Early History of (Open)PGP

Lutz Donnerhacke

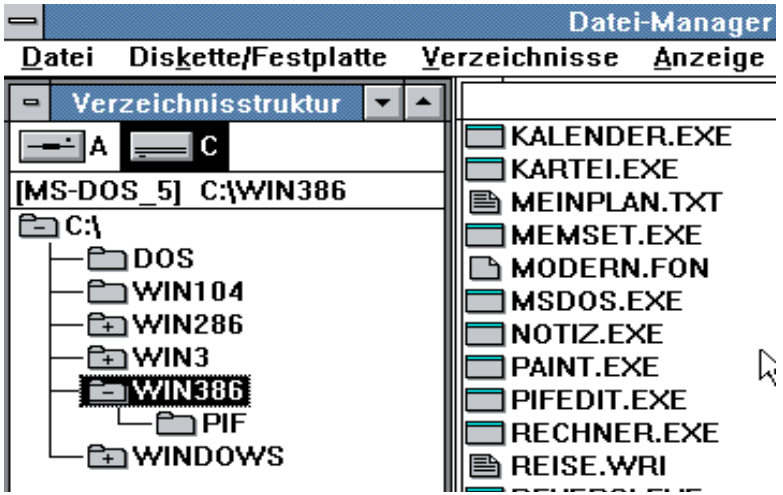
Early Adopter

```
pub  2048R/39F37F5D 1996-04-25 Lutz Donnerhacke <lutz@donnerhacke.de>
     Key fingerprint = A4 C1 50 8F 00 D9 28 60  70 BB 0B 5D D9 3A 0B B6
uid  Lutz Donnerhacke <Lutz.Donnerhacke@Jena.Thur.De>

pub  1127R/DB089309 1997-03-17 Lutz Donnerhacke <lutz@iks-jena.de>
     Key fingerprint = 1C 1C 63 11 EF 09 D8 19  E0 29 65 BE BF B6 C9 CB
```

In the beginning (~1990)

- Mailbox Operator (AS-Node)
  - Modems – no Internet
  - Mostly offline
  - Use the available OS’



Extended communications

- Access to Internet at the university
  - In 1990 most universities in Germany stick to OSI
- Lost mailbox due to HDD crash
  - Switched to Linux (0.96.xx)
  - Restarted Mailbox with UUCP (Thüringen Netz)
- UseNET (instead of Fido)
  - Read about PGP, tried to understand

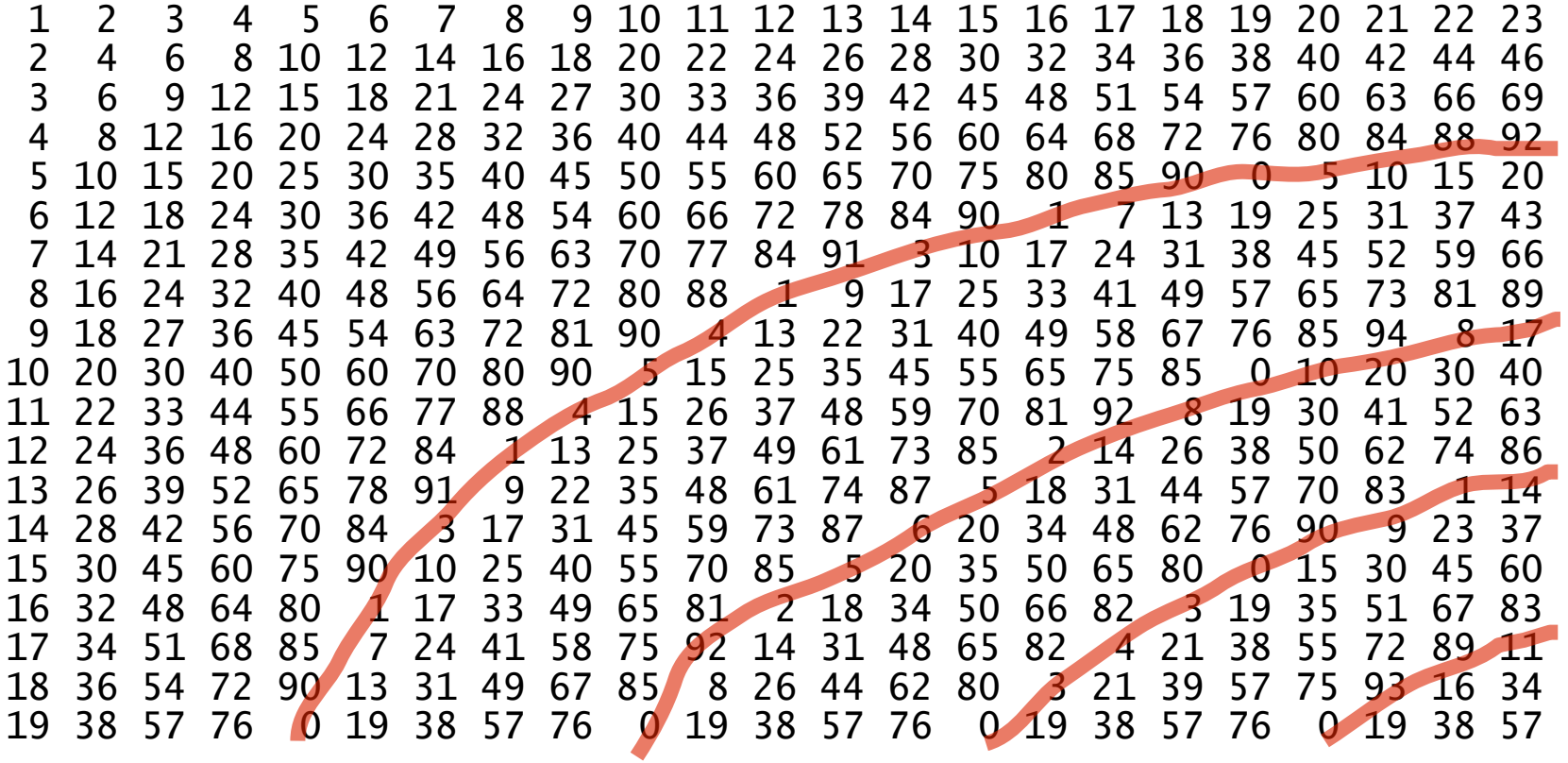
Phil Zimmermann

- PGP 1 was really bad
- PGP 2 was sound
  - Hard crypto algorithms
  - Efficient storage
  - Embedded PKI
  - Embedded trust model
- Published 1991 (by mistake)
  - Widespread usage

What the hell?

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69
4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92
5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	0	5	10	15	20
6	12	18	24	30	36	42	48	54	60	66	72	78	84	90	1	7	13	19	25	31	37	43
7	14	21	28	35	42	49	56	63	70	77	84	91	3	10	17	24	31	38	45	52	59	66
8	16	24	32	40	48	56	64	72	80	88	1	9	17	25	33	41	49	57	65	73	81	89
9	18	27	36	45	54	63	72	81	90	4	13	22	31	40	49	58	67	76	85	94	8	17
10	20	30	40	50	60	70	80	90	5	15	25	35	45	55	65	75	85	0	10	20	30	40
11	22	33	44	55	66	77	88	4	15	26	37	48	59	70	81	92	8	19	30	41	52	63
12	24	36	48	60	72	84	1	13	25	37	49	61	73	85	2	14	26	38	50	62	74	86
13	26	39	52	65	78	91	9	22	35	48	61	74	87	5	18	31	44	57	70	83	1	14
14	28	42	56	70	84	3	17	31	45	59	73	87	6	20	34	48	62	76	90	9	23	37
15	30	45	60	75	90	10	25	40	55	70	85	5	20	35	50	65	80	0	15	30	45	60
16	32	48	64	80	1	17	33	49	65	81	2	18	34	50	66	82	3	19	35	51	67	83
17	34	51	68	85	7	24	41	58	75	92	14	31	48	65	82	4	21	38	55	72	89	11
18	36	54	72	90	13	31	49	67	85	8	26	44	62	80	3	21	39	57	75	93	16	34
19	38	57	76	0	19	38	57	76	0	19	38	57	76	0	19	38	57	76	0	19	38	57

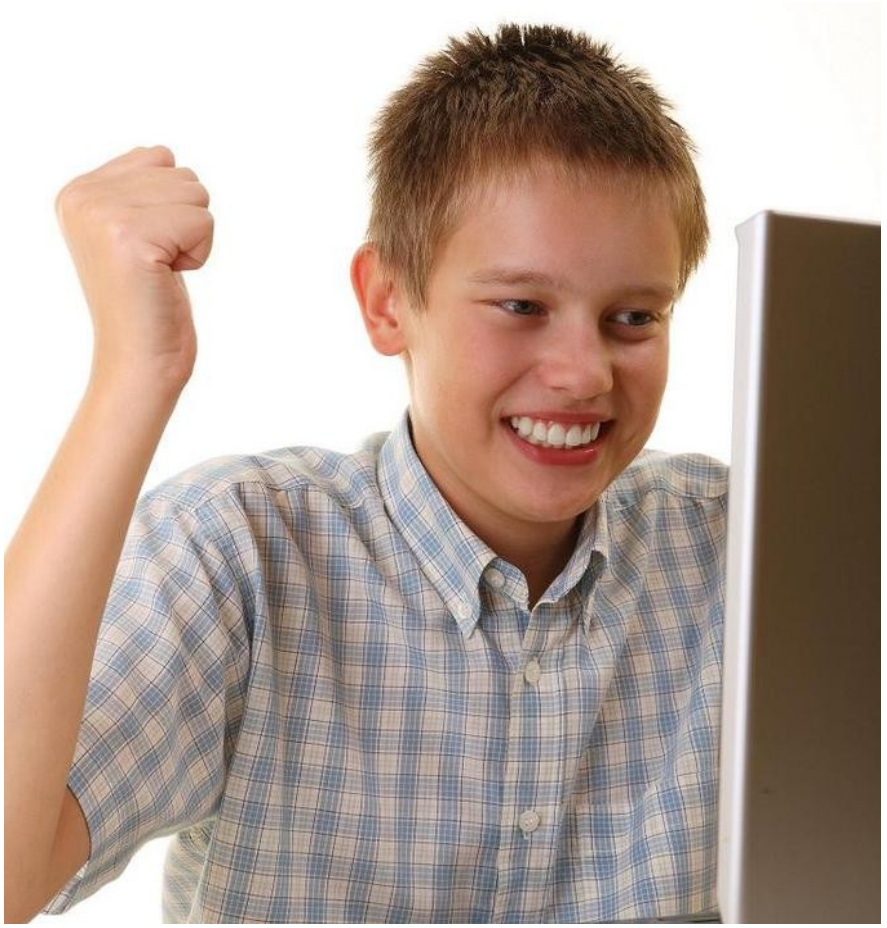
What the hell!



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69
4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92
5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	0	5	10	15	20
6	12	18	24	30	36	42	48	54	60	66	72	78	84	90	1	7	13	19	25	31	37	43
7	14	21	28	35	42	49	56	63	70	77	84	91	3	10	17	24	31	38	45	52	59	66
8	16	24	32	40	48	56	64	72	80	88	1	9	17	25	33	41	49	57	65	73	81	89
9	18	27	36	45	54	63	72	81	90	4	13	22	31	40	49	58	67	76	85	94	8	17
10	20	30	40	50	60	70	80	90	5	15	25	35	45	55	65	75	85	0	10	20	30	40
11	22	33	44	55	66	77	88	4	15	26	37	48	59	70	81	92	8	19	30	41	52	63
12	24	36	48	60	72	84	1	13	25	37	49	61	73	85	2	14	26	38	50	62	74	86
13	26	39	52	65	78	91	9	22	35	48	61	74	87	5	18	31	44	57	70	83	1	14
14	28	42	56	70	84	3	17	31	45	59	73	87	6	20	34	48	62	76	90	9	23	37
15	30	45	60	75	90	10	25	40	55	70	85	5	20	35	50	65	80	0	15	30	45	60
16	32	48	64	80	1	17	33	49	65	81	2	18	34	50	66	82	3	19	35	51	67	83
17	34	51	68	85	7	24	41	58	75	92	14	31	48	65	82	4	21	38	55	72	89	11
18	36	54	72	90	13	31	49	67	85	8	26	44	62	80	3	21	39	57	75	93	16	34
19	38	57	76	0	19	38	57	76	0	19	38	57	76	0	19	38	57	76	0	19	38	57

RSA does have a structure!

Naive? Surprised!



- No cryptographic background
- Overwhelmed
- Addicted to PGP
- Use it extensively
- Search for fast factorization methods
- CypherPunks (ML)

PGP for UseNET

- Use PGP for signing UseNET postings
  - http://altlasten.lutz.donnerhacke.de/mitarb/lutz/pgpnews.html
- Missed a “certification infrastructure”
  - UseNET is build hierarchical
  - ✗ PGP is Web of Trust
  - UseNET is operated as an automatic oligopoly
  - ✗ PGP works offline

```
pub  1024R/D3033C99 1996-05-18 <moderator@dana.de>
     Key fingerprint = 5B B0 52 88 BF 55 19 4F  66 7D C2 AE 16 26 28 25
uid                            de.admin.news.announce
```

RFC 1991

Network Working Group
Request for Comments: 1991
Category: Informational

D. Atkins
MIT
W. Stallings
Comp-Comm Consulting
P. Zimmermann
Boulder Software Engineering
August 1996

PGP Message Exchange Formats

- PGP became commercial
  - Customers required standard conformity
  - An RFC seems to fulfil this PR need
- RFC contained the first documentation of PGP (mainly the README.txt)
  - A lot of information missing, No peer review

Individual Network CA

- Individual Network e.V.
  - Private organisation to enhance communication
  - Real Internet access for private people (instead of CompuServ, AOL, Universities, UUNet, Xlink)
- With Ingmar Camphausen:
  - Use connections to all German regions to build trust
  - Established IN-CA for X.509 and PGP
  - Tried to circumvent a crypto regulation through CA features

```
pub  2048R/19990101 1999-01-13 Root CA des Individual Network e.V.
                    <in-ca@individual.net> (SIGN EXPIRE:2000-12-31)
     Key fingerprint = E9 27 BD 6C 4A 21 99 57  E5 B6 49 BC A5 71 F3 B1
```

PGP 2.6.3(i)n

- Phil Zimmermann:
  - From freedom fighter to CEO to pariah
- Especially for certification purposes
- Extended key management
  - Revocation reasons, group keys, expire times, key usage
- Keys (>1024bit) by using a different library
- Several bug fixes (incl. Security patches)
- Source code is straight from hell

ftp://ftp.iks-jena.de/pub/mitarb/lutz/crypt/software/pgp/

Intermezzo

- PGP Inc merged with Viacrypt
  - Based on RSADSI (the 1024bit lib)
  - Split versions between the companies (even/odd)
- PGP3 – a library for a new packet format
- Viacrypt sold PGP4 (based on PGP2)
- PGP Inc made the new version PGP5
  - Renamed PGP3
  - Build some GUI around

PGP 5

- New incompatible format
  - Lot of cool new features
  - GAK (became a synonym for espionage key)
  - Algorithms changed (licence problems)
- Code cleanup (rewrite)
  - New code can’t be exported
  - US-Gov sued Phil for export of PGP2
- 1st amandment
  - Print source in OCR as a book

Importing PGP5

- HIP97 or CCC99
  - ‘97 – PGP5.0i
  - Some proof readings
- Correct OCR scans
  - Embedded checksums
  - We do not check the code!
- Horrible bug in get_random()

```
int c, r;
r = fread(&c, sizeof c, 1, RAND);
return r;
```

OpenPGP

- PGP Inc was sold to Network Associates (NAI)
- Rewrite of RFC 1991
  - Includes PGP5 format
  - Jon Callas missed timelines of IETF
  - Europeans take over (welcome to the IETF)

Network Working Group
Request for Comments: 2440
Category: Standards Track

J. Callas
Network Associates
L. Donnerhacke
IN-Root-CA Individual Network e.V.
H. Finney
Network Associates
R. Thayer
EIS Corporation
November 1998

OpenPGP Message

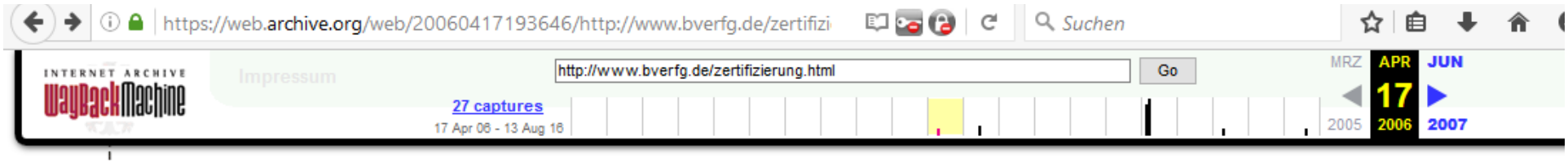
Common Criteria

- Highest level is “proof-able correct software”
  - Does not include the requirements of lower levels
- Idea: Publish source code as RFC
  - Compilable standards are ***correct***
  - Requires a different language

ftp://ftp.iks-jena.de/pub/mitarb/lutz/crypt/software/pgp/OpenPGP/

```
/* structure of a public key */
public_key:
public_key_packet maybe_trust key_compromise
| public_key_packet maybe_trust signed_userIDs
| public_key_packet maybe_trust signed_userIDs subkeys
| public_key_packet maybe_trust zero_certificate signed_userIDs
| public_key_packet maybe_trust zero_certificate signed_userIDs subkeys
;
```

Federal Constitutional Court



BUNDES-VERFASSUNGS-GERICHT

- Aktuell
- Richter
- Organisation
- Pressemitteilungen
- Entscheidungen
- Bibliothek
- Links
- Impressum

AbsNr. 3

2.2. Eine versteckte Signatur

Wenn Sie ein Urteil aufrufen, werden Sie keine Signatur bemerken, denn die derzeitigen Browser sind noch nicht in der Lage solche Sicherungsmechanismen korrekt zu verarbeiten. Wenn Sie sich jedoch den Quelltext ansehen, dann werden Sie am Beginn der Seite eine Zeile finden in der "*BEGIN PGP SIGNED MESSAGE*" steht. Am Ende der Seite findet sich dann ein weiterer Abschnitt, der mit "*BEGIN PGP SIGNATURE*" eingeleitet wird und die eigentliche Signatur enthält.

AbsNr. 4

2.3. Der Mechanismus zur Überprüfung

Für die Signatur wurde das Programm *PGP* verwendet. Es ist unter http://www.pgpi.com/ für alle gängigen Betriebssysteme erhältlich.

AbsNr. 5

Nachdem Sie PGP korrekt installiert haben, was von generellem Nutzen für Ihre Privatsphäre sein dürfte, müssen Sie die Schlüssel derjenigen Mitarbeiter des Bundesverfassungsgerichts in Ihr PGP importieren, die die Urteile signiert haben. Es handelt sich um Mitarbeiter der Dokumentationsstelle des Bundesverfassungsgerichts. Dazu gehen Sie wie folgt vor:

AbsNr. 6

1. Rufen Sie mit Ihrem Browser den Key-Server der Zertifizierungsinstanz auf unter:
   https://www.iks-jena.de/cgi-bin/ca-iks.lookup.pl

2. Suchen Sie in dem vorgegebenen Formular für die PGP-Suche nach "*bundesverfassungsgericht.de*". Es wird nun eine Liste von Namen und Schlüsseln ausgeworfen.

Federal Constitutional Court

- Contact to the court at EDV-Gerichtstag
  - Discussing OpenPGP as compilable standard
- Need for tamper resistant publication method
  - Sometimes the printing process introduces errors
  - Printed version is legal until the error is corrected
  - Real cases after a “missing *not*” in sentences
- Embed inline PGP in comments
  - HTML code can be saved and validated with PGP/GPG

Modern history

- RFC3156 (RFC2015) embeds PGP in Mail
  - No more ASCII-armor (or?)
- Werner Koch published GnuPG
  - Most people switched from PGP to GPG
- PGP Corp brought PGP back from NAI
- RFC4880 reflected latest changes (not many)
- RFC4398 (RFC2538) PGP in DNS(Sec)
  - DANE on the track to an RFC
- PGP Corp acquired by Symantec
  - Source code not longer free

Questions?