freeware

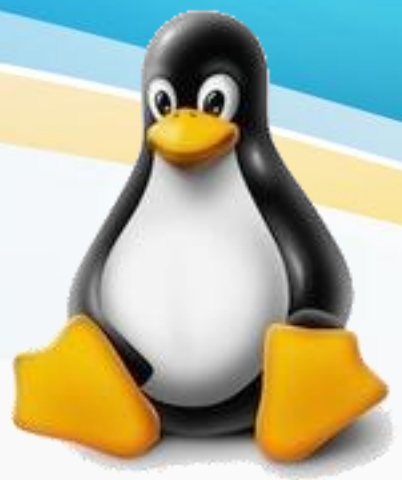
OTP-Crypt.com

- die perfekte Verschlüsselung -

OTP-Crypt.com

#3: Zufallszahlen für OTP's

Verfügbar für Windows© und Linux©



… das beste Verfahren zum Aufbewahren und Teilen von Geheimnissen …

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)

OTP-Crypt.com

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

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.

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. 🙂