freeware

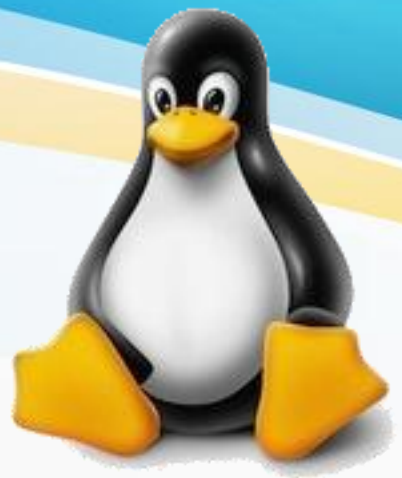
OTP-Crypt.com

- die perfekte Verschlüsselung -

OTP-Crypt.com

#4: Wie die Verschlüsselung funktioniert

Verfügbar für Windows© und Linux©



… das beste Verfahren zum Aufbewahren und Teilen von Geheimnissen …

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. 🙂