Security - Ziele

Vertraulichkeit

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Vertraulichkeit

- Speicherung der Daten
- Übertragung der Daten
- Lesen von Daten nur durch autorisierte Personen

Maßnahmen

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Vertraulichkeit

- Speicherung der Daten
- Übertragung der Daten
- Lesen von Daten nur durch autorisierte Personen

Maßnahmen

- (symmetrische/asymmetrische) Verschlüsselung von Daten

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Integrität

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Integrität

- keine unbemerkte Manipulation von Daten
- Änderungen an Daten müssen immer nachvollziehbar sein

Maßnahmen

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Integrität

- keine unbemerkte Manipulation von Daten
- Änderungen an Daten müssen immer nachvollziehbar sein

Maßnahmen

- Hashverfahren (u.a. Prüfsummen)

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Authentizität

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Authentizität

- Echtheit, Überprüfbarkeit
- Hier: Datenursprung, Sender

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Authentizität

- Echtheit, Überprüfbarkeit
- Hier: Datenursprung, Sender

Verbindlichkeit (non repudiation)

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Authentizität

- Echtheit, Überprüfbarkeit
- Hier: Datenursprung, Sender

Verbindlichkeit (non repudiation)

- „Unabstreitbarkeit“ einer Nachricht
- Bsp. Abschluss eines (Kauf)-Vertrages

Maßnahmen

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Security - Ziele

Authentizität

- Echtheit, Überprüfbarkeit
- Hier: Datenursprung, Sender

Verbindlichkeit (non repudiation)

- „Unabstreitbarkeit“ einer Nachricht
- Bsp. Abschluss eines (Kauf)-Vertrages

Maßnahmen

- digitale Signatur (z.B. Updates, Pakete aus Paketquellen)

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>
Institut für Informatik

Krypt. Hashfunktion

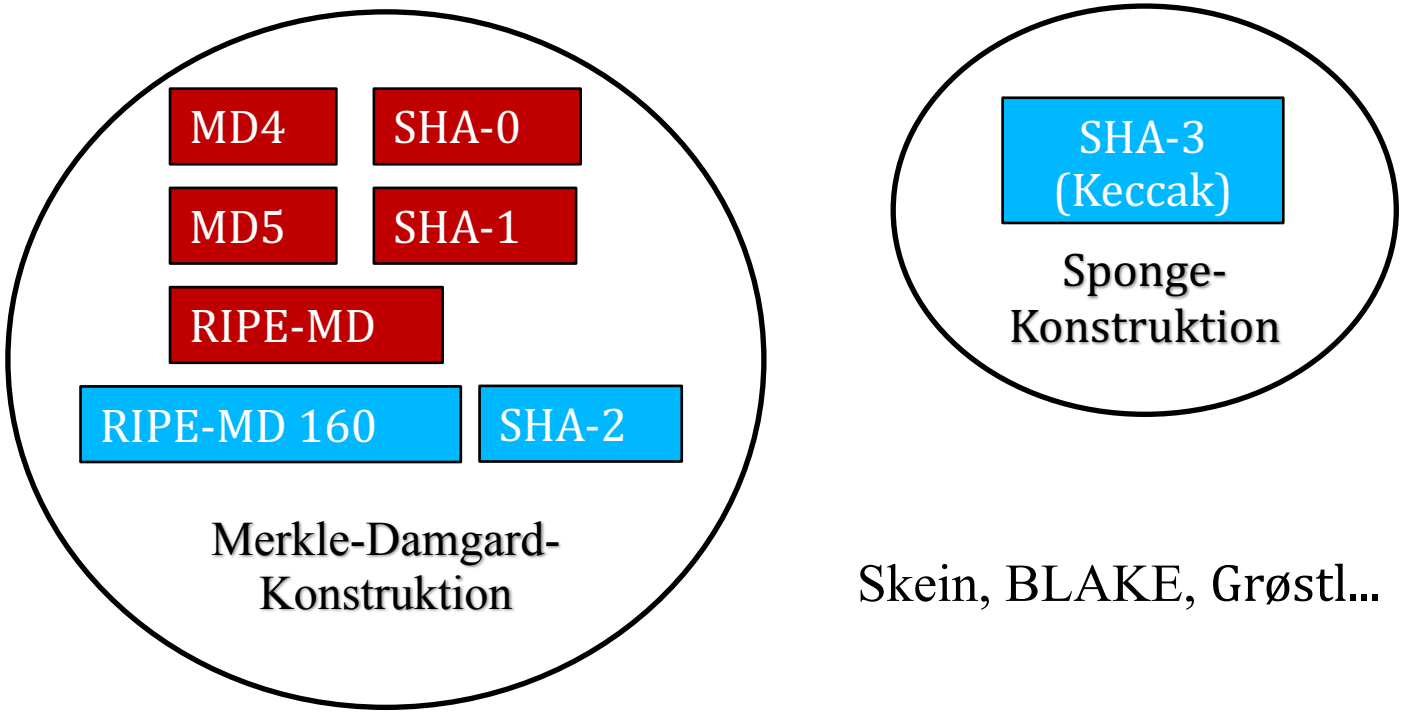
HASHEN != VERSCHLÜSSELN

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

HASHEN != VERSCHLÜSSELN



Skein, BLAKE, Grøstl...

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>
Institut für Informatik

Krypt. Hashfunktion

$$h: \{0,1\}^m \rightarrow \{0,1\}^n \; mit \; m \geq n$$

Eigenschaften

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

$$h: \{0,1\}^m \rightarrow \{0,1\}^n \; mit \; m \geq n$$

Eigenschaften

- **Einwegfunktion** $y = f(x)$ „$einfach$“, $f^{-1}(y) = x$ „$schwer$“

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

$$h: \{0,1\}^m \rightarrow \{0,1\}^n \; mit \; m \geq n$$

Eigenschaften

- **Einwegfunktion** $y = f(x)$ „$einfach$“, $f^{-1}(y) = x$ „$schwer$“
- **nicht injektiv → Kollisionen möglich aber unerwünscht (Kollisionsresistenz)**

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>
Institut für Informatik

Krypt. Hashfunktion

$$h: \{0,1\}^m \rightarrow \{0,1\}^n \; mit \; m \geq n$$

Eigenschaften

- **Einwegfunktion** $y = f(x)$ „$einfach$“, $f^{-1}(y) = x$ „$schwer$“
- **nicht injektiv → Kollisionen möglich aber unerwünscht (Kollisionsresistenz)**
  - **Schwache Kollisionsresistenz → finde kein x' zu x mit $h(x) = h(x')$**
  - **Starke Kollisionsresistenz → finde keine x, x' mit $h(x) = h(x')$**

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

$$h: \{0,1\}^m \rightarrow \{0,1\}^n \; mit \; m \geq n$$

Eigenschaften

- **Einwegfunktion** $y = f(x)$ „$einfach$“, $f^{-1}(y) = x$ „$schwer$“
- **nicht injektiv → Kollisionen möglich aber unerwünscht (Kollisionsresistenz)**
- **(wünschenswert) surjektiv** $\forall y \in Y \; \exists x \in X: f(x) = y$

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

$$h: \{0,1\}^m \rightarrow \{0,1\}^n \; mit \; m \geq n$$

Eigenschaften

- **Einwegfunktion** $y = f(x)$ „$einfach$“, $f^{-1}(y) = x$ „$schwer$“
- **nicht injektiv → Kollisionen möglich aber unerwünscht (Kollisionsresistenz)**
- **(wünschenswert) surjektiv** $\forall y \in Y \; \exists x \in X: f(x) = y$
- **Effizienz**

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

$$h: \{0,1\}^m \rightarrow \{0,1\}^n \; mit \; m \geq n$$

Eigenschaften

- **Einwegfunktion** $y = f(x)$ „$einfach$“, $f^{-1}(y) = x$ „$schwer$“
- **nicht injektiv → Kollisionen möglich aber unerwünscht (Kollisionsresistenz)**
- **(wünschenswert) surjektiv** $\forall y \in Y \; \exists x \in X: f(x) = y$
- **Effizienz**
- **Lawineneffekt/Chaoseffekt**

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

Geburtstagsparadox

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

Geburtstagsparadox

$p(n)$ → Wahrscheinlichkeit dafür, dass mind. 2 Personen am gleichen Tag Geburtstag haben.

$q(n)$ → Wahrscheinlichkeit dafür, dass mind. 2 Personen an einem bestimmten gleichen Tag Geburtstag haben.

Wie muss groß muss n sein,

damit $p, q > 0.5$?

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

Geburtstagsparadox

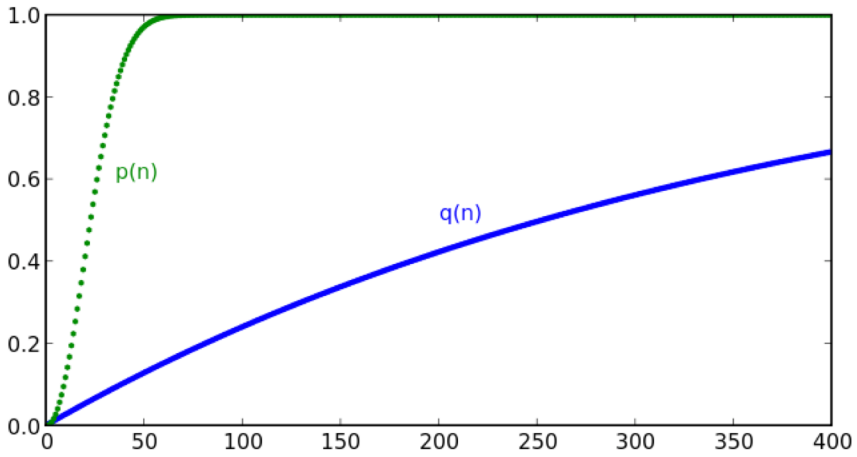
$p(n)$ → Wahrscheinlichkeit dafür, dass mind. 2 Personen am gleichen Tag Geburtstag haben.

Anm. (JT): Falsch, hier müsste stehen, dass eine Person an einem gegebenen Tag Geburtstag hat.

$q(n)$ → Wahrscheinlichkeit dafür, dass mind. 2 Personen an einem bestimmten gleichen Tag Geburtstag haben.

Wie muss groß muss n sein,

damit $p, q > 0.5$?



Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

Geburtstagsparadox

$p(n)$ → Wahrscheinlichkeit dafür, dass mind. 2 Personen am gleichen Tag Geburtstag haben.

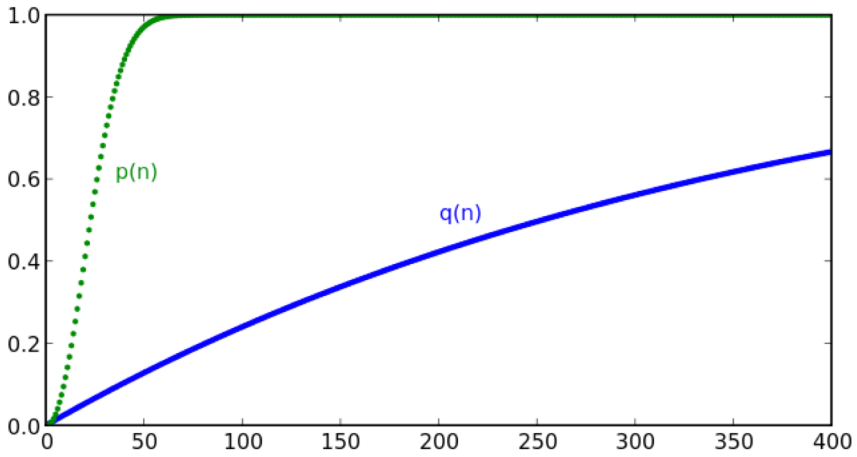
n = 23

$q(n)$ → Wahrscheinlichkeit dafür, dass mind. 2 Personen an einem bestimmten gleichen Tag Geburtstag haben.

n = 253

Wie muss groß muss n sein,

damit $p, q > 0.5$?



Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>

Institut für Informatik

Krypt. Hashfunktion

Verwendung

- **(nicht krypto.) Hashmaps/Hashtabellen**
- **(nicht zwangsläufig krypto.) Prüfsummen**
- **Signieren von Nachrichten, Nachrichten-Headern**
- **Integritätsprüfung**
- **Passwörter hashen**
- **Pseudozufallsgeneratoren**

Jonas Treumer <treumer@tu-freiberg.de>
Ben Lorenz <lorenzb@tu-freiberg.de>
Institut für Informatik