logjam
weak Diffie-Hellman

Georg Held
Student HaW-Landshut

Einleitung - Was ist logjam?

Einleitung - Urban Dictionary

logjam (/define.php?term=logjam)

logjam (log-jam) - noun

1) When you defecate and a chunk of fecal matter is pinched off/left behind and you are unable to push this small remainder out.

As a result, when you wipe, you can never get completely clean, because every **time (/define.php?term=time)** you apply toilet paper you push a little bit of the pinch off poop nugget out, re-dirtying your balloon knot.

Einleitung - weakdh.org

Exploit auf Protokollebene gegen TLS mit DHE publiziert 2015 von einem multinationalen Team von Forschern des CNRS, Inria Nancy-Grand Est, Inria Paris-Rocquencourt, Microsoft Research, Johns Hopkins University, University of Michigan und der University of Pennsylvania

Einleitung - Agenda

- Einleitung
- TLS-Protokoll
- DH Schlüssel Austausch
- Number Field Sieve
- logjam
- Fazit

TLS

TLS - Was ist TLS?

- dient zum Aufbau einer sicheren Kommunikation über unsichere Kanäle
- besteht (fast) immer aus zwei Phasen: Schlüsselaustausch und verschlüsselte Kommunikation => Notwendigkeit von asymmetrischer und symmetrischer Kryptographie
- beruht auf X.509 Zertifikaten (öffentlicher RSA Schlüssel + CA Signaturen)
- das wichtigste Werkzeug für verschlüsselte Kommunikation im Internet
- verwendet verschiedene Cipher Suits, die sich über die Jahre geändert haben

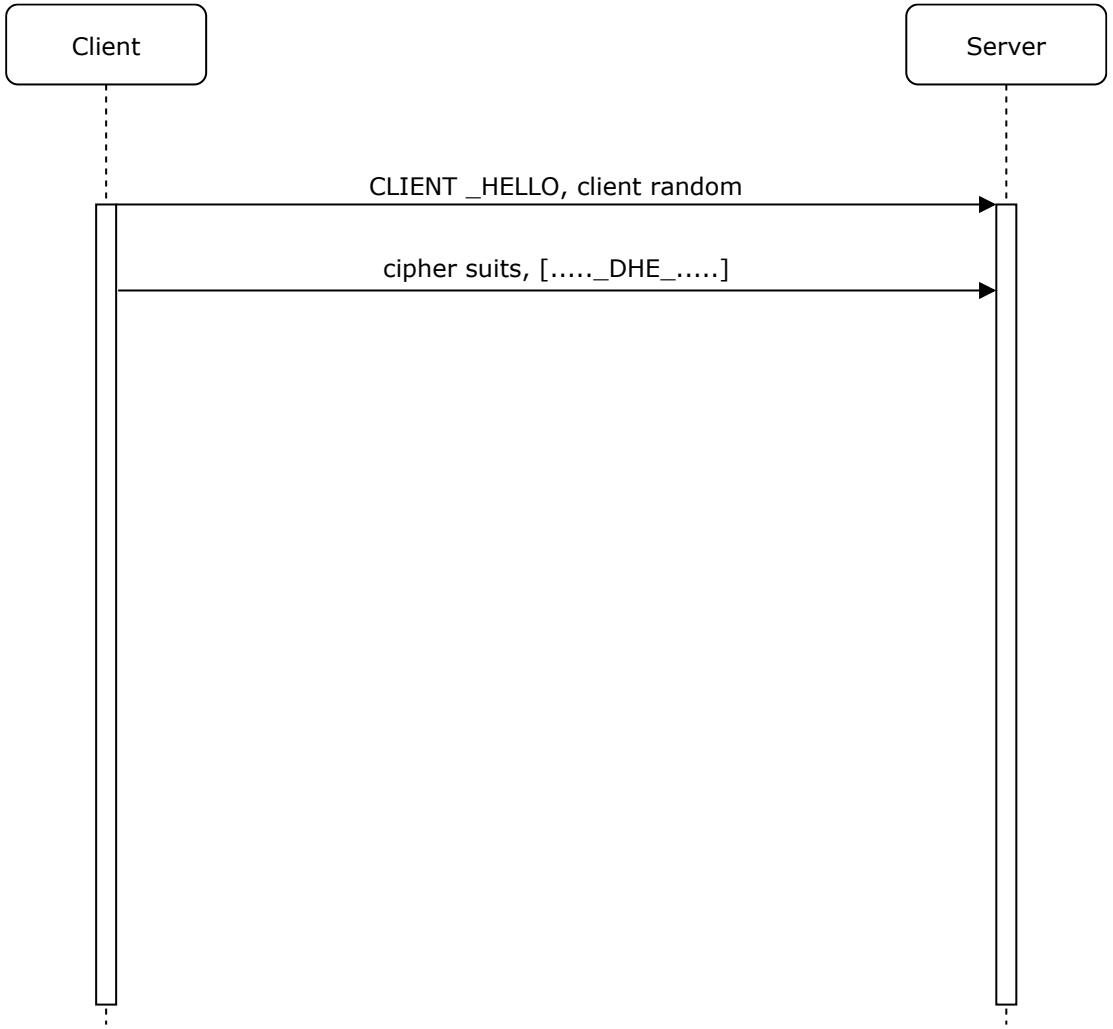
TLS - Cipher Suits

```
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_WITH_IDEA_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_DSS_WITH_DES_CBC_SHA
TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_RSA_WITH_DES_CBC_SHA
TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

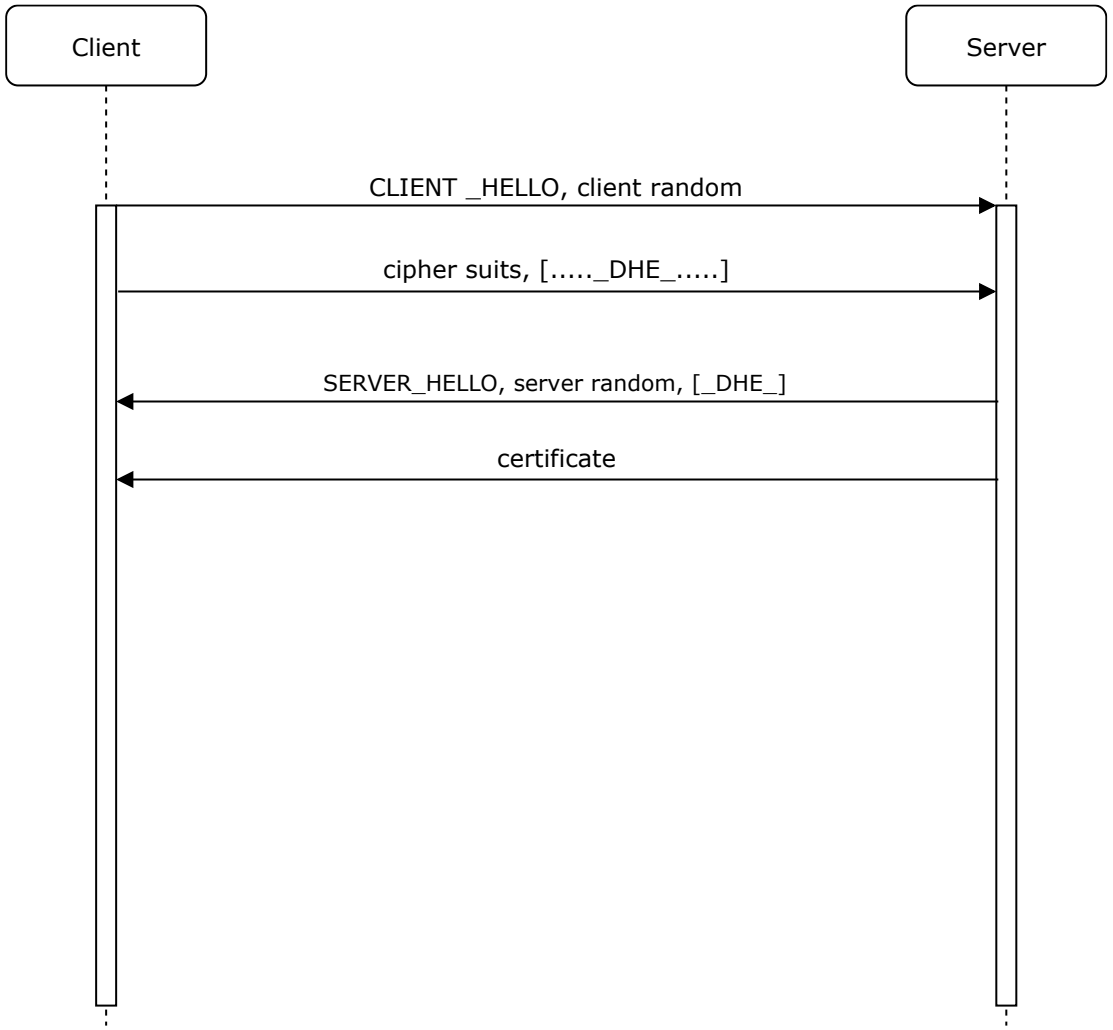
TLS Export Grade

- stammt aus dem Kalten Krieg und dem *First Crypto War*
- Kryptographie fiel unter das Kriegswaffenkontrollgesetz (United States Munitions List)
- Beschränkungen der Schlüssellängen (symmetrisch auf ca. 40-bit, asymmetrisch 512-bit) durch die Export Administrations Regulations(EAR)
- aufgehoben durch die Executive Order 13026 von 1996, EAR wurde aber erst 1999 angepasst
- SSL3 ist von 1996

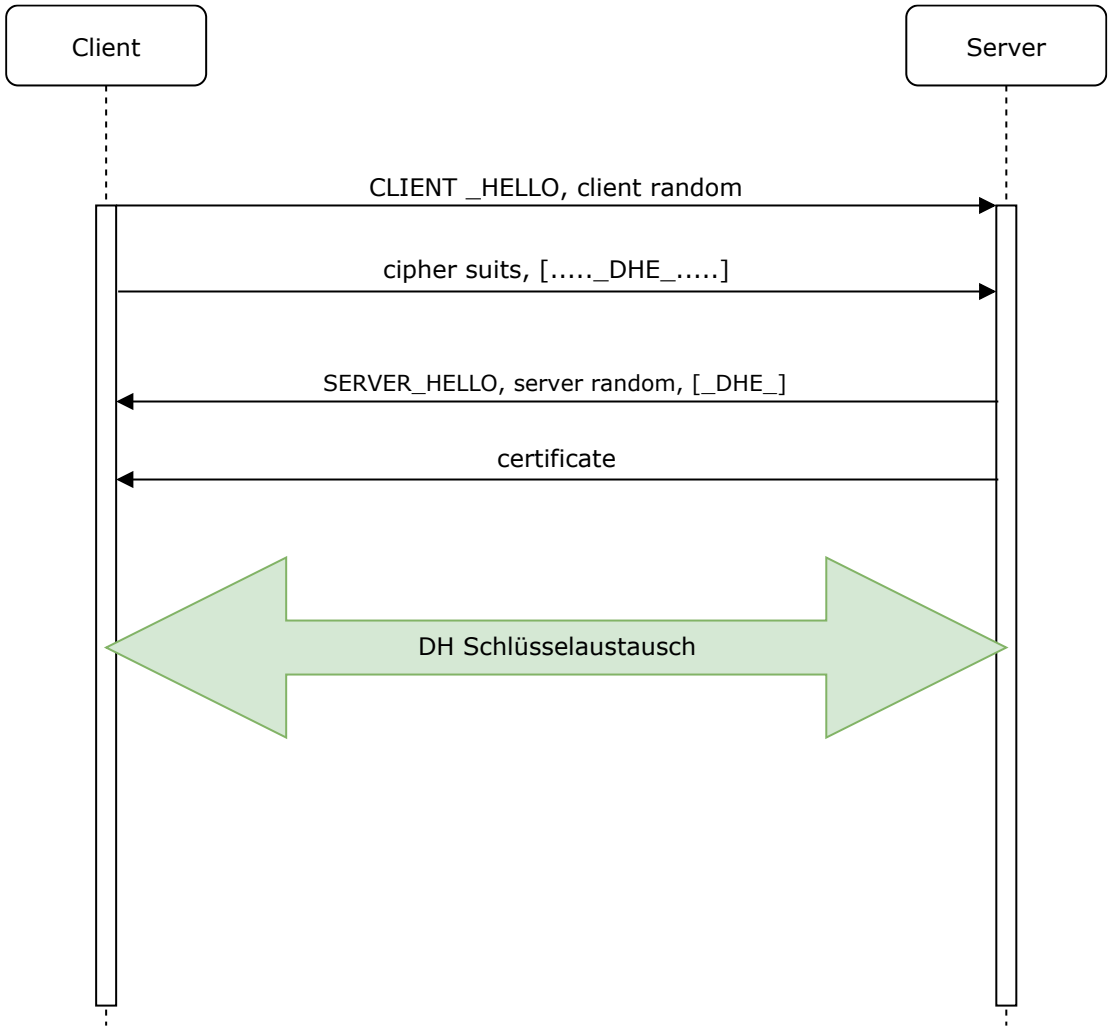
TLS - Handshake(1)



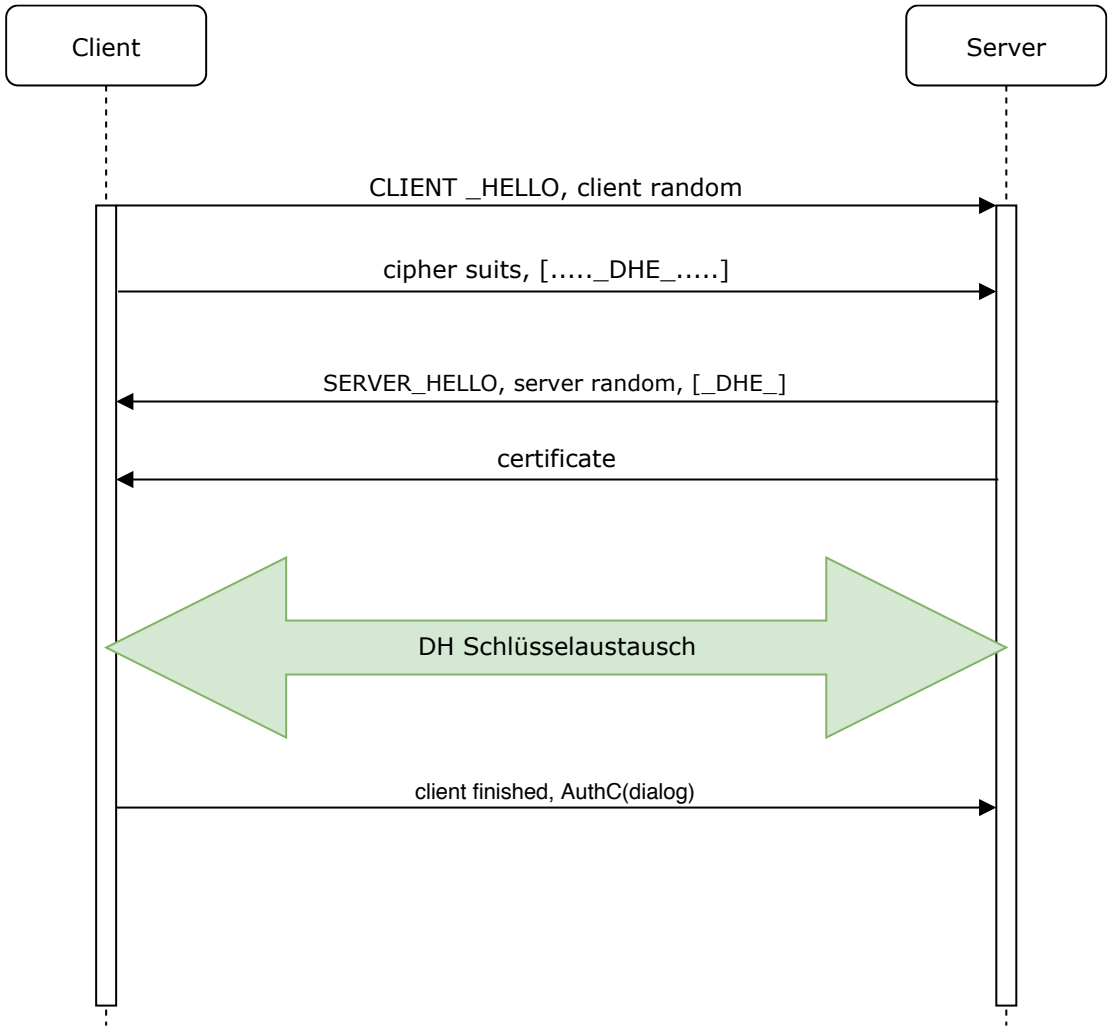
TLS - Handshake(2)



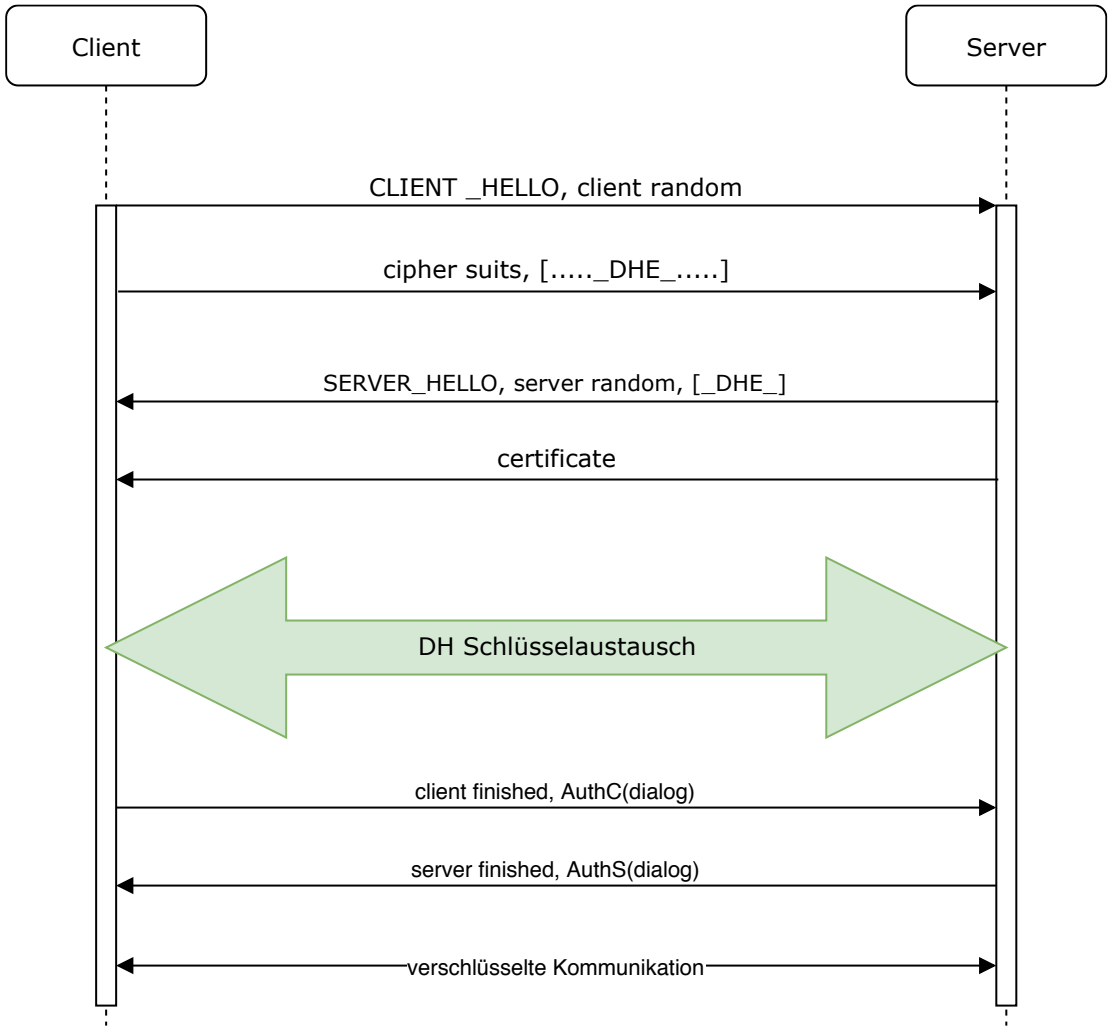
TLS - Handshake(3)



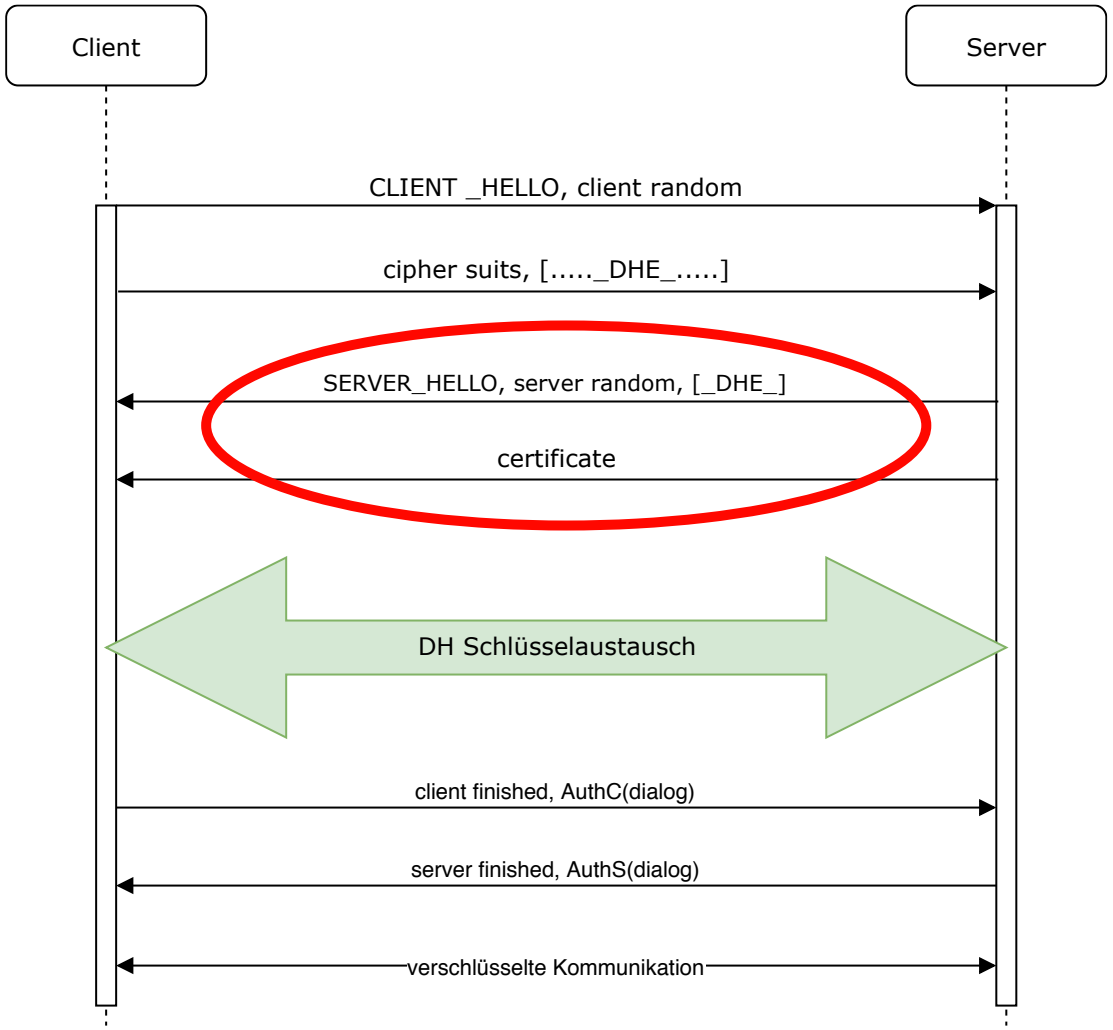
TLS - Handshake(4)



TLS - Handshake(5)



TLS - Handschake Sicherheitlücke

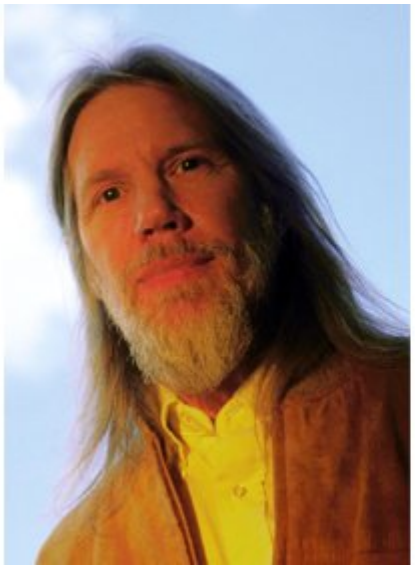


Diffie-Hellman

D-H - Überblick

- *New Directions in Cryptography* Whitfield Diffie und Martin Hellman 1976
- erste Public Key Verfahren
- bietet in Form von Diffie-Hellman Ephemeral (DHE) sogenannte *perfect forward secrecy*
- beruht auf dem Problem des diskreten Logarithmus (hoffentlich NP-Vollständig), im Gegensatz zu RSA (Primfaktorzerlegung)
- 2015 Turing Award

D-H - Erfinder

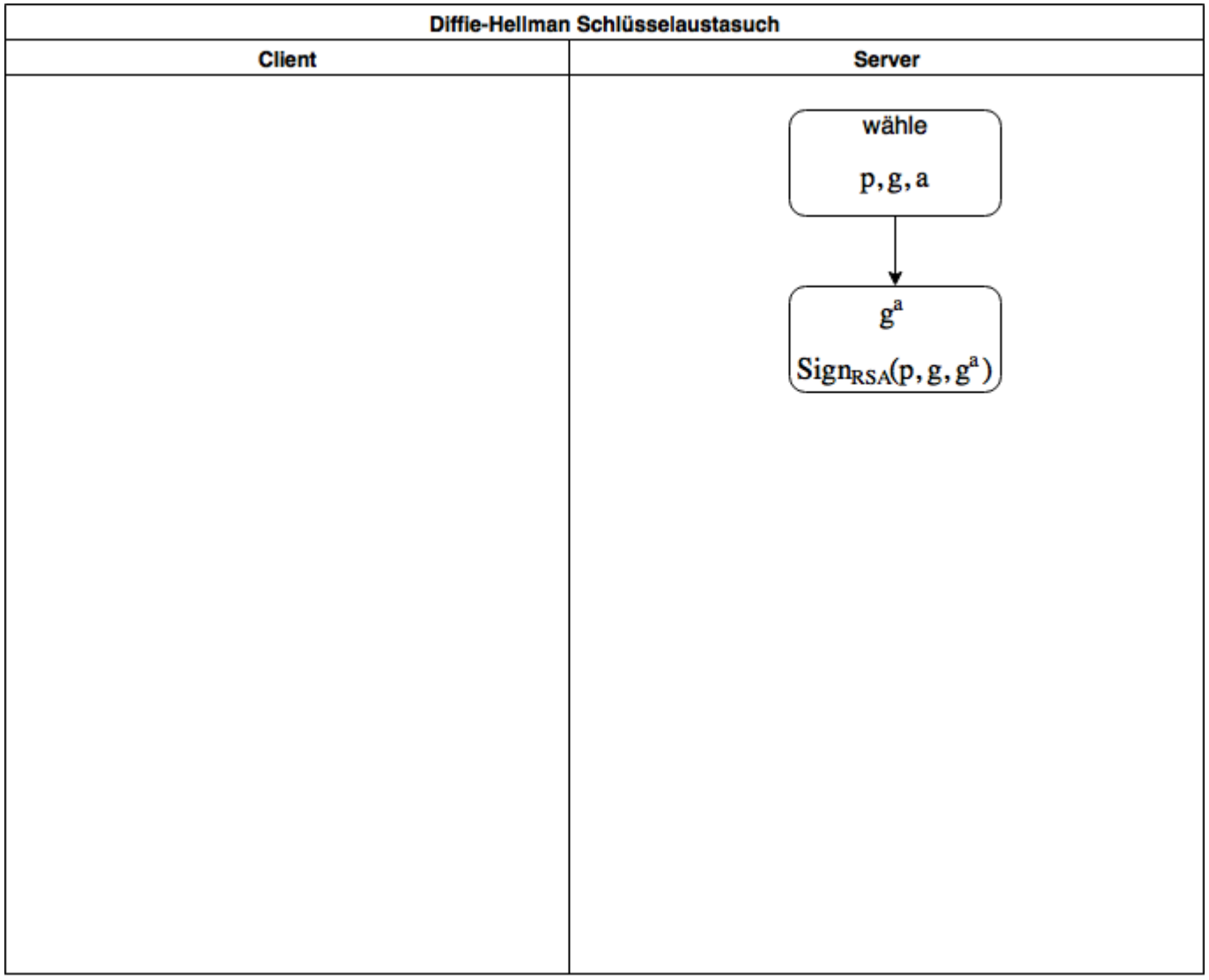


Whitfield Diffie & Martin Hellman

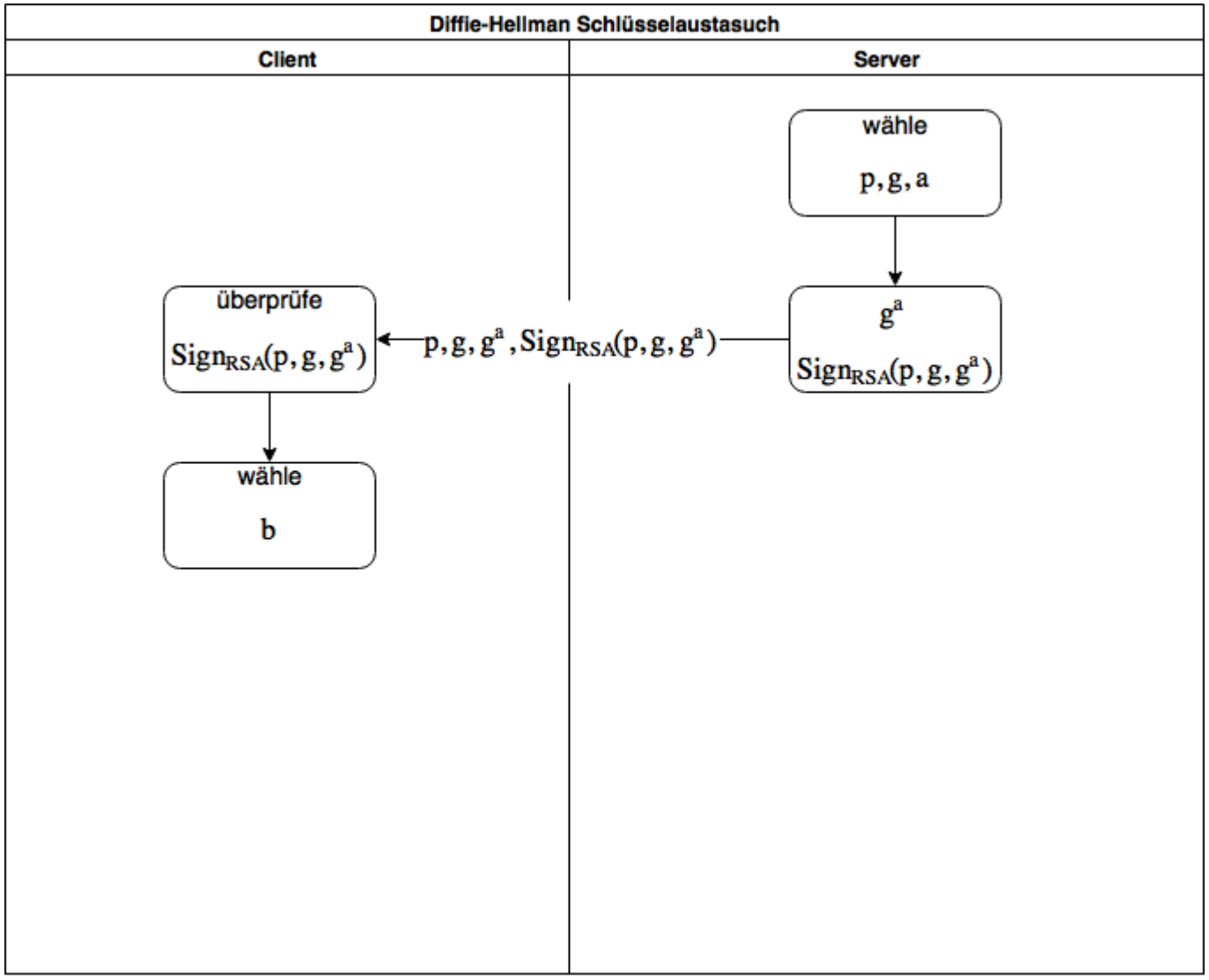
D-H - Übung

Changing the names would be easier, but if you're not comfortable lying, try only making friends with people named Alice, Bob, Carol, etc.

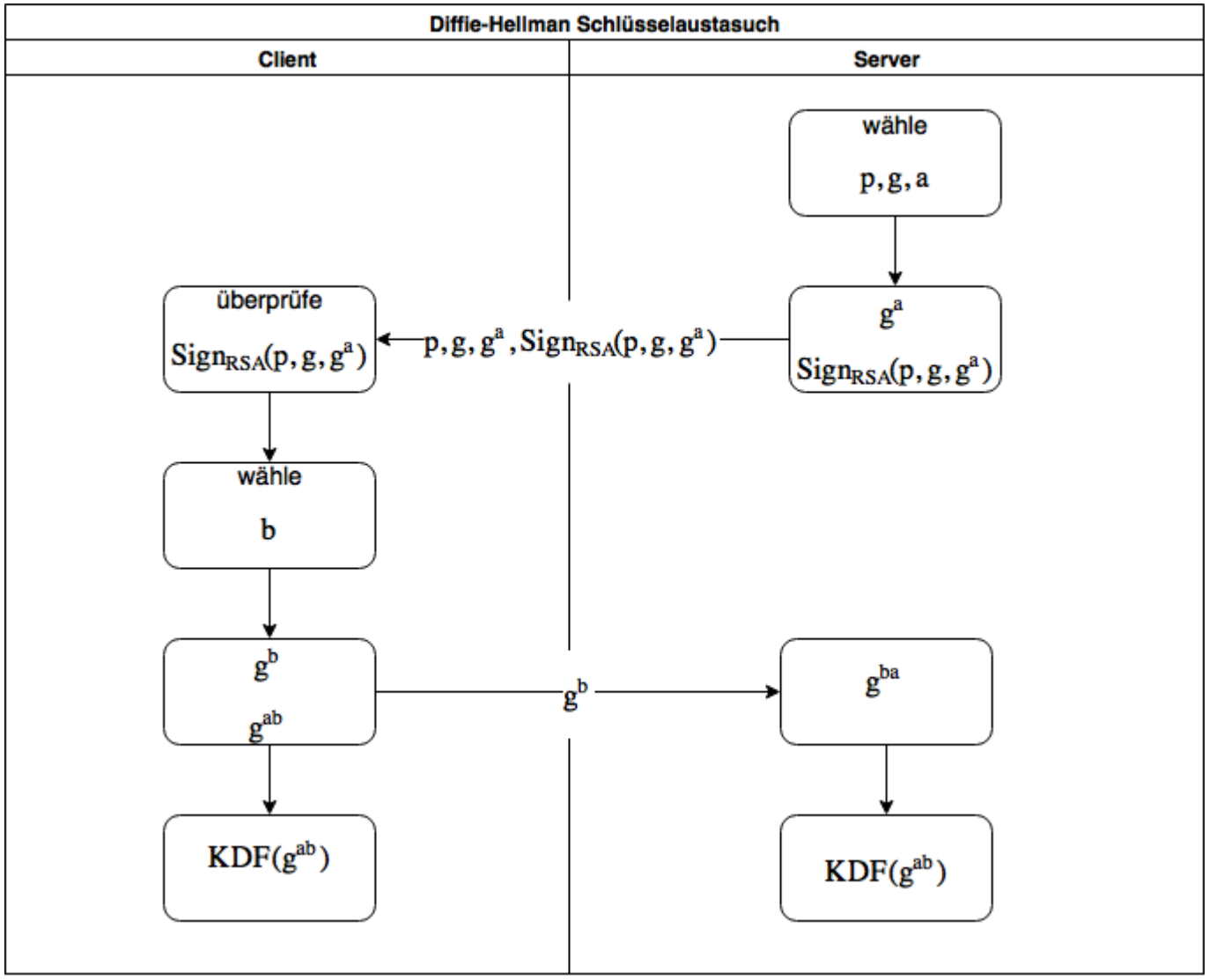
D-H - TLS Handshake(1)



D-H - TLS Handshake(2)



D-H - TLS Handshake(3)



D-H - Export

- 512-bit Primzahlen
- die zwei häufigsten Primzahlen werden für 92.3% aller EXPORT DHE Server verwendet

```
Apache: 0x9fdb8b8a004544f0045f1737d0ba2e0b
          274cdf1a9f588218fb435316a16e3741
          71fd19d8d8f37c39bf863fd60e3e3006
          80a3030c6e4c3757d08f70e6aa871033

mod_ssl:0xd4bcd52406f69b35994b88de5db89682
          c8157f62d8f33633ee5772f11f05ab22
          d6b5145b9f241e5acc31ff090a4bc711
          48976f76795094e71e7903529f5a824b
```

Number Field Sieve (NFS)

NFS - Übersicht

- Algorithmus aus der Zahlentheorie
- sowohl anwendbar auf RSA als auch auf DH
- schon lange bekannt, aber eher unter Mathematikern

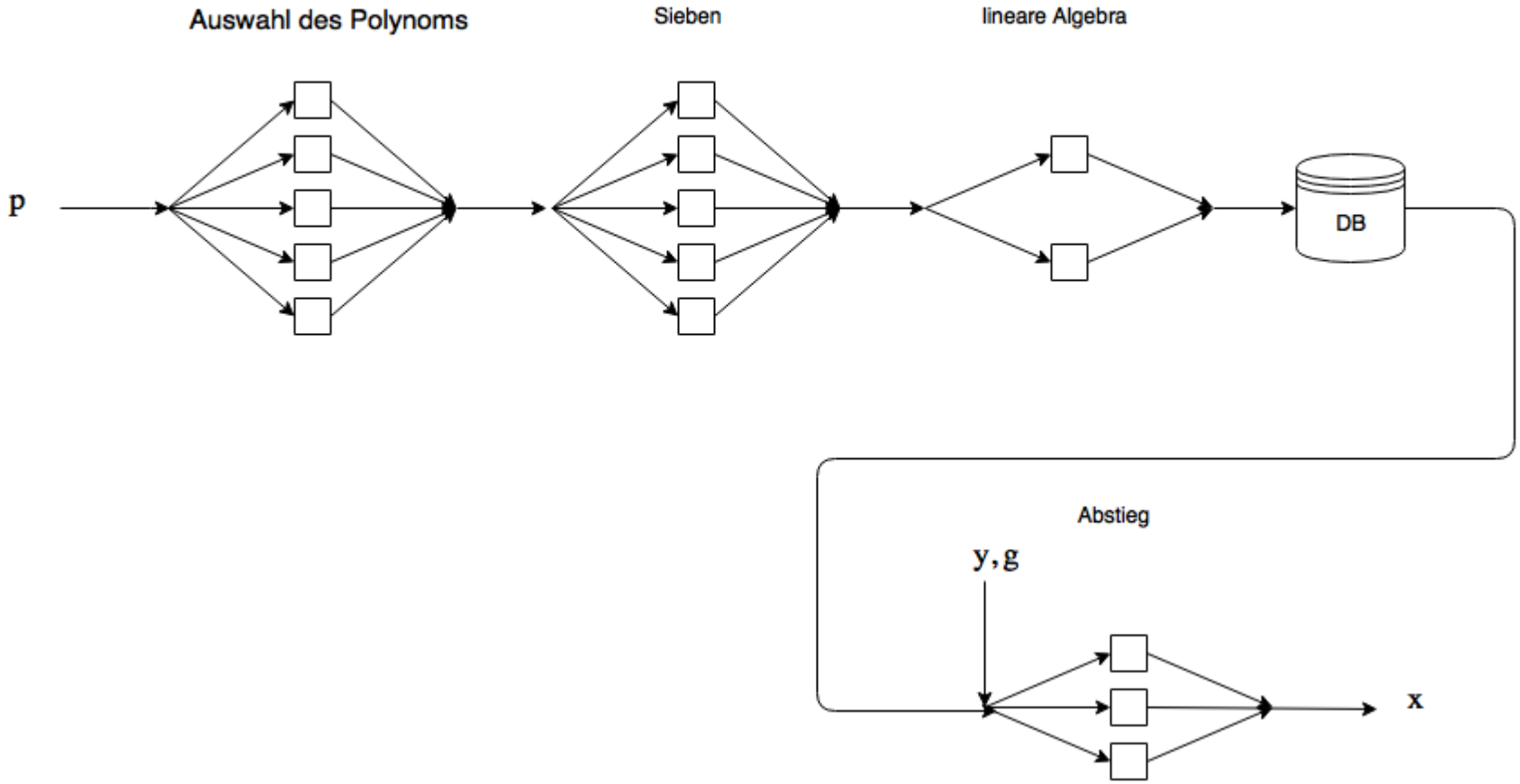
$$\Theta(e^{1.9\ (\log N)\text{^}1/3\ \ (\log\log N)\text{^}2/3})$$

Laufzeiten in Prozessor Jahren:

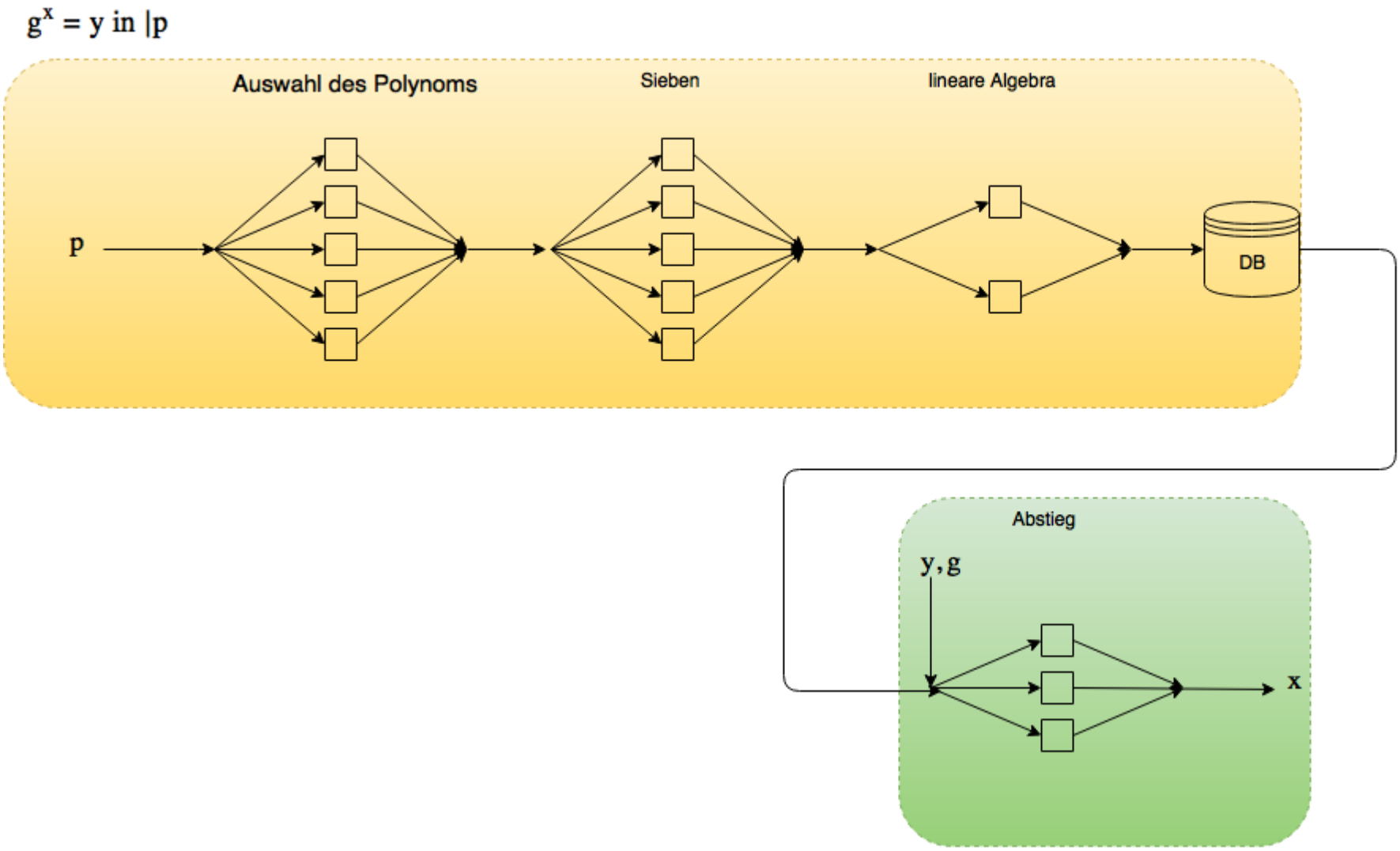
RSA-512	0.88
DH-512	9,20
RSA-768	900
DH-768	36.500
RSA-1024	1.120.000
DH-1024	45.000.000

NFS - Ablauf(1)

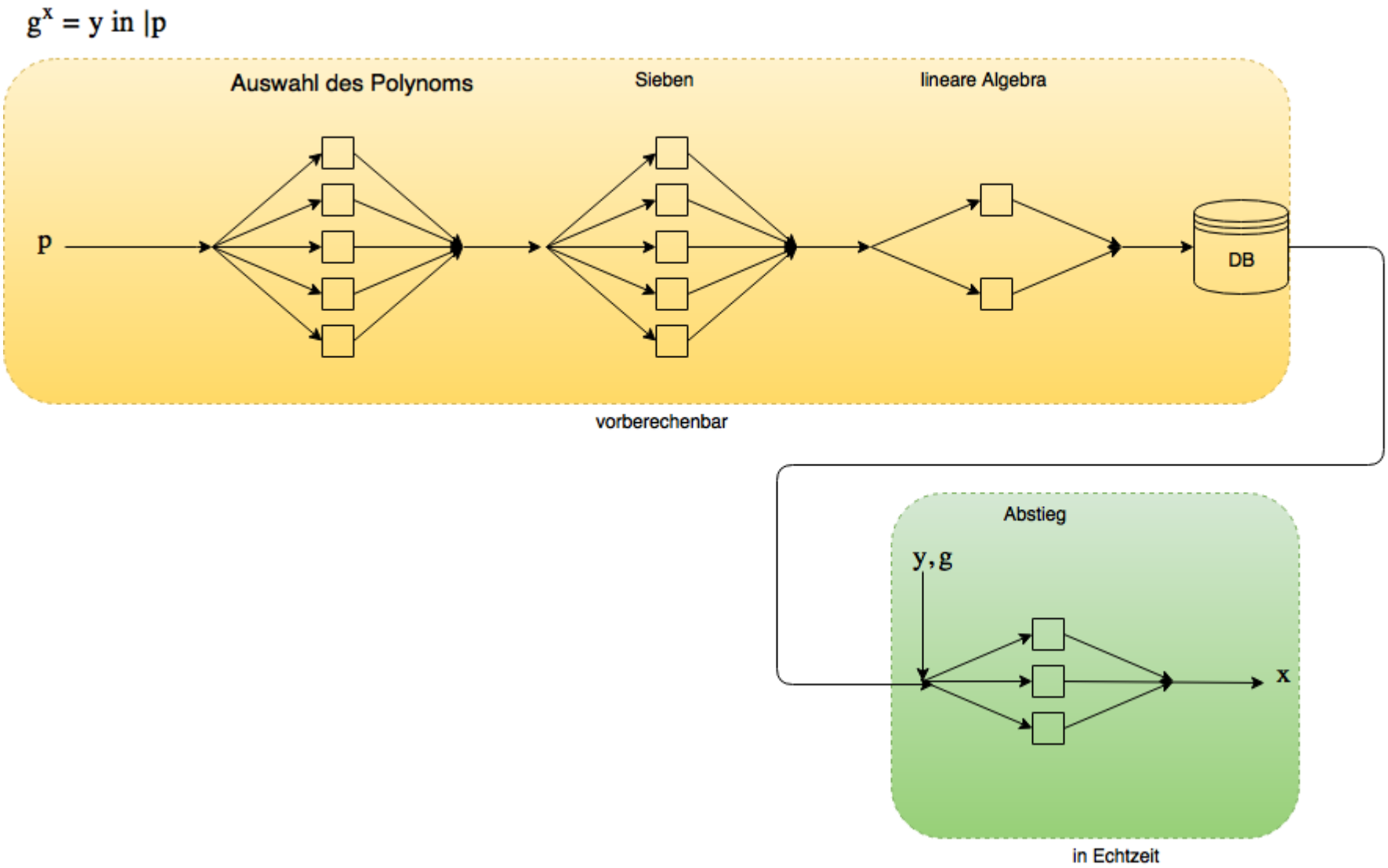
$g^x = y \text{ in } |p$



NFS - Ablauf(2)


$g^x = y \text{ in } |p$
Auswahl des Polynoms
Sieben
lineare Algebra
p
DB
Abstieg
y, g
x

NFS - Ablauf unterteilt



NFS - Laufzeit unterteilt

Laufzeiten in Prozessor Jahren:

	Vorberechnung	Abstieg
RSA-512	0,88	
DH-512	9,20	10 Min
RSA-768	900	
DH-768	36.500	2 Tage
RSA-1024	1.120.000	
DH-1024	45.000.000	30 Tage

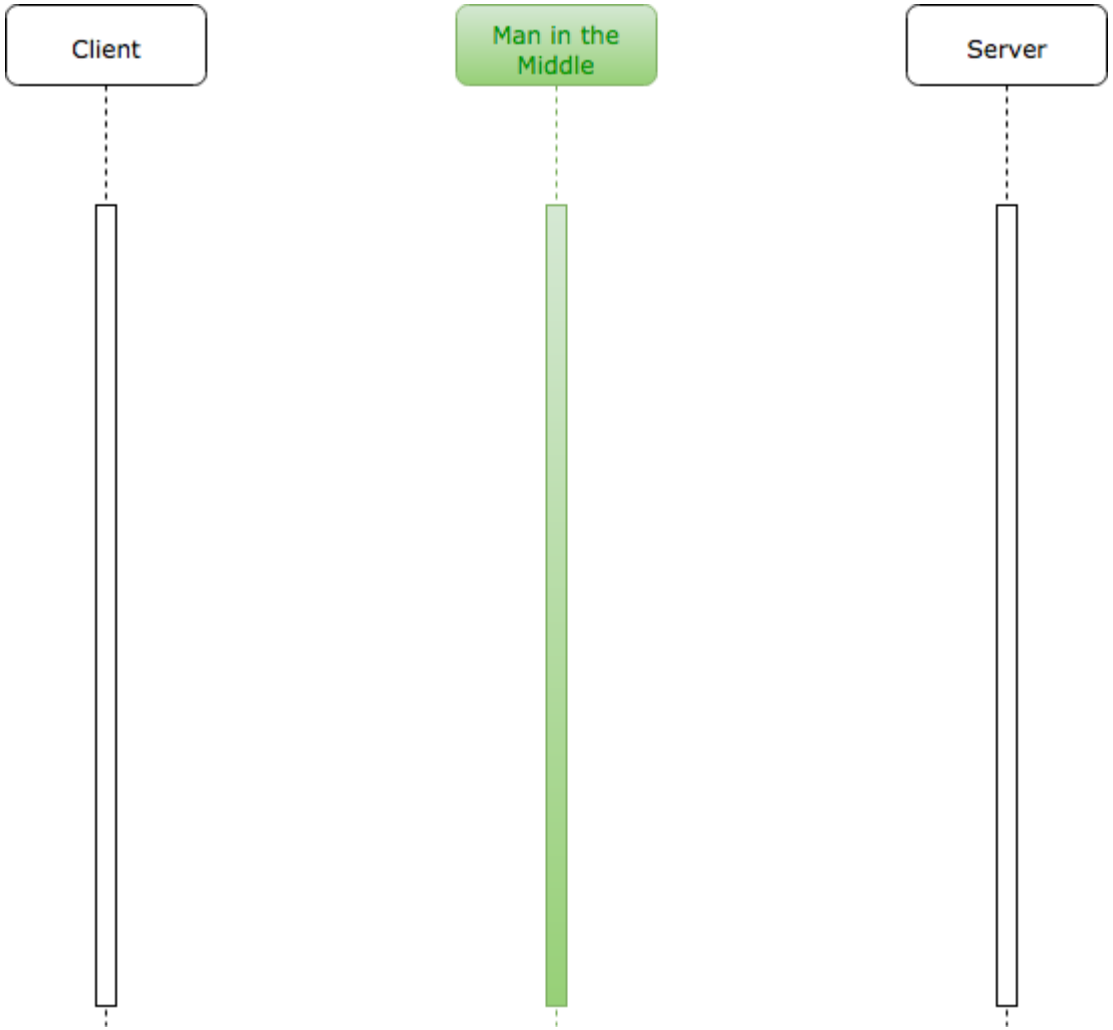
logjam

logjam - Rekapitulation

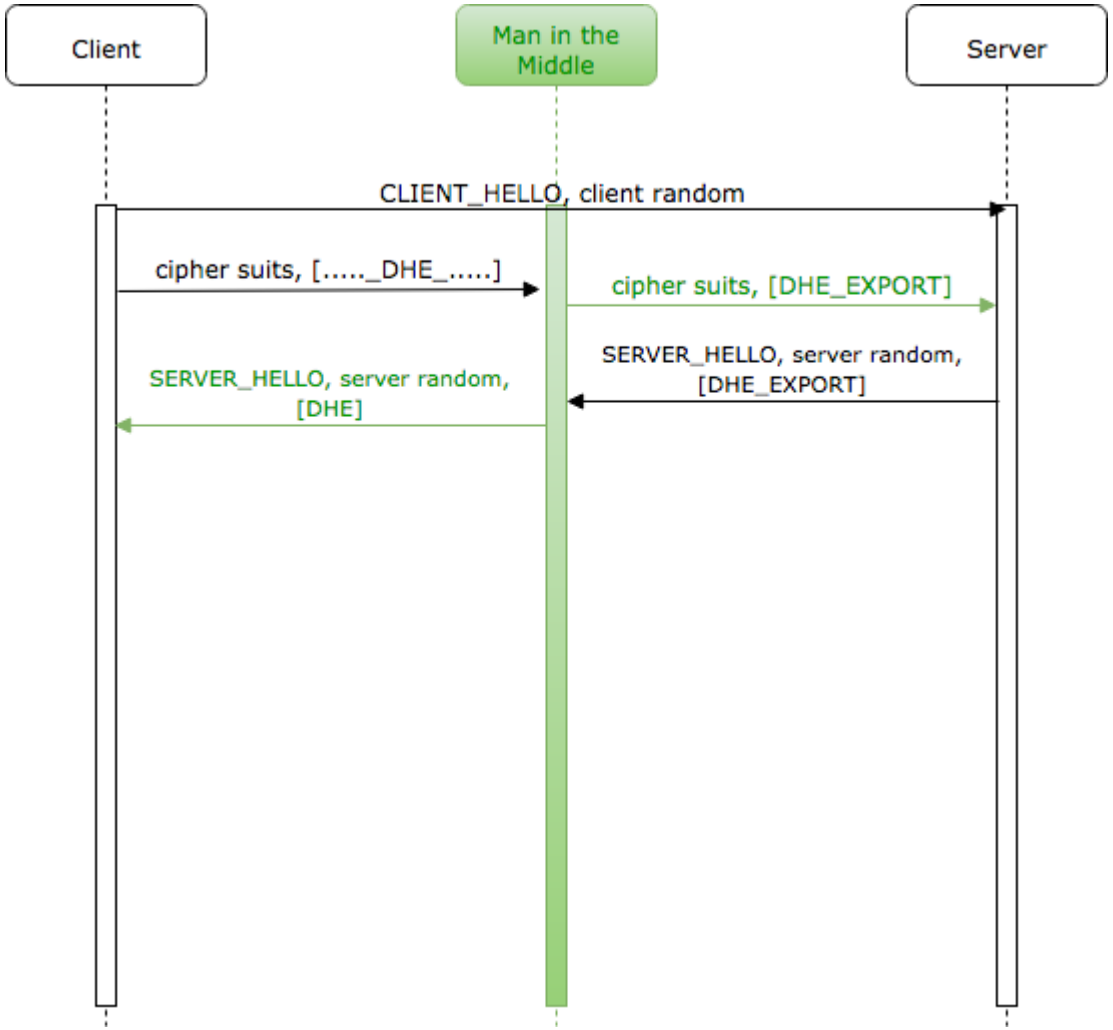
- TLS Handshake Protokoll Schwäche
- wenige 512-bit Primzahlen in freier Wildbahn
- zweiteiliger Algorithmus für die Berechnung des diskreten Logarithmus

Wie baue ich einen Exploit?

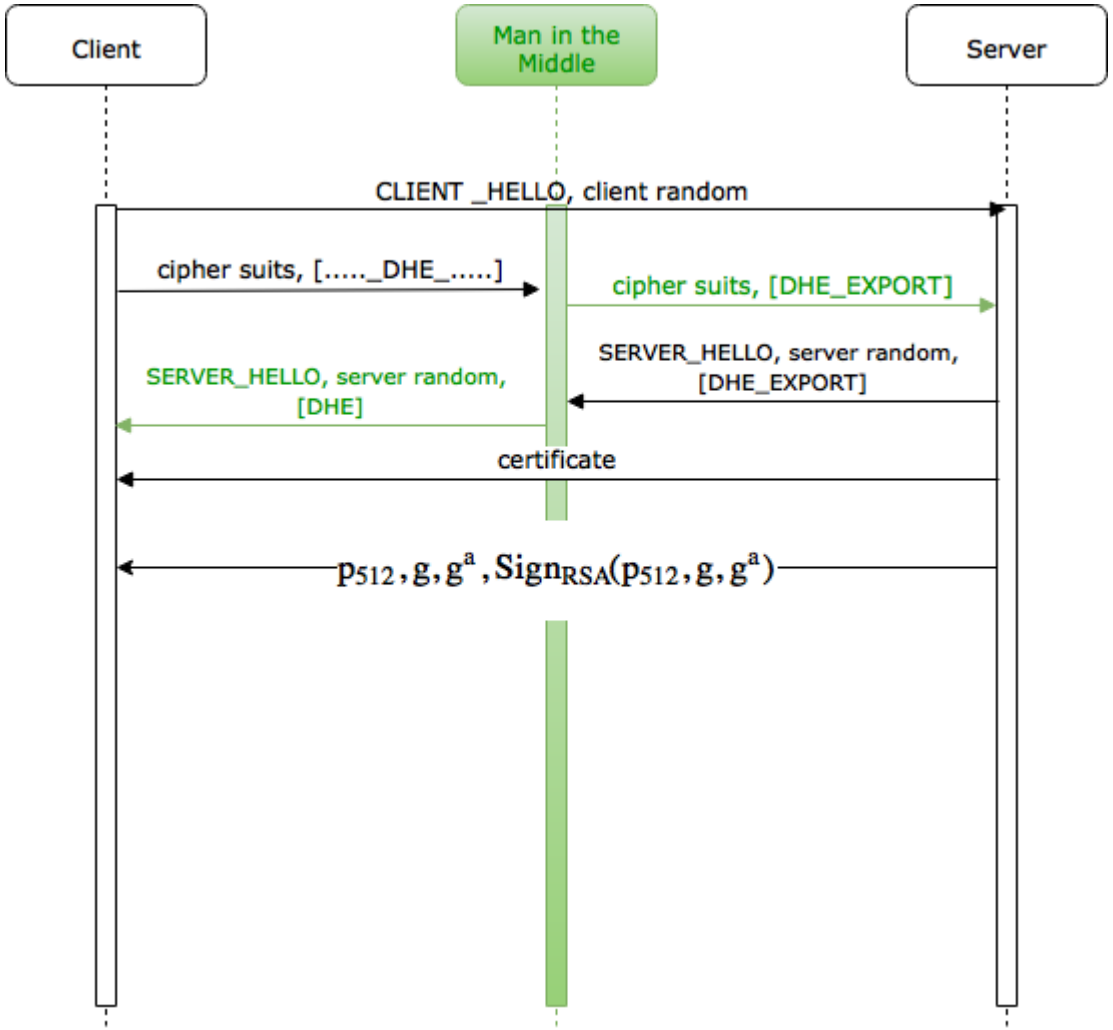
logjam - Exploit(1)



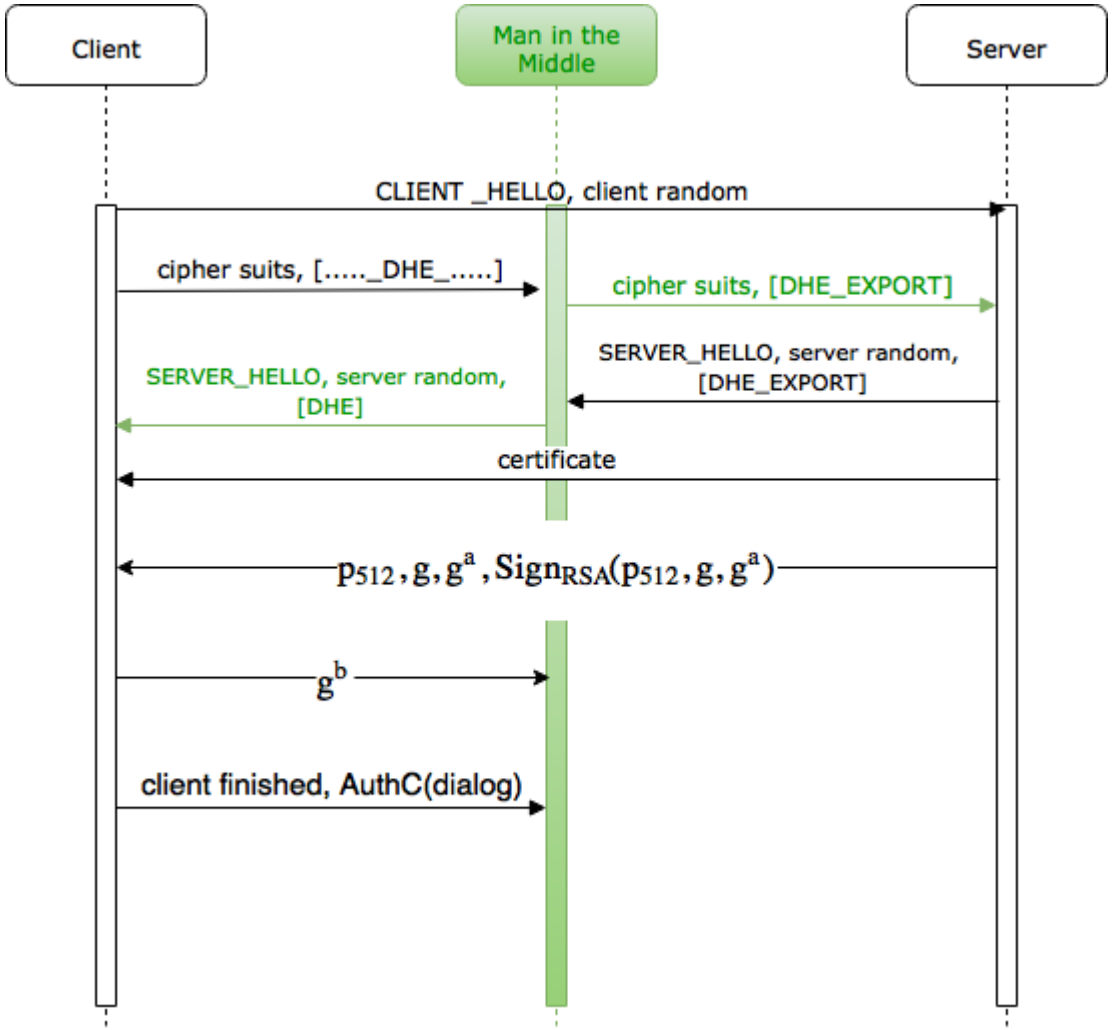
logjam - Exploit(2)



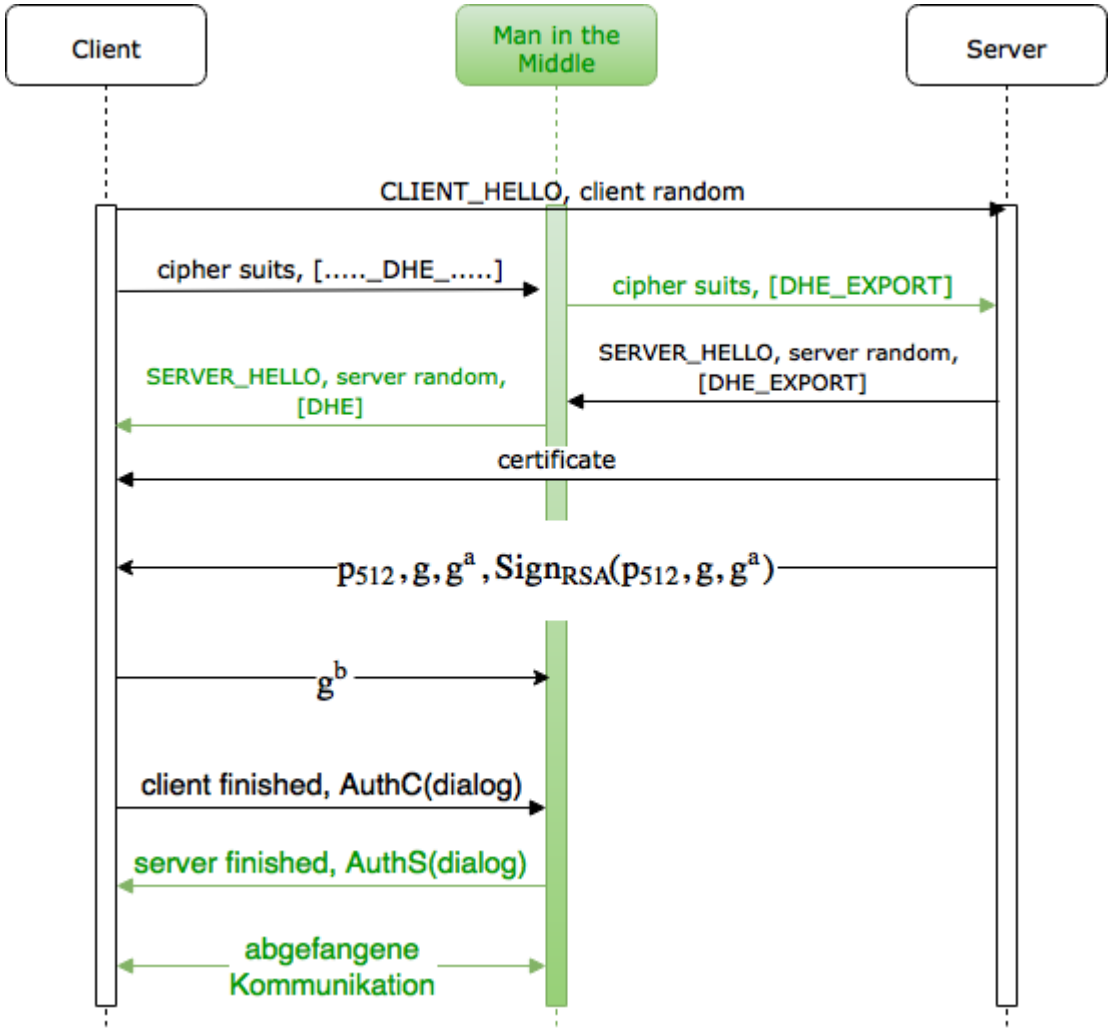
logjam - Exploit(3)



logjam - Exploit(4)



logjam - Exploit(5)



logjam - Zusammenfassung

1. Ich suche einen Server der noch EXPORT_DHE unterstützt (2015 8.4% der Top 1M Domains).

2. Ich berechne den ersten Teil des NFS (ca. 75$ mit AWS EC2 Instanzen).

3. Ich klinke mich als *Man in the Middle* zwischen meinem Ziel und dem Server ein.

4. Ich halte einen halbwegs leistungsstarken Server (16 Kerne) für den zweiten Teil des NFS bereit.

5. Ich kann in Echtzeit TLS Verbindungen knacken.

6. ... .

logjam - Abwehrstrategien

Als Client:

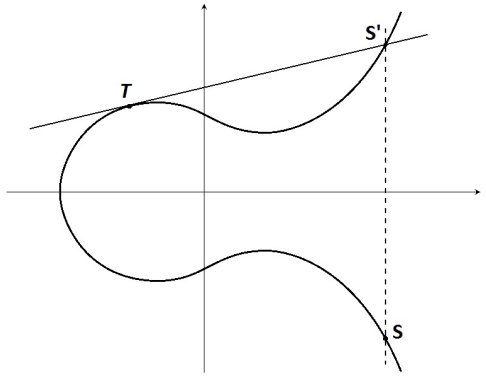
- schlechte Karten (Protokollebene)
- aktuelle Browser akzeptieren keine Primzahlen < 768-bit
- warten auf TLS1.3

Als Server:

- `jdk.tls.ephemeralDHKeySize=2048`
- Eliptic Curves (wahrscheinlich kein NFS möglich)
- regelmäßig neue Primzahlen verwenden (nicht ganz trivial)

Fazit


```
Crypto Backdoors sind Zombies
```




```
Theorie ist wichtig
```

Quellen

- https://weakdh.org/ David Adrian et al.
- IT-Sicherheit WiSe2015 Prof. Dr. rer. nat. Peter Hartmann
- Executive Order 13026 Bill Clinton https://www.gpo.gov/fdsys/pkg/FR-1996-11-19/pdf/96-29692.pdf
- EAR Bereau of Industry and Security https://www.bis.doc.gov/index.php/documents/regulation-docs/434-part-772-definitions-of-terms/file
- New Directions in Cryptography Whitfield Diffie und Martin Hellman 1976
- Number Field Sieve Katja Schmidt-Samoa https://www.cdc.informatik.tu-darmstadt.de/~samoa/NFS.pdf

Bilder

- xkcd https://xkcd.com/1323/
- GFDL
- Public Domain
- CC
- Georg Held

Fragen?

Live-Demo

twitter.com/DLogBot?lang=de (https://twitter.com/DLogBot?lang=de)

sage.haw-landshut.de/home/sghelldd/23/ (https://sage.haw-landshut.de/home/sghelldd/23/)

Thank you

Georg Held
Student HaW-Landshut
s-gheldd@haw-landshut.de (mailto:s-gheldd@haw-landshut.de)