Übung GSS Blatt 3

SVS – Sicherheit in Verteilten Systemen

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; 2 Punkte)

Aufgabe 1: Zugangs- und Zugriffskontrolle

c) Die Absicherung eines Systems mittels einer Zugriffskontrolle setzt hingegen **immer auch eine vorherige Zugangskontrolle** voraus. Warum? (Pflicht; 2 Punkte)

- 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? (Pflicht; 2 Punkte)

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? (Pflicht; 2 Punkte)

– 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

Pilotprojekt am Frankfurter Flughafen:

- vollautomatische Passkontrolle und Einreise anhand biometrischem Reisepass

- Vorgang:
  - Reisende scannen ihren elektronischen Pass selbständig ein
  - Vergleich von in Pass hinterlegtem Foto mit Kameraaufnahme

Quelle: http://cdn1.spiegel.de/images/image-24300-galleryV9-mfrh.jpg

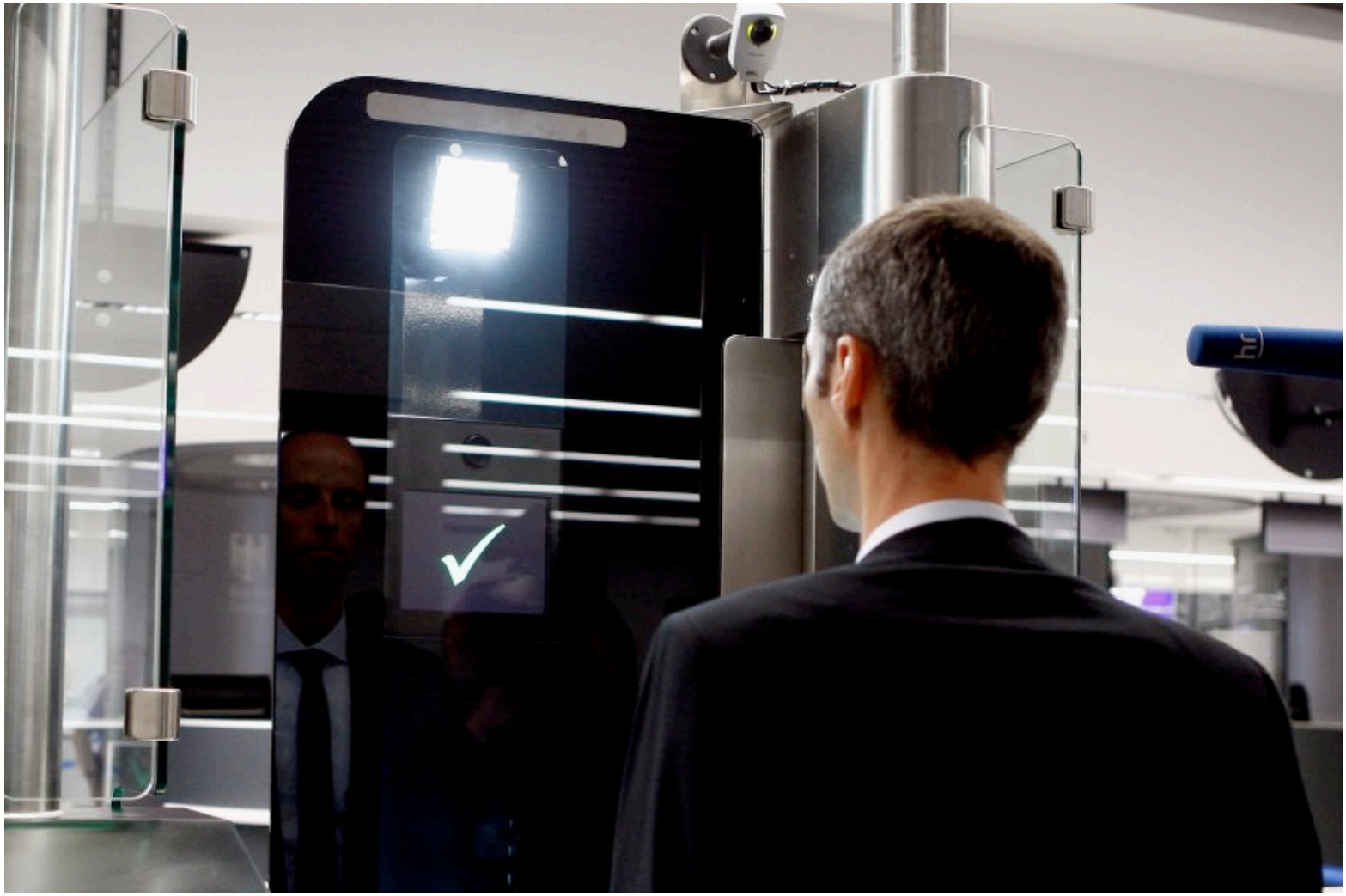
Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 2: Biometrische Techniken: EasyPASS

Quelle: http://cdn1.spiegel.de/images/image-24300-galleryV9-mfrh.jpg

Aufgabe 1: Zugangs- und Zugriffskontrolle

- Teilaufgabe 2: Biometrische Techniken: EasyPASS



Quelle: http://cdn3.spiegel.de/images/image-24306-galleryV9-moti.jpg

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)

Aufgabe 1: Zugangs- und Zugriffskontrolle

Exkurs: Biometrischer Reisepass

- Basic Access Control und Active Authentication

optisches Lesen der MRZ

RF-Chip kennt K (56 Bit)

Aktivierung durch elektr. Feld abwarten, Zufallszahl Rand1 wählen und senden

Response entschlüsseln, Rand1 prüfen, k_{Reader} zwischenspeichern, Schlüsselhälfte k_{Chip} wählen, Response (3-DES) auf Rand2 bilden: K(Rand1,Rand2,k_{Chip}) und senden

Elektrisches Feld
Proximity coupling <=10cm

Rand1

K(Rand1,Rand2,k_{Reader})

K(Rand1,Rand2,k_{Chip})

Leser bildet Schlüssel K (56 Bit) aus MRZ: K=h (PassID,GebD,GültD), aktiviert elektr. Feld und wartet Empfang von Rand1 ab

wählt Zufallszahl Rand2, Schlüsselhälfte k_{Reader} und bildet Response (3-DES) auf Rand1: K (Rand1,Rand2,k_{Reader}) und sendet

Response entschlüsseln, Rand2 prüfen

Alle weitere Kommunikation wird mit (k_{Reader},k_{Chip}) verschlüsselt (3-DES mit CBC)

Machine Readable Zone (MRZ):

```
P<D<<NAME<<VORNAMEN<<<<<<<<<<<<<<<
123456789P<<JJMMDDP<JJMMDDP<<<<<<P
```

Passnummer Geburtsdatum Gültigkeitsdatum
jeweils mit Prüfziffer versehen

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

Aufgabe 1: Zugangs- und Zugriffskontrolle

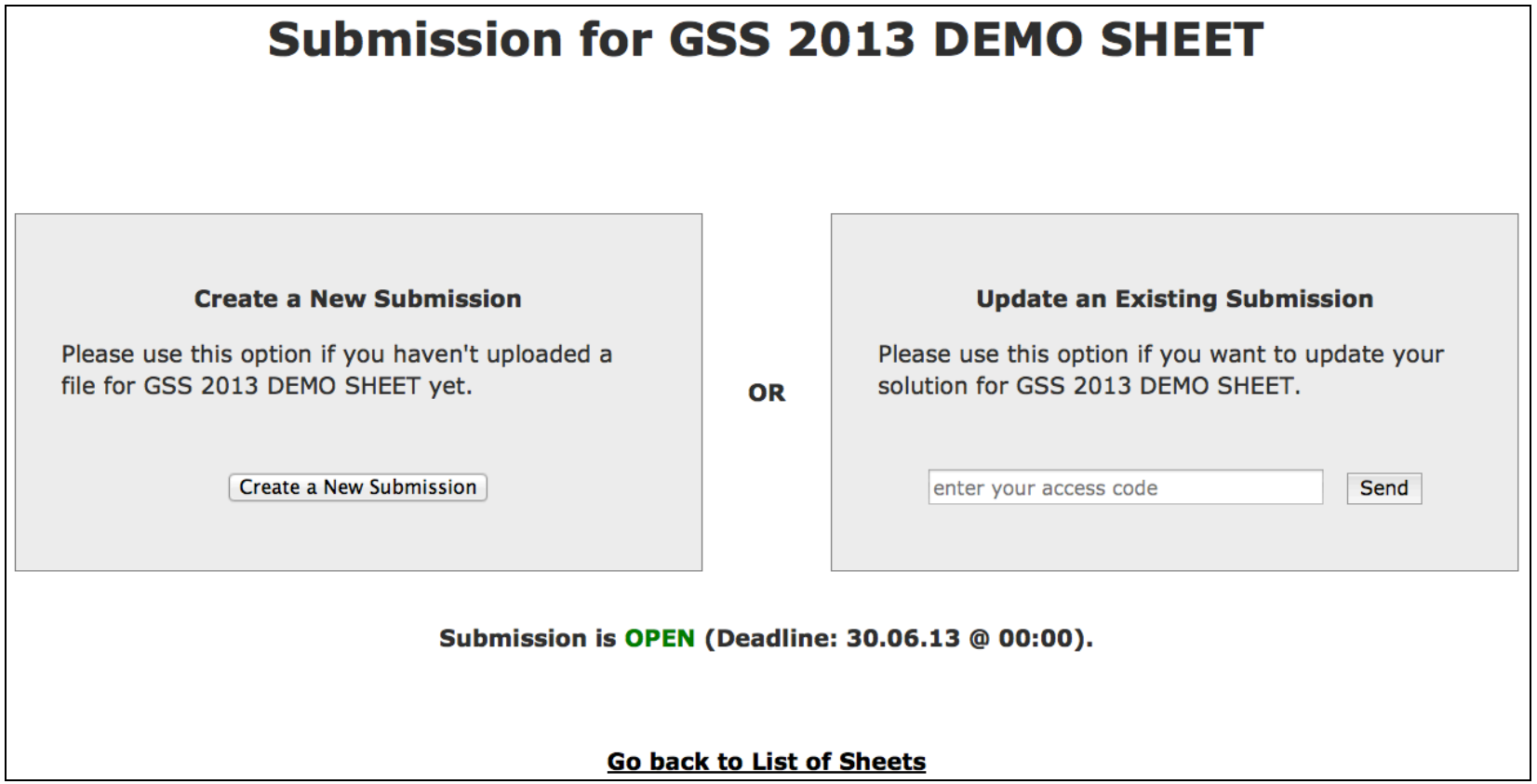
Exkurs: Biometrischer Reisepass

- 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?
- Webserver beantwortet 1000 Anfragen pro Sekunde



Aufgabe 3: Real-World-Brute-Force Angriff

- Zwei Teilprobleme:
  1. Wie viele Codes gibt es insgesamt?
  2. Wie viele Versuche braucht der Angreifer bis zum 1. „Treffer“?

1. Ermittlung Anzahl der möglichen Access-Codes
   - Beispiel-Codes

GSS4-ZGGCJ-Z743P-9PK47-3Z3P3

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

Aufgabe 3: Real-World-Brute-Force Angriff

- Zwei Teilprobleme:
  1. Wie viele Codes gibt es insgesamt?
  2. Wie viele Versuche braucht der Angreifer bis zum 1. „Treffer“?

1. Ermittlung Anzahl der möglichen Access-Codes
   - Beispiel-Codes

GSS4-ZGGCJ-Z743P-9PK47-3Z3P3

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

   - Kommen wirklich alle Großbuchstaben und Ziffern vor?

Aufgabe 3: Real-World-Brute-Force Angriff

- Zwei Teilprobleme:
  1. Wie viele Codes gibt es insgesamt?
  2. Wie viele Versuche braucht der Angreifer bis zum 1. „Treffer“?

1. Ermittlung Anzahl der möglichen Access-Codes

- Beispiel-Codes

GSS4-ZGGCJ-Z743P-9PK47-3Z3P3

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

- 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 ($4{,}24*10^{28}$)

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-W3F9K-NT2EN-3KYSA-EZWH2   => 14 +5       = 19
GSS4-GAK3X-XEY7Z-JH4J4-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:

$S = {}^{27}/_{27} + {}^{27}/_{26} + \ldots + {}^{27}/_{3} + {}^{27}/_{2} + {}^{27}/_{1}$

S = 105,1 Stellen (d.h. 6 Codes)

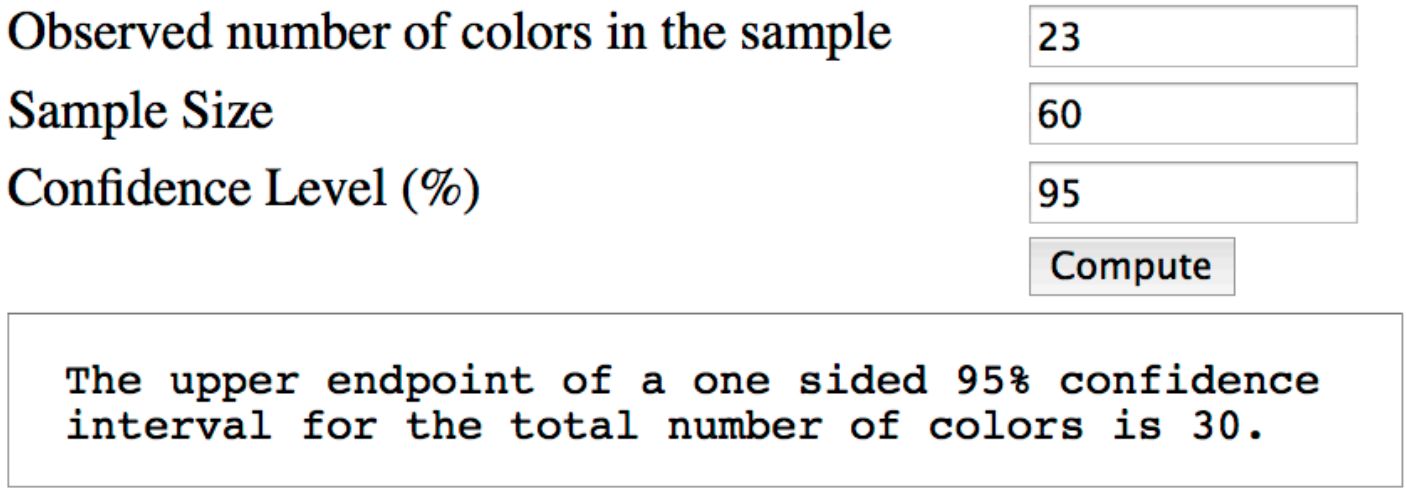
wenn man genaues n nicht kennt:
für n=36 gilt: S=150,3 (8 Codes)

Quelle: J. S. Croucher: **Collecting coupons — A mathematical approach**. *Australian Senior Mathematics Journal 20 (2), 31–35*, 2006.

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!



(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.

Quelle: http://javeeh.net/statapps/Coupon.html

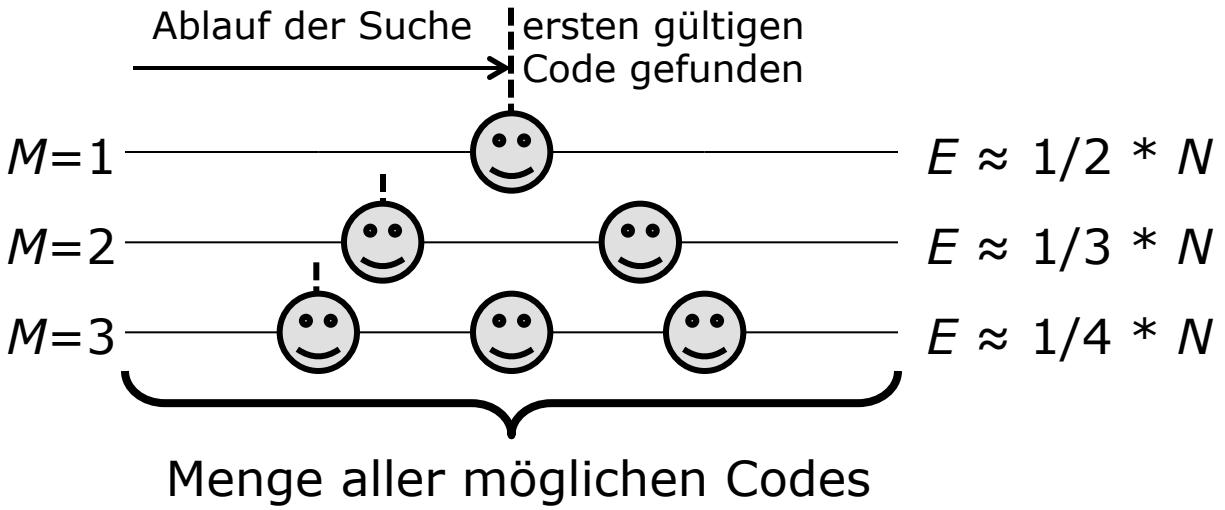
Aufgabe 3: Real-World-Brute-Force Angriff

- Zwei Teilprobleme:
  1. Wie viele Codes gibt es insgesamt? → $N = 27^{20}$
  2. **Wie viele Versuche braucht der Angreifer bis zum 1. „Treffer“?**

- Wenn es **nur einen gültigen Code** gibt
  - Erwartungswert E für Anzahl d. Versuche: $0{,}5 * N = 2{,}12*10^{28}$
  - Aber: Im Submission-Tool sind typischerweise bereits einige Lösungen hinterlegt.
    (Beispiel: ***M*=100 gültige Codes**)

Aufgabe 3: Real-World-Brute-Force Angriff

- Wie viele Versuche braucht der Angreifer 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 → *E* = 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.“