freeware

OTP-Crypt.com

- die perfekte Verschlüsselung -

OTP-Crypt.com

Verfügbar für Windows© und Linux©

… das beste Verfahren zum Aufbewahren und Teilen von Geheimnissen …

Wie sicher ist OTP-Crypt

OTP-Crypt.com

- Wie sicher ist OTP-Crypt?

- OTP = One-Time-Pad ist ein Verschlüsselungsverfahren das nachweislich nicht gebrochen werden kann.
- Es gilt als das sicherste (perfekte) Verschlüsselungsverfahren – weltweit.

- Das OTP besteht aus Zufallszahlen, die mit Ihren Dokumenten oder Dateien verschlüsselt werden. Das OTP ist Ihr persönlicher Schlüssel. Die OTP-Schlüssel und die Anwendungssoftware erhalten Sie auf diesen Seiten.

Welche Daten können verschlüsselt werden?

OTP-Crypt.com

Es kann jede einzelne Datei für sich verschlüsselt werden. Wenn Sie für jede Datei einen individuellen Schlüssel verwenden, dann entspricht es den Regeln für eine perfekte Verschlüsselung. Diese Vorgehensweise gilt als unknackbar.

In der Computerpraxis werden mit speziellen Programmen ganze Festplatten verschlüsselt. Beim Start muss der Anwender das Passwort angeben. Nun steht die gesamte Festplatte mit den einzelnen Dateien für den Anwender zur Bearbeitung bereit. Hier gibt es also einen Schlüssel für tausende von Dateien. Es ist außerdem sehr unsicher, da der Schlüssel (Passwort) sich auf der Festplatte befindet. Jeder Benutzer, der das Passwort kennt, hat Zugang. Man kann die Sicherheit dieses Systems mit einem Haustürschlüssel vergleichen, der unter der Fußmatte liegt.

Ähnlich unsicher ist eigentlich die gesamte Softwarepalette, die Dateien verschlüsselt und dabei den Schlüssel in diese Datei hinterlegt.

Welche Daten können verschlüsselt werden?

OTP-Crypt.com

Für jedes dieser Softwareprogramme gibt es entsprechende Software um an den internen Schlüssel zu gelangen.

Für Ihre Datensicherung ist es unpraktisch, tausende von Schlüsseln einzusetzen. Natürlich wäre dabei die Verwaltung des riesigen Schlüsselkastens eine sehr umfangreiche und fast nicht zu lösende Aufgabe. Auch ist die Sicherheit verloren, wenn andere Personen in den Besitz des Schlüsselkastens gelangen. Diese Szenarien lassen sich beliebig erweitern ...

Verschlüsseln Sie ganze Ordner, indem Sie diese Ordner vorher mit entsprechender Pack-Software (Winzip, RAR, usw.) zusammenfassen und anschließend diese eine gepackte Datei mit OTP-Crypt und ihrem eigenen individuellen Schlüssel verschlüsseln.

Bedenken Sie, dass der Schlüssel immer größer sein muss als die zu verschlüsselnde Datei. OTP-Crypt lässt außerdem keine kleineren Schlüssel in der Bedienung der Software zu.

Welche Versionen von OTP-Crypt gibt es?

OTP-Crypt.com

Die Software ist für Windows© und Linux© erhältlich. Die Versionen gibt es nur für 64bit. Für jedes Betriebssystem gibt es eine Version mit graphischer Oberfläche. Die graphische Version ist jeweils die Hauptversion. Mit ihr können in gewohnter Umgebung sowohl Dateien verschlüsselt, als auch wieder entschlüsselt werden.

Zusätzlich gibt es je 2 Versionen für den Konsolen- bzw. Terminalmodus. Diese Versionen eignen sich für die Automation der Ver- und Entschlüsselung von Datenbeständen und ist eher für versierte Benutzer in beruflicher Umgebung gedacht.

Welche Versionen von Schlüsseln gibt es?

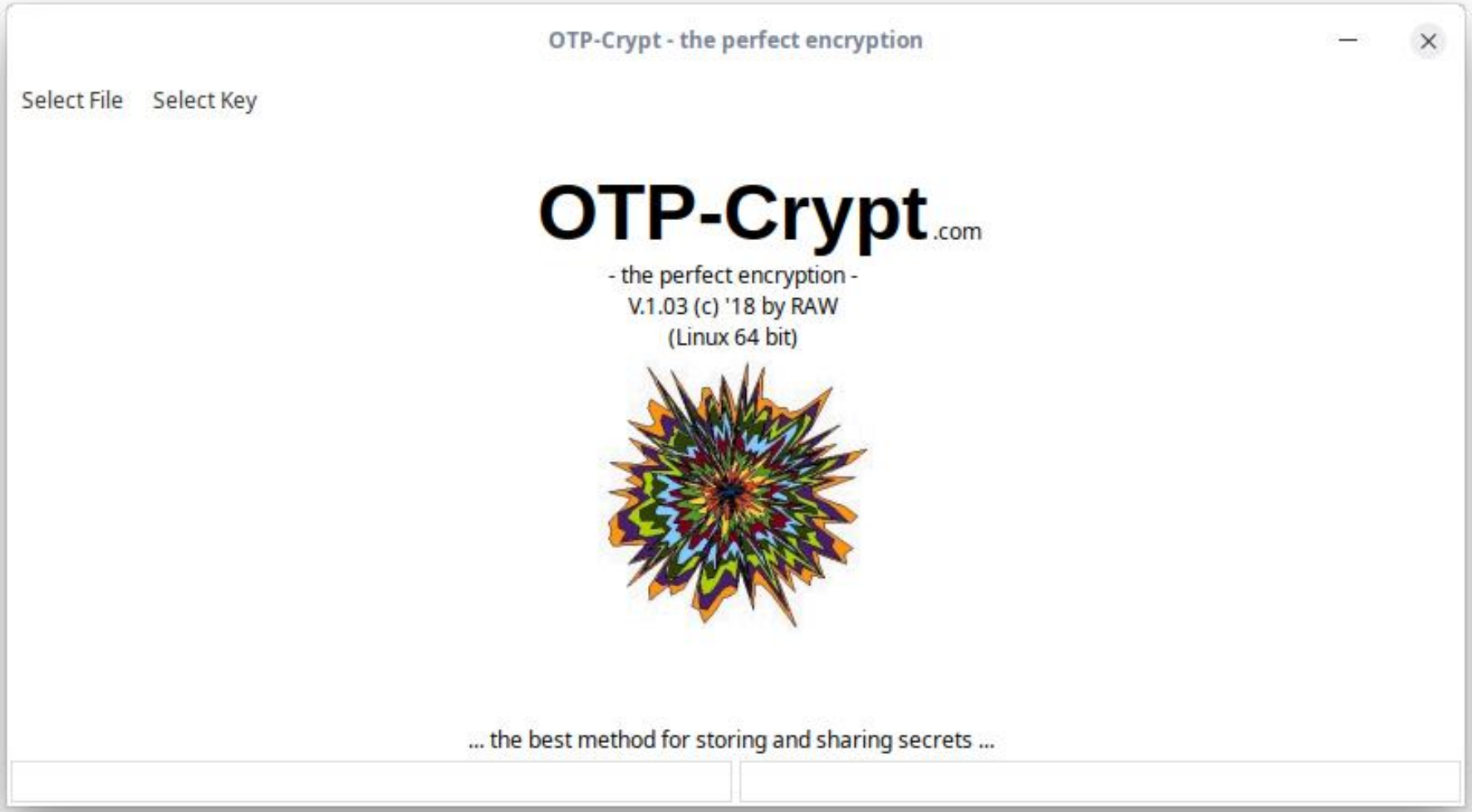
OTP-Crypt.com

Alle Schlüssel, die auf diesen Seiten zum Download bereitgestellt werden, sind Dateien mit absolut zufälligen Inhalten. Diese Schlüsseldateien sind ausschließlich durch unsere Hardware-Generatoren erzeugt worden. Die Sicherheit ist allerdings verfallen, da diese Schlüssel öffentlich downloadbar sind.

Wenn Sie individuelle Schlüssel benötigen, so setzen Sie sich bitte mit uns in Verbindung.

Jeder Schlüssel ist individuell hergestellt und besitzt im Dateinamen seine eigene CRC32-Prüfsumme. Er lässt sich damit einfach von anderen Schlüsseln unterscheiden. Ein typischer Dateiname könnte ‚key_0ef7ee65.otpkey' lauten. Die Endung ‚.otpkey' ist als Kennung notwendig. Die CRC32-Prüfsumme findet sich aus Sicherheitsgründen nicht in den Dateinamen der verschlüsselten Datei wieder.

Die graphische Oberfläche



OTP-Crypt.com

Die Varianten für Windows© und Linux© sind gleich aufgebaut.

OTP-Crypt.com

1. Wählen Sie eine Datei ‚Select File‘ aus. Nach dem Klick müssen Sie zuerst ‚ENCRYPT‘ oder ‚DECRYPT‘ auswählen. Das Menu wird entsprechend angehakt. Durchsuchen Sie ihren Datenbestand und wählen die Datei aus. Unten in der linken Fußzeile wird die Auswahl angezeigt.
2. Wählen Sie im Menü ‚Select Key‘. Wählen Sie im Normalfall ‚… your private key‘ oder ‚… other key‘, wenn Sie einen Fremdschlüssel zum Ver- oder Entschlüsseln einsetzen möchten (dient zum Datenaustausch mit anderen Personen). Unten rechts in der Fußzeile wird die Auswahl angezeigt.
3. Entscheiden Sie bei der Sicherheitsabfrage zwischen Ja und Nein, ob eine Verschlüsselung stattfinden soll oder nicht.
4. Bei ‚Ja‘ können Sie OTP-Crypt beenden. Die verschlüsselte Originaldatei wird im Konsolen- bzw. Terminalmodusicht nicht gelöscht und bleibt Ihnen erhalten. Die neue verschlüsselte Datei bekommt mit ‚.otpcrypt‘ eine zusätzliche Endung.

Die Varianten für Windows© und Linux© sind gleich aufgebaut.

OTP-Crypt.com

5. Verfahren Sie zur Entschlüsselung von Dateien in ähnlicher Weise.
6. Wird eine verschlüsselte Datei entschlüsselt, so wird ohne Nachfrage die originale Datei überschrieben. Sie erhalten so den originalen Zustand der Datei ohne Nachfrage zurück.

Die Bedienung der Software ist für den Anwender so einfach wie möglich gehalten.

Der Konsolen- bzw. Terminalmodus

OTP-Crypt.com

Es gibt jeweils ein Programm für die Verschlüsselung (otp-encrypt) und ein Programm für die Entschlüsselung (otp-decrypt). Sie entscheiden sich bei Aufruf des Programms für den jeweiligen Zweck.

Wir hätten auch nur ein einziges Programm entwickeln können, welche die Ver- und Entschlüsselung enthält. Dazu hätten Sie einen zusätzlichen Parameter beim Aufruf mit abgeben müssen. Nach kurzer Zeit hätten Sie aber die Reihenfolge der 3 Aufrufe verwechselt. Diese Variante erschien uns zu fehlerbehaftet. Sie brauchen in diesen 2 Varianten nur jeweils 2 Parameter angeben. Der erste Parameter ist die Datei, die Sie ver- oder entschlüsseln wollen. Der zweite Parameter ist die Angabe des Schlüssels. Beide Parameter sind natürlich mit den Pfadangabe zu versehen.

Die Bedienung der Software ist wie in der graphischen Version, so einfach wie möglich gehalten. Das bedeutet aber nicht, dass die Software keine Intelligenz besitzt.

Der Konsolen- bzw. Terminalmodus

OTP-Crypt.com

Gewisse Vorkehrungen, wie eine Verriegelung, erhöhen auch hier den Bedienkomfort:

Encrypt:

- Keine Dateien mit Inhalt (otp,key) im Namen erlaubt
- Zu verschlüsselnde Dateien erhalten keinen neuen Namen
- Zu verschlüsselnde Dateien erhalten die Endung: Name.otp-crypted
- Nur 2 Namen im Aufruf notwendig: Name.irgendwas mit private.otpkey
- Beispiel: Aus Name.irgendwas wird Name.irgendwas.otp-crypted

Decrypt:

- Nur der Type Name.irgendwas.otp-crypted mit private.otpkey ist zulässig
- Beispiel: Aus Name.irgendwas.otp-crypted wird automatisch: Name.irgendwas

Was noch von Interesse ist

OTP-Crypt.com

Das Ver- und Entschlüsseln von Dateien findet aus Gründen der Performance im Arbeitsspeicher statt. In heutiger Zeit steht hinreichend Speicherplatz zur Verfügung.

Achten Sie daher bei älteren Computern auf ausreichend Speicherplatz.

Die Bedienung im Konsolen- bzw. Terminalmodus gestaltet sich schwieriger als die Bedienung der Software in der graphischen Oberfläche. Gelegentlich werden Bedienfehler durch den Nutzer verursacht.

Die Fehlerausgabe wird nach Prüfung mit einem Error-40 quittiert.

Error-40 bedeutet, dass sich der Fehler 40 cm vor dem Monitor befindet. 🙂

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):

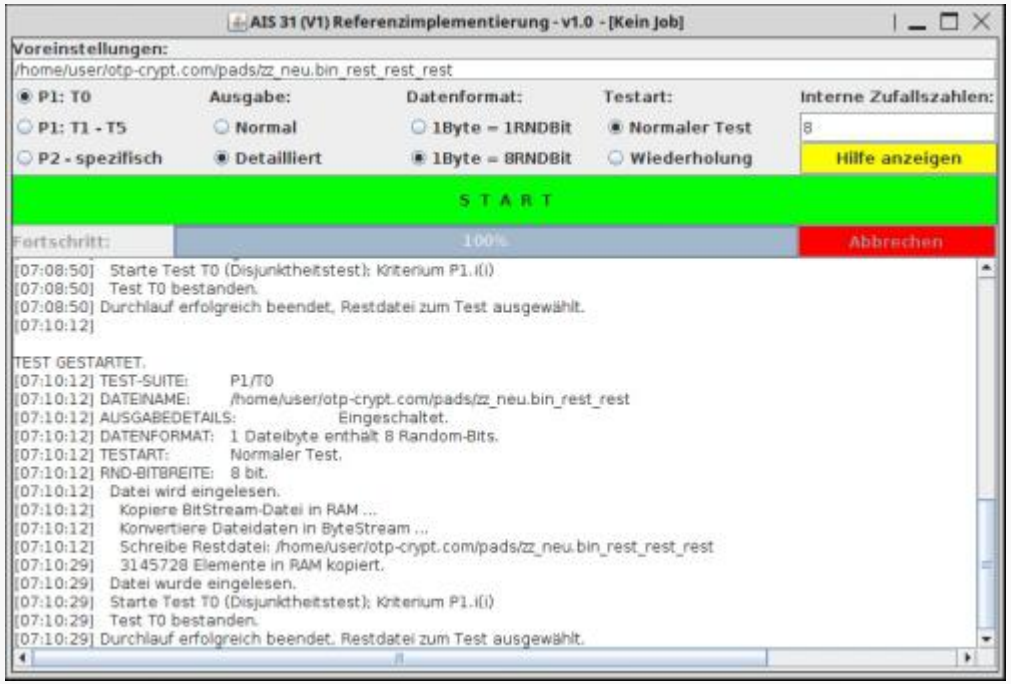
Bundesamt für Sicherheit in der Informationstechnik (BSI)

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:

OTP-Crypt.com

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
```

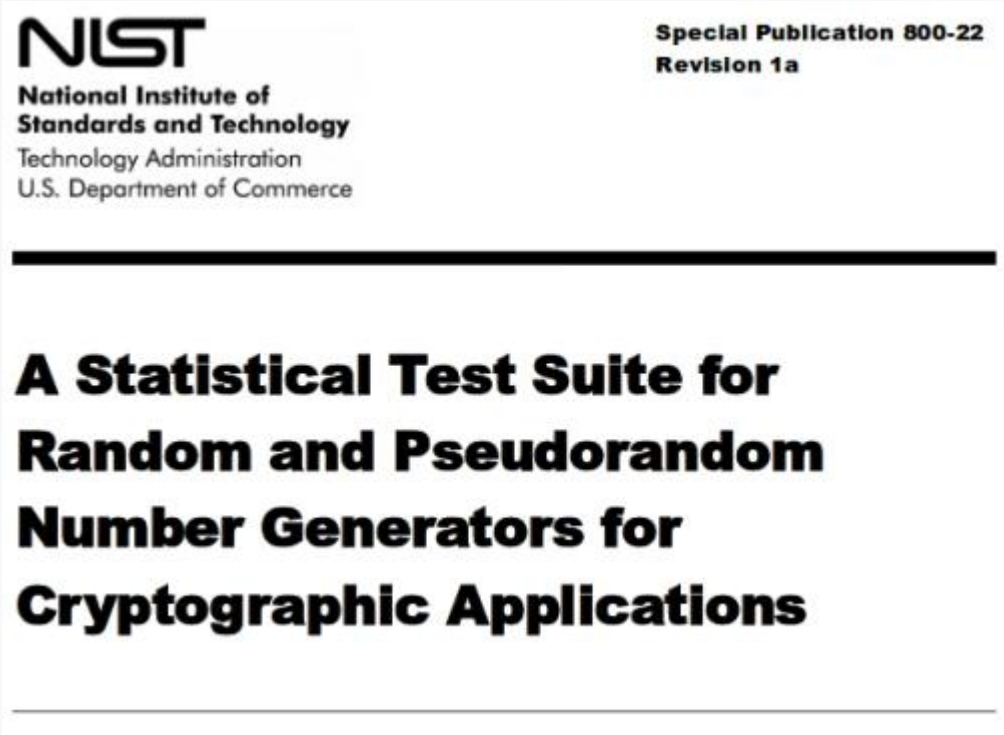
Alle Tests (Monobit, Poker, Runs, Long run, Continuous run) nach FIPS 140-2 wurden bestanden.

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
```

Zufallszahlen für OTP’s

OTP-Crypt.com

Wir versuchen hier mit kurzen Worten, das Thema Zufallszahlen in einfacher Weise darzustellen.

Sie haben sich, liebe Leser, bis jetzt wahrscheinlich nur im Bereich der Spiele damit auseinandergesetzt.

Erlesen Sie sich hier etwas Fachwissen. Es geht um kryptographische Sicherheit, daher wird dieses interessante Thema von uns hier näher beschrieben.

Die Unvorhersehbarkeit von Ereignissen nennt man Zufall.

Zufallszahlen für OTP’s

OTP-Crypt.com

Beispiel:

Werden Münzen geworfen, so gibt es nur den Zustand „Kopf“ oder „Zahl“. Dieser Zustand ist vor dem Münzwurf nicht vorhersehbar.

Vor dem Münzwurf können wir versuchen zu erraten, welches Ereignis, „Kopf“ oder „Zahl“, eintritt.

Glauben Sie, dass das Ergebnis rein zufällig und für eine Verschlüsselung von Daten brauchbar ist? Weit gefehlt. Das Ergebnis ist nicht zufällig genug und wird manchmal mathematisch nachbearbeitet. Warum das so ist, das können Sie hier lesen … (s. Run’s)

Zufallszahlen für OTP’s

- Der errechnete Zufall

OTP-Crypt.com

Wenn Sie am Computer Zufallszahlen erhalten, sind diese nicht zufällig entstanden, sondern sie stammen aus einer Berechnung, die im Ergebnis nur sehr zufällig aussieht.

Man spricht daher von Pseudo-Zufallszahlen.

Für hochsichere kryptographische Aufgaben dürfen diese Pseudo-Zufallszahlen niemals verwendet werden. Die Formeln zur Berechnung der Zufallszahlen sind nicht nur den Programmieren bekannt.

Jede Formel braucht einen individuellen Startwert, die sogenannte Saat, um zufälliges Aussehen zu generieren. Jede dieser Pseudo-Zufallszahlen lassen sich wiederholt mit gleichen Startwerten generieren. Die Generatoren (Software) zur Erzeugung von Pseudo-Zufallszahlen werden RNG (Random Number Generator) genannt.

Zufallszahlen für OTP’s

- Chaos und Zufall

OTP-Crypt.com

Wir versuchen in unserer heutigen Gesellschaft alles zu ordnen. Unvorhersehbare Situationen sind nicht erwünscht, schon gar nicht im Computer. Die Computer sind nicht für zufällige Zustände konstruiert worden.

Sollte dieser Zustand jedoch einmal eintreten, so steht in jedem Fall ein „Error“ an.

Alle Vorgänge sollten aus Sicht der Wissenschaft erklärbar sein. Da hat Chaos und Zufall keinen Platz. Die Ausnahmen bilden Untersuchungen von Wettervorhersagen, Verkehrsanalysen, sowie in geringem Umfang die statistische Mathematik, um nur einige zu nennen.

Um eine zufällige Zahlenmenge zu generieren, wird spezielle Hardware in Verbindung mit leistungsstarker Software benötigt. Genau hier setzt unsere Entwicklung an.

Zufallszahlen für OTP’s

- Quantentheorie (Quantenmechanik, Quantenphysik)

OTP-Crypt.com

Unter zu Hilfenahme der Quantentheorie können unerklärliche Phänomene teilweise im Ansatz erklärt werden.

Käufliche Produkte in der alternativen Medizin werden oft mit dem Schlagwort „Quantenphysik“ in Verbindung gebracht. Das dient aber eher dem Absatz der Produkte, als dem tatsächlichen beworbenen Zweck.

Auch Produkte zur Erzeugung von Zufallszahlen werden teilweise mit dem Schlagwort beworben. Die generierten Zufallszahlen sind eher nicht nach der Quantentheorie entstanden.

In der ursprünglichen Verwendung ging es in der Quantenphysik nicht um zufällig ablaufende Prozesse, sondern um die abweichenden Messungen zu den damals üblichen Berechnungsmethoden. Die Phänomene in der Quantenphysik stehen im Widerspruch zu den uns bekannten und beobachtbaren Vorgängen.

Zufallszahlen für OTP’s

- Quantentheorie (Quantenmechanik, Quantenphysik)

Der Ort und die Geschwindigkeit eines Teilchens können nicht gleichzeitig und schon gar nicht beliebig genau gemessen werden. Je kleiner das Messobjekt wird, desto größer wird die Verfälschung durch das Messgerät selber. Das Messgerät hat physikalische Grenzen bzgl. der Genauigkeit und Auflösung.

In unserem Fall bewegt sich diese „Unschärfe“ vor allem im mikroskopischen Bereich.

Im optischen Bereich wird mit einzelnen Photonen gearbeitet. Hier wird nicht der Ort und die Geschwindigkeit gemessen, sondern es werden halbdurchlässige Spiegel bzgl. der Polarisation der Photonen benutzt. Die horizontale oder vertikale Polarisation entspricht je einem Grundzustand (Null oder Eins).

Die Chance der Aufteilung liegt bei 50%. Welches Photon gemessen wird, kann definitiv nicht vorhergesagt werden.

Zufallszahlen für OTP’s

- Quantentheorie (Quantenmechanik, Quantenphysik)

OTP-Crypt.com

Beim Zerfall radioaktiver Produkte kann über den Zerfallszeitpunkt keine konkrete Aussage gemacht werden. Hier wird auch von einer Unschärfe gesprochen. Trotz Kenntnis der sogenannten Halbwertzeit, ist es unmöglich vorherzusagen, welches Atom das sein wird. Der radioaktive Zerfall bleibt in gewisser Weise dem Zufall überlassen.

Bisher kennen wir 2 logische Zustände, nämlich Null oder Eins. Es gibt in der Quanteninformationstheorie noch einen dritten Zustand, das QBit (Quanten Bit).

Nehmen wir an, es gäbe 2 Spalten, durch das ein Photon hindurch gehen kann. Nehmen wir weiter an, es geht durch die linke Spalte. Dann gilt der Zustand logisch 0. Geht es durch die rechte Spalte, so gilt der Zustand 1. Wenn aber das Photon durch beide Spalten (Überlagerung) gleichzeitig geht, so spricht man von einem dritten Zustand. Wenn eine Informationseinheit alle 3 Zustände annehmen kann, so spricht man an Anlehnung an die herkömmliche Definition von einem QBit (Quanten Bit).

Zufallszahlen für OTP’s

- Quantentheorie (Quantenmechanik, Quantenphysik)

OTP-Crypt.com

Es wird seit einiger Zeit versucht, arbeitsfähige Computer zu bauen, die mit den 3 Zuständen rechnen können. Diese Computer werden Quantencomputer(Quanten Bit) genannt.

Die einfachste Aufgabe ist für einen Quantencomputer das Erzeugen von Zufallszahlen. Alle möglichen Zahlen würden in ein Quantenregister geladen werden. Hinterher wird es wieder ausgelesen. Auf Quantencomputer gibt es einen speziellen Befehl, der alle QBits in den Zustand beider Grundzustände versetzt, also in die Überlagerung. Alle Rechenoperationen mit den Quantenregistern müssen mit ihren Eigenschaften erhalten bleiben. Alle im Quantenregister gespeicherten Zahlenwerte werden erhalten, indem extrem schnell parallele Rechnungen durchgeführt werden. Hierbei entsteht keine Unordnung und es geht keine Information verloren.

In der Quantenkryptographie liegt die Hoffnung auf extrem schnelle Computer, die eventuell das unknackbare OTP-Verfahren gefährden können.

Zufallszahlen für OTP’s

- Quantentheorie (Quantenmechanik, Quantenphysik)

Das ist aber unmöglich, da die Rechengeschwindigkeit keinen Einfluss auf das Ergebnis hat.

Man bekommt nur sehr schnell nichts heraus.

Die quantenphysikalische Schlüsselübertragung für das OTP-Verfahren wird hier nicht näher beschrieben. Es wird für die Kommunikation zwischen 2 Orten eingesetzt. Dazu ist spezielle Hardware notwendig. Im Internet sind jedoch mehr als 2 Orte miteinander verbunden.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

Die hardwarebasierten Zufallsgeneratoren werden auch TRNG (True Random Number Generator) genannt.

Grundsätzlich muss immer als Quelle der Zufallszahlen ein Rauschen vorliegen, dass messtechnisch erfasst werden kann.

Die physikalischen Rauschquellen unterscheiden sich nach ihrer Art.

Die Anforderungen an ein ideales Rauschen sind sehr hoch angesetzt.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Analoge Zufallsgeneratoren

OTP-Crypt.com

Analoges Rauschen ist z.B. in der Audiotechnik zu finden. Jeder kennt diesen Zustand, wenn ein Radiosender nicht richtig eingestellt ist. Es gibt für diese Art von Rauschen spezielle Auswertungen, die sich auf Wetterphänomene (Blitze bei Gewittern) stützen sollen. Auch der Grenzbereich sehr laut eingestellter Verstärker, erzeugt ein störendes Rauschen.

Rauschsignale in der

Audiotechnik werden zum Ausmessen von Räumen

Hochfrequenztechnik werden für die Eigenschaften in der Satellitentechnik

verwendet.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Analoge Zufallsgeneratoren

OTP-Crypt.com

Es ist u.a. auch ein analoges Rauschen vorhanden, wenn bestimmte elektronisches Bauteile (Z-Diode) mit einer zu hohen Spannung angesteuert werden. Diese Rauschspannung ist sehr gering und muss mit nachgeschalteten Verstärkern aufbereitet werden. Das erzeugte Rauschen ist ein weißes Rauschen aufgrund der thermischen Unruhe der Materie.

Die Rauschsignale werden, in Anlehnung an das Licht, in verschiedene Farbspektren unterteilt. Kurze Wellenlängen werden mit „Blauen Rauschen“, große Wellenlängen hingegen mit „Roten Rauschen“ bezeichnet.

Sichtbares Licht wird mit „Weißem Rauschen“ bezeichnet und enthält alle Wellenlängen. Hier können zufällige Zustände erwartet werden. Es eignet sich als einziges Signal für die Generierung von Zufallszahlen. Wenn das „weiße Rauschen“ einen erhöhten Frequenzanteil enthält, spricht man von „Rosa Rauschen“.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Digitale Zufallsgeneratoren

OTP-Crypt.com

Digitales Rauschen ist nicht zu verwechseln mit digitalen Zufallsgeneratoren. Wenn die Rauschquelle ein analoger Zufallsgenerator war, kann eine digitale Auswertestufe nachgeschaltet werden.

Diese liefert Nullen und Einsen aufgrund analoger Gegebenheiten und gilt als echter Zufallsgenerator.

Digitale Zufallsgeneratoren gehören zu den Pseudo-Zufallsgeneratoren. Es handelt sich um sehr einfach konstruierte Generatoren. Sie arbeiten mit digitalen Schieberegistern. Durch Rückkopplung der Schieberegister kommt es zur entscheidenden Qualität der Zufallszahlen. Die Ausgangsdaten können in gleicher Weise wiederholt werden.

Als Beispiel wird ein elektronischer Würfel genannt.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Quanten Zufallsgeneratoren

OTP-Crypt.com

Die Entscheidung, ob eine Null oder eine Eins vorliegt, ist hier nicht an thermischen Effekten gebunden.

Die quantenmechanische Entscheidung eines Photons, dass eine Ja / Nein Entscheidung am halbdurchlässigen Spiegel trifft, kann direkt Digital nachverarbeitet werden.

Derartige Rauschgeneratoren werden am Markt angeboten.

Die Schlüsseltechnologie sind Einphotonen-Quellen und Einphotonen-Detektoren.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Urknall Zufallsgeneratoren

OTP-Crypt.com

Das Hintergrundrauschen des Weltalls wurde durch den Urknall verursacht.

Auf den ersten Blick scheint genau dieser Vorgang der optimale Zustand zu sein, um ideale Zufallszahlen zu erhalten.

Leider ist das nicht der Fall. Das Rauschen der Hintergrundstrahlung im Weltall ist mit starken Störsignalen durchsetzt. Die Störsignale werden z.B. durch Pulsare hervorgerufen. Der Andromeda-Nebel hat z.B. eine stark ausgeprägte frequenztechnische Signatur. Daher wird das Frequenzspektrum des Andromeda-Nebels durch passende mathematische Filter herausgerechnet.

Qualitativ ist es ein vernichtendes Urteil …

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Radioaktive Zufallsgeneratoren

OTP-Crypt.com

Ein instabiler Atomkern ist mit einem Überschuss an Neutronen versehen.

Seine stabilen Isotopen sind in geringerer Anzahl vorhanden.

Der radioaktive Zerfall beruht auf dem quantenphysikalischen Effekt und lässt sich zur Erzeugung von Zufallszahlen nutzen.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Störungen und Einflüsse

OTP-Crypt.com

- Die Erzeugung von Zufallszahlen muss zweifelsfrei zufällig sein. Externe Einflüsse auf Zufallsgeneratoren beeinträchtigen das System soweit, dass es nicht mehr als chaotisches System angesehen werden kann.

- Bei elektronischen Bauteilen ist der größte externe Einfluss thermischer Natur. Die Raumtemperatur hat ebenfalls Einfluss auf die Betriebstemperatur von elektronischen Bauteilen und sollte entsprechend stabil geregelt bzw. gehalten werden. Auch die Betriebsspannung muss sehr stabil (Drift) vorhanden sein.

- Einen großen Einfluss besitzen elektromagnetische Störungen, hervorgerufen durch Rundfunk, bzw. Mobilfunk. Auch ein einfacher Lichtschalter steuert über die Netzspannung definierte Signale ein. Ganz wichtig ist die Schaltung an sich, da sich hier das Eigenrauschen, sowie elektromagnetische Störungen der verwendeten Bauteile verheerend auswirken.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Störungen und Einflüsse

OTP-Crypt.com

- Der radioaktive Zerfall läuft weitgehend unabhängig von der Temperatur ab. Allerdings hat der Luftdruck starken Einfluss bei der Detektion der Teilchen. Ein geringerer Luftdruck bedeutet gleichzeitig eine Erhöhung der detektierten Zerfälle, ein höherer Luftdruck steht der Detektion als Widerstand entgegen. Außerdem ist die Anzahl der Teilchen sehr gering. Bedingt durch die Halbwertzeit, ist nur eine geringe Ausbeute an Zufallszahlen möglich.

- Das Hintergrundrauschen des Weltalls erzeugt eigene Störungen. Es ist wohl mehr ein knattern als ein Rauschen…

- Blitze bei Gewittern besitzen ein ähnliches Signaturmuster wie Störungen beim Einschalten elektrischer Verbraucher.

Die Qualität der erzeugten Zufallszahlen hängt sehr stark von der Art des Rauschens ab.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Störungen und Einflüsse

OTP-Crypt.com

Beispiel:

Vergleichen sie die Erzeugung von Zufallszahlen mit einem breit gehaltenen Wasserstahl. Der Wasserstrahl fällt in der Wasserabgabe sehr grob aus.

Sie können den Wasserstrahl mit verschiedenen technischen Konstruktionen immer feiner zerstäuben.

Irgendwann entsteht feinster Nebel.

Im Prinzip ähnlich sind unsere hardwarebasierten Zufallsgeneratoren zu verstehen.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Fazit

OTP-Crypt.com

Als störsicher kommt nur der quantenoptische Zufallsgenerator in Betracht.

Temperatur und Luftdruck sollen bei den Ausgangsdaten einen Störanteil von unter 1 Prozent ergeben. Die klassischen Einflüsse sollen bei diesem Wert zu vernachlässigen sein.

Das wird an dieser Stelle bestritten! Ein Störanteil von 1 Prozent kann bei qualitativ hochwertigen Zufallszahlen nicht akzeptiert werden.

Das Problem betrifft in erster Linie die Gleichverteilung von Nullen und Einsen, hervorgerufen durch Unterschiede in der Ausrichtung und Montage der halbdurchlässigen Spiegel, sowie Toleranzen in der Herstellung.

Zufallszahlen für OTP’s

- Hardware Zufallsgeneratoren

- Fazit

OTP-Crypt.com

In der alternativen Medizin gelten Einflüsse des Bewusstseins als gemessene Störgröße. Verschiedene Untersuchungen sollen die Ergebnisse bestätigt haben. Auch die geographische Ausrichtung (Nord-Süd, West-Ost) der Zufallsgeneratoren in der Nähe von Atomkraftwerken soll einen Einfluss auf statistischer Basis zeigen. Ebenfalls können Sonnenaufgänge in gewisser Weise das zufällige Auftreten der Zahlen stören.

Diese Untersuchungen liegen leider bis zu 40 Jahre zurück. Modernste Elektronik aus heutiger Zeit (autarke Datenlogger) würden die Ergebnisse bestätigen oder verwerfen.

In allen vorgenannten Fällen werden immer bestimmte Muster in die Zufallszahlen eingespeist.

Zufallszahlen für OTP’s

- Pflicht zur Nachbearbeitung der Rohdaten

OTP-Crypt.com

Es liegt in der Natur der Sache, das alle hardwarebasierten Zufallsgeneratoren keinen idealen Bitstrom aus Nullen und Einsen liefern. Auch der zu Anfang besprochene Münzwurf liefert keinen idealen Bitstrom. Verschiedene statistische Auswertungen decken für den Bitstrom die Unzulänglichkeiten auf. Die Anforderungen an den Bitstrom sind sehr hoch. Hier muss mit speziellen Filtern nachbearbeitet werden, damit der Bitstrom zufälliger ausfällt.

Als Beispiel soll folgende Bitfolge dienen. Nehmen wir die Bits mit den Werten „110000000010“. Sie erkennen hier mehrere Bits hintereinander mit dem Wert „0“. Diese Werte sind zwar zufällig entstanden (Münzwurf), aber für die Verschlüsselung von Daten sind viele gleiche hintereinander auftretende Bits unbrauchbar.

Gleiche hintereinander folgende Bits (Nullen oder Einsen) nennt man „Run“. Sie liegen zwangsläufig zwischen 2 Bitwechsel.

Zufallszahlen für OTP’s

- Pflicht zur Nachbearbeitung der Rohdaten

OTP-Crypt.com

Ein sehr einfacher aber wirksamer Filter besteht aus abwechselnden Nullen und Einsen, also „010101010101“. Man spricht hier von einer Bitinvertierung. Die Ausgangsbitfolge wird mathematisch mit dem Filter xor’ed. Der Taschenrechner kann in der HEX-Darstellung die Berechnung durchführen. Als Ergebnis wird „100101010111“ ausgegeben. Das sieht wesentlich zufälliger aus.

Ein weiterer Filter teilt den Bitstrom in Gruppen zu je 2 Bits. Die Definition besagt, das die Bitmuster „00“ und „11“, also diejenigen 2er Bits die keine Änderung enthalten, gelöscht werden. Aus den restlichen 2er Bits, also „01“ und „10“, werden entsprechend die Ausgangsbits abgeleitet. Aus „01“ wird „0“, aus „10“ wird „1“.

Die Nachbearbeitung der Rohdaten wandelt den originalen Bitstrom um!

Dabei ist mit einer erheblichen Reduzierung der Datenmenge zu rechnen. Die Größe des originalen Bitstrom verringert sich auf realistische 3 bis 4 Prozent.

Das ist eine sehr geringe Ausbeute der Datenmenge.

Zufallszahlen für OTP’s

- Statistik und Analyse

OTP-Crypt.com

Um eine Aussage über die Qualität von Zufallszahlen zu erhalten, werden statistische Tests herangezogen.

Die Qualitätskriterien von Zufallszahlen werden manchmal über eine Ja / Nein Aussage getroffen. Daher wurde vor einigen Jahren die FIPS-140 Prüfung verwendet. Diese engen statistischen Kriterien erlauben eine Aussage über die Zufälligkeit eines Bitstrom.

Ein hardwarebasierter Zufallsgenerator kann diese engen statistischen Kriterien nicht erfüllen. Der Bitstrom muss immer mit Filtern nachbearbeitet werden. (Pseudo-Zufallsgeneratoren bestehen den FIPS-140 Test ohne Probleme und ohne Nachbearbeitung)

Um den Minimalanforderungen an einen zufälligen hardwarebasierten Bitstrom gerecht zu werden, muss der Bitstrom die FIPS-140 Prüfung, wenn auch durch Nachbearbeitung, bestehen.

Zufallszahlen für OTP’s

- Statistik und Analyse

OTP-Crypt.com

Eine statistische Analyse geht weit über die bekannten Berechnungen, wie Mittelwertbildung, Effektivwert oder Standardabweichung, hinaus.

Die Fast Fourier Transformation FFT zeigte in der Vergangenheit nicht die zu erwartende Aussagekraft. Die FFT wird nur noch bedingt eingesetzt.

Es soll Hersteller von hardwarebasierten Zufallsgeneratoren geben, die einen hybriden Bitstrom erzeugen. Der erzeugte Bitstrom der Hardware wird mit einem erzeugtem Bitstrom von Pseudo-Zufallszahlen verschmolzen.

Diese Produkte sind unserer Meinung nach nicht sehr vertrauenswürdig. Sie liefern keine natürliche Zufälligkeit von Daten.

Zufallszahlen für OTP’s

- Statistik und Analyse

- Einfüsse

OTP-Crypt.com

Außerdem besteht die Möglichkeit, den Bitstrom der Zufallszahlen mit einer Fremdinformation zu codieren.

Auch diese Produkte sind unserer Meinung nach nicht sehr vertrauenswürdig.

An dieser Stelle beenden wir den Einblick in die statistischen Möglichkeiten zur Qualitätskontrolle von Zufallszahlen.

Möchten Sie tiefer in das Thema einsteigen, dann folgen sie bitte den unten aufgeführten links.

Zufallszahlen für OTP’s

- Statistik und Analyse

- Externe Links

OTP-Crypt.com

- NIST (National Institute of Standards and Technology)
  (https://csrc.nist.gov/Projects/Random-Bit-Generation)
- DieHarder
  (http://webhome.phy.duke.edu/~rgb/General/dieharder.php)
- ENT
  (http://www.fourmilab.ch/hotbits/)

Zufallszahlen für OTP’s

- Geringe Ausbeute an Zufallszahlen

OTP-Crypt.com

Um 1990 war die Entwicklung von Hard- und Software zur Erzeugung von elektronisch generierten Zufallszahlen recht aktiv.

Die Verschlüsselung von Texten, Textdokumenten und kurzen Nachrichten war mit ein paar Zufallszahlen ideal zu bewerkstelligen.

Alle Daten passten bequem auf eine Diskette (Floppy Disk) mit einem Speicherplatz um 1 MB.

Die Geschwindigkeit der Datenübertragung zwischen dem hardware Zufallsgenerator und dem Computer betrug mittels der seriellen Schnittstelle um die 4 KByte/s (38400 Baud).

Zufallszahlen für OTP’s

- Geringe Ausbeute an Zufallszahlen

OTP-Crypt.com

Wir rechnen an dieser Stelle mal aus, wie lange es mit der herkömmlichen Methode dauern würde, um eine DVD mit Zufallszahlen zu befüllen.

Beispielrechnung:

Für 1 MB Speicherplatz mit 4 KByte/s benötigen wir (1000 KB / 4 KB) = 250 Sekunden / MB.

Für 1 GB rechnen wir (1000 MB mal 250 s / MB) = 250.000 Sekunden. Das entspricht ca. 4167 Minuten.

Nun ist es an der Zeit, den mittleren Nettogewinn nach der Filterung auf ca. 4 Prozent festzulegen. 25 mal 4 Prozent ergibt 100 Prozent. 25 mal 4167 Minuten ergibt 104175 Minuten. In Stunden gerechnet erhalten wir 1736 Stunden. Ein Arbeitstag wird mit 8 Stunden gerechnet.

Zufallszahlen für OTP’s

- Geringe Ausbeute an Zufallszahlen

OTP-Crypt.com

Ein Monat liegt bei einer 5-Tage Woche bei ca. 21,7 Arbeitstagen. Wir rechnen 21,7 Arbeitstage mal 8 Stunden. Das ergibt 173,6 Stunden. Also entsprechen exakt 1736 Stunden Arbeitszeit geteilt durch 173,6 Stunden = 10 Monate.

Eine einseitige DVD hat eine Speicherkapazität von ca. 4,7x GB. Wir haben bisher nur mit 1 GB gerechnet. Wir müssen die 10 Monate noch mit 4,7 multiplizieren. Das ergibt dann im Ergebnis ca. 47 Monate.

Ergebnis:

Es wird ungefähr 4 Jahre dauern, um eine DVD mit Zufallszahlen zu befüllen!

Zufallszahlen für OTP’s

- Geringe Ausbeute an Zufallszahlen

OTP-Crypt.com

Ein Monat liegt bei einer 5-Tage Woche bei ca. 21,7 Arbeitstagen. Wir rechnen 21,7 Arbeitstage mal 8 Stunden. Das ergibt 173,6 Stunden. Also entsprechen exakt 1736 Stunden Arbeitszeit geteilt durch 173,6 Stunden = 10 Monate.

Eine einseitige DVD hat eine Speicherkapazität von ca. 4,7x GB. Wir haben bisher nur mit 1 GB gerechnet. Wir müssen die 10 Monate noch mit 4,7 multiplizieren. Das ergibt dann im Ergebnis ca. 47 Monate.

Ergebnis:

Es wird ungefähr 4 Jahre dauern, um eine DVD mit Zufallszahlen zu befüllen!

Zufallszahlen für OTP’s

- Geringe Ausbeute an Zufallszahlen

OTP-Crypt.com

Die Ausbeute an Zufallszahlen konnte bis in die heutige Zeit hinein nicht wesentlich gesteigert worden.

Glauben sie uns, wenn wir sagen, dass es an technischen Problemen liegt, die hier einer Weiterentwicklung entgegen stehen.

Die Ausbeute an Zufallszahlen ist zu gering, um in heutiger Zeit große Datenbestände zu verschlüsseln.

Daher finden Sie in der Literatur oft Bildmaterial von Zufallszahlen in Papierform. Auch fehlt nicht der Hinweis, das ein OTP nur einmal verwendet werden darf.

(Die Menge an Zufallszahlen hätte man noch auswendig lernen können).

Zufallszahlen für OTP’s

- Geringe Ausbeute an Zufallszahlen

OTP-Crypt.com

Alle Beiträge die sie im Internet bzgl. der Kryptographie finden, beziehen sich im Kern nur auf Zufallsmengen, die aus Platzgründen noch auf Papier geschrieben werden konnten.

An Datenmengen, die den Inhalt einer Diskette sprengen, wurde kaum gedacht.

Der Sprung von Megabyte nach Gigabyte hielten viele Autoren für zu utopisch…

Um mit diesen Datenmengen kryptographisch umgehen zu können, haben wir entsprechende Software entwickelt.

Wie die Verschlüsselung funktioniert

- Vorwort

OTP-Crypt.com

Die Verschlüsselung wurde durch den amerikanischen Kryptologen Frank Miller im Jahr 1882 vorgeschlagen. Gilbert Vernam meldete das Verfahren 35 Jahre später zum Patent an. Joseph O. Mauborgne nannte das Verfahren später One Time Pad, oder einfach nur Einmal-Block.

In Deutschland wurde diese Methode 1921 erfolgreich im diplomatischen Dienst der Weimarer Republik umgesetzt. Die gedruckten Blöcke mit den zufällig erstellten Ziffern wurden zur Verschlüsselung, ähnlich einem sehr langen Wurm der nur aus Zahlen besteht, nach einem mathematischen Verfahren verwendet. Dieses Verfahren wurde auch mit Lochstreifen eingesetzt. Dabei kamen Maschinen zu Einsatz, die gleichzeitig mehrere Lochstreifen verarbeiten konnten. Dieser individuelle Wurm wurde in Deutschland auch als i-Wurm bezeichnet. Als Beispiel für den Einsatz dieses Verfahrens ist bis in die heutige Zeit hinein das „Rote Telefon“ zu nennen. Die hochsichere direkte Fernschreibverbindung zwischen dem amerikanischen Präsidenten und dem sowjetischen Generalsekretär wird durch dieses Verfahren geschützt.

Wie die Verschlüsselung funktioniert

- Wichtige Bedingungen

OTP-Crypt.com

Für eine Verschlüsselung von Texten oder Dateien wird kein Password verwendet, sondern es wird der ganze Text oder die ganze Datei mit dem Schlüssel (Zufallszahlen) sozusagen verschmolzen.

Die Erzeugung von qualitativ hochwertigen Zufallszahlen in ausreichender Menge stellt dabei die eigentliche Herausforderung dar. Dieses Problem wurde durch uns gelöst.

Das Ergebnis kann nicht entschlüsselt werden und gilt weltweit als unknackbar.

Es gilt als das beste Verfahren zum Aufbewahren und Teilen von Geheimnissen.

Wie die Verschlüsselung funktioniert

- Wichtige Bedingungen

OTP-Crypt.com

Dabei sind jeweils 2 Punkte einzuhalten:

- Der Schlüssel muss so lang sein wie der zu verschlüsselnde Text oder die zu verschlüsselnde Datei.

- Der Schlüssel darf nur ein einziges Mal verwendet werden.

1. Bei einer Archivierung von geheimen Daten muss der Schlüssel und die verschlüsselte Datei an 2 getrennten Orten aufbewahrt werden.

2. Für eine geheime Kommunikation zwischen 2 Parteien muss der Schlüssel nur solange aufbewahrt werden, bis die versendete Datei wieder entschlüsselt wurde. Danach müssen beide Schlüssel sofort vernichtet werden.

Wie die Verschlüsselung funktioniert

- Vernanverschlüsselung von Hand

OTP-Crypt.com

Die Vernamverschlüsselung ist recht einfach zu verstehen. Es wird nur die Addition oder die Subtraktion verwendet. Die Berechnung wird auf Papier durchgeführt.

Für das Alphabet wird ein Zeichenvorrat (z.B. A-Z, Sonderzeichen, und die Zahlen 0-9) angelegt. Dieser Zeichenvorrat ist z.B. 45 Zeichen lang. Um beim Entschlüsseln Verwechselungen auszuschließen, werden für die 45 Zeichen die Zahlen 5 – 50 gewählt.

Beispiel:

Alphabet: Buchstabe A = Stelle 5, Buchstabe B = Stelle 6 … Buchstabe Z = Stelle 30.
Sonderzeichen ! = Stelle 31, … bis Sonderzeichen Stelle 39.
Die Zahl 0 = Stelle 40 bis Zahl 10 = Stelle 50.

Wie die Verschlüsselung funktioniert

- Vernanverschlüsselung von Hand

OTP-Crypt.com

Nun haben wir unser Alphabet in Zahlen geordnet.

Jetzt fehlt noch der zu verschlüsselnde Text, oder auch Klartext genannt.

Wir verwenden ein Kinderlied aus dem Jahr 1824 mit dem Titel: *Fuchs Du hast die Gans gestohlen*.

Dieses Kinderlied ist wohl jedem Leser bekannt.

Wir verwenden hier als Beispiel nur das letzte Wort – gestohlen…

Wie die Verschlüsselung funktioniert

- Vernanverschlüsselung von Hand

- Verschlüsseln

OTP-Crypt.com

Bringen wir nun den Klartext mit unserem Alphabet in eine Tabelle.

Klartext	g	e	s	t	o	h	l	e	n
Als Zahl	11	9	23	24	19	12	16	9	18

Wir erhalten hintereinander geschrieben die Zahlen: 1192324191216918

Aus traditionellen Gründen und zur besseren Lesbarkeit unterteilen wir diesem Zahlenwurm in Gruppen zu je 5 Zahlen: 11923_24191_ 21691_8....

Für den Schlüssel denken wir uns 45 Zufallszahlen, von der 5. Stelle bis zur 50. Stelle aus.

Wie Sie jetzt merken, ist diese Aufgabe gar nicht so einfach zu lösen. Diesen Schlüssel unterteilen wir in 5er-Gruppen. Er könnte lauten: 12345_67890_09876_54321

Wie die Verschlüsselung funktioniert

- Vernanverschlüsselung von Hand

- Verschlüsseln

OTP-Crypt.com

Nun tragen wir die 5er-Gruppen in eine Tabelle ein.

Als Zahl	11923	24191	21691	8....
Schlüssel	12345	67890	09876	5....

Jetzt werden die untereinander stehenden Ziffernfolgen addiert und zwar nach der Rechenregel Modulo 10.

Die Erklärung sieht in Wikipedia© sehr kompliziert aus, ist aber in der Praxis einfach anzuwenden:

1: Stelle: 1 + 1 = 2

2. Stelle: 1 + 2 = 3

Wie die Verschlüsselung funktioniert

- Vernanverschlüsselung von Hand

- Verschlüsseln

OTP-Crypt.com

3. Stelle: 9 +3 = 12 // Streiche die 1. Stelle, wenn das Ergebnis größer oder gleich 10 ist.

4. Stelle: 2 + 4 = 6

5. Stelle: 3 + 5 = 8

6. Stelle: 2 + 6 = 8

7. Stelle: 4 + 7 = 11 // Streiche die 1. Stelle, wenn das Ergebnis größer oder gleich 10 ist.

… usw.

Wir fassen den Zahlenwurm in 5er-Gruppen zusammen: 23268_81… usw.

Wie die Verschlüsselung funktioniert

- Vernanverschlüsselung von Hand

- Entschlüsseln

OTP-Crypt.com

Der erzeugte Zahlenwurm lautet: 23268_81... usw.

Der Schlüssel lautet: 12345_67... usw.

1. Stelle: 2 -1 = 1

2. Stelle: 3 -2 = 1

3. Stelle: 2 -3 = 9 // Füge die 1. Stelle hinzu, wenn das Ergebnis negativ wird. (12 – 3 = 9)

4. Stelle: 6 – 4 = 2

5. Stelle: 8 – 5 = 3

Wie die Verschlüsselung funktioniert

- Vernanverschlüsselung von Hand

- Entschlüsseln

OTP-Crypt.com

6. Stelle: 8 – 6 = 2

7. Stelle: 1 – 7 = 4 // Füge die 1. Stelle hinzu, wenn das Ergebnis negativ wird. (11 – 7 = 4)

… usw.

Wir erhalten als Ergebnis die aktuelle Stelle im Alphabet: 11_9_23_24, also die Buchstaben G_E_S_T_… usw.

Wie Sie sehen, ist das Ver- und Entschlüsseln von Texten eine umfangreiche Aufgabe.

Die Modulo 10 Addition ist für den Menschen, der das Dezimalsystem benutzt, geeignet. Dateien, bzw. hexadezimale- oder Binärwerte sind nur für den Computer kein Problem.

Wie die Verschlüsselung funktioniert

- Verschlüsselungsverfahren durch den Computer

OTP-Crypt.com

Verschlüsselungsverfahren durch den Computer

Die Verschlüsselung erfolgt beim Computer nicht nach der Modulo 10 Addition.

Es werden direkt die binären Inhalte mittels XOR (Kontravalenz) verknüpft.

Diese Rechenregel beherrschen alle Computer als Grundrechenart.

Das Prinzip ist dasselbe wie bei der Vernamverschlüsselung von Hand.

Diese Rechenoperation wird auch Modulo 2 Addition genannt.

Wie die Verschlüsselung funktioniert

- Kryptoanalyse

OTP-Crypt.com

Wenn ein Schlüssel nur einmal verwendet wird und der Schlüssel genau so lang ist wie der Klartext, dann gibt es keinen Ansatz für einen kryptoanalytischen Angriff. Wenn diese Regeln eingehalten werden, ist eine perfekte Verschlüsselung garantiert.

Diese Aussage, für sich betrachtet, ist richtig. 🙂

Wir wollen Ihnen aber noch ein paar Tipps im Umgang mit dem OTP-Verfahren an die Hand geben.

Wenn der Text oder die Datei den hexadezimalen Wert 0 (Null) beinhaltet, so entspricht das Ergebnis dem originalen Schlüsselinhalt an dieser Position. (z. B.: 0 xor 35 = 35)

Stellen Sie sich eine zu verschlüsselnde Datei mit lauter Nullen als Inhalt vor!

Wie die Verschlüsselung funktioniert

- Kryptoanalyse

- Unsere Empfehlungen

OTP-Crypt.com

Komprimieren sie vorher alle zu verschlüsselnden Texte und Dateien. (.zip, .rar, etc.)

Verschlüsseln Sie niemals eine Datei, die sie von einer fremden Person zur Verschlüsselung bekommen haben.

Diese Person besitzt ja den Klartext und die verschlüsselte Datei. Sie kann den originalen Schlüssel herausrechnen.

Das gilt auch für die Verschlüsselung bekannter Inhalte.

Bekannte Inhalte können pdf-Dateien, Hinweistexte wie Betriebsanleitungen oder auch Header-Dateien von Word-Dokumenten sein. 🙂

Wie die Verschlüsselung funktioniert

- Kryptoanalyse

- Noch eine Eigenart zum Schluss:

OTP-Crypt.com

Wenn eine Datei verschlüsselt wird, so erhält man eine verschlüsselte Datei. Diese Datei ist jedoch nicht von einem anderen Schlüssel zu unterscheiden und kann ebenfalls als Schlüssel weiter gegeben werden.

Dieser neue Schlüssel kann also Klartextinformation (Seriennummer, Adressen, große Texte, etc.) enthalten.

Eine Person die den 1. Schlüssel besitzt, kann den Klartext entschlüsseln. Dieser (neue) 2. Schlüssel ist kompromittiert und nicht als vertrauenswürdig einzustufen.

Schlüssel dürfen nicht mit Fremdinformation gemischt werden und sollten nur aus Rohdaten, ohne Einsatz von Filtern, entstanden sein. 🙂

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. 🙂