doch nicht?...



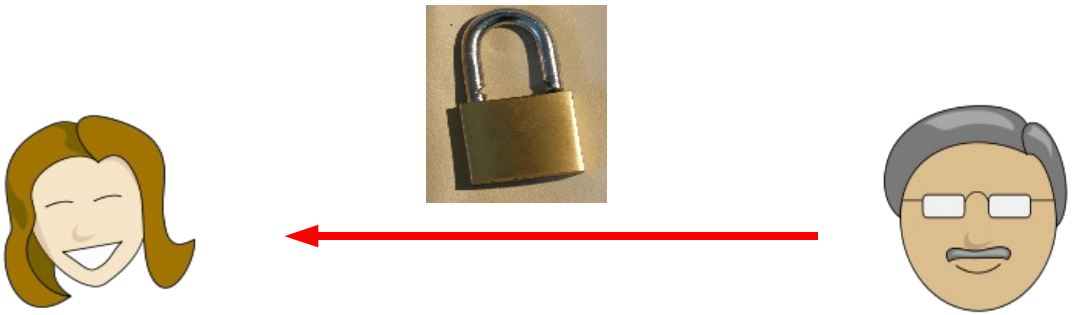
Nachbar von Bob. Hat sich an dessen Netzwerk angeschlossen und kann dort alle Daten sehen und verändern.

Das ist eigentlich egal, denn Alice und Bob haben die Nachricht verschlüsselt. Aber er hat einen Weg gefunden, sie trotzdem reinzulegen.

Man-in-the-middle Attack

Der Schwachpunkt ist die Schlüsselübergabe

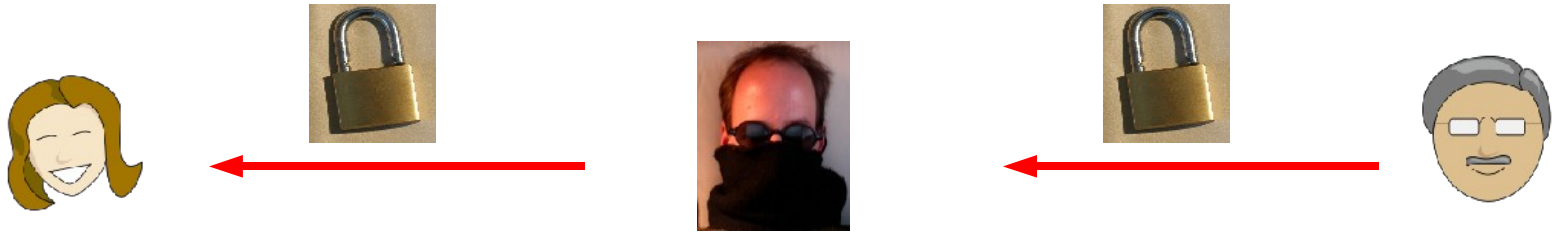
So war es eigentlich gedacht:



1.Bob schickt Alice seinen öffentlichen Schlüssel

Man-in-the-middle Attack

Aber so ist es gelaufen:

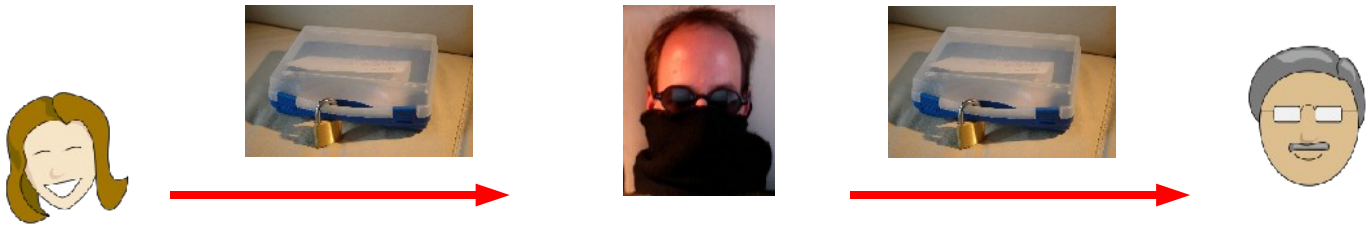


Man-in-the-middle Attack

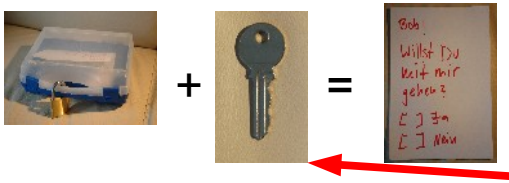
Aber so ist es gelaufen:

Alice glaubt, den öffentlichen Schüssel von Bob bekommen zu haben.
Tatsächlich hat sie aber den von Mallory bekommen.

Abfangen, entschlüsseln und wieder verschlüsseln

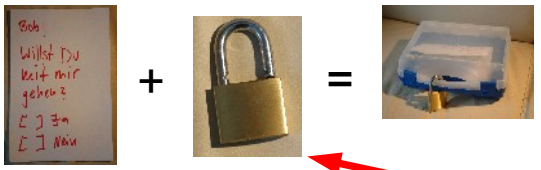


Mallory kann die Nachricht entschlüsseln, lesen und sogar verändern

1. 

Mallorys Privater Schlüssel

Anschließend verschlüsselt er sie mit Bobs öffentlichem Schlüssel und schickt die Nachricht weiter.

2. 

Bobs öffentlicher Schlüssel

Was tun wir dagegen?

Was tun wir dagegen?

- Alice muss Bobs angeblichen Schlüssel überprüfen, bevor sie ihn verwendet.
- Oder sie kann irgendwie anders feststellen, dass Bobs Schlüssel wirklich Bobs Schlüssel ist.
- Oder sie fliegt zu Bob und holt sich den Schlüssel direkt bei ihm ab.

Schlüssel überprüfen

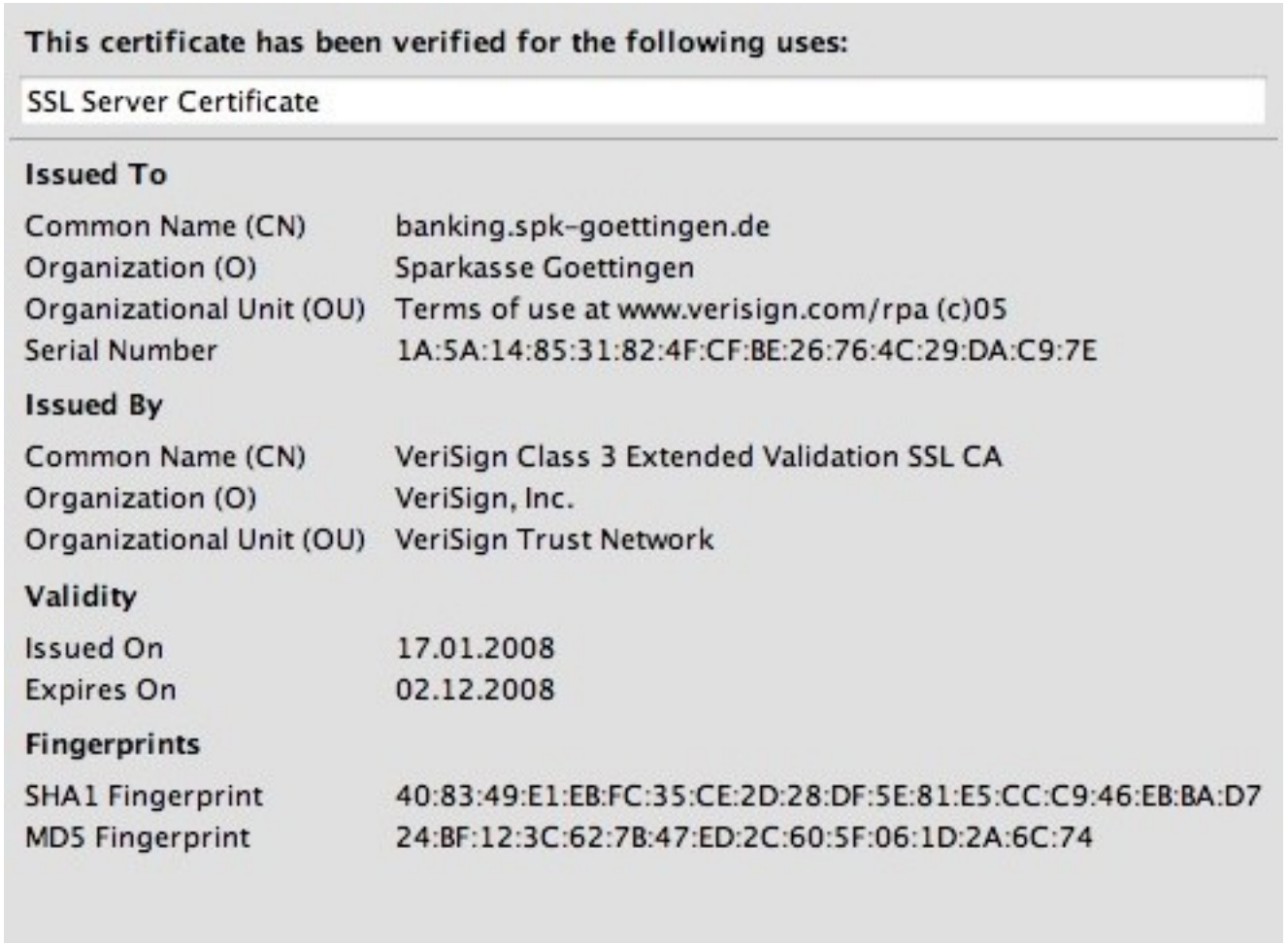
- Auf einem Kanal, auf dem sie über Bobs Identität sicher sein kann, zum Beispiel Telefon, den Schlüssel vorlesen.
- Die Sache hat nur einen Haken:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.5 (GNU/Linux)

mQGiBEPgoHoRBACNwcJDQUyOKgux9YVPeMl40hhTTZ9WLE2BP3V2oY/jeKEVvTco
q/fkUx1cWxHYJo5LE3im7RMZ9Vh4Wz4ZibNpQoB61E/HUV83VAa8LYXmYCyAKeq1
814CGRsM7ZK0BC5F8SeWls3LoWCXefgFsOU/X3MwKzaE8Gxx+plxBgz07wCgrRoy
I6kKMZZn5HQhN3INfXXxzV8D/RIv3cZgpi1KlMd2XtamOdPg74vLNYOYoEJMiPB6
u4gLy2KDOSYNPI4VPlpHKBvvEuKyDyJzPTt7SaClma93xnU8HxXM2v8E/WupVyMO
WUJPiLMSvmB2bLpRqdkLWp9ZICjVA8qmlH4Eqqcqv2MH3hZlG/qAUckjDZHITidO
YxrTA/9NP5lbLkzYsXqWRR7nEQMMUMBAvIjaKDcXsaKlAJXxf84cznj+Kj4wXn0w
4I7WngXl3Jb126sKsiGI4KwBoE74Bq06AAru/UaaRiREeFZ7ZKjDdZ6+Pm6VxmVh
i0rVpFPAgqu8pDU34TYfm9Zhe01BTtmQcC6UuSExpZhLo/tLwrQjS3Jpc2NoYW4g
Sm9kaWVzIDxram9kaWVzQHNlcm5ldC5kZT6IZAQTEQIAJAUCQ+CgegIbAwUJA8Jn
AAYLCQgHAwIDFQIDAxYCAQIeAQIXgAAKCRCsMIcX9BPdwSfTAJ4jT24zkfdbf5CL
TCFUA5VFQ/E9UQCgkuLVJtkIFv31ovWbTIUsasnBti+5AQ0EQ+CgexAEAJRZV+9A
5vGayJmEMONpu7nhpOJtPp2l0LeBCh13IKpj0TNUA+rDiIyxiuDyRw8yNuXx3LAh
h+b6Y/8ZMb6LulE5LnNdb4uG9acTAWpD82u964TDYFfjBqGyPEYxE8K4UiI6wdQ4
joKkERwPSVTFXdQ907Ybu7TyDQVm3fOgcQzTAAMGA/4m0lZbl4VTVkMPcpZUbu6h
YVk5Y+TRj3lOMTnJswBc+6IVD3VdSej0t1PS9Ay0khZ7+NNchAfI1IXqU8j0xj9c
EkWxUvspAqb5i9phMYj5nDgeobHEAcZBRajNep/llM03Af+P7WlD5ywPkwak6Yho
THigsCrNAQMOvx+rv+zsCYhPBBgRAgAPBQJD4KB7AhsMBQkDwmcAAAoJEKwwhxf0
E93BGpQAn3QfSdy7MUpg/NlxPMEkBqKVj7vWAJ9LIJRzo4/PBIw1mB9MZz3ZuzLe
pg==
=2LTq
-----END PGP PUBLIC KEY BLOCK-----
```

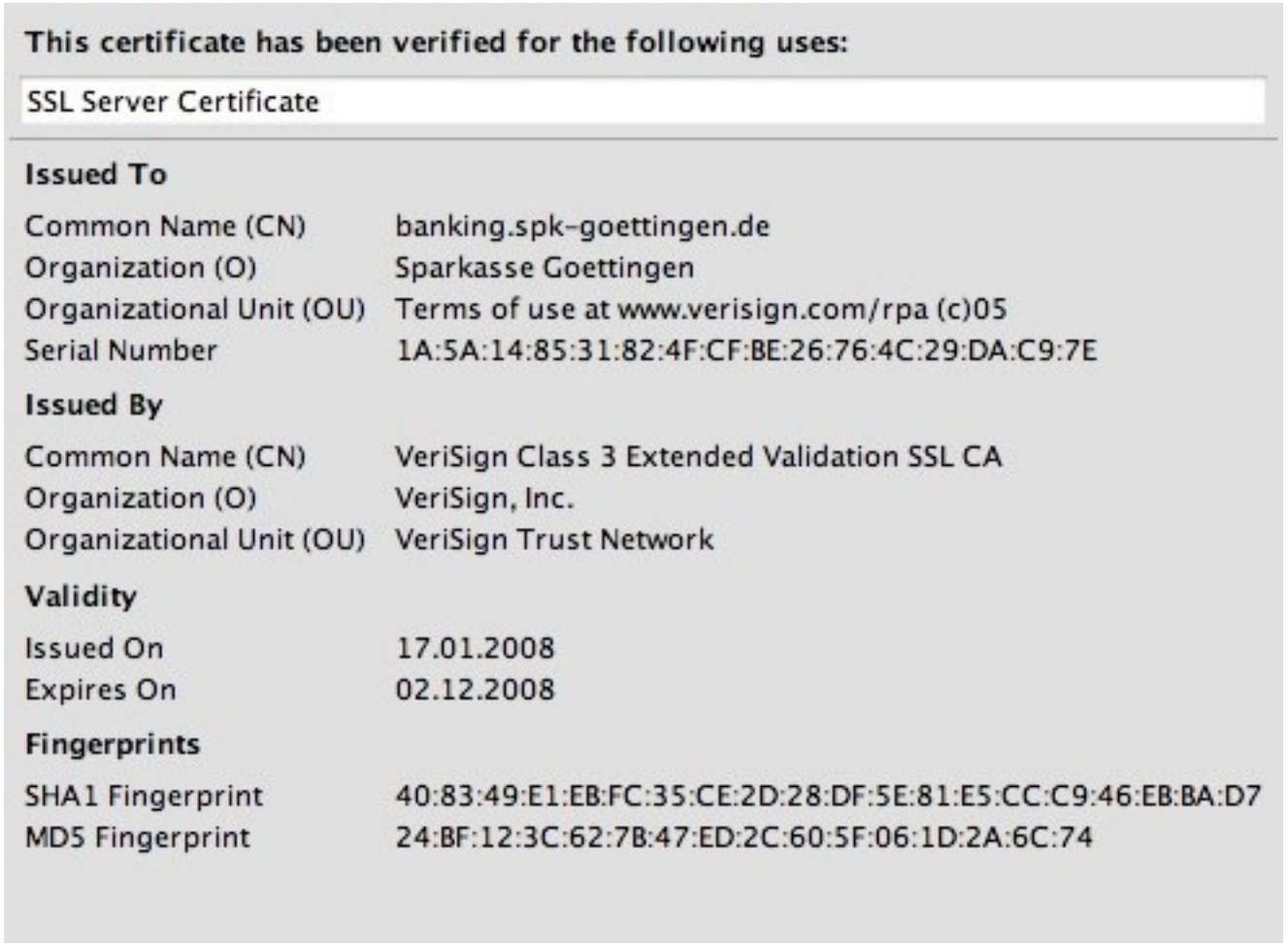
So ein Schlüssel ist ganz schön lang.

Fingerprint



Zur Überprüfung des Schlüssels nimmt man den Fingerprint. Der ist viel kürzer.

Fingerprint



Übrigens kann Bob auch ihre Sparkasse sein!

Was noch?

- Mehr Krypto-Wissen:
  - Digitale Signaturen
  - Public Key Infrastruktur
  - Key Server
  - Web of trust
  - CACert

Was noch?

- Unzählige Anwendungen, die Public Key Kryptografie verwenden, um die Kommunikation zu sichern:
  - Thunderbird: Mails Verschlüsseln
  - Pidgin: Chats verschlüsseln
  - Firefox: Webseiten verschlüsselt empfangen
  - ...

- Angela: Just think about it. Our whole world is sitting there on a computer. It's in the computer, everything: your, your DMV records, your, your social security, your credit cards, your medical records. It's all right there. Everyone is stored in there. It's like this little electronic shadow on each and everyone of us, just, just begging for someone to screw with, and you know what? They've done it to me, and you know what? They're gonna do it to you.

Das Netz. 1995.

Credits

- © Matt Britt for the Internet Routing Map:
  http://de.wikipedia.org/wiki/Bild:Internet_map_1024.jpg
  licensed under Creative Commons Attribution 2.5 License
- © Wapcaplet for the Alice and Bob heads:
  http://en.wikipedia.org/wiki/Image:Crypto_clipart1.svg
  licensed under „GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. Subject to disclaimers.“
- © For this Document: Krischan Jodies
  licensed under licensed under Creative Commons Attribution License 2.5
- Thanks, Guys!