



Übung GSS Blatt 5

SVS – Sicherheit in Verteilten Systemen

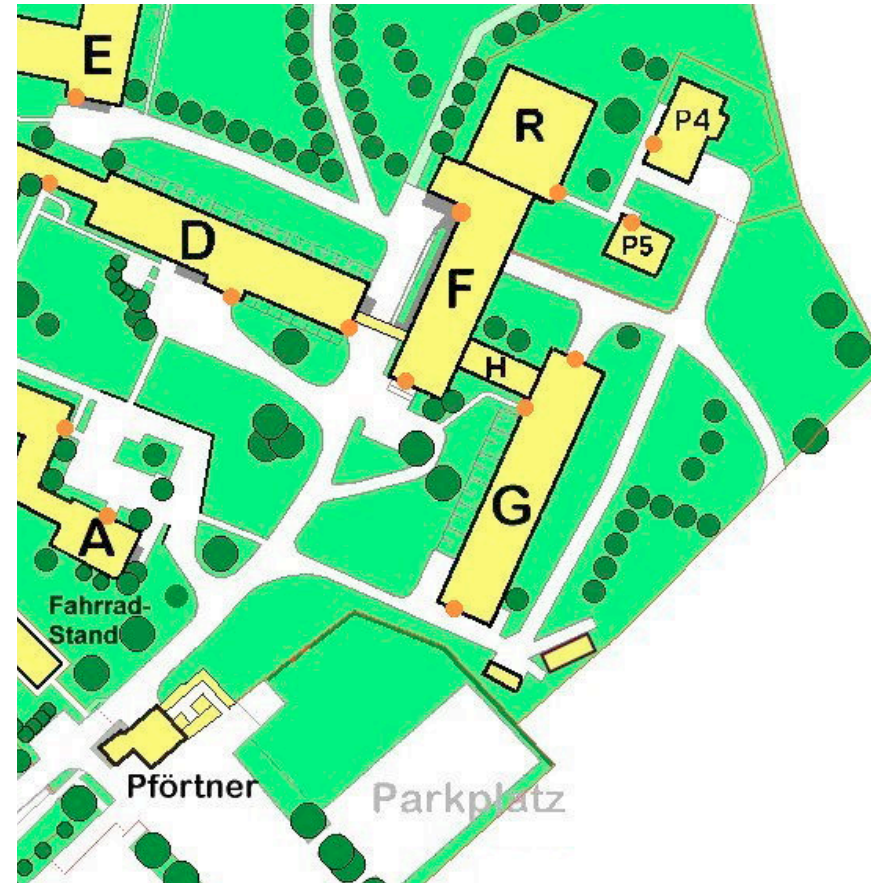


Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

Einladung zum SVS-Sommerfest

- SVS-Sommerfest
 - **am 12.07.16 ab 17 Uhr**
 - Ihr seid eingeladen! :-)
- Es gibt
 - Thüringer Bratwürste im Brötchen oder Grillkäse
 - kalte Getränke
- Ort:
 - Campus Stellingen
 - voraussichtlich hinter Haus G
- Bitte mit E-Mail-Adresse anmelden
 - Deadline: 08.07.16 12.00 Uhr
 - **<http://tinyurl.com/svsbbq16>**



Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 1: In der IT-Sicherheit unterscheidet man zwischen den Systemfunktionen *Zugriffskontrolle* und *Zugangskontrolle*. Informieren Sie sich über die beiden Techniken.
 - a) Erläutern Sie stichpunktartig den Zweck der jeweiligen Technik. (Pflicht; 2 Punkte)

Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 1: In der IT-Sicherheit unterscheidet man zwischen den Systemfunktionen *Zugriffskontrolle* und *Zugangskontrolle*. Informieren Sie sich über die beiden Techniken.
 - a) Erläutern Sie stichpunktartig den Zweck der jeweiligen Technik. (Pflicht; 2 Punkte)
 - **Zugangskontrolle**
 - Dienstnutzung soll nur berechtigten Partnern möglich sein.
 - Verhindern von unbefugter Inanspruchnahme von Betriebsmitteln.
 - ggf. Feststellung der Identität des Kommunikationspartners

Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 1: In der IT-Sicherheit unterscheidet man zwischen den Systemfunktionen *Zugriffskontrolle* und *Zugangskontrolle*. Informieren Sie sich über die beiden Techniken.
 - a) Erläutern Sie stichpunktartig den Zweck der jeweiligen Technik. (Pflicht; 2 Punkte)
 - **Zugriffskontrolle**
 - Kontrolle von Operationen oder Zugriffen auf bestimmten Betriebsmitteln oder Daten
 - Subjekte sollen nicht die gleichen Rechte haben
 - Nachvollziehbarkeit des Zugriffs (Dokumentationsfunktion)
 - Einhaltung von Sicherheitsrichtlinien (z.B. Vier-Augen-Prinzip)

Aufgabe 1: Zugangs- und Zugriffskontrolle

- b) Ist es sinnvoll, ein System mit einer Zugangskontrolle auszustatten, **jedoch keine Mechanismen zur Zugriffskontrolle zu implementieren**? Begründen Sie Ihre Antwort mit einem Beispiel. (Pflicht; 2 Punkte)

Aufgabe 1: Zugangs- und Zugriffskontrolle

- b) Ist es sinnvoll, ein System mit einer Zugangskontrolle auszustatten, **jedoch keine Mechanismen zur Zugriffskontrolle zu implementieren**? Begründen Sie Ihre Antwort mit einem Beispiel. (Pflicht; 2 Punkte)
- sinnvoll, wenn es reicht, den Nutzerkreis einzuschränken
 - kein Verwaltungsaufwand für Zugriffskontrolle
 - Beispiele:
 - Wenn sowieso nur eine Person das System nutzt (Privater Computer / Mobiltelefon)
 - Wenn alle Nutzer gleichberechtigt sind / Vertrauen genießen (Systeme in einer kleinen Firma)
 - Wenn die Implementierung unmöglich oder zu teuer ist (privater Wand-Tresor; Schließfach; Tür)

Aufgabe 1: Zugangs- und Zugriffskontrolle

- c) Die Absicherung eines Systems mittels einer Zugriffskontrolle setzt hingegen **immer auch eine vorherige Zugangskontrolle** voraus. Warum? (Pflicht; 1 Punkt)

Aufgabe 1: Zugangs- und Zugriffskontrolle

- c) Die Absicherung eines Systems mittels einer Zugriffskontrolle setzt hingegen **immer auch eine vorherige Zugangskontrolle** voraus. Warum? (Pflicht; 1 Punkt)
- Im Rahmen der Zugriffskontrolle wird entschieden, welche Operationen von einem bestimmten Subjekt auf bestimmten Objekten durchgeführt werden dürfen.
 - Um diese Kontrolle zu implementieren, muss der Zugriffsmonitor das jeweilige Subjekt *kennen*. Für diese **Identifikation** des Subjekts ist die Zugangskontrolle zuständig.

Aufgabe 1: Zugangs- und Zugriffskontrolle

d) File-Sharing-Dienste

- File-Sharing-Dienste (z.B. Dropbox) ermöglichen Ordnerfreigabe (*Share-this-Folder-Link*)
- Mit dem Link kann **jeder** auf den freigegebenen Ordner zugreifen (auch ohne Konto und Login)
- Wie sind hier Zugangs- und Zugriffskontrolle realisiert? (Optional)

Aufgabe 1: Zugangs- und Zugriffskontrolle

d) File-Sharing-Dienste

- File-Sharing-Dienste (z.B. Dropbox) ermöglichen Ordnerfreigabe (*Share-this-Folder-Link*)
 - Mit dem Link kann **jeder** auf den freigegebenen Ordner zugreifen (auch ohne Konto und Login)
 - Wie sind hier Zugangs- und Zugriffskontrolle realisiert? (Optional)
-
- Die **Zugangskontrolle** erfolgt in diesem Fall implizit durch die Weitergabe des Links – unterliegt also dem Nutzer.
 - Die **Zugriffskontrolle** findet beim File-Sharing-Dienst statt und besteht darin, welche Operationen (z.B. nur Lesen oder auch Schreiben) die Subjekte durchführen dürfen, denen der Link gegeben wurde.
 - *Gruppenrechte*

Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 2: Biometrische Techniken: EasyPASS

Neues Grenzkontrollsystem an mehreren deutschen Flughäfen:

- (teil-)automatisierte Passkontrolle und Einreise anhand des biometrischen Reisepasses
- Vorgang:
 - Reisende scannen ihren elektronischen Pass selbständig ein
 - Vergleich von in Pass hinterlegtem Foto mit Kameraaufnahme

Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 2: Biometrische Techniken: EasyPASS



Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 2: Biometrische Techniken: EasyPASS



Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 2: Biometrische Techniken: EasyPASS
 - a) Informieren Sie sich über die biometrischen Techniken im elektronischen Reisepass der Bundesrepublik Deutschland und die Funktionsweise von *EasyPASS*. (Optional)

nach: Dr. Dennis Kügler: Risiko Reisepass?
Schutz der biometrischen Daten im RF-
Chip, ct 5 (2005) 88

Aufgabe 1: Zugangs- und Zugriffskontrolle

Exkurs: Biometrischer Reisepass

- Basic Access Control
 - Auslesen der biometrischen Daten benötigt optische Daten der maschinenlesbaren Zone
 - Schutz des digitalen Fotos
- Active Authentication
 - Soll 1:1-Kopien authentischer Daten auf gefälschten Pässen (Chips) verhindern
 - Authentikation eines Originalchips mittels Challenge-Response
- Symmetrisch verschlüsselte Kommunikation
 - zwischen Pass und Lesegerät
- Passive Authentication
 - Digitale Signatur der gespeicherten Biometriedaten
 - Verwendet PKI

Technische Spezifikation: <http://www.icao.int/mrtd/>



Aufgabe 3: Real-World-Brute-Force Angriff

- Abschätzung der Sicherheit der Access-Codes im Submission-Tool
- Wie lange dauert es bei einem realen System im Mittel bis der Angreifer den ersten (d.h. einen beliebigen) Access-Code erraten hat?

Submission for GSS 2015 DEMO SHEET

Create a New Submission

Please use this option if you haven't uploaded a file for GSS 2015 DEMO SHEET yet.

Create a New Submission

OR

Update an Existing Submission

Please use this option if you want to update your solution for GSS 2015 DEMO SHEET.

Submission is **OPEN** (Deadline: 30.05.15 @ 14:56).

[Go back to List of Sheets](#)

Aufgabe 3: Real-World-Brute-Force Angriff

- Teilaufgabe 1 (Pflicht; 2 Punkte):
 - *Angenommen, das Upload-Tool generiert seine Codes aus einem Zeichenvorrat von 36 Zeichen und 100 Studenten haben bereits eine Lösung für ein Übungsblatt über das Upload-Tool eingereicht. Sie wollen zufällig einen gültigen Sicherheitscode erraten. Wie groß ist die Wahrscheinlichkeit, dass Sie bei einem Versuch einen dieser 100 bereits vergebenen Sicherheitscodes erraten?*
- Zwei Teilprobleme:
 1. Wie viele Codes gibt es insgesamt?
 2. Wie groß ist die Wahrscheinlichkeit, einen „Treffer“ zu erraten?

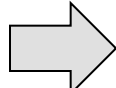
Aufgabe 3: Real-World-Brute-Force Angriff

- Teilaufgabe 1 (Pflicht; 2 Punkte):
- Zwei Teilprobleme:
 1. **Wie viele Codes gibt es insgesamt?**
 2. Wie groß ist die Wahrscheinlichkeit, einen „Treffer“ zu erraten?

1. Ermittlung Anzahl der möglichen Access-Codes

- Beispiel-Codes

GSS4-ZGGCJ-Z743P-9PK47-3Z3P3

4*5 zufällige Großbuchstaben und Ziffern  36^{20} Codes
($1,34 \cdot 10^{31}$)

Aufgabe 3: Real-World-Brute-Force Angriff

- Teilaufgabe 1 (Pflicht; 2 Punkte):
 - Zwei Teilprobleme:
 1. Wie viele Codes gibt es insgesamt? $\rightarrow N = 36^{20}$
 2. **Wie groß ist die Wahrscheinlichkeit, einen „Treffer“ zu erraten?**
- 2. Wenn es **nur einen gültigen Code** gibt
 - Wkt. für einmaliges Ziehen: Anz. d. gültigen Codes / Anz. aller Codes: $1/36^{20} \approx 7,481 \cdot 10^{-32}$
 - Aber: Im Submission-Tool sind typischerweise bereits einige Lösungen hinterlegt. Annahme: **$M=100$ gültige Codes**
 $100/36^{20} \approx 7,481 \cdot 10^{-30}$

Aufgabe 3: Real-World-Brute-Force Angriff

- Teilaufgabe 2 (Optional):
 - *Ermitteln Sie anhand der vom System zur Verfügung gestellten Informationen, wieviele unterschiedliche Zeichen tatsächlich zur generierung der Codes vom Upload-Tool verwendet werden und wie lange es im Mittel mindestens dauern würde, bis Sie Zugriff auf die Lösung von mindestens einer anderen Gruppe hätten, wenn der Webserver konstant 1000 Anfragen pro Sekunde beantworten würde. Dokumentieren Sie, wo erforderlich, Ihre Annahmen.*
- Zwei Teilprobleme:
 1. Wie viele Codes gibt es insgesamt wirklich?
 2. Wie lange braucht der Angreifer im Mittel bis zum 1. „Treffer“?

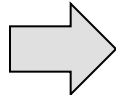
Aufgabe 3: Real-World-Brute-Force Angriff

- Teilaufgabe 2 (Optional):
- Zwei Teilprobleme:
 1. **Wie viele Codes gibt es insgesamt wirklich?**
 2. Wie lange braucht der Angreifer im Mittel bis zum 1. „Treffer“?

1. Ermittlung Anzahl der möglichen Access-Codes

- Beispiel-Codes; keine Annahme über den Zeichenvorrat

GSS4-ZGGCJ-Z743P-9PK47-3Z3P3

4*5 zufällige Großbuchstaben und Ziffern  36²⁰ Codes
(1,34*10³¹)

- Kommen wirklich alle Großbuchstaben und Ziffern vor?

Aufgabe 3: Real-World-Brute-Force Angriff

- Teilaufgabe 2 (Optional):
- Zwei Teilprobleme:
 - 1. Wie viele Codes gibt es insgesamt wirklich?**
 2. Wie lange braucht der Angreifer im Mittel bis zum 1. „Treffer“?

1. Ermittlung Anzahl der möglichen Access-Codes

- Beispiel-Codes; keine Annahme über den Zeichenvorrat

GSS4-ZGGCJ-Z743P-9PK47-3Z3P3

4*5 Großbuchstaben und Ziffern ➡ 36^{20} Codes
($1,34 \cdot 10^{31}$)

- Kommen wirklich alle Großbuchstaben und Ziffern vor?
 - nein: alle miteinander verwechselbaren Zeichen fehlen
 - nur 27 mögliche Zeichen pro Stelle:

2	3	4	6	7	9	A	C	D	E	F	G	H	J
K	L	M	N	P	Q	R	S	T	W	X	Y	Z	

➡ 27^{20} Codes
($4,24 \cdot 10^{28}$)

Aufgabe 3: Real-World-Brute-Force Angriff

- Ermittlung der Anzahl der Zeichen

- Mehrere Codes erzeugen und Zeichensatz aufstellen

unique
chars

GSS4- MD79Q - AHET2 - FWCNM -FEFNT	=> 14	= 14
GSS4-W 3F9K -NT2EN-3K YSA -E Z WH2	=> 14 +5	= 19
GSS4- GAK3X -XEY7Z- JH4 J4-MECQC	=> 14 +5 +4	= 23

Problem: Viele Duplikate!

- Motivation:

- Je weniger Zeichen man später ausprobieren muss, desto schneller ist der Brute-Force-Angriff erfolgreich. Vergisst man aber auch nur ein Zeichen, wird man u.U. **nie** Erfolg haben.
- Wie viele Codes muss man erzeugen bis man alle Zeichen gesehen hat?

- Annahme:

alle Zeichen werden aus Zufallsquelle gleichverteilt und unabhängig gezogen

Aufgabe 3: Real-World-Brute-Force Angriff

Coupon Collector's Problem

„Wie viele Sticker muss man kaufen, bis man von jedem Fußball-Spieler einen Sticker im Album kleben hat?“

Anwendung auf Access-Codes

Bei $n=27$ Zeichen im Mittel:

$$S = \frac{27}{27} + \frac{27}{26} + \dots + \frac{27}{3} + \frac{27}{2} + \frac{27}{1}$$

$$S = 105,1 \text{ Stellen (d.h. 6 Codes)}$$

wenn man genaues n nicht kennt:
für $n=36$ gilt: $S=150,3$ (8 Codes)



Aufgabe 3: Real-World-Brute-Force Angriff

Coupon Collector's Problem

- *Im Mittel* braucht man bei 27 verschiedenen Zeichen 6 Access-Codes, um alle Zeichen gesehen zu haben.
- Wie viele sollte man generieren? → Konfidenzintervalle bestimmen!

Observed number of colors in the sample	<input type="text" value="23"/>
Sample Size	<input type="text" value="60"/>
Confidence Level (%)	<input type="text" value="95"/>
	<input type="button" value="Compute"/>

The upper endpoint of a one sided 95% confidence interval for the total number of colors is 30.

(Ungenauigkeit der Schätzung beachten: hier wird **Ziehen mit Zurückliegen** angenommen)

→ Treten bei 174 Zeichen (9 Codes) 27 verschiedene Zeichen auf, hat man mit 95% Konfidenz alle möglichen Zeichen gesehen.

Aufgabe 3: Real-World-Brute-Force Angriff

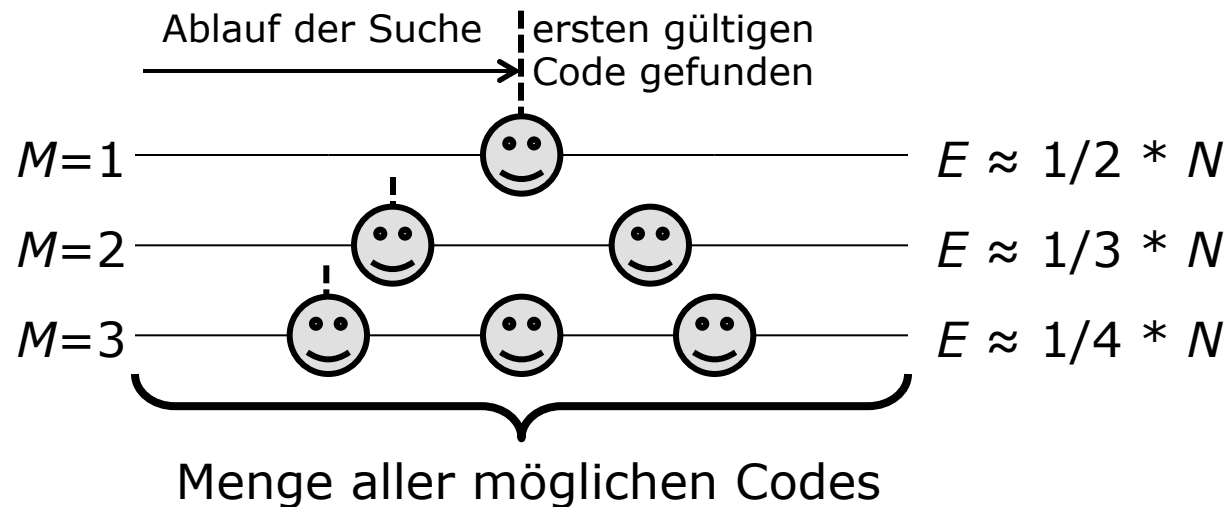
- Teilaufgabe 2 (Optional):
- Zwei Teilprobleme:
 1. Wie viele Codes gibt es insgesamt? $\rightarrow N = 27^{20}$
 2. **Wie lange braucht der Angreifer im Mittel bis zum 1. „Treffer“?**
- 2. Wenn es **nur einen gültigen Code** gibt
 - Erwartungswert E für Anzahl d. Versuche:

$$0,5 * N \approx 2,12 * 10^{28}$$
 - Aber: Im Submission-Tool sind typischerweise bereits einige Lösungen hinterlegt.
 (Annahme: **$M=100$ gültige Codes**)

Aufgabe 3: Real-World-Brute-Force Angriff

2. Wie lange braucht der Angreifer im Mittel bis zum 1. „Treffer“?

- Intuitive Bestimmung des Erwartungswertes:



- Der Raum der zu durchsuchenden Codes verkleinert sich also bei M gültigen Codes im Mittel um den Faktor $M+1 \rightarrow E \approx 4,20 * 10^{26}$
- Bei 1000 Versuchen/sec dauert die Suche im Mittel immer noch $1,33 * 10^{16}$ Jahre

Aufgabe 3: Real-World-Brute-Force Angriff

- Zusatzfrage: Wie viele Codes muss man durchsuchen, bis man „ziemlich sicher“ mindestens einen gefunden hat?
- Analytische Lösung:
 - „**Negative** (auch: inverse) **hypergeometrischer Verteilung**
 - modelliert bei einer Folge von Versuchen die Anzahl der Fehlschläge bis man mindestens s gute Elemente gezogen hat.
 - hier: $s=1$
 - Die **kumulierte Verteilungsfunktion** drückt aus, wie wahrscheinlich man beim Durchsuchen einer bestimmten Menge von Codes mindestens einen Treffer erzielt.

Aufgabe 3: Real-World-Brute-Force Angriff

- Wie viele Codes muss man durchsuchen bis man „ziemlich sicher“ mindestens einen gefunden hat?

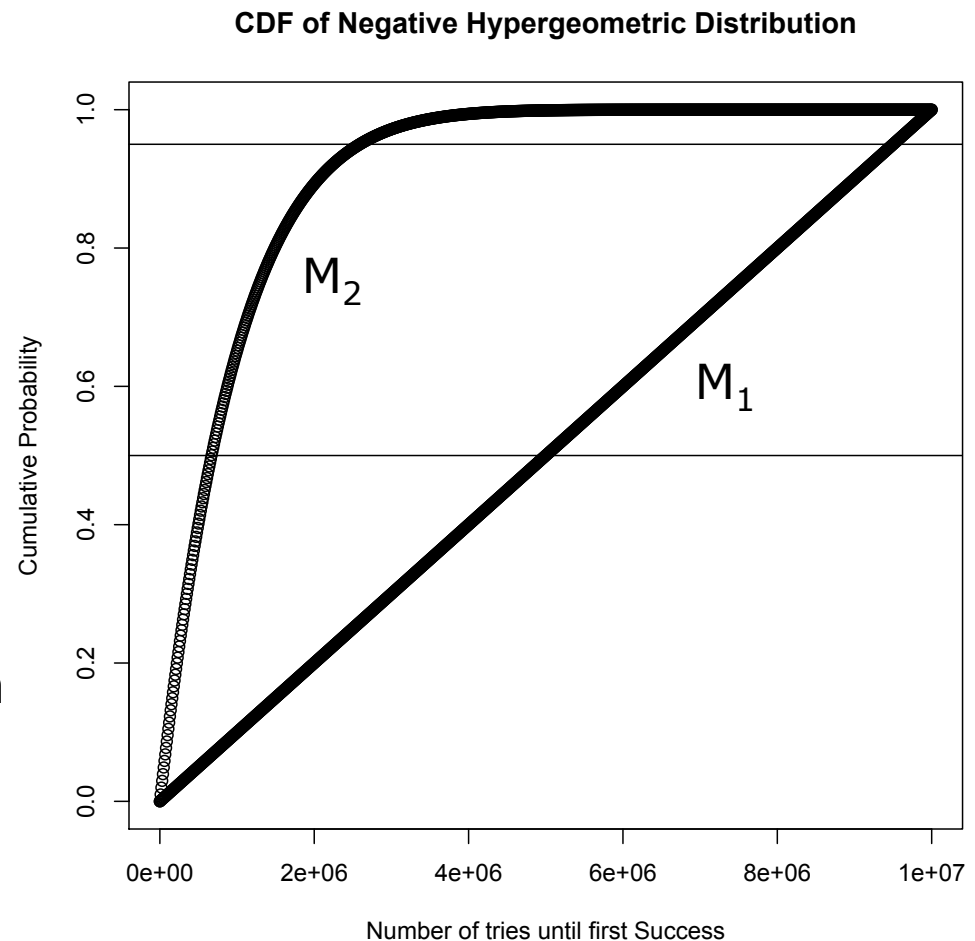
Beispiel:

$N = 10$ Millionen Codes

$M_1 = 1$ gültiger Code

$M_2 = 10$ gültige Codes

„Bei 10 Codes wird schon nach dem Durchsuchen von 25% des Suchraums in 95% der Fälle ein Treffer erzielt.“



Einladung zum SVS-Sommerfest

- SVS-Sommerfest
 - **am 12.07.16 ab 17 Uhr**
 - Ihr seid eingeladen! :-)
- Es gibt
 - Thüringer Bratwürste im Brötchen oder Grillkäse
 - kalte Getränke
- Ort:
 - Campus Stellingen
 - voraussichtlich hinter Haus G
- Bitte mit E-Mail-Adresse anmelden
 - Deadline: 08.07.16 12.00 Uhr
 - **<http://tinyurl.com/svsbbq16>**

