freeware

OTP-Crypt.com

- die perfekte Verschlüsselung -

OTP-Crypt.com

#2: Techn. Stand von OTP-Crypt

Verfügbar für Windows© und Linux©

… das beste Verfahren zum Aufbewahren und Teilen von Geheimnissen …

Technischer Stand von OTP-Crypt

OTP-Crypt.com

- Hardware:

Die Generierung von Zufallszahlen haben wir, aus technischer Sicht gesehen, ganz neu entwickelt.

Die Eigenentwicklung unserer Hardware in Verbindung mit messtechnischer Software, erlaubt uns bei der Erzeugung von Zufallszahlen eine optische Überwachung der Qualität.

Im Live-Stream-Modus benutzen wir die FFT Analyse. Sie wird im Monitor-Modus direkt angezeigt und visualisiert etwaige Abweichungen. Hier kann bei Bedarf sofort eingegriffen werden.

Die Qualität der erzeugten Zufallszahlen wurde dahingehend gesteigert, das schon unsere Rohdaten den FIPS-140 Test bestehen.

Technischer Stand von OTP-Crypt

OTP-Crypt.com

- Hardware:

Weiterführende Prüfungen (DieHarder, ENT, NIST (National Institute of Standards and Technology), etc.) bestätigen die hohe Qualität unserer Zufallszahlen.

Auf Wunsch können wir die „Zufälligkeit“ der Daten noch weiter erhöhen. Dabei setzen wir selbstverständlich keine Filter ein, die nur zum Schein die Zufälligkeit erhöhen.

Die tägliche Menge an erzeugten Zufallszahlen könnte mehrere DVD’s, randvoll mit Zufallszahlen, betragen.

Eine Mengenbegrenzung findet nicht aus technischen Gründen, sondern aus arbeitstechnischen Gründen statt.

Technischer Stand von OTP-Crypt

OTP-Crypt.com

- Software:

Wie allgemein bei Software üblich, wird es über die Zeit verbesserte Versionen geben. So auch bei uns. Die Entwicklung neuer verbesserter Anwendungssoftware wird angestrebt.

Die aktuellen Datenmengen werden unglaublich schnell verarbeitet. Die Routinen zum Laden, Speichern und zum Verschlüsseln sind bzgl. der Geschwindigkeit optimiert.

Für die Datenverarbeitung im Hintergrund sind durch uns kleine Tools auf Basis der Programmiersprache C und Assembler entwickelt worden. Bei diesen Tools ist kaum noch mit einer Steigerung der Geschwindigkeit durch Softwareoptimierung zu rechnen.

Am Bedienkomfort der Anwendungssoftware (Schnittstelle zum Internet) wird es noch sehr viel, auch über längere Zeiträume, zu verbessern geben. Hier sehen wir unsere zukünftigen Schwerpunkte.

Technischer Stand von OTP-Crypt

- Die Qualität der Zufallszahlen:

OTP-Crypt.com

Die Qualität der Zufallszahlen

Die erzeugten Zufallszahlen müssen bestimmte Kriterien bzgl. der Qualität erfüllen.

Hierzu gibt es Prüf-Software von verschiedenen staatlichen Behörden und Instituten diverser Länder. Auch wissenschaftliche Ausarbeitungen mit bestimmten Testroutinen sind softwaretechnisch umgesetzt worden.

Wir zeigen Ihnen hier auszugsweise, wie die Test-und Prüfsoftware unsere Zufallszahlen durchlaufen.

Diese Zusammenfassung beweist unseren hohen Qualitätsanspruch der erzeugten Zufallszahlen.

Technischer Stand von OTP-Crypt

OTP-Crypt.com

- Bundesamt für Sicherheit in der Informations-technik (BSI):

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Tool mit dem Namen AIS 31 herausgebracht.

Hier wird sichergestellt, dass in Kryptoprodukten die verwendeten Zufallszahlengeneratoren nur zufällige und nicht vorhersagbaren Daten liefern.

Technischer Stand von OTP-Crypt

OTP-Crypt.com

- Bundesamt für Sicherheit in der Informations-technik (BSI):

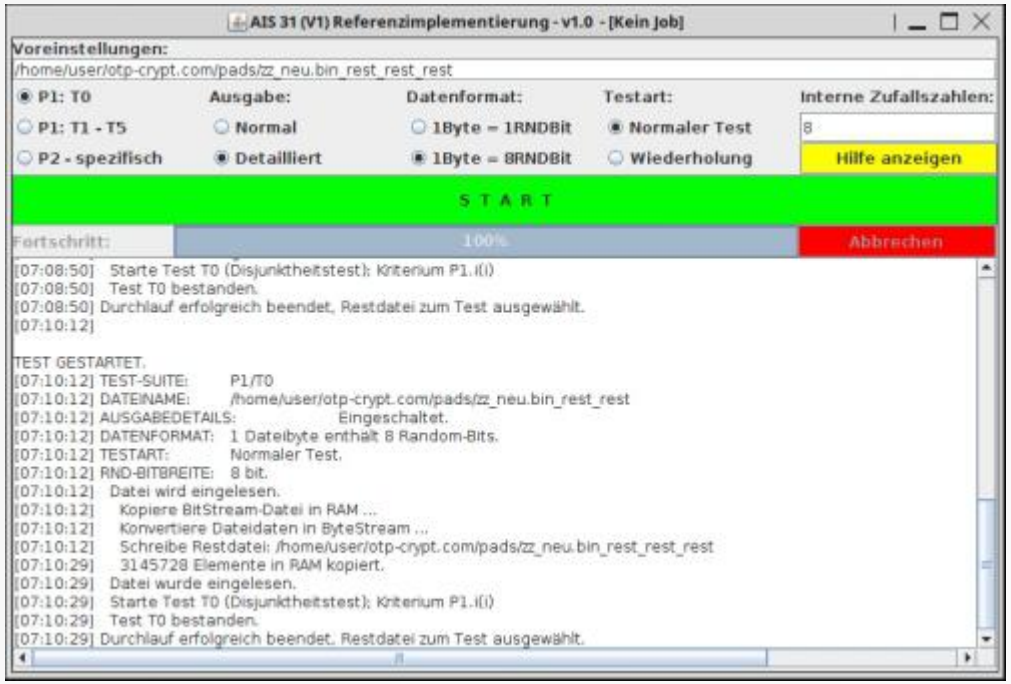
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Tool mit dem Namen AIS 31 herausgebracht.

Hier wird sichergestellt, dass in Kryptoprodukten die verwendeten Zufallszahlengeneratoren nur zufällige und nicht vorhersagbaren Daten liefern.

Technischer Stand von OTP-Crypt

- **Bundesamt für Sicherheit in der Informations-technik (BSI):**



Erfolgreicher Einsatz des Test- und Prüfprogramms AIS 31

OTP-Crypt.com

Technischer Stand von OTP-Crypt

- TÜV Informationstechnik GmbH:

Zum Angebot der TÜViT gehört die Bewertung, Prüfung und Zertifizierung von IT-Prozessen, IT-Systemen und IT-Produkten.Die deutsche Prüfstelle ist zur Prüfung (Kryptoalgorithmen) der Tests FIPS 140-1 und FIPS 140-2 (engl.) von der NIST zugelassen und akkreditiert.

```
Copyright (c) 2004 by Henrique de Moraes Holschuh
This is free software; see the source for copying conditions.  There is NO warranty;

rngtest: starting FIPS tests...
rngtest: bits received from input: 2000032
rngtest: FIPS 140-2 successes: 100
rngtest: FIPS 140-2 failures: 0
rngtest: FIPS 140-2(2001-10-10) Monobit: 0
rngtest: FIPS 140-2(2001-10-10) Poker: 0
rngtest: FIPS 140-2(2001-10-10) Runs: 0
rngtest: FIPS 140-2(2001-10-10) Long run: 0
rngtest: FIPS 140-2(2001-10-10) Continuous run: 0
rngtest: input channel speed: (min=635.783; avg=2486.765; max=4768.372)Mibits/s
rngtest: FIPS tests speed: (min=4.012; avg=15.816; max=33.287)Mibits/s
rngtest: Program run time: 122294 microseconds
```

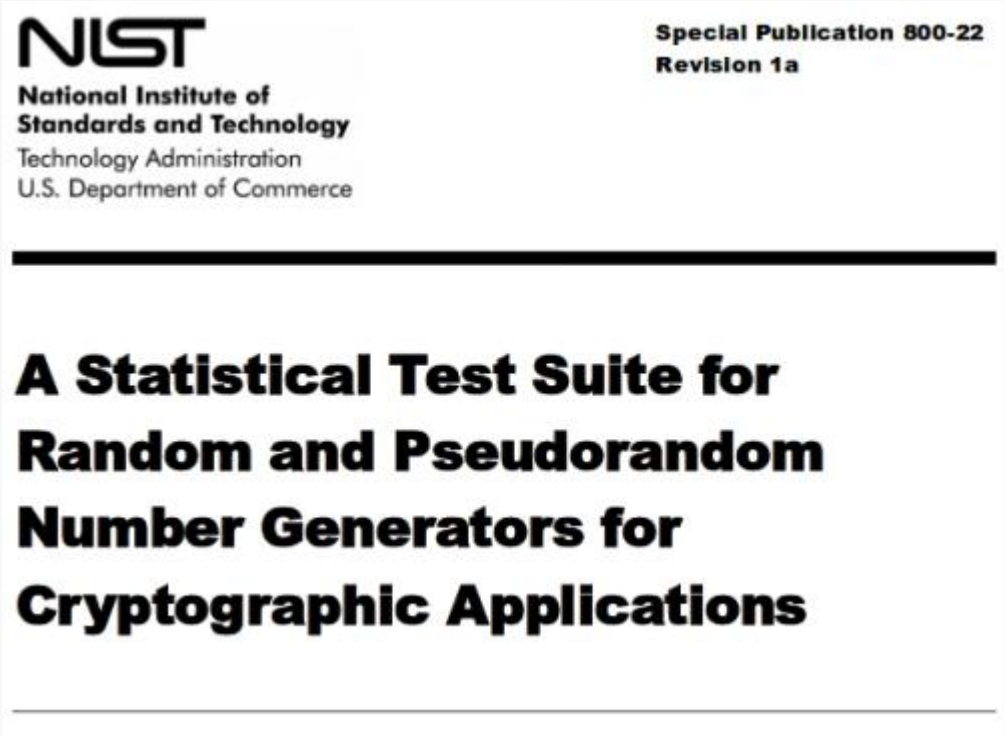
Alle Tests (Monobit, Poker, Runs, Long run, Continuous run) nach FIPS 140-2 wurden bestanden.

Technischer Stand von OTP-Crypt

- National Institute of Standards and Technology (NIST):

OTP-Crypt.com

Die NIST ist eine Bundesbehörde in den vereinigten Staaten.


NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-22
Revision 1a

A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

Test-Suite nach Special Publication 800-22, (auch FIPS 140-2 und sts 2.1.2)

Technischer Stand von OTP-Crypt

- Das Programm ENT:

OTP-Crypt.com

Das Programm ENT

Das Programm ENT ist mittlerweile zu einem Standard geworden.

Besonders der Chi Quadrat Test ist sehr aussagekräftig. Die wichtigsten Tests in ENT behandeln die

- Entropy
- Kompression
- Chi Quadrat
- Mittelwert
- Monte Carlo
- Serial correlation

Technischer Stand von OTP-Crypt

- Das Programm ENT:

OTP-Crypt.com

Für den Chi Quadrat Test wird folgendes interpretiert:

Nicht zufällig: Wenn der Wert größer 99 Prozent oder kleiner 1 Prozent ist. (> 99% or < 1%)

Verdächtig: Wenn der Wert zwischen 95 Prozent und 99 Prozent oder zwischen 1 Prozent und 5 Prozent liegt. (> 95% and < 99% or > 1% and < 5%)

Fast verdächtig: Wenn der Wert zwischen 90 Prozent und 95 Prozent oder zwischen 5 Prozent und 10 Prozent liegt. (> 90% and < 95% or > 5% and < 10%)

```
Entropy = 8.000000 bits per byte.

Optimum compression would reduce the size
of this 1000000000 byte file by 0 percent.

Chi square distribution for 1000000000 samples is 224.03, and randomly
would exceed this value 91.94 percent of the times.

Arithmetic mean value of data bytes is 127.5004 (127.5 = random).
Monte Carlo value for Pi is 3.141516133 (error 0.00 percent).
Serial correlation coefficient is -0.000013 (totally uncorrelated = 0.0).
```

Ausgabe der wichtigsten Tests über die Qualität von Zufallszahlen.

Technischer Stand von OTP-Crypt

- Das Programm dieharder:

Das Programm dieharder ist das umfangreichste Tool zur Ermittlung der Qualität von Zufallszahlen. Verschiedene Tests wurden hier zusammengefasst.

Auszug diverser Tests in Aktion. Auch sts-Tests wurden bestanden.

Um diese Tests zu bestehen, muss die Datei aus Zufallszahlen eine sehr hohe Qualität aufweisen.

```
#=============================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown          #
#=============================================================================#
   rng_name    |rands/second|   Seed   |
        mt19937|  5.23e+07  |3123452746|
#=============================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#=============================================================================#
   diehard_birthdays|   0|       100|     100|0.92038499|  PASSED
      diehard_operm5|   0|   1000000|     100|0.39239949|  PASSED
  diehard_rank_32x32|   0|     40000|     100|0.86487362|  PASSED
    diehard_rank_6x8|   0|    100000|     100|0.95989703|  PASSED
   diehard_bitstream|   0|   2097152|     100|0.79375352|  PASSED
        diehard_opso|   0|   2097152|     100|0.92092628|  PASSED
        diehard_oqso|   0|   2097152|     100|0.87092259|  PASSED
         diehard_dna|   0|   2097152|     100|0.50235274|  PASSED
diehard_count_1s_str|   0|    256000|     100|0.97154859|  PASSED
diehard_count_1s_byt|   0|    256000|     100|0.88477929|  PASSED
 diehard_parking_lot|   0|     12000|     100|0.13938738|  PASSED
    diehard_2dsphere|   2|      8000|     100|0.59083811|  PASSED
    diehard_3dsphere|   3|      4000|     100|0.99737899|   WEAK
     diehard_squeeze|   0|    100000|     100|0.57495619|  PASSED
        diehard_sums|   0|       100|     100|0.17207349|  PASSED
        diehard_runs|   0|    100000|     100|0.44649455|  PASSED
        diehard_runs|   0|    100000|     100|0.85858446|  PASSED
       diehard_craps|   0|    200000|     100|0.96014339|  PASSED
       diehard_craps|   0|    200000|     100|0.88446651|  PASSED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.91446772|  PASSED
 marsaglia_tsang_gcd|   0|  10000000|     100|0.42640252|  PASSED
         sts_monobit|   1|    100000|     100|0.82071819|  PASSED
            sts_runs|   2|    100000|     100|0.62667058|  PASSED
          sts_serial|   1|    100000|     100|0.82151524|  PASSED
```

Kontakt

OTP-Crypt.com

Senden Sie eine E-Mail an unsere interne Mailingliste:

support@otp-crypt.com

Wir beantworten Anfragen in:

- Deutsch
- Englisch
- Französisch
- Spanisch

Anfragen, die nicht auf Deutsch eingehen, werden länger dauern. Unvollkommenes Deutsch ist willkommen. 🙂