Cnlab / CSI Herbsttagung 2014

WIE FUNKTIONIEREN DIE ANGRIFFE DER NSA?

Quelle: Wikipedia

Angriff über Zufallsgeneratoren: Was ist passiert?

- RSA BSAFE is a FIPS 140-2 validated cryptography library offered by RSA Security.

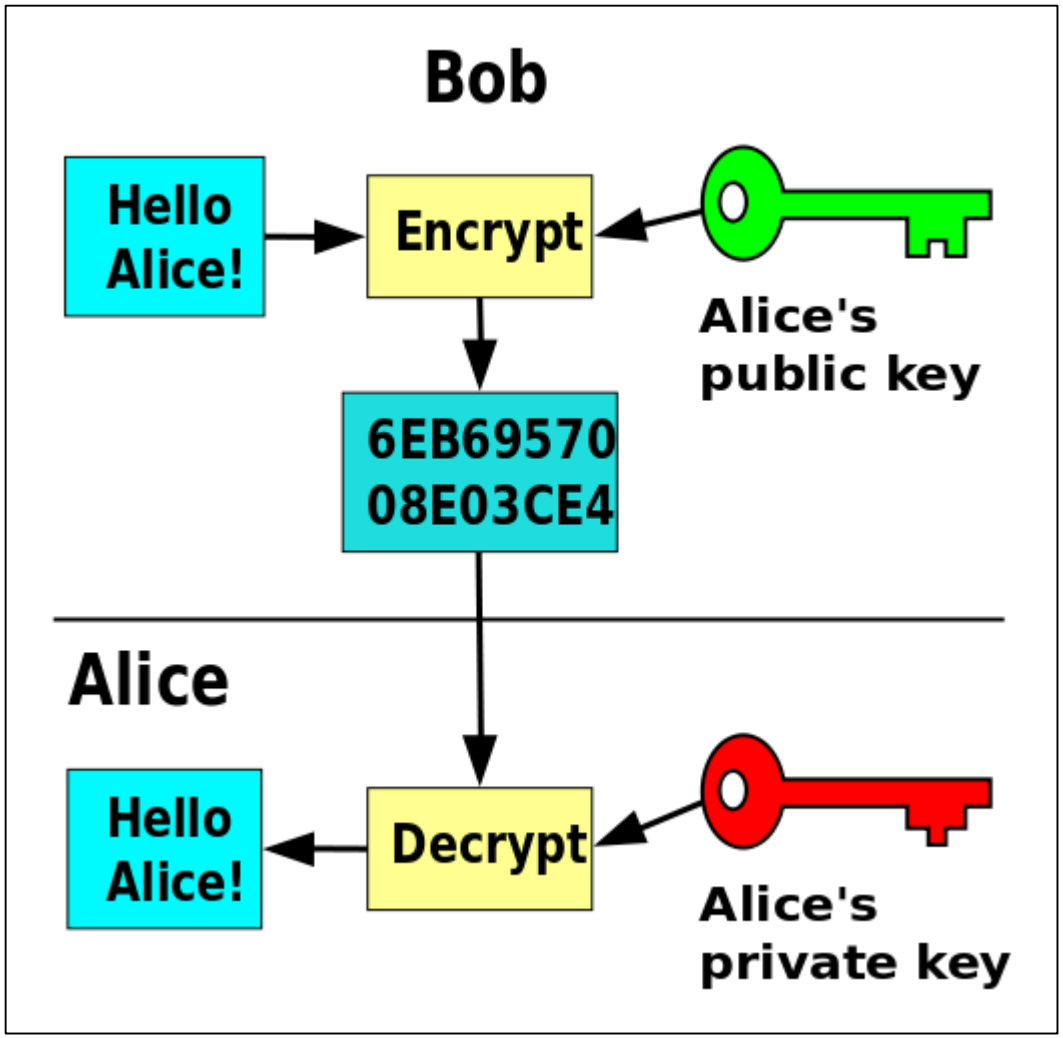
- From 2004 to 2013 the default random number generator in the library contained a backdoor from the American National Security Agency, as part of NSA's secret Bullrun program.

Warum Angriff über Random-Generatoren?

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

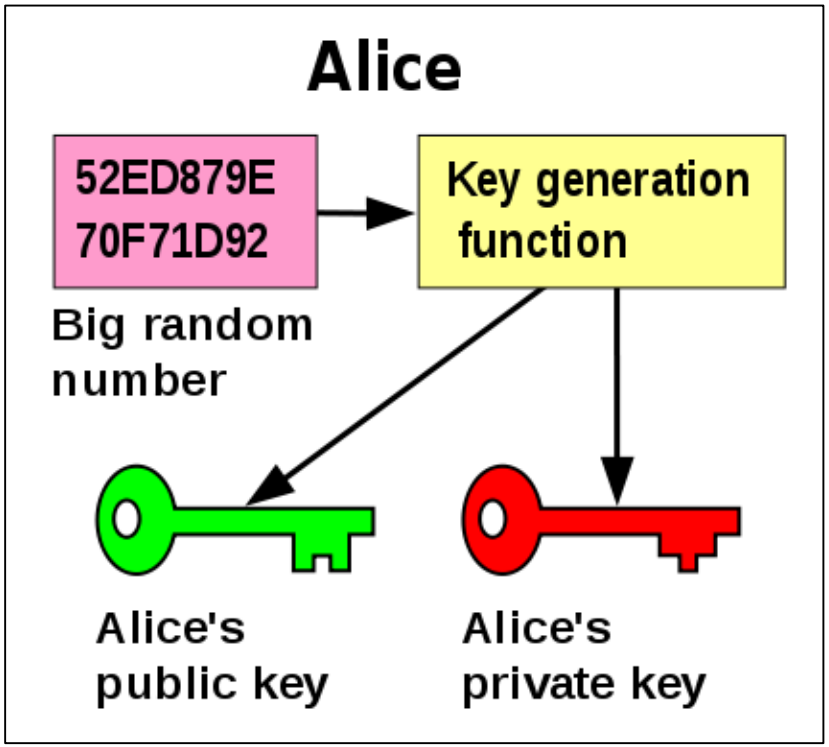
Quelle: Wikipedia

Public-Key-Systeme (asymmetrische Systeme)



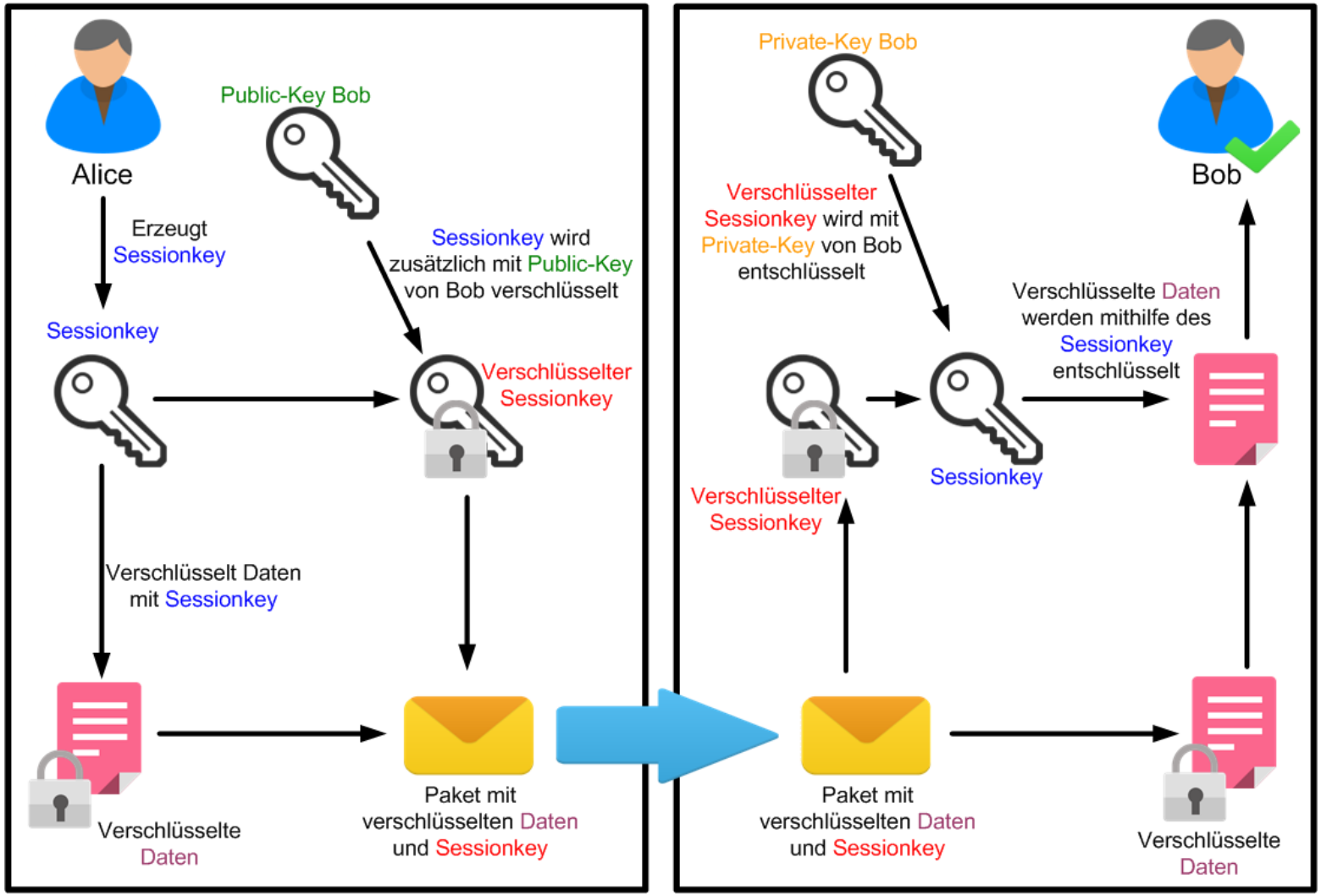
Quelle: Wikipedia

Erzeugung von asymmetrischen Keys



Quelle: Wikipedia

Hybride Verschlüsselungsverfahren



Das Beispiel SSL

Client

Server

generate client random

Client Hello (client random number)

generate server random

Server hello (algorithm, server random number)

Server certificate

- verify certificate
- **generate pre-master secret**
- enrypt pre-master secret with server key

Encrypted pre-master secret

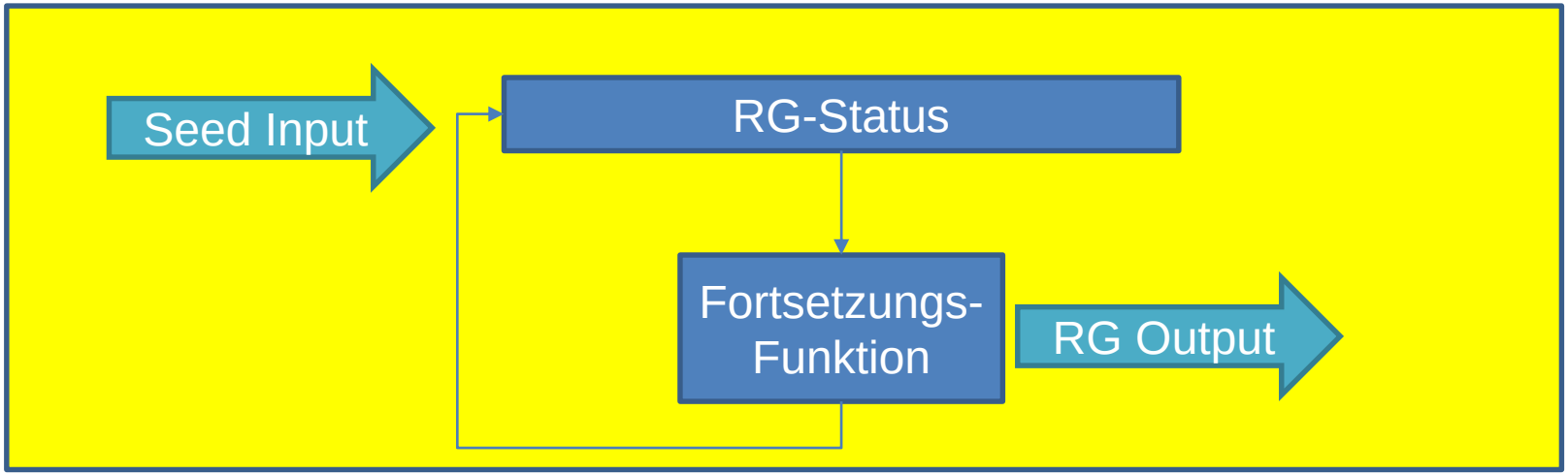
Session Key=f(client random, server random, pre-master secret)

Session key=f(client random, server random, pre-master secret)

Encrypted data

Wie macht man Zufallszahlen

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

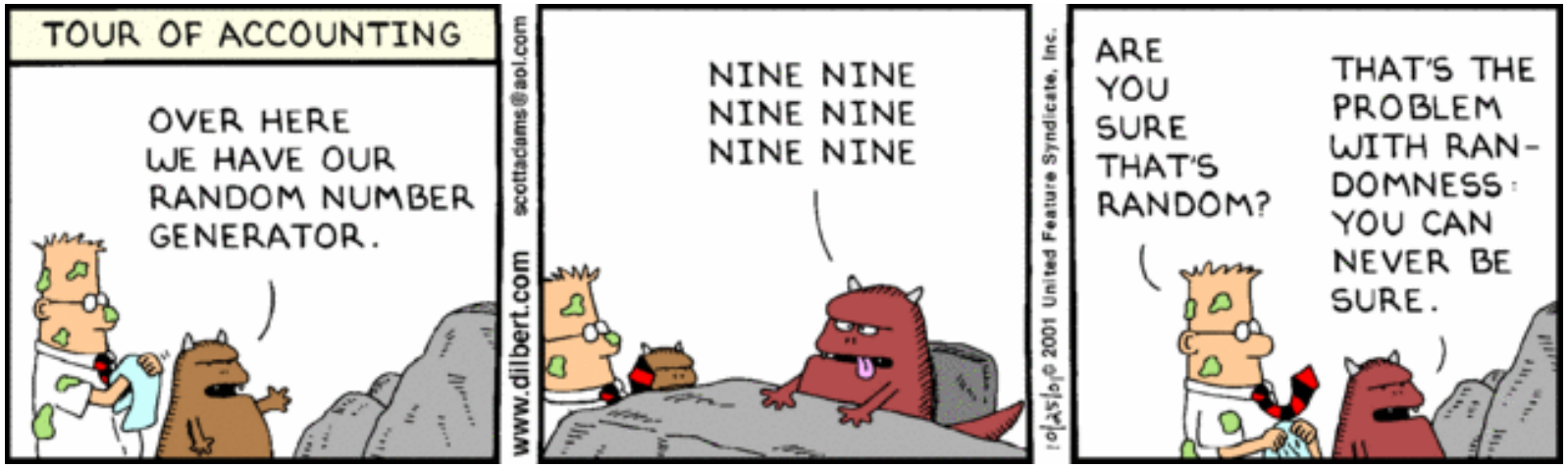


Random-Generator in OpenSSL

- 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
      - GryptGenRandom (Microsoft Crypto API)

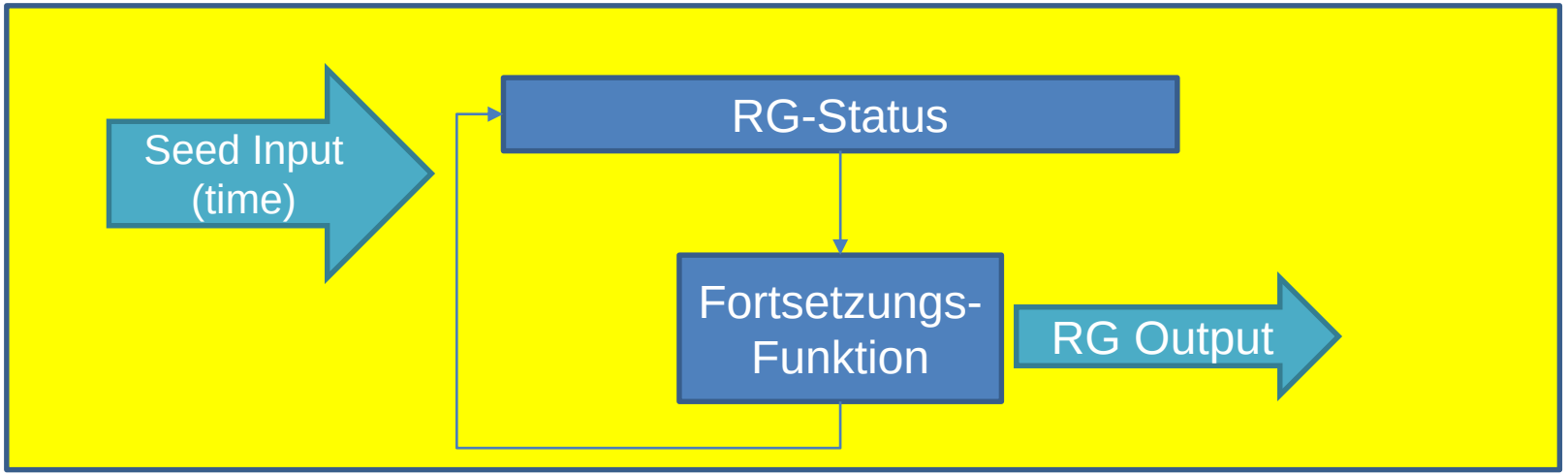
Warum Angriff über Random-Generatoren?



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

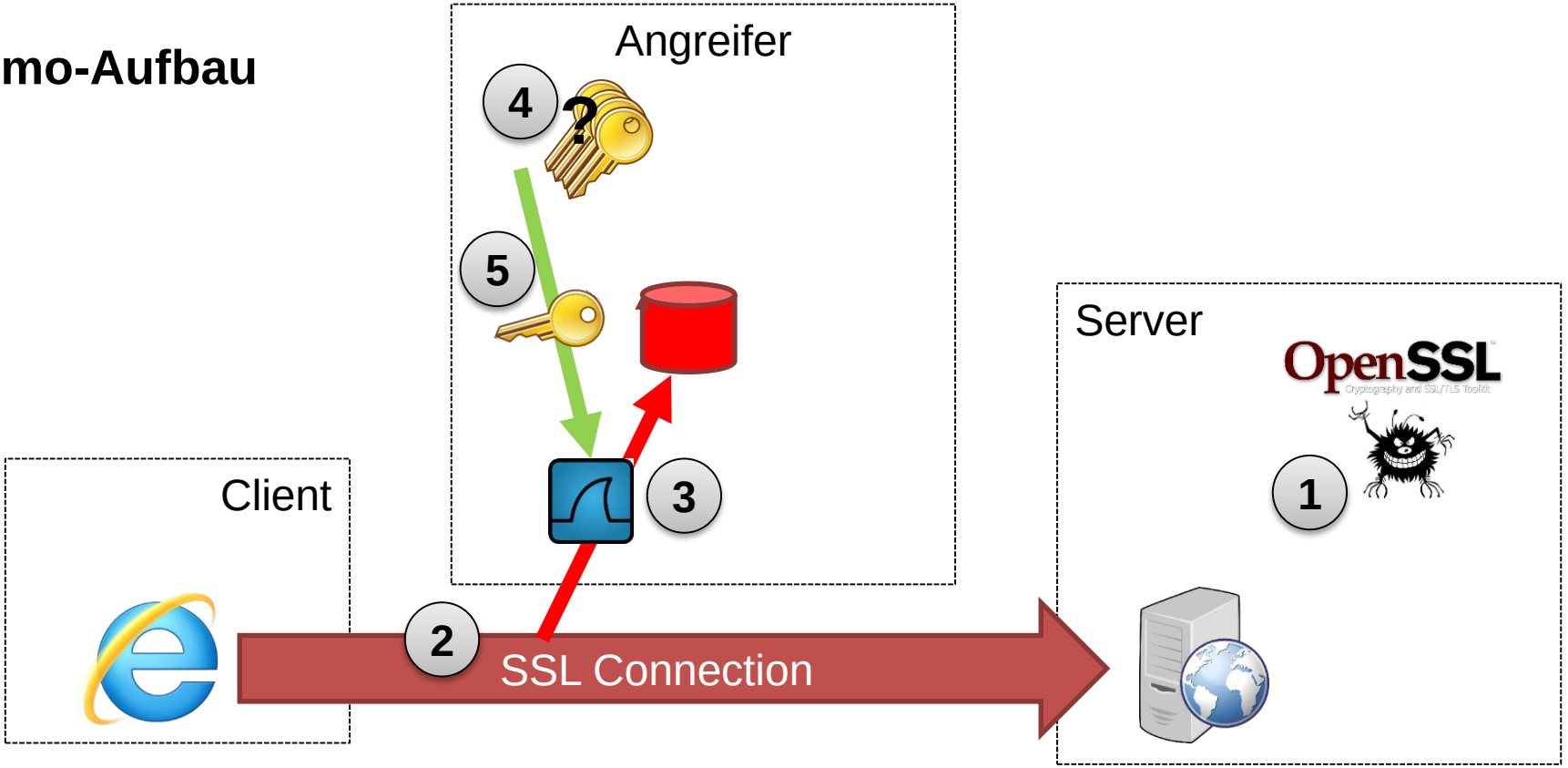
Anpassungen am OpenSSL RG



Test Resultate DIEHARD Test Suite

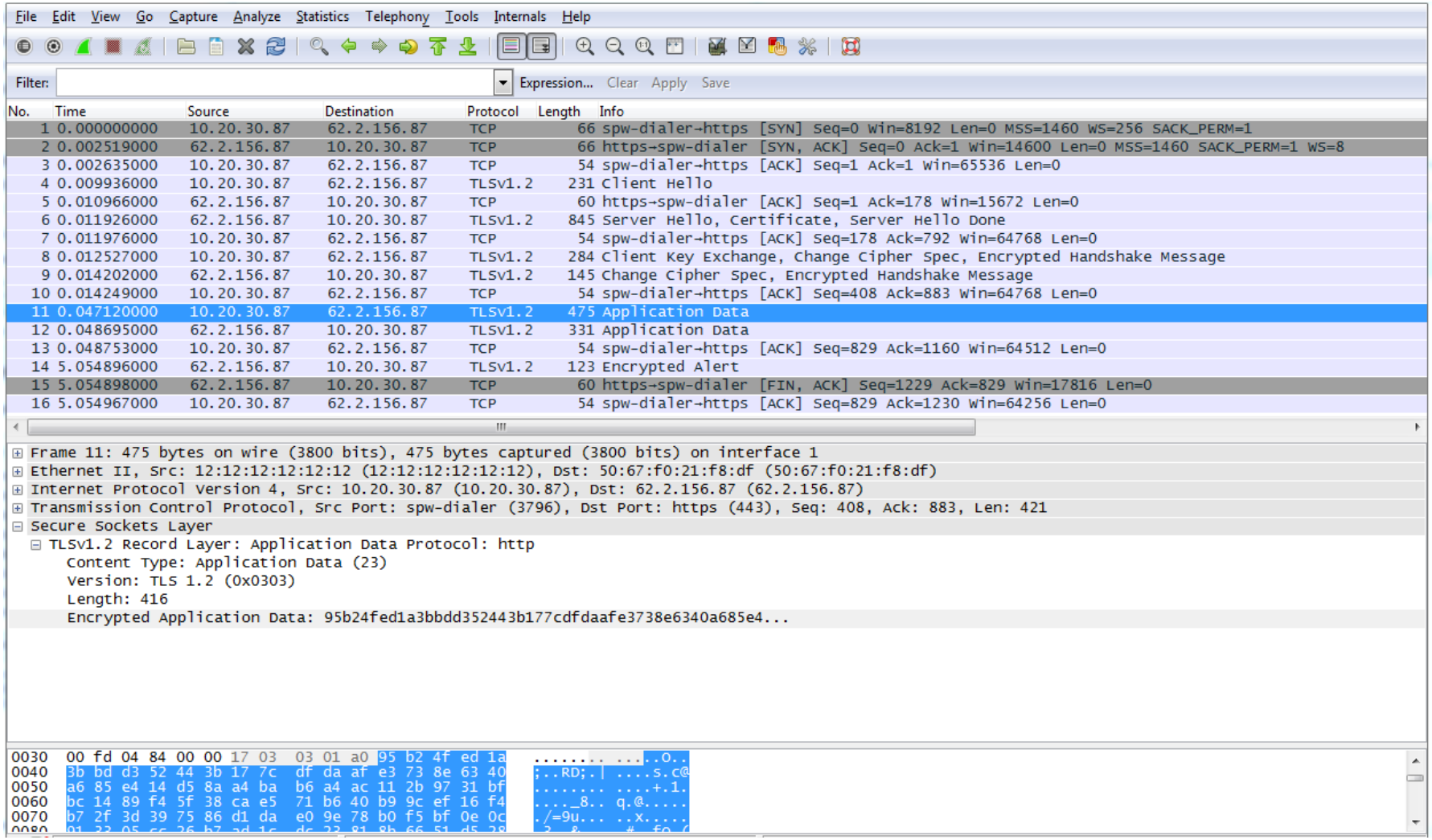
Test Name	P-value	Result
Birthday Spacing Test	0.387	Pass
Overlapping 5-Permutation Test	0.328	Pass
Binary Rank Test (32x32 matrices)	0.985	Pass
Bitstream Test	0.548	Pass
Count-the-1's Test (on stream of bytes)	0.316	Pass
Parking Lot Test	0.752	Pass
Minimum Distance Test	0.449	Pass
3D Spheres Test	0.196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

Demo-Aufbau

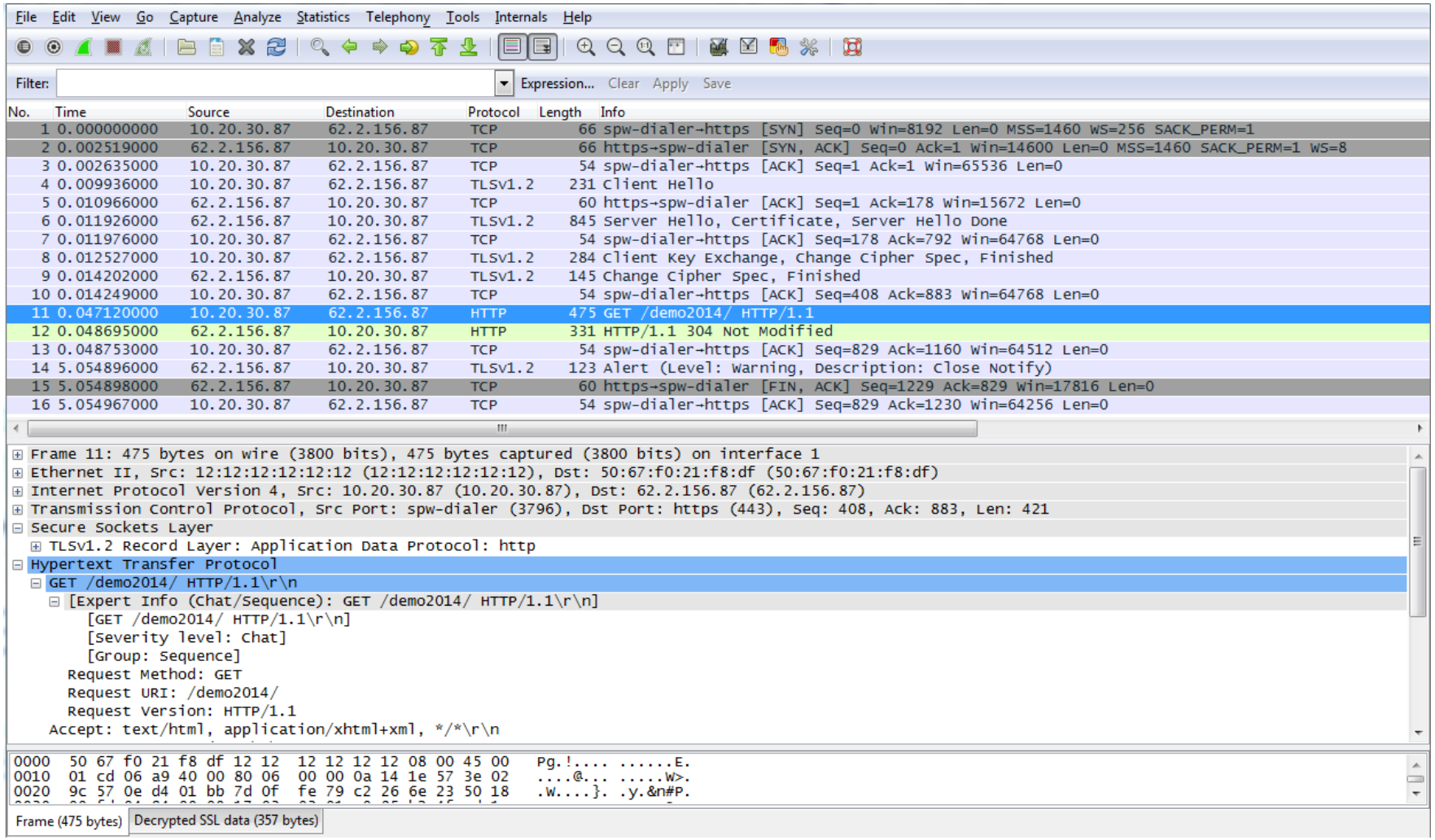


1. Schlüsselerzeugung mit modifizierten OpenSSL
2. SSL-Verbindungen vom Browser zum Web-Server
3. Verkehr wird durch den Angreifer aufgezeichnet
4. Der verwendete Schlüssel wird gesucht
5. Verkehr kann entschlüsselt werden

Demo (3): Aufzeichnen der verschlüsselten Verbindung



Demo (5): Entschlüsselung mit gefundenem Schlüssel



Danke

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