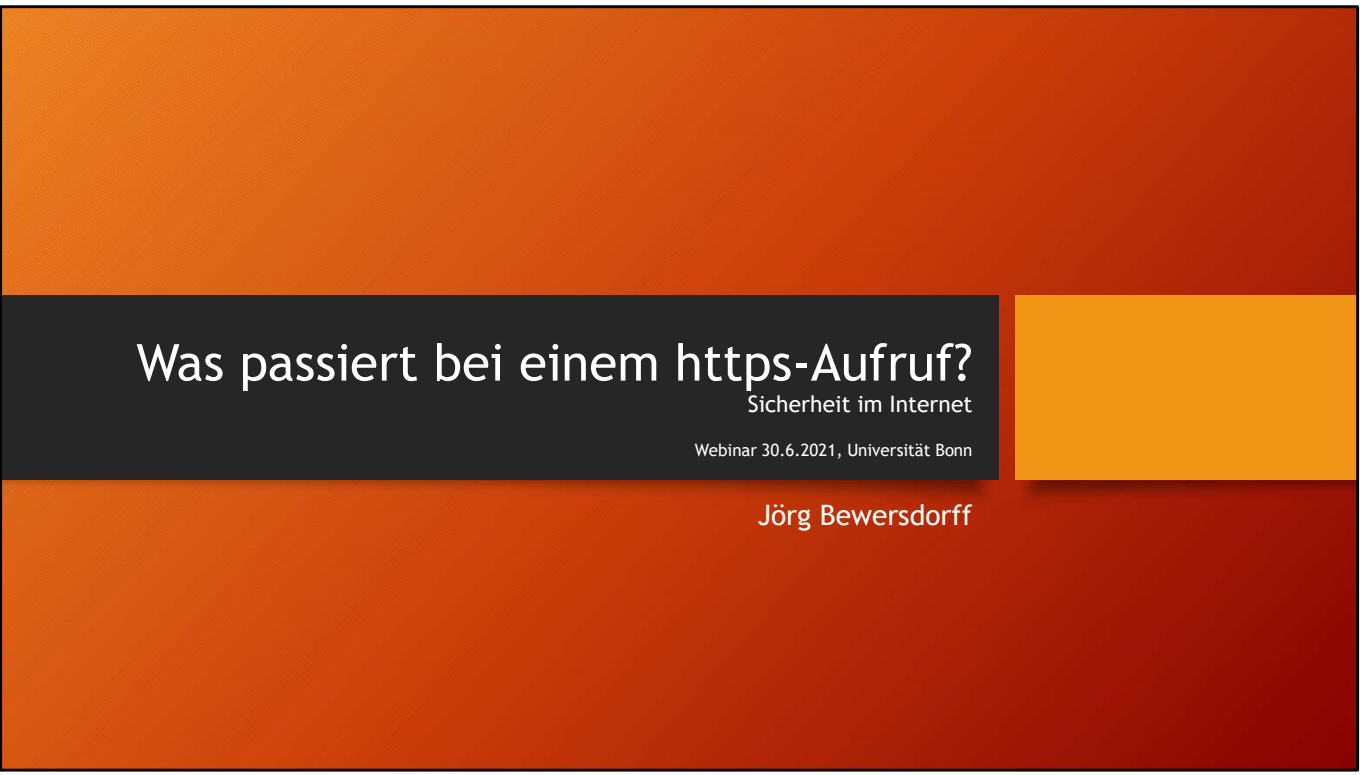


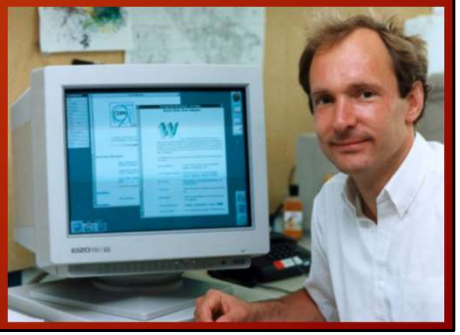
Vortragsmanuskript:

Angesichts der heutigen Dominanz amerikanischer Internetkonzerne ist es kaum vorstellbar, dass das „World Wide Web“ eine …

Internet: Von den Vorläufern zum WWW

- Ab 1969 wurden Rechnernetze von Forschungs-einrichtungen zunehmend untereinander vernetzt.
- Dabei schrittweise Entwicklung der heutigen Internet-Technologien, insbesondere von sog. „**Protokollen**“ (Vereinbarung über die Regelung von Kommunikation) für
  - die Adressierung von Rechnern und Netzen und
  - den Transport von Daten.

  für Anwendungen wie Email, FTP, …
- **1989 Konzept des WWW** als System verknüpfter Dokumente durch Tim Berners-Lee am CERN
- **1991 Start des WWW** …

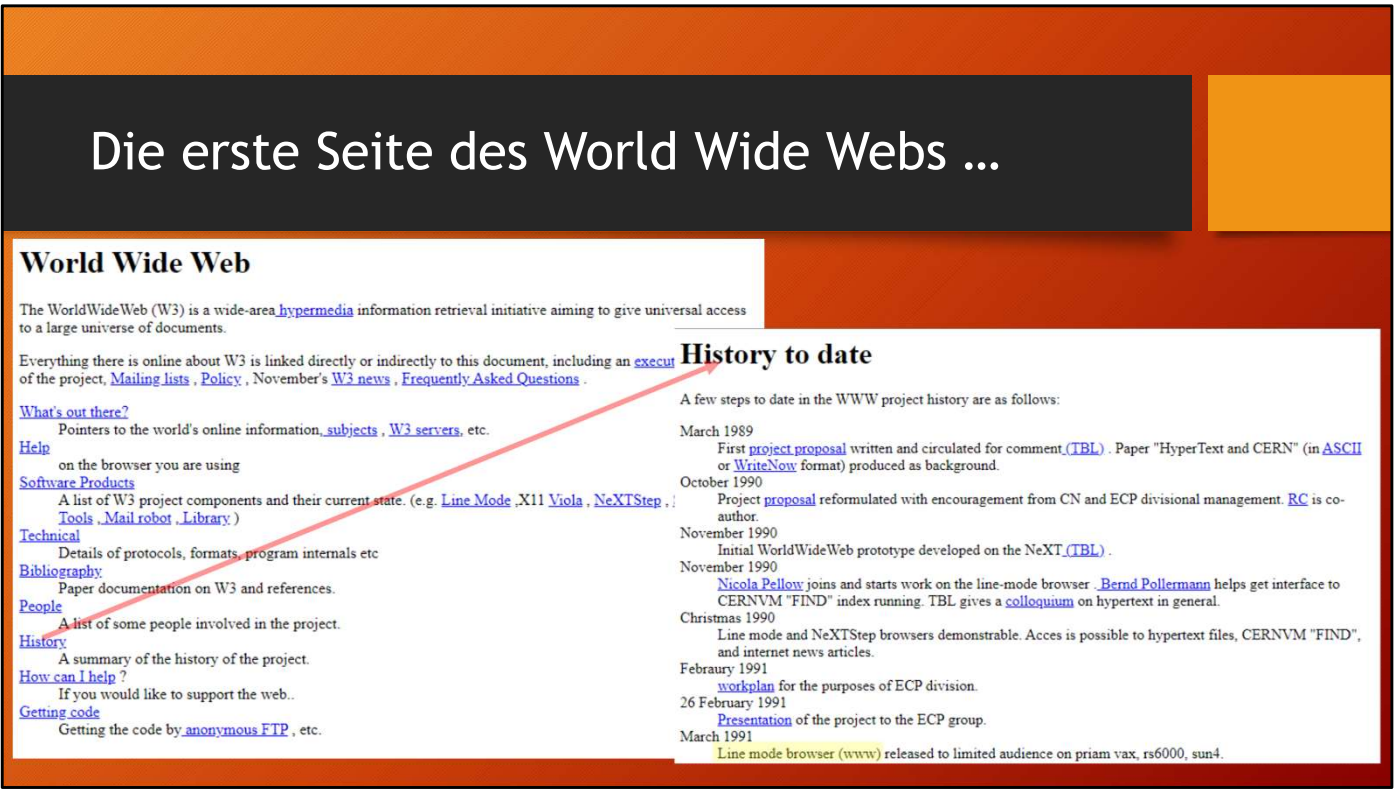


… europäische Erfindung ist.

Zwar startete das Internet als ein „Netz zwischen den Netzen“ von Forschungseinrichtungen schon in den 1970ern, aber erst das „World Wide Web“ machte das Internet intuitiv bedienbar und damit massentauglich, auch wenn einzelne der noch heute gebrauchten Anwendungen wie Email und FTP zur Dateiübertragung älter sind.

Das WWW entstand 1991 am CERN in Genf, also an einem Ort, wo die europäische Kooperation bestens funktioniert, wie es auch in anderen Bereichen wünschenswert wäre. Ein einzelnes Hadron im CERN-Beschleuniger passiert viele tausend Mal pro Sekunde die EU-Außengrenze zur Schweiz, völlig unberührt durch die Probleme beim EU-Schweizer-Rahmen-abkommen.

Die erste Seite des World Wide Webs …



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an execut of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

History to date

A few steps to date in the WWW project history are as follows:

March 1989
First project proposal written and circulated for comment (TBL) . Paper "HyperText and CERN" (in ASCII or WriteNow format) produced as background.
October 1990
Project proposal reformulated with encouragement from CN and ECP divisional management. RC is co-author.
November 1990
Initial WorldWideWeb prototype developed on the NeXT (TBL) .
November 1990
Nicola Pellow joins and starts work on the line-mode browser . Bernd Pollermann helps get interface to CERNVM "FIND" index running. TBL gives a colloquium on hypertext in general.
Christmas 1990
Line mode and NeXTStep browsers demonstrable. Acces is possible to hypertext files, CERNVM "FIND", and internet news articles.
Febraury 1991
workplan for the purposes of ECP division.
26 February 1991
Presentation of the project to the ECP group.
March 1991
Line mode browser (www) released to limited audience on priam vax, rs6000, sun4.

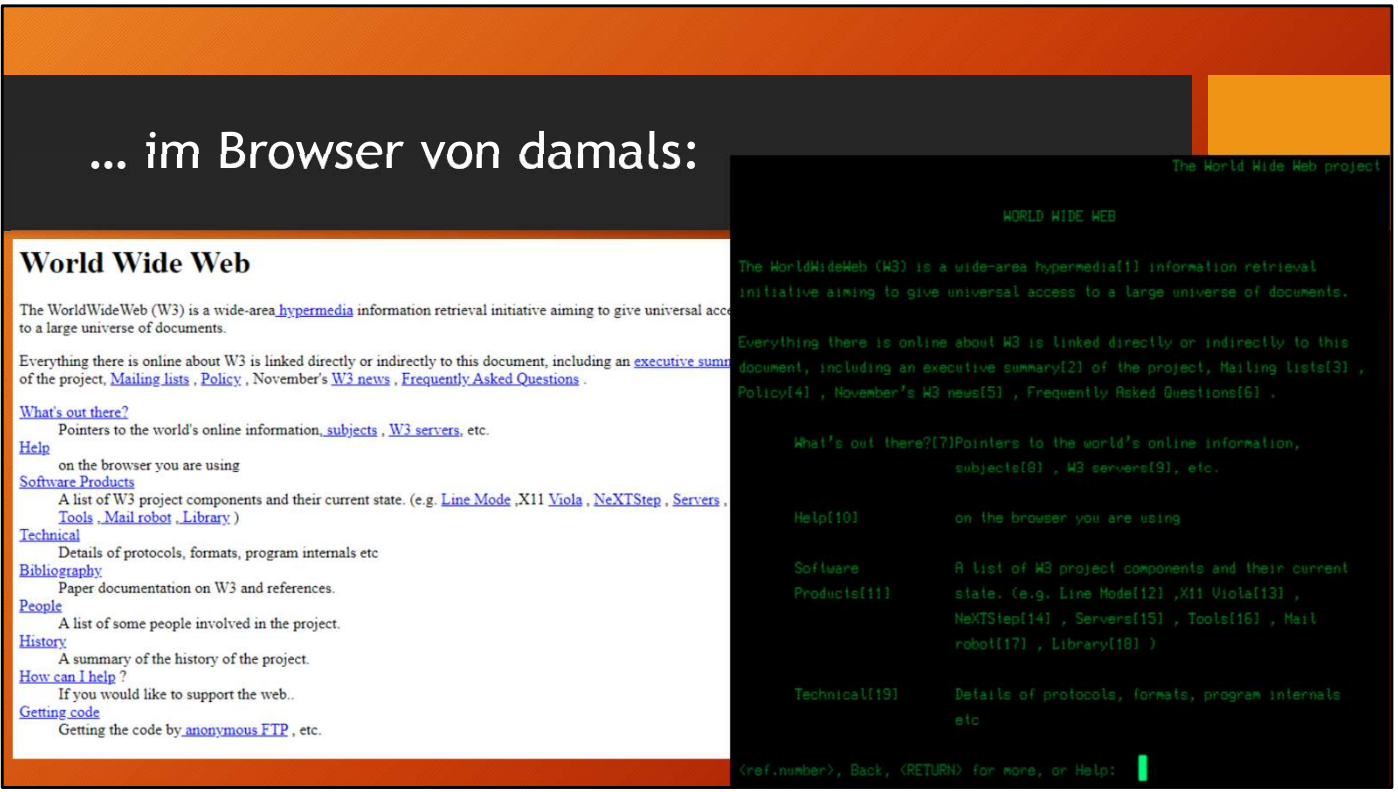
Links zu sehen ist die historisch erste WWW-Seite, die das Projekt selbst dokumentiert.

Ein Klick auf den „History“-Link führt zum rechts abgebildeten „History“-Dokument, wo unten, von mir gelb markiert, unter „März 1991“ die Programmierung des ersten Browsers erwähnt wird.

Das war damals noch ein rein textbasierter Browser, dessen primitive Funktionalität nur Textdokumente anzeigen konnte.

Das hat dann …

… im Browser von damals:



World Wide Web

The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal acc
to a large universe of documents.

Everything there is online about W3 is linked directly or indirectly to this document, including an executive summ
of the project, Mailing lists , Policy , November's W3 news , Frequently Asked Questions .

What's out there?
Pointers to the world's online information, subjects , W3 servers, etc.
Help
on the browser you are using
Software Products
A list of W3 project components and their current state. (e.g. Line Mode ,X11 Viola , NeXTStep , Servers ,
Tools , Mail robot , Library)
Technical
Details of protocols, formats, program internals etc
Bibliography
Paper documentation on W3 and references.
People
A list of some people involved in the project.
History
A summary of the history of the project.
How can I help ?
If you would like to support the web..
Getting code
Getting the code by anonymous FTP , etc.

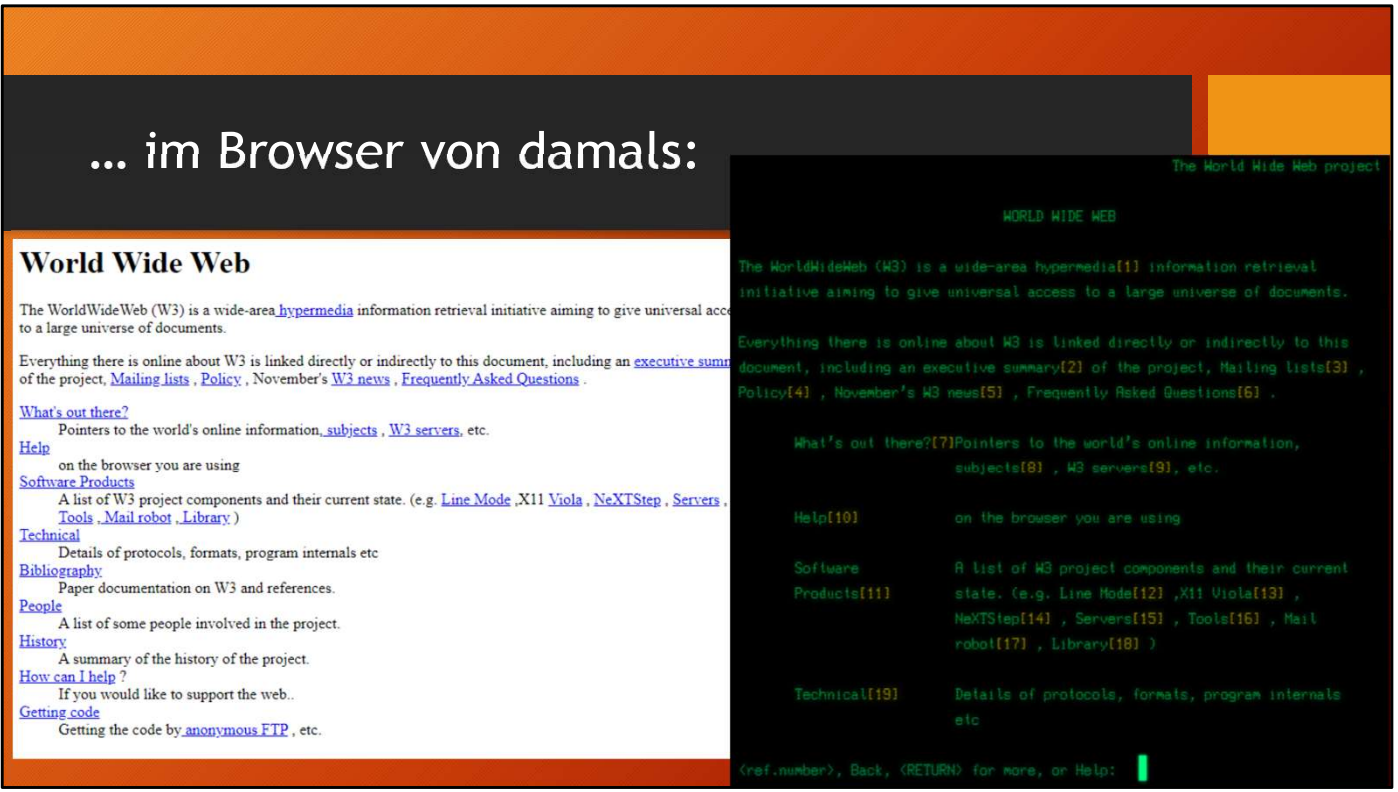
… wie rechts abgebildet ausgesehen.

Da die Bedienung ohne Maus oder gar Touchpad möglich sein musste, waren die Links durchnummeriert, etwas besser sichtbar …

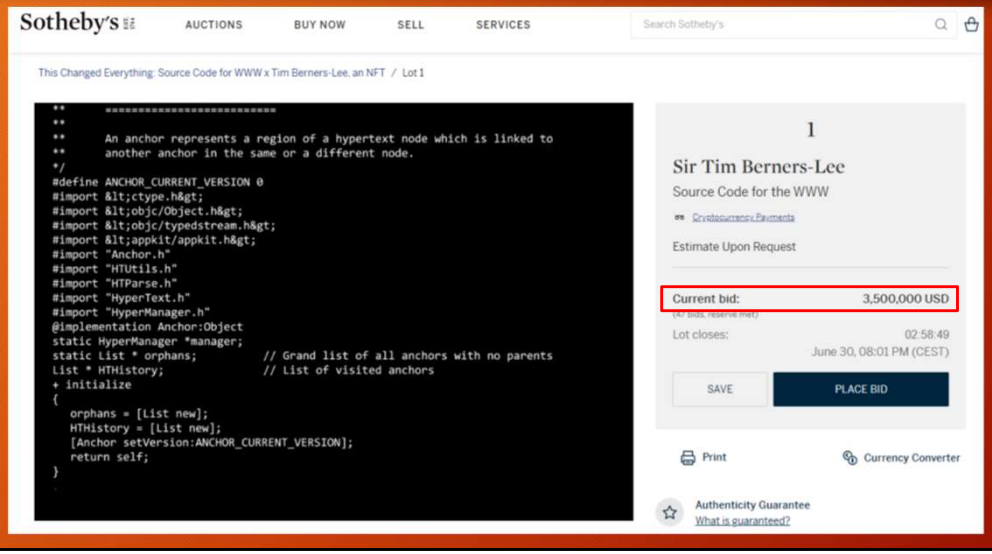
… in meiner Nachkolorierung.

Übrigens läuft beim Auktionshaus Sotheby‘s noch knapp zwei Stunden eine Versteigerung …

… im Browser von damals:



Bei Interesse …



… des Quellcodes von Berners-Lee inklusive einer künstlerischen Animation. Das Anfangsgebot von 1.000 USD war eben auf 3,5 Mill US-$ gestiegen.*

Eigentlich preiswert, wenn man bedenkt, was im Internet verdient wird.

(*) Nachbemerkung:
In den beiden letzten Stunden der Auktion stieg das Gebot noch auf 5.434.500 US-$.

WWW = HTML + HTTP

HTML= Hypertext Markup Language (eine sog. „formale Sprache“)

für die Beschreibung von Layout und Funktionalität von Webseiten:

- Die **Syntax** basiert maßgeblich auf Auszeichnungen in Form von Einschlüssen der Form `<kennung>…</kennung>`
- Die **semantische** Interpretation erfolgt durch einen Browser.

http://www.bewersdorff-online.de/meine-erste-seite.html

Dokumenten-Inhalt - Organisation

```
<!DOCTYPE html>
<html>
  <head>
    <title>Der Titel, der im Fenster angezeigt wird</title>
  </head>
  <body>
  <h1>Der "Header" meiner ersten Seite</h1>
  <h2>Das erste Kapitel</h2>
    <p>Der eigentliche Text ...</p>
    <p>Ein zweiter Absatz. Mehr zu HTML findet man z.B. bei
    <a href="http://de.wikipedia.org/wiki/HTML">Wikipedia</a>.</p>
  </body>
</html>
```

Das World Wide Web besteht im Wesentlichen aus zwei Technologien, deren Abkürzungen Sie alle von WWW-Adressen wie unten links kennen:

HTML und HTTP.

Gemeinsamer Kern beider Technologien ist das Kürzel „HT“ für „Hypertext“. Dazu gleich mehr.

Zunächst aber zu HTML:

HTML steht für „Hypertext Markup Language“ und ist eine sog. „formale Sprache“, wie Programmiersprachen definiert durch eine eindeutige Syntax, deren Grammatik-Regeln klar definieren, wie Dokumente gebildet werden dürfen.

Unten rechts sehen Sie ein Beispiel und links die Interpretation davon im Browser, wobei …

WWW = HTML + HTTP

HTML= Hypertext Markup Language (eine sog. „formale Sprache“)

für die Beschreibung von Layout und Funktionalität von Webseiten:

- Die **Syntax** basiert maßgeblich auf Auszeichnungen in Form von Einschlüssen der Form `<kennung>…</kennung>`
- Die **semantische** Interpretation erfolgt durch einen Browser.

http://www.bewersdorff-online.de/meine-erste-seite.html

Dokumenten-Inhalt - Organisation

```
<!DOCTYPE html>
<html>
  <head>
    <title>Der Titel, der im Fenster angezeigt wird</title>
  </head>
  <body>
  <h1>Der "Header" meiner ersten Seite</h1>
  <h2>Das erste Kapitel</h2>
    <p>Der eigentliche Text ...</p>
    <p>Ein zweiter Absatz. Mehr zu HTML findet man z.B. bei
    <a href="http://de.wikipedia.org/wiki/HTML">Wikipedia</a>.</p>
  </body>
</html>
```

… eine farbliche Markierung das Nachvollziehen der semantischen Interpretation vereinfacht.

Deutlich sichtbar sind die für die HTML-Syntax typischen, in Winkelklammern gesetzten Kennungen, Auszeichnungen bzw. Markups:

- *h1*, *h2* etc. für *header*, also Überschriften, verschiedener Ordnung, sowie
- p für *paragraph* , also Absatz.

Die Markups strukturieren den eigentlichen Textinhalt und ermöglichen damit ein entsprechendes Layout.

Funktional essentiell sind die Links mit Hilfe des Markups *a*. Die Vorbilder für die Links sind die Verweise in klassischen Lexika. Bereits in den 1980ern verwendete man Links in Textdateien, die man als „Hypertext“ bezeichnete.

WWW = HTML + HTTP

HTTP= Hypertext Transfer Protocol

Vereinbarung darüber, **wie Browser** (oder ein Programm mit einem Teil dieser Funktionalität) **und** das **Web-Server**-Programm **miteinander kommunizieren**:

- **Kommandos** für den Browser **zum Abruf von Dokumenten** und Senden der Daten von Web-Formularen.
- **Verhalten** des Web-Servers **beim Liefern der abgerufenen Daten** inkl. dem Fall einer Fehlersituation (z. B. bei Anforderung eines nicht existenten Dokuments).

Hin- und zurückgeschickte Textnachrichten

Anfrage:

```
GET meine-erste-seite.html HTTP/1.1
HOST: bewersdorff-online.de
User-Agent: User-Agent:Mozilla/5.0 (Windows NT 6.1;
...
[…]
```

Antwort:

```
HTTP/1.1 200 OK
Date: Mon, 14 Jun 2021 11:07:03 GMT
Last-Modified: Mon, 14 Jun 2021 09:24:28 GMT
[…]
Content-Type: text/html;

<!DOCTYPE html>
<html>
  <head>
[…]
```

Anmerkung:
HTTP ist ein „zustandsloses“ Protokoll, d. h.: Jeder Datenabruf steht eigentlich für sich allein, hat keinen Bezug zu ggf. vorherigen Abrufen. Um „Sessions“ zu ermöglichen, wurden Cookies erschaffen, die massenhaft für andere Zwecke verwendet werden.

Die zweite WWW-Basistechnologie ist HTTP, als sog. *Protokoll* eine Vereinbarung darüber, nach welchen Regeln Browser und Web-Server miteinander kommunizieren.

Konkret geben die Regeln im Wesentlichen vor, wie der Abruf einer bestimmten Datei durch den Browser als Client und die darauf erfolgende Antwort des Web-Servers aussehen muss. Rechts sieht man die gesendete Textnachricht, die ein Browser zum Server schickt, um dort eine Datei abzurufen. Darunter findet man die Textnachricht, die der Server als Antwort sendet,

Protokolle beschreiben auch immer, was im Fehlerfall zu tun ist, wenn z. B. die angeforderte Datei auf dem angesprochenen Webserver gar nicht existiert.

Eine kurze Anmerkung zu Cookies, die Ursprung nervender Werbung sind wie auch inzwischen vorgeschriebener Zustimmungsabfragen, die aber oft nicht weniger störend sind.

Bestimmte Cookies sind aber unverzichtbar, weil aufeinander folgende HTTP-Anfragen ohne Cookies *völlig unabhängig* voneinander wären: Logisch aufeinander aufbauende Datenabrufe wie z. B. ein Bestellprozess wären sonst gar nicht möglich.

Sicherheit …

- … spielte in der Anfangszeit des Internets nur in Bezug auf die Rechner und deren Schutz gegen unautorisierte Zugriffe eine Rolle,
- … **nicht** aber in Bezug Gefahren von **einfach möglichen (!) „Man-in-the-middle“-Attacken** zum
  - **Verfälschen von transportierten Inhalten,**
  - **Mitlauschen der Kommunikation,**
  - **Vortäuschen einer falschen Urheberschaft** des einen Inhalt Abrufenden („Client“ = Browser) und des Bereitstellenden („Server“) und

Im Internet können die transportierten Daten auf jedem Rechner, über den die Kommunikation abgewickelt wird, gelesen und sogar verfälscht werden. Man nennt dies „Man in the middle“-Attacken.

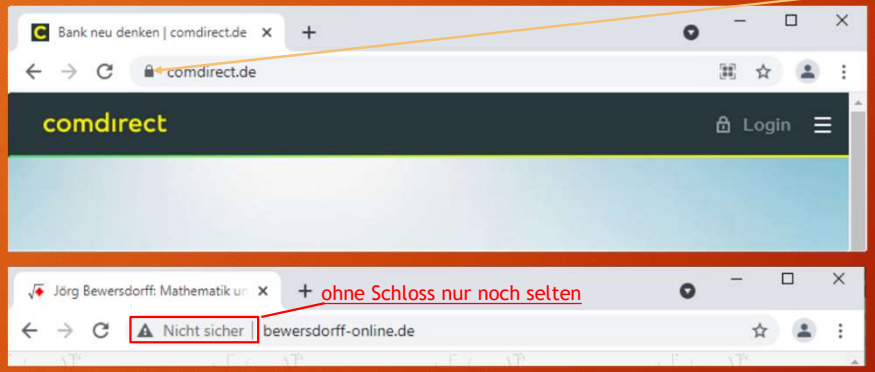
In den Anfangstagen des WWW, als nur wissenschaftliche Informationen ausgetauscht wurden, waren solche Angriffsmöglichkeiten natürlich unbedeutend.

Nicht nur beim Online-Banking wären aber Mitlauschen und Verfälschen von übertragenen Daten sowie das Vortäuschen einer falschen Identität fatal.

Daher …

Fatal, nicht nur beim Online-Banking …

Bin ich wirklich auf der Seite meiner Bank? Klicken Sie auf das Schloss-Symbol.

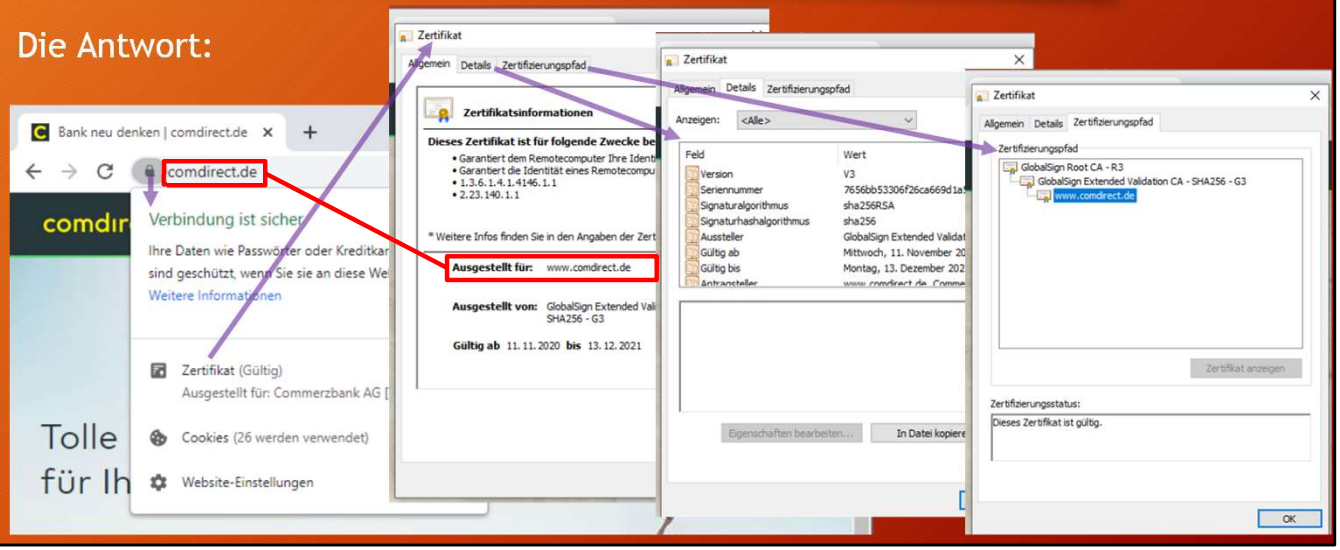


… können Sie heute bei fast allen WWW-Angeboten das gebotene Sicherheitsniveau prüfen. Klicken Sie einfach auf das Schloss-Symbol in der Adresszeile Ihres Browser.

Nicht verschlüsselt angebotene Inhalts sind die Ausnahme wie links unten.

Was der Browser verrät …

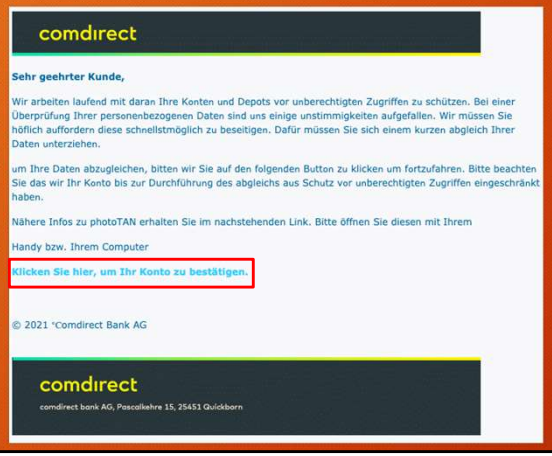
Die Antwort:



Der Browser gibt einerseits die Zusammenfassung, dass alles in Ordnung ist und, wenn Sie wollen, auch noch die Details, wenn auch in kryptischer Form.

Nicht immer wird die Antwort so ausfallen …

Kaum positiv nach einem Klick auf ein solches Email:



comdirect

Sehr geehrter Kunde,

Wir arbeiten laufend mit daran Ihre Konten und Depots vor unberechtigten Zugriffen zu schützen. Bei einer Überprüfung Ihrer personenbezogenen Daten sind uns einige unstimmigkeiten aufgefallen. Wir müssen Sie höflich auffordern diese schnellstmöglich zu beseitigen. Dafür müssen Sie sich einem kurzen abgleich Ihrer Daten unterziehen.

um Ihre Daten abzugleichen, bitten wir Sie auf den folgenden Button zu klicken um fortzufahren. Bitte beachten Sie das wir Ihr Konto bis zur Durchführung des abgleichs aus Schutz vor unberechtigten Zugriffen eingeschränkt haben.

Nähere Infos zu photoTAN erhalten Sie im nachstehenden Link. Bitte öffnen Sie diesen mit Ihrem

Handy bzw. Ihrem Computer

Klicken Sie hier, um Ihr Konto zu bestätigen.

© 2021 *Comdirect Bank AG

comdirect

comdirect bank AG, Pascalkehre 15, 25451 Quickborn

Mit solchen Mitteln würden sich auch die Links enttarnen lassen, die man in Phishing-Mails findet. Da auch andere Gefahren drohen, sollte man seine Neugierde aber besser zügeln.

Wie lässt sich Sicherheit erreichen?

- **HTTPS** (S für „secure“) ist eine **verschlüsselte Variante von HTTP**:
  - HTTPS basiert auf HTTP und einer zusätzlichen Verschlüsselung (TLS).
  - HTTPS **verschlüsselt den beidseitigen Datenverkehr** und erlaubt es, die **Integrität der besuchten Webseite** zu prüfen.
- Verschlüsseln heißt:

  Ein Text, der **Klartext**, wird mit einem **im Prinzip bekannten Verfahren** und einem **unbekannten Schlüssel** transformiert, so dass das Ergebnis, der **Geheimtext**, völlig unverständlich ist, es sei denn, man kennt den Schlüssel zum Dechiffrieren.
- **Symmetrisches** Verfahren: Dechiffrier-Schlüssel = Chiffrier-Schlüssel
- **Asymmetrisches** Verfahren: Dechiffrier-Schlüssel ≠ Chiffrier-Schlüssel

Mitlauschen und Verändern von Daten lassen sich verhindern, wenn die Daten verschlüsselt transportiert werden.

Eine Verschlüsselung besteht immer aus einem *Verfahren*, das im Prinzip sogar offengelegt werden kann, *und* einem Parameter, *Schlüssel* genannt, der das Verfahren parametrisiert und geheim bleiben muss.

Allerdings unterscheidet sich der spontane Besuch einer Website deutlich von der Kommunikation von z. B. einem Außenministerium zu seinen Botschaften, zu denen der Schlüssel zuvor sicher im Diplomatengepäck transportiert werden kann.

Was tun?

Glücklicherweise kennt die Mathematik seit 50 Jahren einen Ausweg in Form sogenannter asymmetrischer Verschlüsselungsverfahren, die auf einem *Paar* von Schlüsseln beruhen:

- einer zum *Ver*schlüsseln und
- einer zum *Ent*schlüsseln,

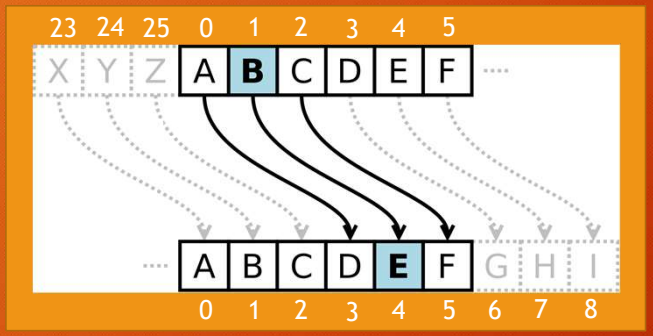
wobei die Kenntnis eines der beiden Schlüssel nicht dazu ausreicht, um den anderen zu bestimmen.

Leider ist die Mathematik der asymmetrischen Verfahren kompliziert. Auch ist die notwendige Rechenzeit deutlich höher als bei symmetrischen Verfahren. Asymmetrische Verfahren werden daher nur verwendet, wenn man ihre exklusiven Vorteile braucht.

Zum Einstieg schauen wir uns daher ein symmetrisches Verfahren an, und zwar …

Historisches Beispiel einer Verschlüsselung

Cäsar-Chiffre



Mathematisch handelt es sich um eine **Addition von 3**, wenn man

- die **Zeichen** beginnend mit „0“ **durchnummeriert**
- und **wie bei der Uhrzeit** nach dem Ende der Nummerierung wieder mit „0“ beginnt.

Zum Dechiffrieren ist der Wert 3 zu **subtrahieren**.

Das Verfahren gewährt offensichtlich keinerlei Sicherheit,

- weil es **viel zu wenig Schlüssel** zulässt (nur 26) und
- weil es **viel zu regelmäßig** ist.

… ein historisches, das aus heutiger Sicht keinerlei Schutz bietet: Einzelne Zeichen werden im Alphabet um drei Positionen verschoben.

Auf Grundlage einer Nummerierung der Buchstaben von 0 bis 25 kann man das Verfahren als rein mathematische Operation auffassen: Beim Verschlüsseln wird die Nummer um 3 erhöht und beim Entschlüsseln um 3 vermindert. Dabei muss analog zur Minutenzählung nach der letzten Nummer, nämlich der Nummer 25 für den Buchstaben „Z“ analog zur 59-ten Minute, wieder die Null kommen.

Viel mehr Sicherheit durch:

- **Man verschlüsselt ganze Textblöcke**, derzeit werden z.B. beim AES-Verfahren mindestens 128 Bit (das sind bis zu 16 „richtige“ Textzeichen) als Minimum angesehen.
- Auch der Schlüssel wird so lang gewählt. Es gibt damit **2^{128} verschiedene Schlüssel** (39-stellige Dezimalzahl).
- Jedem Textblock entspricht eine Zahl von 0 bis $2^{128} - 1$.
- **Zwei Transformationen**, deren **Kombination** deutlich undurchsichtiger ist als reine Additionen, werden genügend oft **wiederholt angewendet**.

➢ Ziel: Ein Angriff darf nicht viel leichter sein als ein **Durchprobieren aller möglichen Schlüssel**.


Bundesamt für Sicherheit in der Informationstechnik

BSI – Technische Richtlinie

Bezeichnung:	**Kryptographische Verfahren: Empfehlungen und Schlüssellängen**
Kürzel:	BSI TR-02102-1
Version:	2021-01
Stand:	24. März 2021

Das gerade gezeigte Verfahren war nicht nur simpel, sondern auch *monoalphabetisch*. Das heißt: Jedes „E“ wurde gleich transformiert, nämlich in ein „H“, egal wo es im Klartext steht. Dadurch sind statistische Analysen möglich des verschlüsselten Textes möglich, weil bestimmte Buchstaben wie „E“ in mitteleuropäischen Sprachen besonders häufig vorkommen.

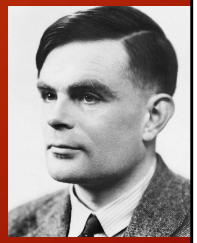
Ein solcher Angriff wird verhindert, wenn man ganze Textblöcke verschlüsselt. Als „Alphabet“ fungieren dann quasi alle Zeichenketten der gewählten Blocklänge. Auch diese Zeichenketten lassen sich durchnummerieren bzw. der Computer behandelt sie intern ja sowieso als Zahlen.

Zum Beispiel verschlüsselt das derzeit immer noch vom BSI, dem Bundesamt für Sicherheit in der Informationstechnik, als genügend sicher angesehene Verfahren AES-128 Blöcke einer Länge von 128 Bits, das sind bis zu 16 „richtige“ Textzeichen.

Als Transformation darf man natürlich keine simple Addition mit dem Schlüssel nehmen. AES kombiniert zwei Operationen auf binärer Ebene, die rechentechnisch schnell abzuwickeln sind, und wiederholt diesen Vorgang mehrfach, bis zwischen Klartext und verschlüsseltem Text keine statistischen Trends mehr erkennbar sind.

Codebreakers: Einst …

Von Alan Turing geknackt: Die ENIGMA der deutschen Wehrmacht



Alan Turing (1912–1954)

Nicht alles, was man für unknackbar hält, muss es auch sein. Bekannt ist, dass es dem britischen Mathematiker und Computerpionier Alan Turing mit seinem Team gelang, im Zweiten Weltkrieg die ENIGMA der deutschen Wehrmacht zu knacken.

Historiker halten dieses Ereignis für mit kriegs-entscheidend, insbesondere beim U-Boot-Krieg.

Der später wegen Homosexualität verurteilte Turing wurde 2013 durch die Queen posthum begnadigt. Turing hatte 1954 Selbstmord begangen während einer Hormonbehandlung, der er statt einer Gefängnisstrafe zugstimmt hatte.

Codebreakers: ... und zukünftig

Kinderseite des NSA von 2013:
”We love cryptology“

America's CryptoKids
Future Codemakers & Codebreakers

Home | Codes & Ciphers | Games & Activities | Student Resources | Characters | About NSA

CryptoKids® America's Future Codemakers & Codebreakers

Hi Kids!

Welcome to the NSA/CSS Kids' page.

We're the CryptoKids® and we love cryptology.

What's cryptology? Cryptology is making and breaking codes. It's so cool. We make codes so we can send secret messages to our friends. And we try to figure out what other people are writing about by breaking their codes. It's a lot of fun.

On this site, you can learn all about codes and ciphers, play lots of games and activities, and get to know each of us - Crypto Cat®, Decipher Dog®, Rosetta Stone®, Slate®, Joules™, T.Top®, CyberTwins™ Cy and Cyndi, and, of course, our leader CSS Sam®.

You can also learn about the National Security Agency/Central Security Service - they're America's real codemakers and codebreakers. Our Nation's leaders and warfighters count on the technology and information they get from NSA/CSS to get their jobs done. Without NSA/CSS, they wouldn't be able to talk to one another without the bad guys listening and they wouldn't be able to figure out what the bad guys were planning.

We hope you have lots of fun learning about cryptology and NSA/CSS. You might be part of the next generation of America's codemakers and codebreakers.

Hier zur Nachwuchsförderung die Kinderseite des US-Auslandsgeheimdienstes NSA, der die weltweite Kommunikation auswertet.

Die Seite stammt aus dem Jahr 2013, übrigens dem Jahr, in dem Frau Merkel das Abhören ihres Handys durch den NSA mit den Worten „Abhören unter Freunden – das geht gar nicht“ kommentierte.

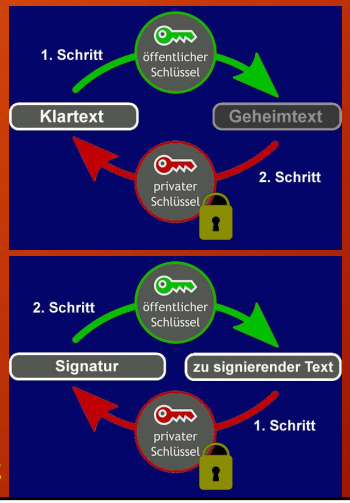
Asymmetrische Verschlüsselungsverfahren …

… beruhen auf zueinander passenden **Schlüsselpaaren** und komplizierten mathematischen Operationen. Sie erlauben

- eine **Verschlüsselung eines** Textes
  - 1. Schritt = **Verschlüsselung** des Textes
  - 2. Schritt = **Entschlüsselung** des Textes

wie auch

- eine **Authentizitätsprüfung eines Textes**
  - 1. Schritt = **Signierung** des Textes
  - 2. Schritt = **Prüfung** seiner **Authentizität**



Will zum Beispiel Alice ein Email an Bob geschützt schicken, dann muss sie es mit Bobs öffentlichem Schlüssel verschlüsseln.

Auf diese Weise kann den Email-Inhalt nur Bob dechiffrieren, weil einzig er seinen privaten Schlüssel kennt.

Meist wird nicht der gesamte Text signiert, sondern nur ein charakteristischer Fingerprint …

In Bezug auf *asymmetrische Verfahren* möchte ich zunächst erläutern, wie man sie einsetzt. Es gibt zwei verschiedene Schlüssel, die ihre Wirkung gegenseitig aufheben, egal welchen ich zuerst nutze. Der Clou entfaltet sich, wenn man einen Schlüssel veröffentlicht und den anderen als strenges Geheimnis hütet.

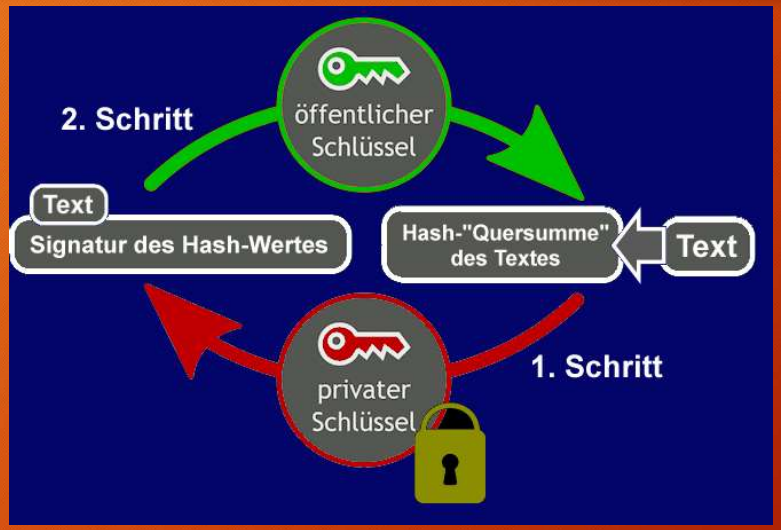
Das obere Bild zeigt die klassische Anwendung zur *Verschlüsselung*: Will zum Beispiel Alice ihr Email an Bob verschlüsseln, dann muss sie es mit *Bobs* öffentlichem Schlüssel tun, weil dann *nur* Bob den Text entschlüsseln kann, da nur er seinen privaten Schlüssel kennt.

Aber was ist, wenn es der Lauscherin Eve gelingt, dass Alice Eves öffentlichen Schlüssel für den öffentlichen Schlüssel von Bob hält?

Bevor wir dieses Problem lösen, wollen wir uns noch die unten dargestellte umgekehrte Reihenfolge anschauen, bei der ein Text zunächst mit dem privaten Schlüssel transformiert wird. Jeder kann nun auf das kryptische Ergebnis das öffentliche Schlüsselpendant anwenden und erhält dann den ursprünglichen Text und zugleich eine Bestätigung der *Authentizität* dafür, dass das private Schlüsselpendant im 1. Schritt vorgelegen hat.

Meistens geht man bei dieser zweiten Anwendung etwas anders vor, indem man …

Authentizität mit Signatur des Hash-Wertes



Der **Hash-Wert** ist eine Art „Quersumme“, aber mit einer Fingerprint-Funktionalität:

- einheitliche Länge unabhängig vom Ausgangstext,
- aufgrund des zur Hash-Bildung verwendeten Verfahrens lässt sich de facto trotzdem kein verfälschter Text finden, der zum gleichen Hash-Wert führt.

Mit dem privaten Schlüssel erhält man eine **Signatur einer einheitlichen Länge**.

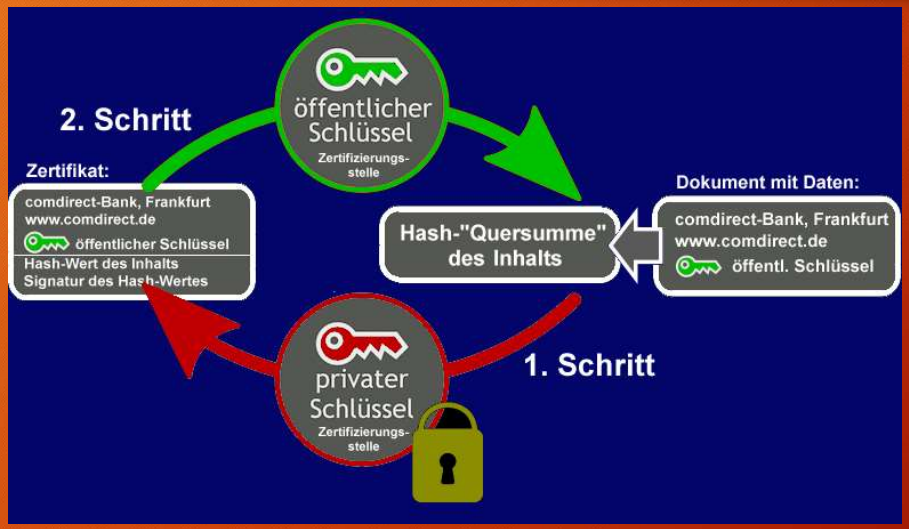
Text, Signatur und öffentlicher Schlüssel können dazu verwendet werden, die Authentizität des Textes nachzuweisen.

… vom Text zunächst eine Art Quersumme, Hash-Wert genannt, bildet. Dabei wird das Hashing-Verfahren derart gewählt, dass diese Verkürzung für den Ausgangstext insofern einen charakteristischen Fingerprint darstellt, da man, anders als bei einer klassischen Quersumme, de facto nie zwei Texte finden wird, die zum gleichen Hash-Wert führen.

Chiffriert man einen solchen Hash-Wert mit dem eigenen privaten Schlüssel, erhält man unabhängig von der Länge des Ausgangstexts eine Signatur mit einer *festen* Länge: Zu sehen auf jedem Kassenbon und eben auf dem Screenshot der comdirect-Seite. Diese Signaturen erlauben es, die Authentizität der Urheberschaft festzustellen, wenn man den öffentlichen Schlüssel kennt

Aber: Wie bei Alices Email an Bob beruht auch hier die Sicherheit des Verfahrens darauf, dass die Urheberschaft des öffentlichen Schlüssels gesichert ist!

Authentizität eines öffentlichen Schlüssels



Ein öffentlicher Schüssel der Bank als Webseiten-Betreiber kann durch eine **übergeordnete Stelle** mittels **deren privatem Schlüssel** in einem **Zertifikat** verbürgt werden.

Für Zertifikate und die ihnen zugrunde liegenden Angaben gibt es die Norm **X.509**.

Dieses Problem kann im Rahmen einer speziellen Authentizitätsprüfung gelöst werden. Dabei kommt eine übergeordnete Zertifizierungsstelle und ihr Schlüsselpaar zum Einsatz.

Die übergeordnete Zertifizierungsstelle *verbürgt die Authentizität* eines Dokuments, *Zertifikat* genannt, das für HTTPS-Seiten die Zuordnung zwischen

- Webadresse,
- dem Betreiber der Website und
- dem öffentlichem Schlüssel

beinhaltet.

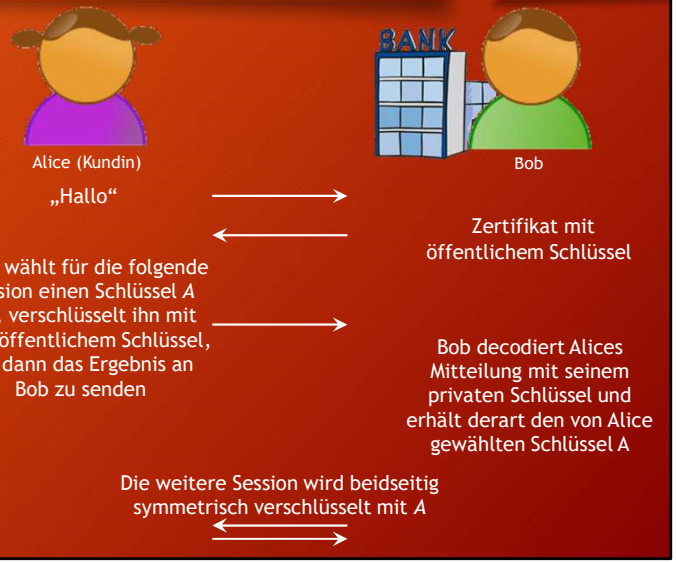
Häufig geschieht diese Art des Authentizitätsnachweises mehrstufig.

Und wie wird bei HTTPS verschlüsselt?

Zum Beginn des Webseiten-Besuchs wird

- mit einem **asymmetrischen Verschlüsselungsverfahren** ein **Schlüssel ausgetauscht**,
- der anschließend **für ein symmetrisches Verschlüsselungsverfahren** verwendet wird.

Klingt kompliziert, ist aber rechentechnisch VIEL einfacher als alles asymmetrisch zu verschlüsseln.



Nun können wir die im Titel gestellte Frage fast, nämlich bis auf die mathematischen Details, beantworten. Was passiert bei einem HTTPS-Aufruf?

Bankkundin Alice erhält zunächst das Zertifikat der aufgerufenen Domain von Bobs Bank. Das Zertifikat enthält insbesondere

- Bobs öffentlichen Schlüssel und
- den Namen von Bobs Bank als Inhaber der Domain.

Mittels der Zertifikatskette zeigt der Browser Alice an, dass der Inhaber der aufgerufenen Seite wirklich Bobs Bank ist.

Danach generiert Alices Browser

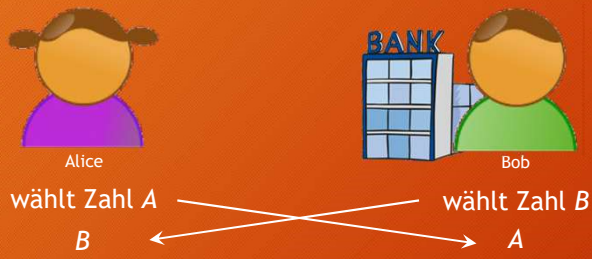
- einen Schlüssel A für ein symmetrisches Verfahren,
- verschlüsselt diesen Schlüssel A asymmetrisch mit Bobs öffentlichem Schlüssel und
- sendet ihn an Bob, der ihn mit seinem privaten Schlüssel entschlüsseln kann.

Die weitere Kommunikation im Online-Banking werden dann beidseitig mit dem Schlüssel A ver- und entschlüsselt.

Soweit das prinzipielle Prozedere.

Die Mathematik der asymmetrischen Verschlüsselungsverfahren will ich zumindest noch andeuten.

Vereinbarung eines Schlüssels: 1. Versuch



Beide einigen sich auf $A + B$ als Schlüssel! OK? Leider nicht!

Vereinbarung eines gemeinsamen Schlüssels, ohne dass einer der Kommunikationspartner ein Schlüsselpaar besitzt:

- Alice bzw. ihr Browser wählt eine Zahl *A*,
- Bob bzw. der Internet-Server seiner Bank wählt eine Zahl *B*

Alice und Bob verwenden nun die nicht übertragene Summe $A + B$ als Schlüssel.

Geht leider nicht: Wer die Übertragung in **beide** Richtungen mithört, kennt auch die Summe.

Da die mathematischen Details mannigfach sind, will ich mich auf ein Verfahren beschränken, bei der das mathematische Prinzip in etwas vereinfachter Version zum Einsatz kommt.

Es geht um ein Verfahren, wie sich zwei Seiten auf einen gemeinsamen Schlüssel einigen können, *ohne* dass eine Seite ein Schlüsselpaar besitzt.

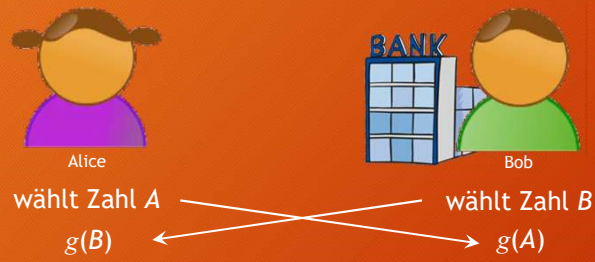
Im ersten Versuch probieren wir, dass der Browser von Alice eine riesige Zufallszahl *A* generiert und die zum Server von Bobs Bank schickt.

Parallel schickt der Server von Bobs Bank eine riesige Zufallszahl *B*, die er generiert hat, an den Browser von Alice.

Würde ein Lauscher nur *einen* der beiden Kanäle abhören, könnte man $A + B$ oder auch $A \cdot B$ als Schlüssel nehmen. Dumm ist aber, wenn ein Lauscher *beide* Kanäle abhört.

Aber der Ansatz vermittelt trotzdem eine gute intuitive Vorstellung davon, was möglich ist, weil man die Idee verfeinern kann …

Mit dem 2. Versuch klappt‘s aber …



Beide einigen sich auf einen Schlüssel, der sowohl aus *A* und $g(B)$ wie auch aus $g(A)$ und *B* berechenbar ist

Verfahren nach Diffie-Hellman:

Browser und Server transformieren ihre Werte *A* und *B* vor der Übertagung zu $g(A)$ und $g(B)$ mit einer geeigneten Rechenvorschrift g. Eine solche Transformation g ist muss zwei Eigenschaften erfüllen:

- *A* und *B* können de facto nicht aus $g(A)$ bzw. $g(B)$ zurückerrechnet werden (g wird dann Einweg-Funktion genannt).
- Aus jedem der beiden Paare *A*, $g(B)$ sowie *B*, $g(A)$, aber **nicht** aus dem Paar $g(A)$, $g(B)$, kann ein gemeinsames Geheimnis berechnet werden.

… zu folgendem Prozedere, dass nach Deffie-Hellman benannt ist. Wieder generieren der Browser von Alice und der Server von Bob astronomisch große Zufallszahlen.

Geschickt werden aber nicht die Originale, sondern die Transformationsergebnisse $g(A)$ und $g(B)$, wobei die Transformation *g* ein öffentlich bekanntes Verfahren nutzt.

Dabei ist die Transformation so gewählt, dass sie zwei Eigenschaften erfüllt:

- Einerseits kann aus einem Transformationsergebnis $g(A)$ der Ursprung *A* nicht berechnet werden, fast wie bei einer Verschlüsselung mit weggeworfenem Schlüssel. Man nennt eine solche Transformation *Einweg-Funktion*.

- Zweitens kann Alice aus dem Paar *A* und $g(B)$ eine Zahl berechnen, die Bob ebenso aus dem Paar *B* und $g(A)$ berechnen kann. Diese Zahl ist dann ein gemeinsames Geheimnis von Alice und Bob. Dabei ist es wichtig, dass die Kenntnis der *beiden* möglicherweise abgelauschten Transformations-ergebnisse $g(A)$ und $g(B)$ *nicht* ausreicht, um das gemeinsame Geheimnis zu berechnen.

Realisiert wird die Transformation g dadurch, dass man zur Berechnung des Ergebnisses $g(A)$ eine bestimmte Elementaroperation *A*-mal durchführt. Dafür gibt es …

Und wie funktioniert die Transformation g?

Erklärt werden kann das leider nur mit „etwas“ Mathematik:

$g(A) = s^A \; (= s \cdot s \cdot \ldots \cdot s \; [A\text{-mal}])$
$g(B) = s^B \; (= s \cdot s \cdot \ldots \cdot s \; [B\text{-mal}])$
$g(A)^B = \left(s^A\right)^B = s^{A \cdot B} = \left(s^B\right)^A = g(B)^A$

$g(A) = A \cdot P \; (= P + P + \ldots + P \; [A\text{-mal}])$
$g(B) = B \cdot P \; (= P + P + \ldots + P \; [B\text{-mal}])$
$B \cdot g(A) = B \cdot (A \cdot P) = (A \cdot B) \cdot P = A \cdot (B \cdot P) = A \cdot g(B)$

Dargestellt sind zwei alternative Wege, wobei die **Berechnungen** auf Basis allgemein fest vorgegebener Werte s bzw. P **nicht im „normalen“ Zahlenbereich** stattfinden, weil dort die Transformation g mittels

- wiederholter Multiplikation $A \rightarrow g(A) = s^A = s \cdot \ldots \cdot s \; [A\text{-mal}]$ (links) bzw.
- wiederholter Addition $A \rightarrow g(A) = A \cdot P = P + \ldots + P \; [A\text{-mal}]$ (rechts)

leicht **zurückgerechnet werden könnte**.

… im Wesentlichen zwei Ansätze einer konkreten Realisierung, die den Methoden der asymmetrischen Verschlüsselungsverfahren gleichen, aber – wie bereits angemerkt – etwas einfacher sind.

Dabei ist die *Idee* der für die Transformation verwendeten Rechenvorschrift eigentlich ganz einfach und verwendet nur elementare Rechenoperationen, die aus der Schule bekannt sind, kaum komplizierter als bei der Summe *A* + *B*.

Dargestellt sind zwei Varianten von Formeln, mit denen Alice (violett) und Bob (grün) jeweils auf verschiedenen Wegen zum gleichen Ergebnis kommen.

Allerdings ist die Realisierung der Berechnung nicht im normalen Zahlenbereich möglich, weil dort die links verwendete Potenzierung mit einer Logarithmus-Bildung bzw. und die rechts verwendete Vervielfachung mit einer Division zurückgerechnet werden könnten.

Geeignete Rechenbereiche (1)

Für den linken Ansatz der letzten Folie, bei der mit einer A- bzw. B-fach **wiederholten Multiplikation** transformiert wurde, eignen sich analog zur Minutenzählung **endliche Zahlenbereiche**, wobei als Basis nicht 60, sondern eine **Primzahl mit mehr als 900 Dezimalzahlen** fungiert.

Rechenbereiche, welche die gestellten Anforderungen erfüllen, sind die bereits erwähnten endlichen Zahlenbereiche, aber eben nicht zur Basis 60 wie bei der Minutenzählung, sondern auf Basis astronomisch großer Primzahlen, wobei das BSI beim Einsatz ab 2023 mindestens 900 Dezimalstellen empfiehlt.

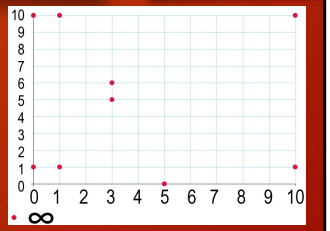
Etwas kleinere Zahlen von nur knapp 100 Dezimalstellen erfordert die zweite Methode, …

Geeignete Rechenbereiche (2)

Auch beim rechten Ansatz der vorletzten Folie, bei der mit einer A- bzw. B-fach **wiederholten Addition** transformiert wird, kommen solche **endlichen Zahlbereiche** zum Einsatz. Diesmal reichen **Primzahlen mit annähernd 100 Dezimalstellen**. Allerdings müssen innerhalb dieses Zahlbereichs zusätzlich noch zwei Wertepaare (a, b) sowie $P = (x, y)$ vorgegeben werden mit

$$y^2 = x^3 + ax + b$$

Der Clou ist, dass man solche Lösungen „addieren“ kann. Deshalb können Alice und Bob zu ihren astronomisch groß gewählten Zahlen A und B die Vielfachen $A \cdot P$ und $B \cdot P$ und schließlich $B \cdot (A \cdot P) = A \cdot (B \cdot P)$ berechnen.



$y^2 = x^3 - x + 1$ über $\mathbf{F}_{11}$

… die in der vorletzten Folie rechts dargestellt wurde.

Allerdings ist die zweite Methode samt ihrer mathematischen Basis deutlich komplizierter, weil es um Lösungen von Gleichungen geht. Daher bleibe ich bei Andeutungen.

Das Bild zeigt die Lösungen der darunter stehenden Gleichung im endlichen Zahlenbereich zur Primzahl 11. Jeder der neun roten Punkte stellt eine Lösung der Gleichung dar, wobei unten links ist noch *ein* Punkt dargestellt ist, der für einen unendlichen fernen Punkt steht.

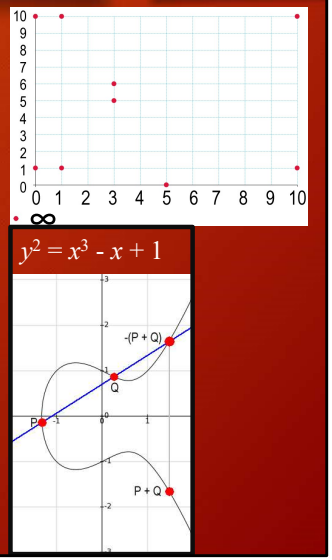
Die zehn Punkte bilden eine „elliptische Kurve über einem endlichen Körper“, womit sie merken, dass in der Mathematik, anders als in der Rechtsauslegung, Wortbedeutungen *völlig* irrelevant sind. Aber natürlich lassen sich die Begriffsbildungen durchaus historisch erklären, insbesondere der Begriff der Kurve. Dazu muss man …

Geeignete Rechenbereiche (2)

Auch beim rechten Ansatz der vorletzten Folie, bei der mit einer A- bzw. B-fach **wiederholten Addition** transformiert wird, kommen solche **endlichen Zahlbereiche** zum Einsatz. Diesmal reichen **Primzahlen mit annähernd 100 Dezimalstellen**. Allerdings müssen innerhalb dieses Zahlbereichs zusätzlich noch zwei Wertepaare (a, b) sowie $P = (x, y)$ vorgegeben werden mit

$$y^2 = x^3 + ax + b$$

Der Clou ist, dass man solche Lösungen „addieren“ kann. Deshalb können Alice und Bob zu ihren astronomisch groß gewählten Zahlen A und B die Vielfachen $A \cdot P$ und $B \cdot P$ und schließlich $B \cdot (A \cdot P) = A \cdot (B \cdot P)$ berechnen.



… nur die Lösungen der Gleichung im Bereich der reellen Zahlen des Zahlenstrahls untersuchen. Dann erhält man das Bild rechts unten, wo auch angedeutet ist, wie man zwei Lösungen *P* und *Q* der Gleichung, das sind in geometrischer Hinsicht die Punkte der Kurve, *addieren* kann.

Das Besondere an der Konstruktion sind zwei Dinge:

- Zum einen ist die Bezeichnung „Addition“ durchaus angebracht, weil sie die üblichen Gesetze der Addition und dabei insbesondere das Assoziativgesetz erfüllt.

- Zum anderen kann man die Koordinaten der „Summe“ *P*+*Q* aus den Koordinaten der beiden Summanden berechnen und zwar mit einer Formel, welche nur die vier Grundrechenarten verwendet, also keine Wurzeln beinhaltet.

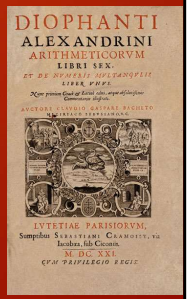
Ich will mit ein paar Anmerkungen zur Geschichte *schließen*:

Die ersten systematischen Untersuchungen von elliptischen Kurven begannen vor circa 200 Jahren.

Allerdings hat die Konstruktion, die der Addition von zwei Punkten auf der Kurve zugrunde liegt, im Prinzip bereits Diophant von Alexandria verwendet, und zwar im Fall, dass die beiden Punkte *P* und *Q* zusammenfallen, so dass eine Tangente im Punkt *P* betrachtet wird.

Diophantos von Alexandria

- Er lebte im spätantik-hellenistischen, römischbesetzten Alexandria,
- wahrscheinlich im 3. Jhd. n. Chr.
- Sein Werk „Arithmetica“ umfasst 13 „Bände“ (Kapitel/Schriftrollen):
  - Die Bände 1–3 und 8–10 liegen seit dem 15. Jhd. in griechischen Versionen vor,
  - die Bände 4–7 entdeckte 1968 Fuat Sezgin in arabischer Übersetzung in der Bibliothek des Imam-Reza-Schreins in der iranischen Pilgerstadt Maschhad,
  - die Bände 11–13 sind nur durch spätere Erwähnungen bekannt.
- Diophant verwendete als Erster (und Einziger für über tausend Jahre) eine Formelschreibweise. Außerdem multiplizierte er „abzuziehende“ (negative) Zahlen, ähnlich wie indische und chinesische Mathematiker, zur ungefähr gleichen Zeit.



Lateinische Übersetzung von 1621

Diophant lebte in spätantiken, römisch besetzten, aber kulturell weiterhin hellenistisch geprägten Alexandria. Wahrscheinlich lebte er im 3. Jahrhundert n. Chr., möglicherweise bereits etwas vorher.

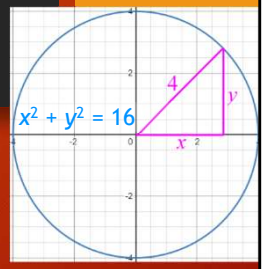
Sein Werk *Arithmetica* ist nur unvollständig überliefert, wobei dem vor drei Jahren verstorbenen, in Frankfurt lehrenden Orientalisten und Wissenschaftshistoriker Fuat Sezgin 1968 ein sensationeller Fund im Iran gelang, als er zuvor anders gedeutete Manuskripte als *Arithmetica-Fragmente* erkannte.

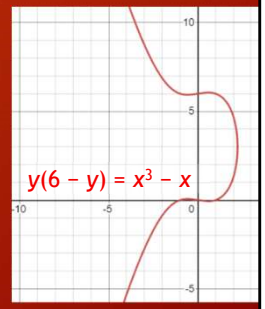
Diophant war der Erste und wohl für über tausend Jahre der Einzige, der sich einer Formelschreibweise bediente. Negative Zahlen waren für ihn keine Lösung, aber durchaus legitim als Zwischenergebnis einer Berechnung.

Methode von Diophant

- Diophant suchte **rationale Lösungen** zu Problemen, die wir heute mit zwei Unbekannten beschreiben wie
  - $x^2 + y^2 = 16$ (Koordinaten der Punkte eines Kreises mit Radius 4) und
  - $y(6 - y) = x^3 - x$ (im Koordinatensystem ergibt das eine elliptische Kurve).
- Seine Formelschreibweise erlaubte aber **nur eine Unbekannte**.
- Vielleicht deshalb reduzierte er seine Suche mit der Zusatzbedingung, in heutiger Notation und Interpretation*, einer geschickt gewählten Geradengleichung wie z. B. $x = 2y - 1$.
- Wenn bei einer elliptischen Kurve die Gerade zu zwei bekannten Punkten gewählt wird, entspricht das der Addition von zwei Punkten.

* Diophant kannte natürlich keine kartesischen Koordinaten!





Diophant löste Probleme, die wir heute als Gleichungen mit zwei Unbekannten interpretieren. Für ihn als Lösung zulässig waren einzig positive rationale Zahlen, also positive Brüche. Erweitert man den Zahlbereich auf alle Zahlen des Zahlenstrahls, lassen sich die Lösungen als Kurven im Koordinatenkreuz darstellen.

Im ersten Beispiel ist das ein Kreis mit Radius 4, was dem Satz von Pythagoras entspricht.

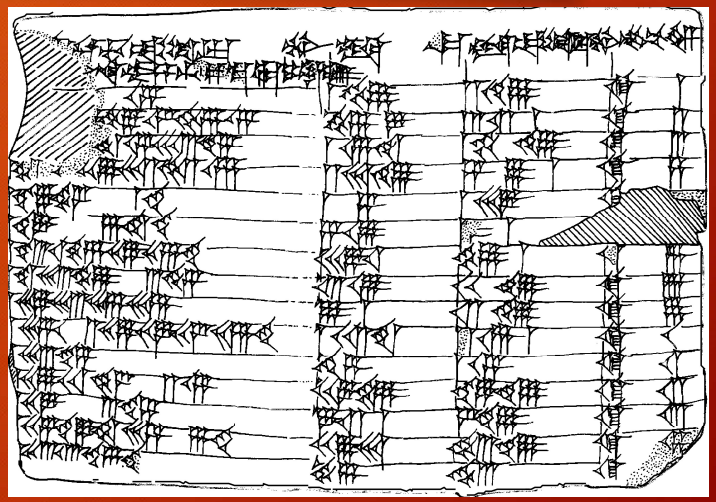
Die zweite Gleichung ist eine elliptische Kurve, auch wenn sie nicht ganz der eben beschriebenen Standardform entspricht.

Da Diophant nur mit einer Unbekannte rechnen konnte, machte er geeignete Ansätze einer Reduktion mit einer Zusatzbedingung, die einer Geradengleichung entspricht.

Aber dies ist genau das, was wir heute als Addition auf einer elliptischen Kurve verstehen.

Für Kreise ist das Verfahren einfacher und wird von Diophant ausführlicher beschrieben, aber wahrscheinlich ist es viel älter, …

Plimpton 322 (Larsa [Irak], 18. Jhd. v. Chr.)



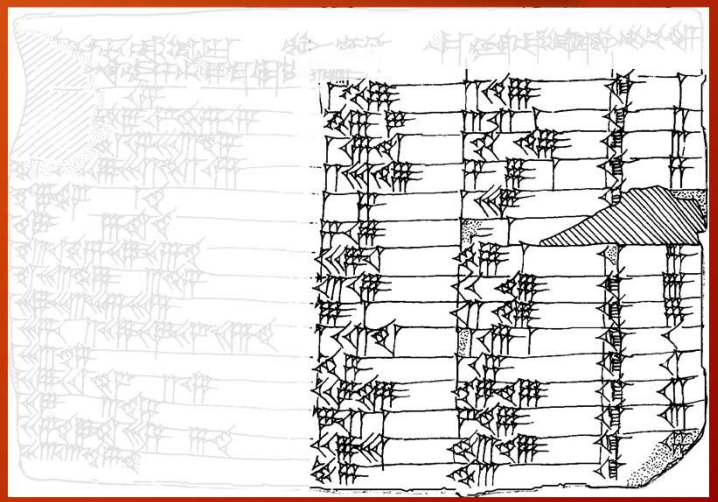
… wie Sie hier sehen.

Es handelt sich um Plimpton 322, eine babylonische Tontafel, die vor fast 4.000 Jahre in der heute irakischen Stadt Larsa erstellt wurde. Sie gehört zur G. A. Plimpton Collection der Columbia University und trägt dort die Nummer 322.

Bemerkenswert ist, dass der größte Teil des Inhalts trotz der babylonischen Keilschrift leicht zu entziffern ist, was ich Ihnen als Abschluss des mathematischen Teils zeigen möchte.

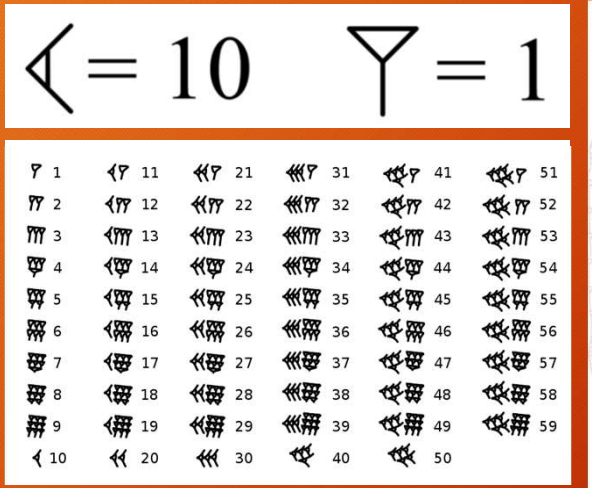
Zunächst konzentrieren wir uns auf den tabellarischen Teil der Tontafel mit 4 Spalten, die etwas mehr als die rechte Hälfte einnehmen …

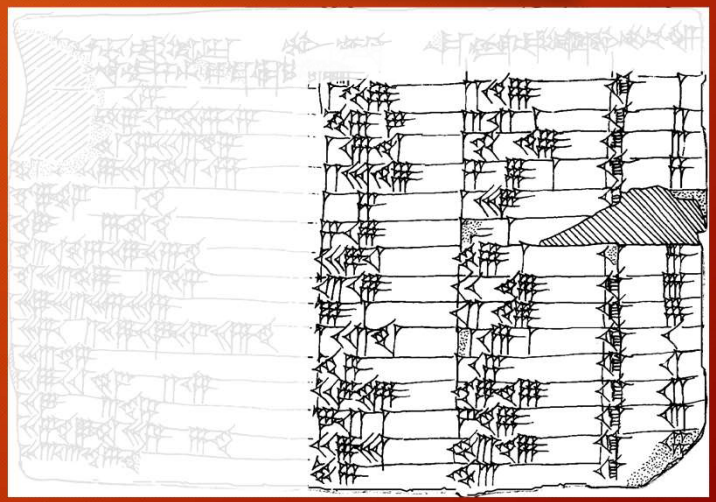
Plimpton 322: Tabelle von Zahlen …



Dort schauen wir uns die Spalten 1, 2 und 4 an, weil die dritte Spalte in jeder Zeile sowieso immer das Gleiche anzeigt.

Plimpton 322: Tabelle von Zahlen …





Babylonier verwendeten zur Schreibweise von Zahlen das Sexagesimalsystem, d. h. mit 60 als Basis statt mit 10 wie in späterer, indisch-arabischer Tradition.

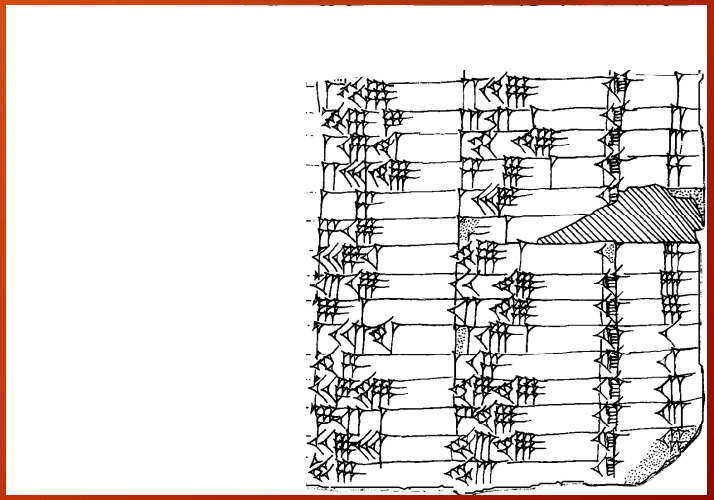
Und bis heute hat die Stunde 60 Minuten, weil uns nichts Besseres eingefallen ist.

Für ihr System brauchten die Babylonier 60 Ziffern, die sie in einer Art Dezimalansatz mit Zehnern und Einern schrieben.

Die *Ziffer* 0, die sie eigentlich gebraucht hätten, kannten sie ebenso wenig wie die *Zahl* 0 und ein Dezimaltrennzeichen, obwohl sie auch Nachkommazahlen kannten, sogar auch bei Plimpton 322 im linken ausgeblendeten Bereich.

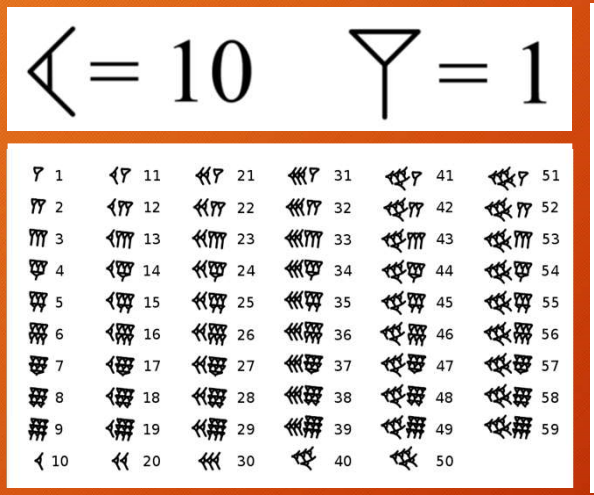
Ohne Ziffer 0 und ohne Dezimaltrennzeichen konnten …

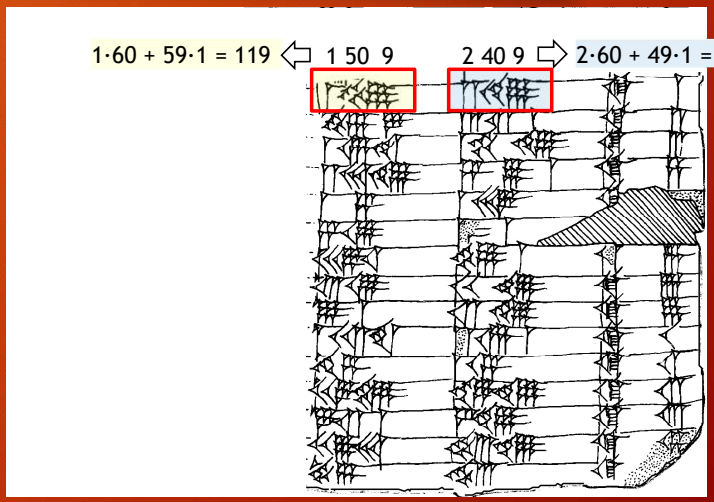
Plimpton 322: Tabelle von Zahlen …



… drei 10-er Zeichen sowohl für 30 wie auch für ein halb stehen, wie bei einer Zeitangabe von „30“, bei der nicht klar wäre, ob 30 Minuten oder 30 Sekunden, also eine halbe Minute, gemeint ist.

Plimpton 322: Wir entziffern …





Am einfachsten ist die rechte Spalte. Dort werden anscheinend nur die Zeilen durchnummeriert.

Und nun zur ersten Zeile:

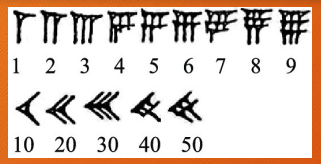
Wir sehen im gelben Bereich links-oben
- ein Einer-Zeichen, dann
- fünf 10er-Zeichen und schließlich
- neun Einer-Zeichen.

Das ergibt 1x60 + 59 = 119.

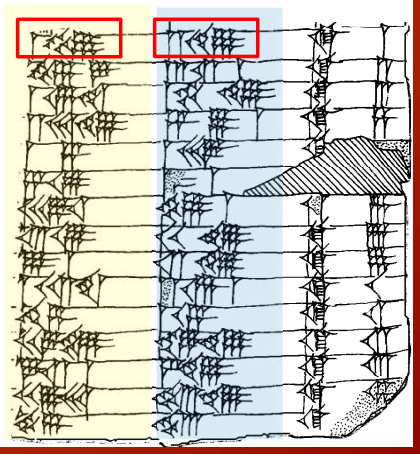
Im blauen Bereich oben-rechts ergibt sich analog 2x60 + 49 = 169.

Wir tragen die Ergebnisse 119 und 169 …

Plimpton 322: … und finden …



x	z		x (sexagesimal)	z (sexagesimal)
119	169		1; 59	2; 49
3367	4825		56; 7	1; 20; 25
4601	6649		1; 16; 41	1; 50; 49
12709	18541		3; 31; 49	5; 9; 1
65	97		1; 5	1; 37
319	481		5; 19	8; 1
2291	3541		38; 11	59; 1
799	1249		11; 10	20; 49
481	769		8; 1	12; 49
4961	8161		11; 22; 41	2; 16; 1
45	75		45	1; 15
1679	2929		27; 59	48; 49
161	289		2; 41	4; 49
1771	3229		29; 31	53; 49
56	106		56	1; 46

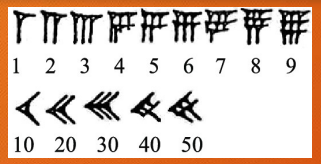


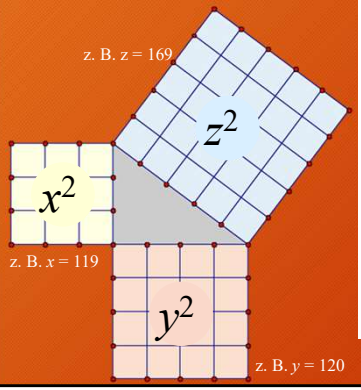
… in eine Tabelle ein und entziffern dann noch den Rest.

Auch damals gab es Schreibfehler, was beim Ritzen in den feuchten Ton unvermeidlich war. Die vermutlich notwendigen Korrekturen sind in rot, ein paar Ergänzungen an zerstörten Stellen sind in blau dargestellt.

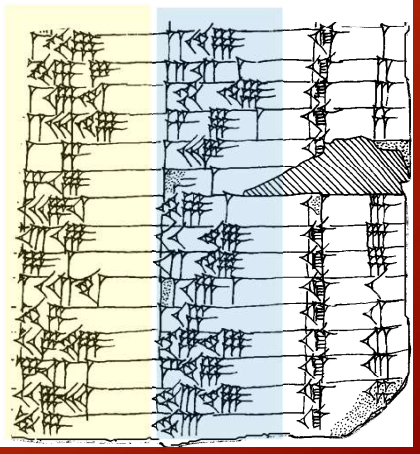
Dass diese wenigen Korrekturen und Ergänzungen das wohl vom Autor Gemeinte widerspiegeln, zeigt sich …

Plimpton 322: … Pythagoreische Tripel





x	z	$y = \sqrt{z^2 - x^2}$	x (sexagesimal)	z (sexagesimal)
119	169	120	1; 59	2; 49
3367	4825	3456	56; 7	1; 20; 25
4601	6649	4800	1; 16; 41	1; 50; 49
12709	18541	13500	3; 31; 49	5; 9; 1
65	97	72	1; 5	1; 37
319	481	360	5; 19	8; 1
2291	3541	2700	38; 11	59; 1
799	1249	960	11; 10	20; 49
481	769	600	8; 1	12; 49
4961	8161	6480	11; 22; 41	2; 16; 1
45	75	60	45	1; 15
1679	2929	2400	27; 59	48; 49
161	289	240	2; 41	4; 49
1771	3229	2700	29; 31	53; 49
56	106	90	56	1; 46



… in einem dann einheitlichen Tabellenaufbau mit lauter pythagoreischen Tripeln. Mit der Formel des Pythagoras können wir jeweils die Länge der unteren, mit *y* bezeichneten Seite des rechtwinkligen Dreiecks berechnen. Die so erhaltenen Werte sind in der mittleren, orange unterlegten Spalte aufgeführt. Alle Werte, und das ist das Bemerkenswerte, sind *ganze* Zahlen.

Die größte Zahl der Tabelle ist 18541, die dann für die Pythagoras-Formel noch zu quadrieren ist.

Resümee: Von der Grundlagenforschung …

- Für die Gleichung $y^2 = 1 - x^2$, die im Koordinatenkreuz einen Kreis um den Ursprung mit Radius 1 beschreibt, liefern die Zahlen von *Plimpton 322* Punkte mit rationalen Koordinaten wie z. B. x = 12709/18541 und y = 13500/18541.
- Diophant demonstrierte „sein“ Verfahren, um für die Gleichung $y(6 - y) = x^3 - x$, die eine elliptische Kurve beschreibt, einen Punkt mit rationalen Koordinaten, nämlich x = 17/9 und y = 26/27, zu berechnen. In heutiger Sicht war dies eine „Verdopplung“ des Punktes (−1,0).
- Eine Systematik dieser Mechanismen wurde beginnend mit dem 19. Jahrhundert erkannt. Dies erlaubte insbesondere eine Verallgemeinerung auf endliche Zahlenbereiche.

Obwohl es verschiedene Deutungen gibt für die Motivation von „Plimpton 322“, ist eine praktische Verwendung kaum plausibel. Zwar wurde der Satz von Pythagoras für das Tripel 3 − 4 − 5 bis fast in unsere Tage unter Verwendung einer Zwölfknotenschnur dazu verwendet, rechte Winkel zu realisieren. Aber die riesigen Werte der Tontafel braucht man dafür sicher nicht.

So erscheint die Geschichte der elliptischen Kurven als ein langer Prozess einer äußerst theoretischen Grundlagenforschung, die plötzlich eine eminent wichtige Anwendung erhalten hat.

… zur Praxis

Wohl niemand der Beteiligten hätte sich die Anwendungen vorstellen können, die heute sekündlich vieltausendfach erfolgen.

3. Domain Parameter Specification

In this section, the elliptic curve domain parameters proposed are specified in the following way.

For all curves, an ID is given by which it can be referenced.

p is the prime specifying the base field.

A and B are the coefficients of the equation y^2 = x^3 + A*x + B mod p defining the elliptic curve.

G = (x,y) is the base point, i.e., a point in E of prime order, with x and y being its x- and y-coordinates, respectively.

q is the prime order of the group generated by G.

h is the cofactor of G in E, i.e., #E(GF(p))/q.

3.3. Domain Parameters for 224-Bit Curves

Curve-ID: brainpoolP224r1

p = D7C134AA264366862A18302575D1D787B09F075797DA89F57EC8C0FF

A = 68A5E62CA9CE6C1C299803A6C1530B514E182AD8B0042A59CAD29F43

B = 2580F63CCFE44138870713B1A92369E33E2135D266DBB372386C400B

x = 0D9029AD2C7E5CF4340823B2A87DC68C9E4CE3174C1E6EFDEE12C07D

y = 58AA56F772C0726F24C6B89E4ECDAC24354B9E99CAA3F6D3761402CD

q = D7C134AA264366862A18302575D0FB98D116BC4B6DDEBCA3A5A7939F

h = 1

Auszug aus einer öffentlich zugänglichen, für kryptographische Anwendungen empfohlenen Bibliothek von ausgiebig untersuchten elliptischen Kurven. Die Parameter sind hexadezimal dargestellt, d. h. zur Basis 16 mit den Ziffern 0, …, 9, A = 10, B = 11, …, F = 15.

Insofern denken Sie vielleicht beim nächsten Aufruf Ihres Online-Bankings daran, dass elliptische Kurven wie die hier aus einer Dokumentation entnommene für Ihre Sicherheit sorgen.

Das alles beruht auf Ergebnissen epochaler Grundlagenforschung

- vor 40 Jahren beim CERN,
- vor über 100 Jahren bei elliptischen Kurven
- und das auf Basis einer 4.000 Jahre alten Tradition eines Interesses für mathematische Gesetzmäßigkeiten.

Und so geht es weiter: Bei der Sicherheit im Internet wird die Quantenphysik in den nächsten Jahren große Veränderungen bringen:

- Quantencomputing wird neue Angriffe ermöglichen.
- Dafür werden mit Quantenkommunikation neue Sicherheitskonzepte möglich werden.

Dass die Mathematik vor 100 Jahren Quantenmechanikern wie Werner Heisenberg und Ernst Schrödinger die mathematischen Konzepte bot, die sie benötigten, brauche ich kaum zu erwähnen.

Ich …

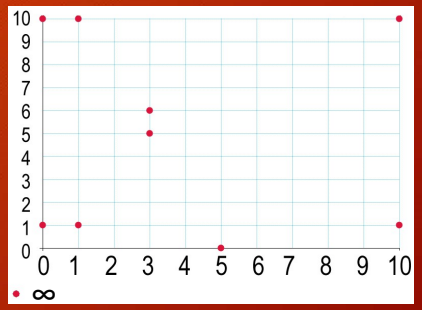
… danke für Ihre Aufmerksamkeit.

Anhang: Elliptische Kurve $y^2 = x^3 - x + 1$ über $\mathbf{F}_{11}$

Additionstabelle für die 10 Punkte:

+	∞	(0,1)	(0,10)	(1,1)	(1,10)	(3,5)	(3,6)	(5,0)	(10,1)	(10,10)
∞	∞	(0,1)	(0,10)	(1,1)	(1,10)	(3,5)	(3,6)	(5,0)	(10,1)	(10,10)
(0,1)	(0,1)	(3,6)	∞	(10,10)	(3,5)	(0,10)	(1,1)	(10,1)	(1,10)	(5,0)
(0,10)	(0,10)	∞	(3,5)	(3,6)	(10,1)	(1,10)	(0,1)	(10,10)	(5,0)	(1,1)
(1,1)	(1,1)	(10,10)	(3,6)	(10,1)	∞	(0,1)	(5,0)	(3,5)	(0,10)	(1,10)
(1,10)	(1,10)	(3,5)	(10,1)	∞	(10,10)	(5,0)	(0,10)	(3,6)	(1,1)	(0,1)
(3,5)	(3,5)	(0,10)	(1,10)	(0,1)	(5,0)	(10,1)	∞	(1,1)	(10,10)	(3,6)
(3,6)	(3,6)	(1,1)	(0,1)	(5,0)	(0,10)	∞	(10,10)	(1,10)	(3,5)	(10,1)
(5,0)	(5,0)	(10,1)	(10,10)	(3,5)	(3,6)	(1,1)	(1,10)	∞	(0,1)	(0,10)
(10,1)	(10,1)	(1,10)	(5,0)	(0,10)	(1,1)	(10,10)	(3,5)	(0,1)	(3,6)	∞
(10,10)	(10,10)	(5,0)	(1,1)	(1,10)	(0,1)	(3,6)	(10,1)	(0,10)	∞	(3,5)

Point:	(1,1)
Inverse:	(1,10)
Order of subgroup:	10
Generated subgroup	(1,1) → (10,1) → (0,10) → (3,6) → (5,0) → (3,5) → (0,1) → (10,10) → (1,10) → ∞



Quelle: graui.de/code/elliptic2/

Die Kurve besteht aus 10 Punkten einschließlich des unendlich fernen Punktes. Die Gruppe ist zyklisch mit z.B. (1,1) als erzeugendem Element