Inhalt

1. Wahrscheinlichkeiten
2. Kombinatorik
3. N hoch k

1. Wie sicher ist mein Passwort?
    1. Nur Großbuchstaben
    2. Mit Kleinbuchstaben
    3. Mit Ziffern
    4. Mit Sonderzeichen
2. Meine Tastatur ist kaputt und kennt nur Kleinbuchstaben
    1. Rein in die Tiefen des Rechners
3. Von Sternen und Atomen
    1. Wie viel Tonnen Humus brauchen wir da wohl?
        1. Aus wie vielen Atomen besteht die Erde?
        2. Aus wie vielen Atomen besteht die Sonne?
        3. Wie sieht es denn mit der Milchstraße aus?
    2. Die letzte Bastion hält! Unser Universum

Im Zusammenhang mit Verschlüsselung kommt man immer wieder mit der s.g. **Schlüssellänge** in Kontakt.

> 256-BIT AES, 1024-BIT RSA, 448-BIT Blowfish,...

Viele sind der Ansicht, dass eine größere Schlüssellänge, eine sicherere Verschlüsselung bedeutet.

FALSCH: Man darf Äpfel nicht mit Birnen vergleichen!

Es gibt prinzipiell zwei Hauptarten von Verschlüsselungsverfahren.

1. Symmetrische Verfahren, die sich dadurch auszeichnen, dass zum Ver- und Entschlüsseln der gleiche Schlüssel verwendet wird.
2. Asymmetrische Verfahren, die sich dadurch auszeichnen, dass zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet werden.

Zur Gruppe der symmetrischen Verfahren gehören zum Beispiel die Verfahren **AES** (*Advanced Encryption Standard*), **Blowfish**, **Twofish** und **Serpent**.

Asymmetrische Verfahren wären zum Beispiel **RSA** und **Elgamal**.

Die beiden Varianten sind unsere Äpfel und Birnen. Sie basieren auf komplett unterschiedlichen mathematischen Verfahren.

Für RSA gibt es folgende Abschätzungen:

- RSA in seiner 1024 BIT Version entspricht in etwa einem 80 BIT symmetrischen Verfahren
- RSA in seiner 2048 BIT Version entspricht in etwa einem 112 BIT symmetrischen Verfahren
- Laut NIST entspräche eine 15360-BIT RSA Variante zum Beispiel dem weit verbreiteten AES Verfahren in der 256 BIT Ausführung

In einem zweiten Schritt muss man ausdrücklich darauf hinweisen, dass die Schlüssellänge kein alleiniges Maß für die Sicherheit eines anerkannten Verfahrens ist. Vorausgesetzt, ein Verfahren ist so realisiert, dass ein s.g. **Brute-Force-Angriff** die beste Möglichkeit bietet, die Verschlüsselung zu knacken, dann kann man die Schlüssellänge als Abschätzung aber heranziehen. Dabei bedeutet **Brute-Force**, dass man alle möglichen Schlüssel nach und nach durchprobieren muss, bis irgendwann einmal der Klartext vorliegt.

> **EINSCHUB:** Es gibt Firmen, die mit großen Schlüssellängen und Unknackbarkeit prahlen. Oft wird auch angegeben, dass ein bestimmtes Verfahren zum Patent angemeldet ist. Wenn Sie im Zusammenhang mit Verschlüsselung auf so etwas treffen, dann ist dies ein eindeutiges Indiz für Müll! Hände weg von solchen Produkten. Man bezeichnet s.g. Verfahren auch als Snakeoil.

Im Nachfolgenden beziehe ich mich ausschließlich auf symmetrische Verfahren. Asymmetrische Verfahren bedürfen eines anderen Ansatzes. Hier versucht man, aus dem s.g. öffentlichen Schlüssel den privaten Schlüssel abzuleiten.

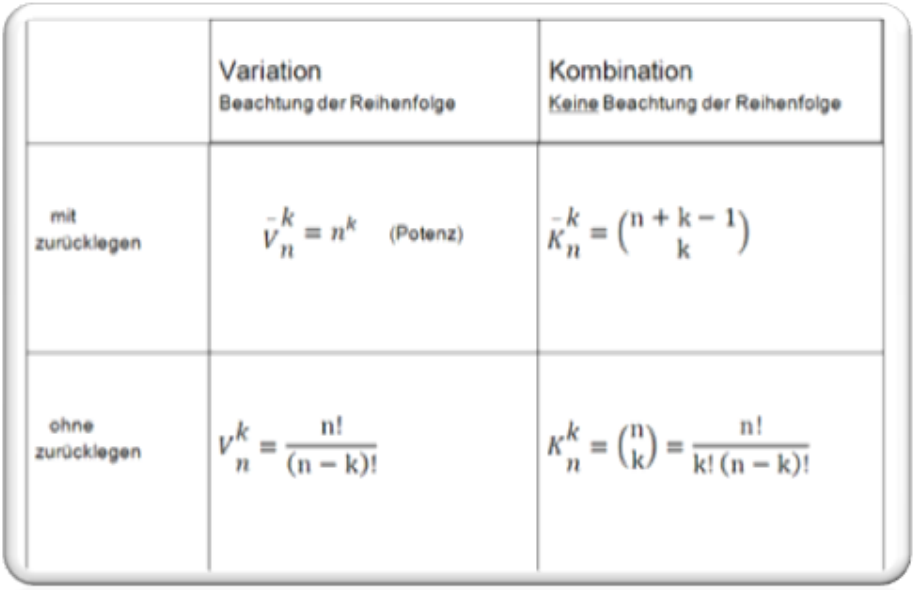
Wahrscheinlichkeiten *

Die meisten von Ihnen werden eine **EC Karte** besitzen. Am Geldautomaten muss man eine 4 stellige PIN eingeben. **Brute-Force** würde jetzt bedeuten, dass ein Dieb damit beginnt, alle möglichen Varianten der PIN zu testen. Also zum Beispiel 0001, dann 0002 und dann 0003. Damit wäre dann auch schon Schluss, da die Karte nach dreimaliger Falscheingabe gesperrt würde. Der Dieb könnte aber auch zunächst einmal die PINs 1234, 2361 und 8745 ausprobieren.

Merken Sie schon etwas?

Wenn nur ausreichend Leute hier diesen Beitrag lesen, wird einer dabei sein, bei dem ich einen Volltreffer gelandet habe. Was ich Ihnen damit sagen möchte ist, dass wir es mit **Wahrscheinlichkeiten** zu tun haben. Es ist eher unwahrscheinlich, dass jemand per Zufall bei 3 Eingaben die richtige PIN erwischt. Die Wahrscheinlichkeit liegt genau genommen bei 0,0003, aber es wäre möglich. Sie kennen das: Lotto Spielen ist Schwachsinn. Die Chancen auf 6 Richtige mit Superzahl liegen bei 1 zu 139 Millionen. Und trotzdem hört man immer mal wieder, dass jemand gewonnen hat.

Kombinatorik *



	Variation Beachtung der Reihenfolge	Kombination Keine Beachtung der Reihenfolge
mit zurücklegen	$\bar{V}_n^k = n^k$ (Potenz)	$\bar{K}_n^k = \binom{n+k-1}{k}$
ohne zurücklegen	$V_n^k = \frac{n!}{(n-k)!}$	$K_n^k = \binom{n}{k} = \frac{n!}{k!\,(n-k)!}$

Variation und Kombination mit und ohne Zurücklegen

Wie viele verschiedene PINs gibt es für unsere EC-Karte?

(*Ich bin mir gar nicht sicher, ob es PINs mit führenden Nullen gibt. Ich gehe im Folgenden davon aus, dass es sie gibt. PINs wie 0001 oder 0000 wären also gültig*).

Mathematisch gesehen haben wir es mit dem Problem

„Ziehen mit Zurücklegen, unter Beachtung der Reihenfolge“

zu tun.

Man zieht also einen **Gegenstand** aus einer **Kiste** (*in unserem Fall, weil PIN, eine Ziffer*), notiert auf, was für ein Gegenstand es war und legt den Gegenstand wieder zurück in die Kiste. Beim nächsten Ziehen könnten wir den Gegenstand also wieder ziehen. „Beachtung der Reihenfolge“ bedeutet schlicht, dass wir einen Unterschied machen, ob man zuerst Gegenstand A und dann Gegenstand B zieht, oder umgekehrt. Bei unserer PIN haben wir es ja mit Ziffern zu tun. Also den folgenden Gegenständen (***0,1,2,3,4,5,6,7,8,9***). Mit diesen Ziffern und dem oben beschriebenen Verfahren haben wir jetzt eine PIN zu erzeugen, die bekanntlich aus 4 Stellen besteht.

Also erstes Mal in die Kiste gefasst, notiert, welche Ziffer es war, ein zweites Mal und so fort.

Hätten wir nur eine einstellige PIN, sieht man leicht ein, dass es genau 10 verschiedene PINs gäbe.

Bei einer zweistelligen PIN leiten wir uns das so ab. Für jede Möglichkeit bei einer einstelligen PIN gibt es ja an der zweiten Stelle wieder 10 Möglichkeiten, die wir aus der Kiste ziehen können. Also für die 0 an erster Stelle, kommen ja an der zweiten Stelle wieder die Varianten mit 0,1,2,3,4,5,6,7,8,9 in Betracht. Auch für die Möglichkeit mit der 1 an erster Stelle gibt es für die zweite Position die Möglichkeiten 0,1,2,3,4,5,6,7,8,9. Das geht so weiter bis wir an der ersten Stelle die 9 stehen haben. Insgesamt gäbe es bei der zweistelligen PIN als 10 X 10 = 100 verschiedene PINs.

0 + (0,1,2,3,4,5,6,7,8,9) = 10
1 + (0,1,2,3,4,5,6,7,8,9) = 10
2 + (0,1,2,3,4,5,6,7,8,9) = 10
3 + (0,1,2,3,4,5,6,7,8,9) = 10
4 + (0,1,2,3,4,5,6,7,8,9) = 10
5 + (0,1,2,3,4,5,6,7,8,9) = 10
6 + (0,1,2,3,4,5,6,7,8,9) = 10
7 + (0,1,2,3,4,5,6,7,8,9) = 10
8 + (0,1,2,3,4,5,6,7,8,9) = 10
9 + (0,1,2,3,4,5,6,7,8,9) = 10
==========

= 10 X 10 = 100

Daraus kann man sich bereits die allgemeine Regel ableiten.

Angenommen wir haben K Stellen, die wir bei der PIN besetzen müssen, dann gäbe es insgesamt 10 X 10 X … X 10 (*k-mal*) Möglichkeiten.
Die 10 wird so oft mit sich selbst multipliziert, wie wir Stellen haben. In unserem Beispiel mit der EC-Karten PIN, die 4 stellig ist, ist k = 4 und es gilt

Anzahl verschiedener PINs bei der EC-Karte = 10 X 10 X 10 X 10 = 10^4 **= 10.000**

Jetzt kann ich Ihnen auch erklären, wieso oben von einer Wahrscheinlichkeit von

0,0003 die Rede ist. Haben Sie die Grafik (*Wahrscheinlichkeit*) gesehen? Dort steht die Formel.

Die **Wahrscheinlichkeit p** berechnet sich zu $\frac{1}{(Anzahl aller Moeglichkeiten)}$.

In einer Kiste befinden sich jetzt alle 10.000 PINs. Ich ziehe jetzt eine. Damit habe ich eine Wahrscheinlichkeit von 1 zu 10.000, also 0,0001, dass ich die richtige erwischt habe.

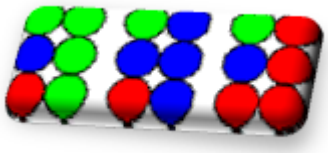
Da ich ja 3 Mal ziehen darf, wird der Wert mit 3 multipliziert (*ich erhöhe ja meine Chancen mit jedem ziehen*) und man kommt auf den besagten Wert.

N hoch k *

Aus diesem hoffentlich anschaulichen Beispiel möchte ich jetzt eine allgemeine Formel ableiten, mit der wir eine Vorstellung von der Sicherheit eines optimal umgesetzten symmetrischen Verfahrens mit bestimmter Schlüssellänge entwickeln können. Wir brauchen nur noch eine Information und schon können wir rechnen.

Im PIN Beispiel hatten wir es mit Ziffern zu tun, von denen es bekanntlich 10 gibt. Diese Zahl 10 ist die **Zahl der Gegenstände**, aus denen eine Reihe aufgebaut wird.

Es könnten auch 3 Gegenstände sein. Zum Beispiel **3 Bälle** in den Farben rot, grün und blau.



Wenn wir zum Beispiel wissen möchten, wie viele mögliche Varianten es gibt, 3 dieser Bälle (*K ist also 3*) vor uns zu legen, gilt:
3 X 3 X 3 = 27

Bezeichnen wir die **Anzahl der Gegenstände**, aus denen wir wählen können mit **N** und die **Zahl der Stellen**, die wir besetzen müssen mit **k**, erhalten wir die allgemeine

Formel

Anzahl Möglichkeiten = N^k

Wie sicher ist mein Passwort? *

Die Frage ist nicht ganz korrekt. Sie werden aber sehen, worauf ich hinaus will.

Viele Jahre wurde empfohlen, dass ein Passwort **8 Zeichen lang** sein sollte.

Wie viele verschiedene Möglichkeiten gibt es denn, ein Passwort aus 8 Zeichen (*8 ist unser k*) aufzubauen. Wie viele Kombinationen müsste ein Angreifer maximal (***worst-case = erst sein letztes eingegebenes Passwort ist das unsrige – So ein Pechvogel!***) ausprobieren (***Brute-Force***), bis er das korrekte Passwort erwischt?

Dazu müssen wir uns zunächst klar machen, aus wie vielen Gegenständen (*das ist dann unser N*) das Passwort aufgebaut ist. Nehmen wir einfach an, wir dürften **nur Großbuchstaben** verwenden. Folglich hätten wir **26 Gegenstände** (*unser N, Alphabet besteht aus 26 Buchstaben*) um die 8 Positionen im Passwort jeweils zu besetzen.

Nur Großbuchstaben *

In unsere Formel eingesetzt erhalten wir

$$26^8 = 208.827.064.576 = 2{,}1 \times 10^{11}$$

WOW! Verdammt viele Varianten.

Mit Kleinbuchstaben *

Dann kommen noch 26 Gegenstände (unsere 26 Kleinbuchstaben) in die Kiste und in die Formel eingesetzt ergibt sich:

$$(26+26)^8 = 52^8 = 53.459.728.531.456 = 5{,}3 \times 10^{13}$$

Gigantisch, oder?!

Mit Ziffern *

Und wieder kommen 10 Gegenstände in die Kiste (die 10 Ziffern). Wir kennen das jetzt schon. Rein in die Formel und

$$(26+26+10)^8 = 218.340.105.584.896 = 2{,}18 \times 10^{14}$$

> Da braucht man schon ordentlich Papier um sich alle Varianten zu notieren
>

Mit Sonderzeichen *

Die Geister scheiden sich etwas, wenn es um die Anzahl an Sonderzeichen geht. Gehen wir von 26 aus.

Unsere Kiste erhält also erneut Zuwachs und weist jetzt 88 Gegenstände auf. Rein in die Formel mit ihnen.

$$(26+26+10+26)^8 = 88^8 = 3{,}6 \times 10^{15}$$

Mir fehlen die Worte

Meine Tastatur ist kaputt und kennt nur Kleinbuchstaben *

Sie kennen das! Wenn Ihnen jemand Ratschläge gibt, wie Ihr Passwort aufzubauen ist, dann ist der folgende Hinweis **immer** dabei!

> **„Verwenden Sie zum Aufbau Ihres Passwortes Groß-/Kleinbuchstaben, Ziffern und Sonderzeichen!“**

Ich selbst mache das. Wir nehmen jetzt einmal unser 8 stelliges Passwort mit allem **Pipapo** als Referenz und sehen uns an, was von dieser Empfehlung zu halten ist.

Wir wissen, dass es $3{,}6\times10^{15}$ verschiedene Passwörter der Länge 8 gibt.

Wie lange müsste ein Passwort, bestehend nur aus Kleinbuchstaben sein, damit es genau so viele Möglichkeiten gibt?

Dazu basteln wir uns eine einfache Gleichung. Links steht die Anzahl an Schlüsseln die wir gerne hätten und rechts unsere bekannte Formel.

$$3{,}6\times10^{15}=n^{k}$$

N kennen wir. Nur Kleinbuchstaben, also 26.

K ist gesucht!

$$3{,}6\times10^{15}=26^{k}$$

Nach k aufgelöst erhält man als Ergebnis ca.

11

[***Das Geheimnis zur Berechnung:*** $\ln\frac{\left(3{,}6\times10^{15}\right)}{\ln\left(26\right)}$ ***; ln = logarithmus naturalis***]

Mit 11 Kleinbuchstaben hat man einen genau so großen Vorrat an möglichen Schlüsseln, wie bei einem 8 Zeichen langen Passwort, welches alles enthält, was die Tastatur hergibt.

Probe:

$$26^{11}=3{,}7\times10^{15}$$

Passt also!

Verzichtet man nur auf die viel beschworenen Sonderzeichen, erhält man:

$$3{,}6\times10^{15}=\left(26+26+10\right)^{k}=\frac{\ln\left(3{,}6\times10^{15}\right)}{\ln\left(62\right)}=8{,}7$$

Wir brauchen also ein 9 Zeichen langes Passwort um bei Verzicht auf Sonderzeichen die gleiche Sicherheit zu erhalten, wie bei einem 8 Zeichen langen Passwort mit

Sonderzeichen.

[***WICHTIG: Die Gefahr die bei Verzicht auf Sonderzeichen erwächst findet sich in s.g. Wörterbuchattacken, gegen die die Software allerdings von Hause aus schützen sollte. Stichwort SALT und Schlüsselableitung***]

Rein in die Tiefen des Rechners *

Zurück zu unseren symmetrischen Verschlüsselungsverfahren. Hier spricht man ja immer von einem **XXX-BIT Verfahren**.

Der Schlüssel besteht hier nicht aus Buchstaben oder Zahlen, sondern aus **BIT**s. Ein BIT besteht aus den zwei Zuständen **0** und **1**.

Diese beiden Zustände sind unsere Gegenstände in der Kiste, aus der wir ziehen und den Schlüssel aufbauen.

> **Das sieht mager aus! Nur 2 Gegenstände in der Kiste. Ein mickriges N in unserer Formel. Aber abwarten!**

Nehmen wir uns **AES** zur Brust! AES ist mit verschiedenen Varianten verfügbar. Wir nutzen in allen Produkten die 256 BIT Variante. Der Schlüssel ist also aus 256 Stellen (***unser k***) aufgebaut.

Jetzt ahnt man schon etwas! Wir rechnen uns einmal aus, wie viele verschiedene Schlüssel der Länge 256 es gibt.

$N^k = 2^{256}$ **= festhalten, Augen zu, Augen wieder auf und, ...**

$1{,}16 \times 10^{77}$

Von Sternen und Atomen *

Wir haben ein Problem!

Menschen können sich unglaublich schwer etwas unter **großen Zahlen** vorstellen.

OK!

10^{77}

klingt cool, steht aber recht unscheinbar einfach so mitten in der Zeile, verbraucht kaum Platz und frisst nicht viel!

Freunde, aufgepasst!:

> [Ein Tipp zum Verständnis:
> Potenzen mit gleicher Basis werden multipliziert, indem man ihre Hochzahlen addiert. Oder anders ausgedrückt.
>
> $10^{10} \times 10^{10} \times 10^{10} \times 10^{10} \times 10^{10} \times 10^{7} = 10^{77}$ (= *unsere Zahl*)]

Wir haben es also mit unglaublichen 10^{77} Schlüsseln zu tun, die **jeweils 256 BIT** lang sind.

Angenommen wir wollten diese Schlüssel abspeichern und könnten jeden Schlüssel in einem einzigen Atom unterbringen. [Anm.: In Wahrheit braucht man natürlich viel mehr Atome um einen solchen Schlüssel zu speichern – Ansonsten wären unsere aktuellen Festplatten noch kleiner **]**

Wie viel Tonnen Humus brauchen wir da wohl? *

Aus wie vielen Atomen besteht eigentlich der Mensch?

Bei **70kg** aus ca. 7×10^{27} Atomen.

Unspektakulär?! Wir bräuchten 10^{49} **Menschen,** fein säuberlich in Atome zerlegt, um unsere Schlüssel zu speichern.

Aus wie vielen Atomen besteht die Erde? *

Das dürften so etwa 6×10^{49} sein. Wir brauchen also 10^{27} Erden. Wird wohl ein recht großer Haufen Humus?!

Aus wie vielen Atomen besteht die Sonne? *

Hier kommen wir auf einen Wert von etwa 10^{57} . Die Sonne wird uns langsam gefährlich meinen Sie? Nicht wirklich, denn auch hiervon benötigen wir 10^{20} .

Jetzt gehen uns langsam die Mittel aus L

Wie sieht es denn mit der Milchstraße aus? *

OK. Die Milchstraße hat nach Schätzungen eine Masse die der von 100×10^{9} **Sonnen** entspricht. Also $10^{11}\times10^{57}=10^{68}$

Verdammt und zugenäht! Wir brauchen 10^{9} **Milchstraßen** in Atome zerlegt, damit wir unsere Schlüssel auf die kleinen Elementarteilchen aufteilen können.

Die letzte Bastion hält! Unser Universum *

Es gibt **einige Milliarden Galaxien.** Die Anzahl der Atome im Universum dürfte bei etwa 10^{78} liegen.

Das war knapp!

Alle Atome im Universum dürften also gerade so ausreichen, um die unglaubliche Anzahl an möglichen Schlüsseln aufnehmen zu können.

Aber mal zurück zur Erde und den bescheidenen 10^{49} Atomen. Machen Sie sich klar, dass selbst dann, wenn man die Erde in ihre atomaren Teilchen zerlegt, nicht genug Möglichkeiten vorhanden sind, auch nur einen kleinen Teil der möglichen Schlüssel zu speichern.

Jetzt leuchtet ein, wie aussichtslos ein Brute Force Angriff auf ein Verfahren ist, bei dem Brute-Force die einzige Möglichkeit darstellt, die Verschlüsselung zu knacken.

Bildnachweis:
Stockfoto-ID: 123869519
Copyright: Forplayday

