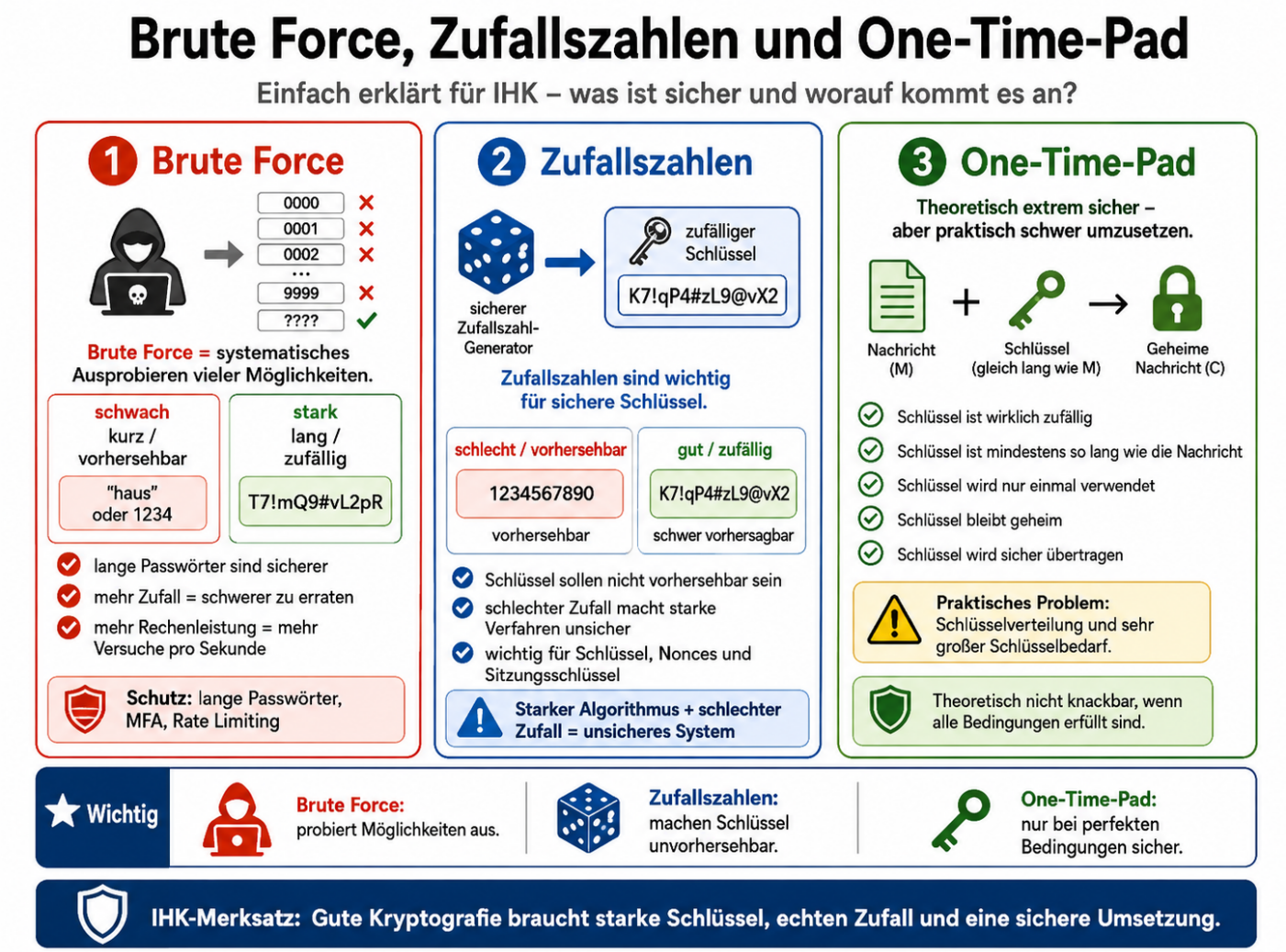
13.7 Brute Force, Zufallszahlen und One-Time-Pad



Kurzüberblick

In dieser Seite geht es um die Frage:

> **Ist Verschlüsselung wirklich nicht zu knacken?**

Die ehrliche Antwort ist:

Es kommt darauf an.

Eine Verschlüsselung kann theoretisch sehr stark sein, aber in der Praxis trotzdem unsicher werden.

Gründe dafür können sein:

- zu kurze Schlüssel
- schlechte Passwörter
- schlechte Zufallszahlen
- gestohlene Schlüssel
- Fehler in der Software
- Hintertüren im Algorithmus
- falsch konfigurierte Systeme
- unsichere Endgeräte
- Benutzerfehler

> **IHK-Merksatz:**
> Starke Verschlüsselung braucht nicht nur einen guten Algorithmus, sondern auch starke Schlüssel, gute Zufallszahlen und eine sichere Umsetzung.

Quelle 11.5 – Zusammenfassung Verschlüsselung

Die Quelle stellt sinngemäß die Frage:

> Ist Verschlüsselung nicht zu knacken?

Dabei werden mehrere wichtige Punkte genannt:

- mögliche Hintertüren in Algorithmen
- fehlerhafte Implementierung in Software
- echte Zufallszahlen
- Brute Force
- steigende Rechenleistung
- ASICs
- One-Time-Pad als besonderer Sonderfall

Diese Punkte sind wichtig, weil sie zeigen:

> Verschlüsselung ist nicht automatisch sicher, nur weil irgendwo „verschlüsselt“ steht.

Warum Verschlüsselung trotzdem scheitern kann

Problem	Erklärung
schwacher Schlüssel	zu kurz oder leicht erratbar
schlechtes Passwort	kann durch Ausprobieren gefunden werden
schlechte Zufallszahlen	Schlüssel können vorhersagbar werden
gestohlener Schlüssel	Angreifer kann entschlüsseln
Softwarefehler	Algorithmus wird falsch umgesetzt
Hintertür	absichtlich eingebaute Schwachstelle
unsicheres Gerät	Klartext oder Schlüssel können direkt abgegriffen werden
Benutzerfehler	Schlüssel oder Passwörter werden falsch behandelt

> **Kurz gesagt:**
> Der beste Algorithmus hilft wenig, wenn Schlüssel, Software oder Benutzerverhalten unsicher sind.

Brute Force

Brute Force bedeutet:

Ein Angreifer probiert systematisch sehr viele Möglichkeiten aus, bis etwas passt.

Zum Beispiel:

- Passwörter ausprobieren
- PINs ausprobieren
- Schlüssel ausprobieren
- Hashes gegen Wörterbücher testen
- Zugangsdaten erraten

> **Merksatz:**
> Brute Force = ausprobieren, bis es passt.

Einfaches Beispiel

Angenommen, ein Passwort besteht nur aus vier Ziffern.

Dann gibt es:

```
0000 bis 9999
```

Also 10.000 Möglichkeiten.

Ein Computer kann solche Kombinationen sehr schnell ausprobieren.

Bei einem langen, zufälligen Passwort wird das viel schwieriger.

Was beeinflusst Brute Force?

Faktor	Auswirkung
Länge des Passworts	längere Passwörter sind schwerer zu knacken
Zeichenvorrat	mehr mögliche Zeichen erhöhen die Anzahl der Kombinationen
Zufälligkeit	zufällige Passwörter sind schwerer zu erraten
Rechenleistung	schnellere Hardware kann mehr Versuche pro Sekunde machen
Schutzmechanismen	Sperren und Wartezeiten bremsen Angriffe
Passwort-Wiederverwendung	erhöht das Risiko bei Datenlecks

Beispiel: Warum Länge wichtig ist

Ein Passwort wie:

```
haus
```

ist viel schwächer als:

```
T7!mQ9#vL2pR
```

Warum?

Das zweite Passwort ist:

- länger
- zufälliger
- schwerer zu erraten
- schwerer per Brute Force zu finden

> **Achtung Prüfungsfalle:**
> Ein langes, zufälliges Passwort ist meistens besser als ein kurzes, kompliziert wirkendes Passwort.

Rechenleistung und Brute Force

Je mehr Rechenleistung ein Angreifer hat, desto schneller kann er Möglichkeiten ausprobieren.

Die Quelle nennt dazu sinngemäß unterschiedliche Leistungsstufen:

Hardware	Bedeutung
normaler PC	vergleichsweise langsam
Grafikkarte	schneller für viele parallele Berechnungen
Spezialhardware	für bestimmte Aufgaben optimiert
ASIC	sehr spezialisierte Hardware

ASIC bedeutet:

anwendungsspezifische integrierte Schaltung

Das heißt:

Ein Chip wird speziell für eine bestimmte Aufgabe gebaut.

> **Kurz gesagt:**
> Mehr spezialisierte Hardware = mehr Versuche pro Sekunde.

Gegenmaßnahmen gegen Brute Force

Maßnahme	Wirkung
lange Passwörter	erhöhen die Anzahl möglicher Kombinationen
zufällige Passwörter	verhindern leichtes Erraten
Passwortmanager	ermöglicht lange, einzigartige Passwörter
Multi-Faktor-Authentifizierung	Passwort allein reicht nicht aus
Rate Limiting	begrenzt Versuche pro Zeit
Account-Sperre	stoppt viele Fehlversuche
starke Schlüssel	erschweren vollständiges Durchprobieren

Maßnahme	Wirkung
moderne Algorithmen	vermeiden bekannte Schwächen

> **IHK-Merksatz:**
> Gegen Brute Force helfen vor allem Länge, Zufall, Begrenzung der Versuche und zusätzliche Faktoren.

Zufallszahlen

Zufallszahlen sind in der Kryptografie extrem wichtig.

Warum?

Schlüssel sollen nicht erratbar sein.

Wenn ein Schlüssel vorhersehbar ist, kann ein Angreifer ihn leichter finden.

Das Problem:

Ein Computer ist grundsätzlich eine Maschine.
Er erzeugt oft nur scheinbaren Zufall, wenn kein guter Zufallszahlengenerator verwendet wird.

Warum schlechte Zufallszahlen gefährlich sind

Angenommen, ein System erzeugt Schlüssel nicht wirklich zufällig.

Dann könnten Schlüssel zum Beispiel:

- wiederholt auftreten
- nach einem Muster entstehen
- aus der Uhrzeit ableitbar sein
- aus wenigen Startwerten berechenbar sein
- für Angreifer vorhersagbar werden

Dann kann ein eigentlich starker Algorithmus unsicher werden.

> **Merksatz:**
> Starker Algorithmus + schlechter Zufall = unsicheres System.

Beispiel: Zufall bei Schlüsseln

Ein guter Schlüssel sollte für einen Angreifer nicht vorhersehbar sein.

Schlecht:

```
1234567890
```

Besser:

```
K7!qP4#zL9@vX2
```

Noch besser ist ein Schlüssel, der von einem sicheren kryptografischen Zufallszahlengenerator erzeugt wurde.

Was muss bei Schlüsseln stimmen?

Eigenschaft	Warum wichtig?
ausreichend lang	erschwert Brute Force
zufällig	verhindert Vorhersagbarkeit
geheim	sonst kann entschlüsselt werden
einmalig oder passend genutzt	Wiederverwendung kann gefährlich sein
sicher gespeichert	verhindert Diebstahl
sicher übertragen	verhindert Abfangen

One-Time-Pad

Das **One-Time-Pad** ist ein besonderer Fall der Verschlüsselung.

Es gilt theoretisch als nicht knackbar, wenn alle Bedingungen erfüllt sind.

Diese Bedingungen sind aber sehr streng.

Bedingungen für ein sicheres One-Time-Pad

Bedingung	Erklärung
Schlüssel ist wirklich zufällig	keine Muster, nicht vorhersagbar
Schlüssel ist mindestens so lang wie die Nachricht	jeder Teil der Nachricht braucht Schlüsselmaterial
Schlüssel wird nur einmal verwendet	Wiederverwendung zerstört die Sicherheit
Schlüssel bleibt geheim	sonst kann entschlüsselt werden

Bedingung	Erklärung
Schlüssel wird sicher übertragen	Schlüssel darf nicht abgefangen werden

> **IHK-Merksatz:**
> One-Time-Pad ist theoretisch extrem sicher, aber praktisch schwer sauber umzusetzen.

Warum ist One-Time-Pad praktisch schwierig?

Das größte Problem ist die Schlüsselverteilung.

Wenn der Schlüssel genauso lang sein muss wie die Nachricht, muss dieser lange Schlüssel vorher sicher zu Bob gelangen.

Das ist unpraktisch.

Nachricht	benötigter Schlüssel
1 MB Datei	mindestens 1 MB Schlüssel
100 MB Datei	mindestens 100 MB Schlüssel
1 GB Datei	mindestens 1 GB Schlüssel

Und dieser Schlüssel muss:

- vorher sicher erzeugt werden
- sicher an Bob übertragen werden
- geheim bleiben
- nach einmaliger Nutzung vernichtet werden
- niemals wiederverwendet werden

Warum darf ein One-Time-Pad-Schlüssel nur einmal verwendet werden?

Wenn derselbe Schlüssel mehrfach verwendet wird, können Angreifer aus mehreren verschlüsselten Nachrichten Muster ableiten.

Dann ist die theoretische Sicherheit verloren.

Deshalb heißt es:

One-Time Pad

Also:

nur einmal verwenden

> **Achtung Prüfungsfalle:**
> One-Time-Pad ist nur sicher, wenn alle Bedingungen wirklich erfüllt sind.

Vergleich: normale Verschlüsselung und One-Time-Pad

Merkmal	Moderne Verschlüsselung	One-Time-Pad
Schlüssel kürzer als Daten möglich	ja	nein
praktisch gut nutzbar	ja	schwierig
theoretisch nicht knackbar	abhängig vom Verfahren	ja, wenn Bedingungen erfüllt
Schlüsselverteilung	handhabbar	sehr schwierig
Wiederverwendung des Schlüssels	abhängig vom Verfahren geregelt	verboten
wichtig für IHK	Grundidee verstehen	Sonderfall kennen

Zusammenhang: Brute Force, Zufall und One-Time-Pad

Diese drei Themen hängen zusammen.

Thema	Kerngedanke
Brute Force	Angreifer probiert Möglichkeiten aus
Zufallszahlen	Schlüssel sollen nicht vorhersagbar sein
One-Time-Pad	theoretisch sicher bei perfektem Zufall und einmaliger Nutzung

Kurz gesagt:

- Brute Force greift schwache oder zu kurze Schlüssel an.
- Gute Zufallszahlen machen Schlüssel schwerer vorhersagbar.
- One-Time-Pad zeigt, wie wichtig echter Zufall und einmalige Nutzung sind.

Typische IHK-Fragen

Was bedeutet Brute Force?

Brute Force bedeutet, dass ein Angreifer systematisch viele Möglichkeiten ausprobiert.

Was wird bei Brute Force ausprobiert?

Zum Beispiel Passwörter, PINs, Schlüssel oder Hashwerte.

Was schützt gegen Brute Force?

Lange und zufällige Passwörter, starke Schlüssel, Begrenzung von Fehlversuchen und Multi-Faktor-Authentifizierung.

Warum sind Zufallszahlen in der Kryptografie wichtig?

Weil Schlüssel nicht vorhersagbar sein dürfen.

Was passiert bei schlechten Zufallszahlen?

Schlüssel können leichter erraten oder berechnet werden.

Was ist das One-Time-Pad?

Ein theoretisch extrem sicheres Verfahren, wenn der Schlüssel wirklich zufällig, mindestens so lang wie die Nachricht, geheim und nur einmal verwendet wird.

Warum ist One-Time-Pad praktisch schwierig?

Weil der Schlüssel sehr lang sein muss und sicher verteilt werden muss.

Prüfungsfalle: „verschlüsselt“ heißt nicht automatisch sicher

Nur weil Daten verschlüsselt sind, heißt das nicht automatisch, dass alles sicher ist.

Man muss fragen:

Frage	Warum wichtig?
Ist der Algorithmus sicher?	schwache Verfahren können gebrochen werden
Ist der Schlüssel lang genug?	kurze Schlüssel sind leichter durchprobierbar
Ist der Schlüssel zufällig?	vorhersehbare Schlüssel sind gefährlich
Ist der Schlüssel geheim geblieben?	gestohlene Schlüssel zerstören Sicherheit
Ist die Software korrekt umgesetzt?	Implementierungsfehler können alles schwächen
Ist das Endgerät sicher?	Klartext kann dort abgegriffen werden

---

Prüfungsfalle: One-Time-Pad nicht mit normalem Passwort verwechseln

Ein One-Time-Pad ist nicht einfach ein normales Passwort.

Ein One-Time-Pad-Schlüssel muss:

- wirklich zufällig sein
- mindestens so lang wie die Nachricht sein
- nur einmal verwendet werden
- geheim bleiben
- sicher übertragen werden

Wenn eine dieser Bedingungen verletzt wird, ist die besondere Sicherheit nicht mehr gegeben.

Zusammenfassung

Brute Force ist das systematische Ausprobieren vieler Möglichkeiten.

Je kürzer oder vorhersehbarer ein Passwort oder Schlüssel ist, desto leichter wird ein Brute-Force-Angriff.

Gute Zufallszahlen sind wichtig, damit Schlüssel nicht erratbar oder berechenbar sind.

Das One-Time-Pad ist theoretisch extrem sicher, aber praktisch schwer umzusetzen, weil der Schlüssel wirklich zufällig, mindestens so lang wie die Nachricht, geheim und nur einmalig verwendbar sein muss.

> **IHK-Spickzettel:**
> Brute Force = systematisches Ausprobieren
> Schutz = lange, zufällige Passwörter und starke Schlüssel
> Zufallszahlen = wichtig für sichere Schlüssel
> schlechter Zufall = unsicheres System
> One-Time-Pad = theoretisch nicht knackbar bei perfekten Bedingungen
> Problem beim One-Time-Pad = sichere Schlüsselverteilung

Revision #3
Created 2 June 2026 23:55:38 by Admin
Updated 3 June 2026 06:18:12 by Admin