

**Cnlab / CSI Herbsttagung 2014**

# **WIE FUNKTIONIEREN DIE ANGRIFFE DER NSA?**

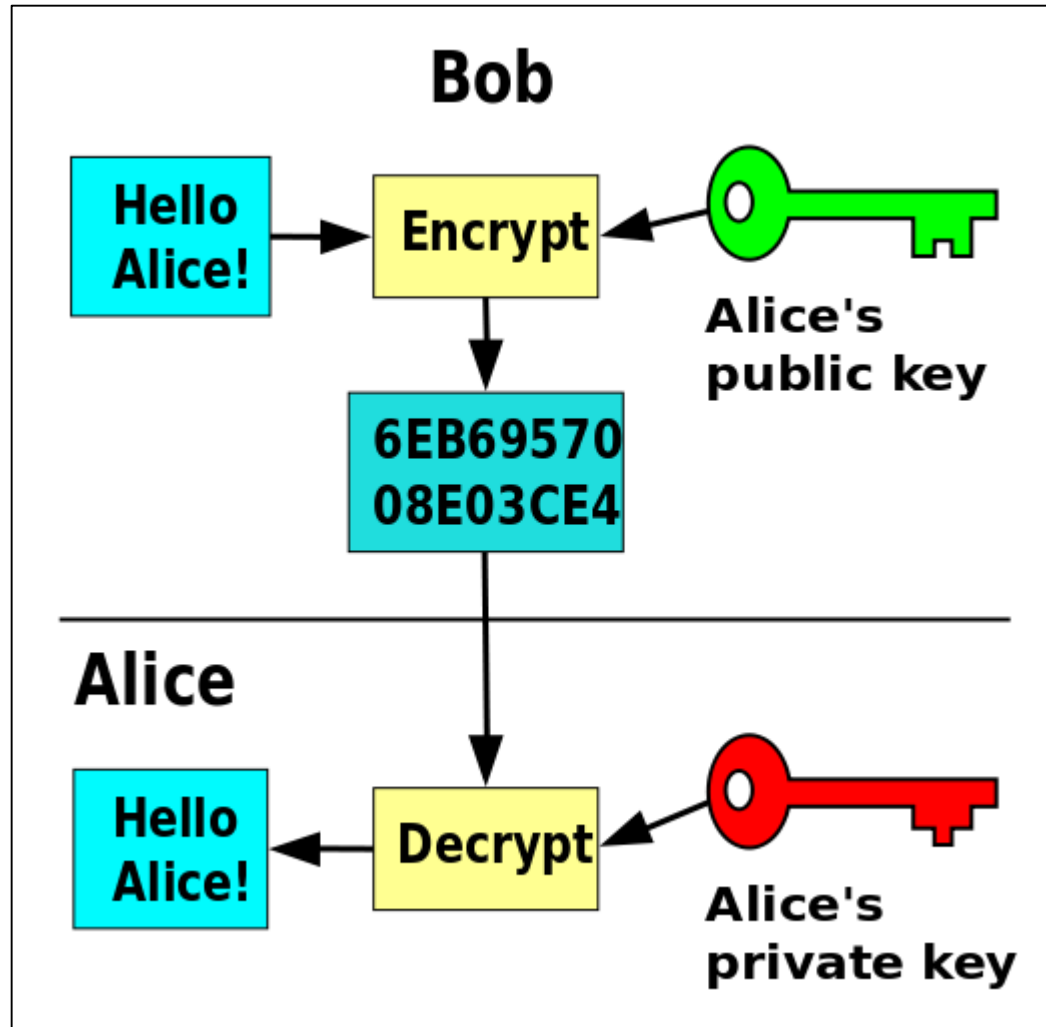
## Angriff über Zufallsgeneratoren: Was ist passiert?

- RSA BSAFE is a FIPS 140-2 validated cryptography library offered by RSA Security.
- From 2004 to 2013 the default random number generator in the library contained a backdoor from the American National Security Agency, as part of NSA's secret Bullrun program.

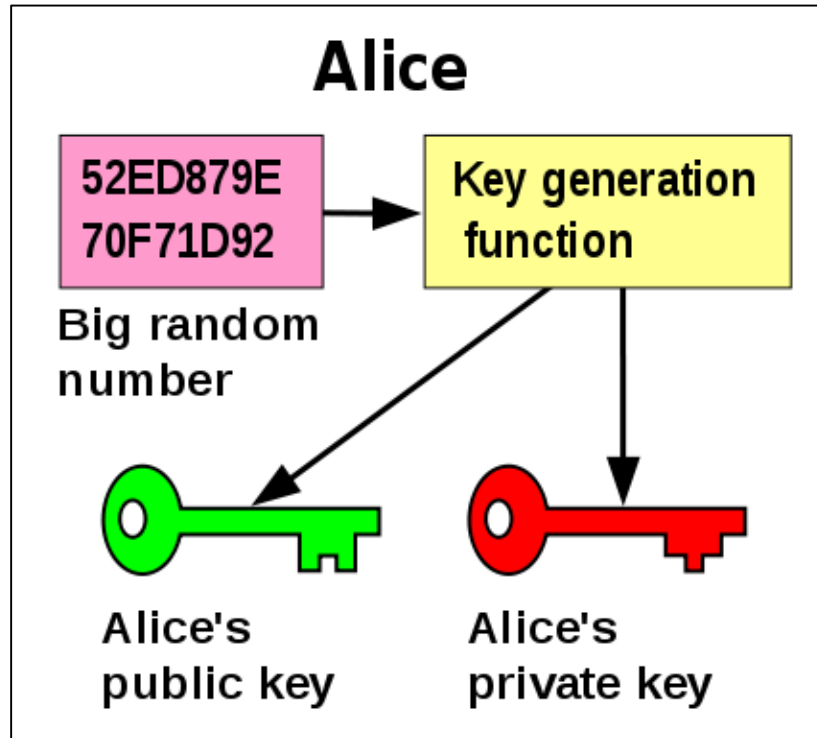
## Warum Angriff über Random-Generatoren?

- Zufallszahlen werden für die Erzeugung von Schlüsseln benötigt.
  - Symmetrische Schlüssel
  - Asymmetrische Schlüssel
- Der RG kann einfach kompromittiert werden
  - z.B. via Seed
- Ein schlechter Seed kann durch Tests an den erzeugten Zufallszahlen nicht nachgewiesen werden.

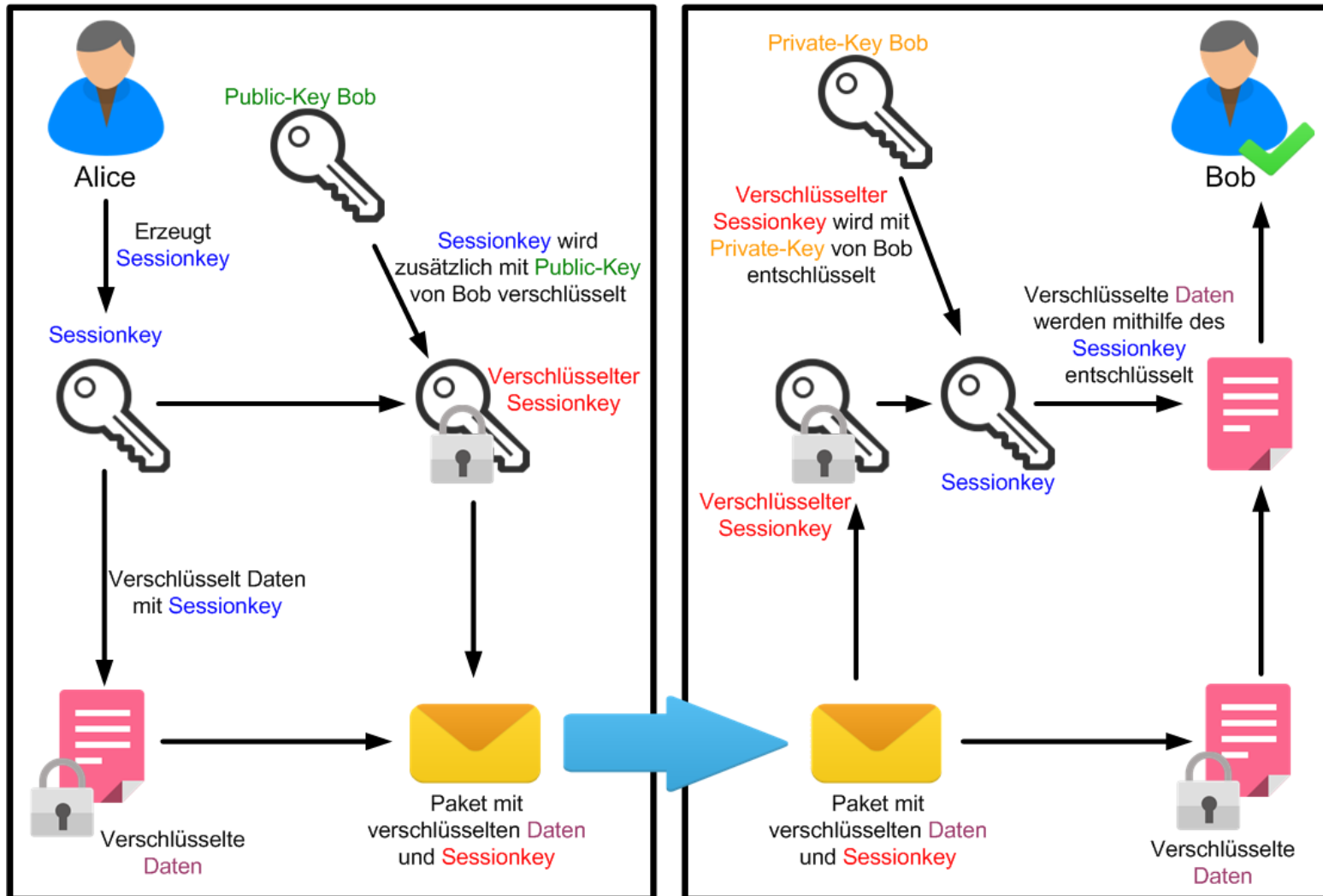
## Public-Key-Systeme (asymmetrische Systeme)



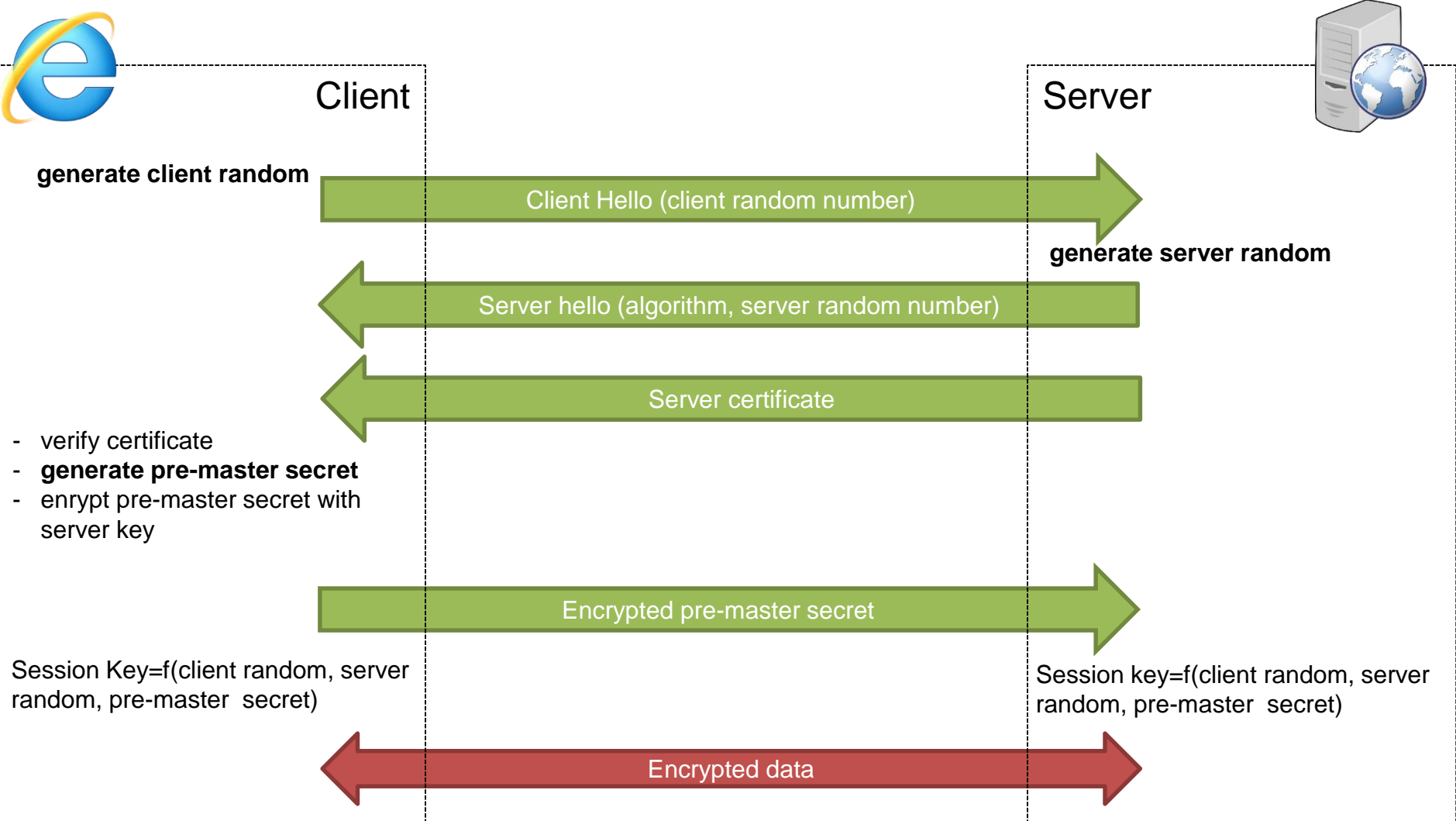
## Erzeugung von asymmetrischen Keys



## Hybride Verschlüsselungsverfahren

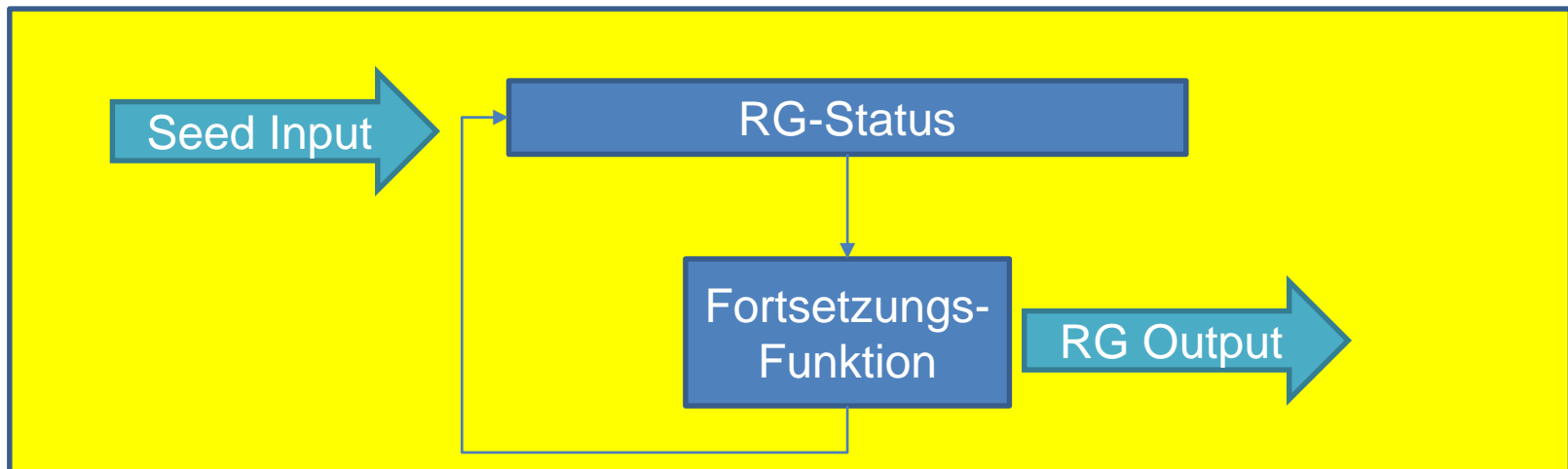


# Das Beispiel SSL



## Wie macht man Zufallszahlen

Characteristic	Pseudo-Random Number Generators	True Random Number Generators
Efficiency	Excellent	Poor
Determinism	Deterministic	Nondeterministic
Periodicity	Periodic	Aperiodic

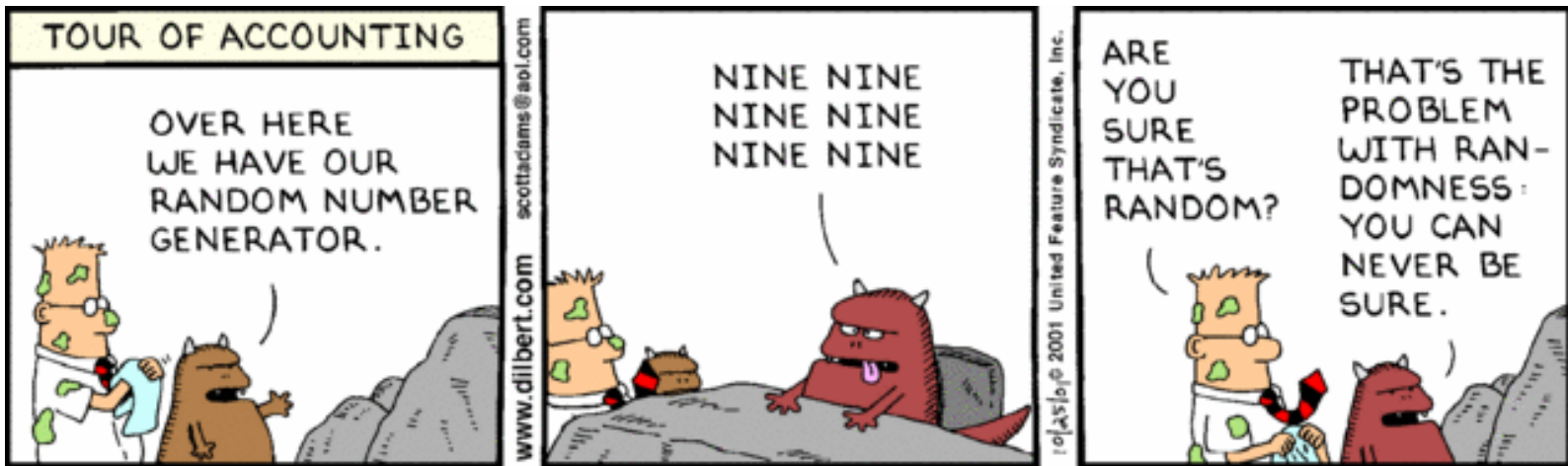




## Random-Generator in OpenSSL

- OpenSSL bietet eine Schnittstelle um den Random-Generator zu ersetzen.
- Default Random-Generator:
  - Fortsetzung-Funktion basierend auf MD5
  - Automatischer 'seed' abhängig von der Plattform:
    - Unix/Linux
      - /dev/urandom
      - Prozess-ID, User-ID, System-info
    - Windows
      - GcryptGenRandom (Microsoft Crypto API)

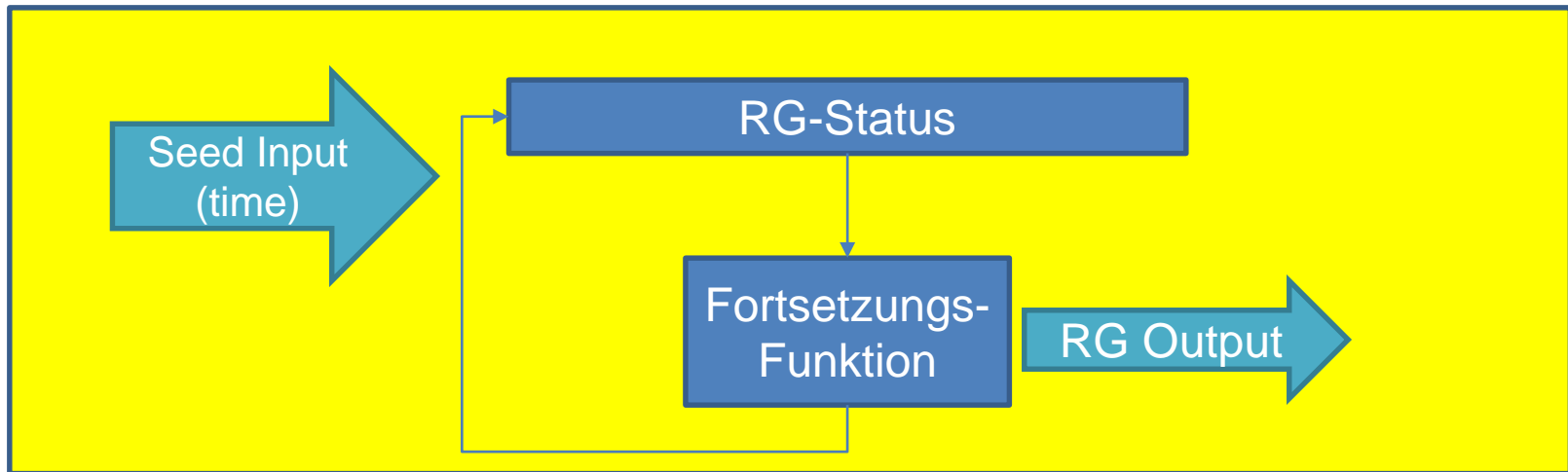
# Warum Angriff über Random-Generatoren?



## Random-Generator Test Tools

- NIST: statistical test suite
  - <http://csrc.nist.gov/rng/>
- DIEHARD test suite
  - <http://www.stat.fsu.edu/pub/diehard/>
- Beide Suiten sind Implementationen der selben Tests
- Der Random-Generator wird als gut betrachtet bei einem Test Resultat  $> 0$  und  $< 1$

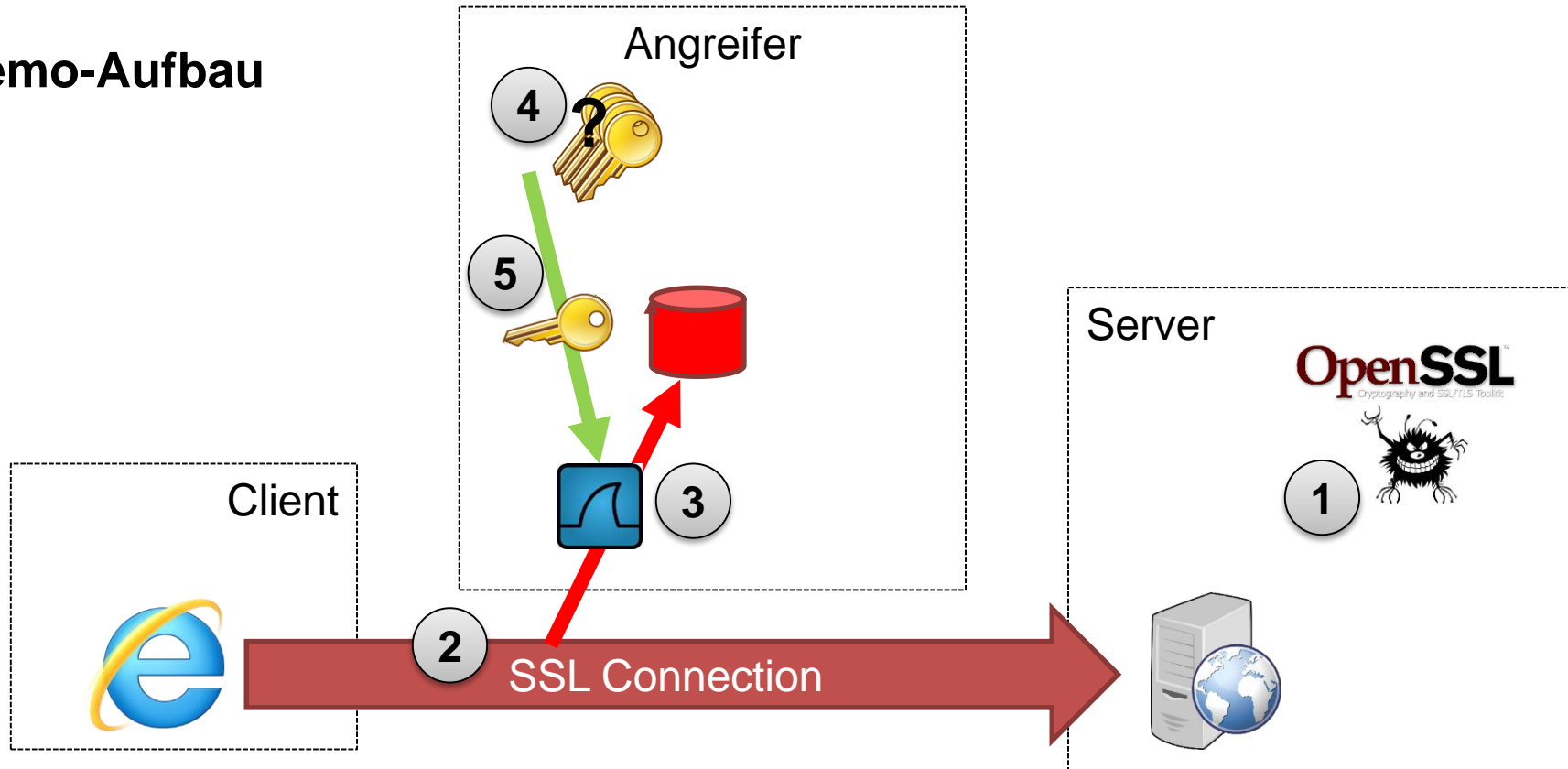
## Anpassungen am OpenSSL RG



## Test Resultate DIEHARD Test Suite

Test Name	P-value	Result
Birthday Spacing Test	0.387	Pass
Overlapping 5-Permutation Test	0.328	Pass
Binary Rank Test (32x32 matrices)	0.985	Pass
Bitstream Test	0.548	Pass
Count-the-1's Test (on stream of bytes)	0.316	Pass
Parking Lot Test	0.752	Pass
Minimum Distance Test	0.449	Pass
3D Spheres Test	0.196	Pass
Overlapping Sums Test	0.110	Pass
Craps Test	0.754	Pass

## Demo-Aufbau



1. Schlüsselerzeugung mit modifizierten OpenSSL
2. SSL-Verbindungen vom Browser zum Web-Server
3. Verkehr wird durch den Angreifer aufgezeichnet
4. Der verwendete Schlüssel wird gesucht
5. Verkehr kann entschlüsselt werden

# Demo (3): Aufzeichnen der verschlüsselten Verbindung

The screenshot displays the Wireshark interface with a list of network packets and a detailed view of a selected frame (Frame 11).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.20.30.87	62.2.156.87	TCP	66	spw-dialer-https [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.002519000	62.2.156.87	10.20.30.87	TCP	66	https-spw-dialer [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=8
3	0.002635000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=1 Ack=1 win=65536 Len=0
4	0.009936000	10.20.30.87	62.2.156.87	TLSv1.2	231	client Hello
5	0.010966000	62.2.156.87	10.20.30.87	TCP	60	https-spw-dialer [ACK] Seq=1 Ack=178 win=15672 Len=0
6	0.011926000	62.2.156.87	10.20.30.87	TLSv1.2	845	Server Hello, Certificate, Server Hello Done
7	0.011976000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=178 Ack=792 win=64768 Len=0
8	0.012527000	10.20.30.87	62.2.156.87	TLSv1.2	284	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
9	0.014202000	62.2.156.87	10.20.30.87	TLSv1.2	145	change cipher spec, Encrypted Handshake Message
10	0.014249000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=408 Ack=883 win=64768 Len=0
11	0.047120000	10.20.30.87	62.2.156.87	TLSv1.2	475	Application Data
12	0.048695000	62.2.156.87	10.20.30.87	TLSv1.2	331	Application Data
13	0.048753000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=829 Ack=1160 win=64512 Len=0
14	5.054896000	62.2.156.87	10.20.30.87	TLSv1.2	123	Encrypted Alert
15	5.054898000	62.2.156.87	10.20.30.87	TCP	60	https-spw-dialer [FIN, ACK] Seq=1229 Ack=829 win=17816 Len=0
16	5.054967000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=829 Ack=1230 win=64256 Len=0

**Frame 11: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface 1**

- Ethernet II, Src: 12:12:12:12:12:12 (12:12:12:12:12:12), Dst: 50:67:f0:21:f8:df (50:67:f0:21:f8:df)
- Internet Protocol Version 4, Src: 10.20.30.87 (10.20.30.87), Dst: 62.2.156.87 (62.2.156.87)
- Transmission Control Protocol, Src Port: spw-dialer (3796), Dst Port: https (443), Seq: 408, Ack: 883, Len: 421
- Secure Sockets Layer
  - TLSv1.2 Record Layer: Application Data Protocol: http
    - Content Type: Application Data (23)
    - Version: TLS 1.2 (0x0303)
    - Length: 416
    - Encrypted Application Data: 95b24fed1a3bbdd352443b177cdfdaafe3738e6340a685e4...

Hex dump of the encrypted data (Frame 11):

```

0030  00 fd 04 84 00 00 17 03 03 01 a0 95 b2 4f ed 1a  ..RD:|...s.c@
0040  3b bd d3 52 44 3b 17 7c df da af e3 73 8e 63 40  .....+.1.
0050  a6 85 e4 14 d5 8a a4 ba b6 a4 ac 11 2b 97 31 bf  .....8.q@....
0060  bc 14 89 f4 5f 38 ca e5 71 b6 40 b9 9c ef 16 f4  ./=9u...x....
0070  b7 2f 3d 39 75 86 d1 da e0 9e 78 b0 f5 bf 0e 0c  ?&.#.fo
0080  01 22 05 c6 26 b7 3d 1c dc 22 81 8b 66 51 d5 28  '."5.c6.67.}.dc."81.8b.66.51.d5.28
    
```

# Demo (5): Entschlüsselung mit gefundenem Schlüssel

The image shows a Wireshark capture of an HTTPS session. The packet list pane shows 16 packets. Packet 11 is the HTTP GET request for /demo2014/. Packet 12 is the corresponding response, which is highlighted in yellow. The packet details pane for packet 12 shows the Hypertext Transfer Protocol section expanded, displaying the raw GET request: `GET /demo2014/ HTTP/1.1\r\n`. The packet bytes pane at the bottom shows the raw data of the frame (475 bytes) and the decrypted SSL data (357 bytes).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.20.30.87	62.2.156.87	TCP	66	spw-dialer-https [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.002519000	62.2.156.87	10.20.30.87	TCP	66	https-spw-dialer [SYN, ACK] Seq=0 Ack=1 win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=8
3	0.002635000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=1 Ack=1 win=65536 Len=0
4	0.009936000	10.20.30.87	62.2.156.87	TLSv1.2	231	Client Hello
5	0.010966000	62.2.156.87	10.20.30.87	TCP	60	https-spw-dialer [ACK] Seq=1 Ack=178 win=15672 Len=0
6	0.011926000	62.2.156.87	10.20.30.87	TLSv1.2	845	Server Hello, Certificate, Server Hello Done
7	0.011976000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=178 Ack=792 win=64768 Len=0
8	0.012527000	10.20.30.87	62.2.156.87	TLSv1.2	284	Client key Exchange, Change Cipher Spec, Finished
9	0.014202000	62.2.156.87	10.20.30.87	TLSv1.2	145	Change Cipher Spec, Finished
10	0.014249000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=408 Ack=883 win=64768 Len=0
11	0.047120000	10.20.30.87	62.2.156.87	HTTP	475	GET /demo2014/ HTTP/1.1
12	0.048695000	62.2.156.87	10.20.30.87	HTTP	331	HTTP/1.1 304 Not Modified
13	0.048753000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=829 Ack=1160 win=64512 Len=0
14	5.054896000	62.2.156.87	10.20.30.87	TLSv1.2	123	Alert (Level: warning, Description: Close Notify)
15	5.054898000	62.2.156.87	10.20.30.87	TCP	60	https-spw-dialer [FIN, ACK] Seq=1229 Ack=829 win=17816 Len=0
16	5.054967000	10.20.30.87	62.2.156.87	TCP	54	spw-dialer-https [ACK] Seq=829 Ack=1230 win=64256 Len=0

Frame 11: 475 bytes on wire (3800 bits), 475 bytes captured (3800 bits) on interface 1

- Ethernet II, Src: 12:12:12:12:12:12 (12:12:12:12:12:12), Dst: 50:67:f0:21:f8:df (50:67:f0:21:f8:df)
- Internet Protocol Version 4, Src: 10.20.30.87 (10.20.30.87), Dst: 62.2.156.87 (62.2.156.87)
- Transmission Control Protocol, Src Port: spw-dialer (3796), Dst Port: https (443), Seq: 408, Ack: 883, Len: 421
- Secure Sockets Layer
  - TLSv1.2 Record Layer: Application Data Protocol: http
- Hypertext Transfer Protocol
  - GET /demo2014/ HTTP/1.1\r\n
    - [Expert Info (Chat/Sequence): GET /demo2014/ HTTP/1.1\r\n]
      - [GET /demo2014/ HTTP/1.1\r\n]
      - [Severity level: Chat]
      - [Group: Sequence]
    - Request Method: GET
    - Request URI: /demo2014/
    - Request Version: HTTP/1.1
    - Accept: text/html, application/xhtml+xml, \*/\*\r\n

0000 50 67 f0 21 f8 df 12 12 12 12 12 12 12 08 00 45 00 Pg.!... ..E.  
 0010 01 cd 06 a9 40 00 80 06 00 00 0a 14 1e 57 3e 02 ....@...w>.  
 0020 9c 57 0e d4 01 bb 7d 0f fe 79 c2 26 6e 23 50 18 .w....}. .y.&#P.

Frame (475 bytes) | Decrypted SSL data (357 bytes)



**Danke**

**Thomas Lüthi**  
thomas.luethi@cnlab.ch  
+41 55 214 33 41

10.9.2014