



Security - Ziele

Vertraulichkeit



Security - Ziele

Vertraulichkeit

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

Maßnahmen



Security - Ziele

Vertraulichkeit

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

Maßnahmen

- (symmetrische/asymmetrische) **Verschlüsselung** von Daten





Security - Ziele

Integrität



Security - Ziele

Integrität

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

Maßnahmen



Security - Ziele

Integrität

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

Maßnahmen

- **Hash**verfahren (u.a. Prüfsummen)





Security - Ziele

Authentizität



Security - Ziele

Authentizität

- Echtheit, Überprüfbarkeit
- Hier: Datenursprung, Sender



Security - Ziele

Authentizität

- Echtheit, Überprüfbarkeit
- Hier: Datenursprung, Sender

Verbindlichkeit (non repudiation)



Security - Ziele



Authentizität

- Echtheit, Überprüfbarkeit
- Hier: Datenursprung, Sender

Verbindlichkeit (non repudiation)

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

Maßnahmen

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)

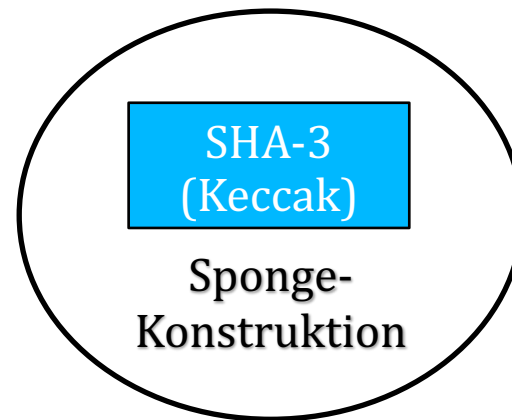
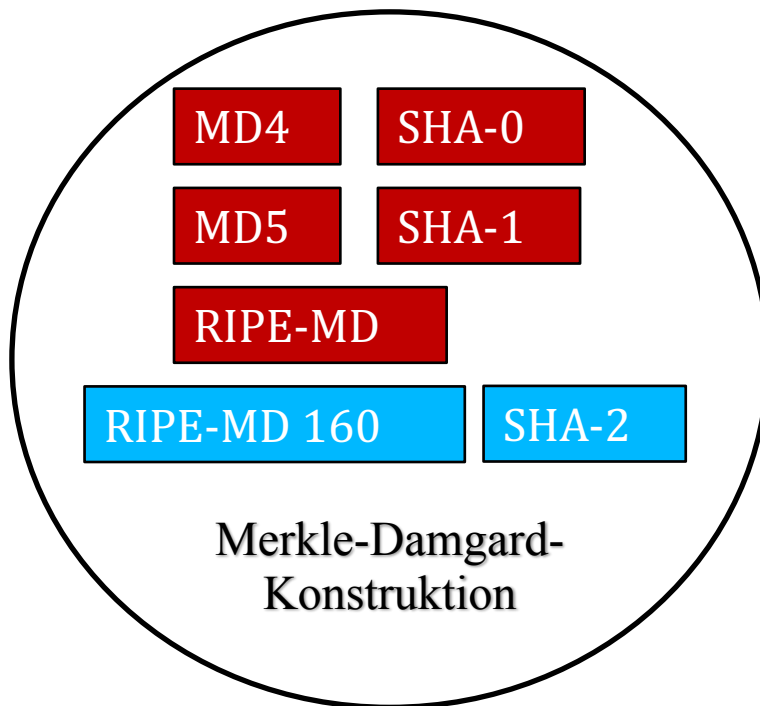


Krypt. Hashfunktion

HASHEN != VERSCHLÜSSELN

Krypt. Hashfunktion

HASHEN != VERSCHLÜSSELN



Skein, BLAKE, Grøstl...

Krypt. Hashfunktion

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

Eigenschaften

Krypt. Hashfunktion

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

Eigenschaften

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

Krypt. Hashfunktion

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

Eigenschaften

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

Krypt. Hashfunktion

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

Eigenschaften

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

Krypt. Hashfunktion

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

Eigenschaften

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

Krypt. Hashfunktion

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

Eigenschaften

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

Krypt. Hashfunktion

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

Eigenschaften

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



Krypt. Hashfunktion

Geburtstagsparadox

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 $p, q > 0.5$?

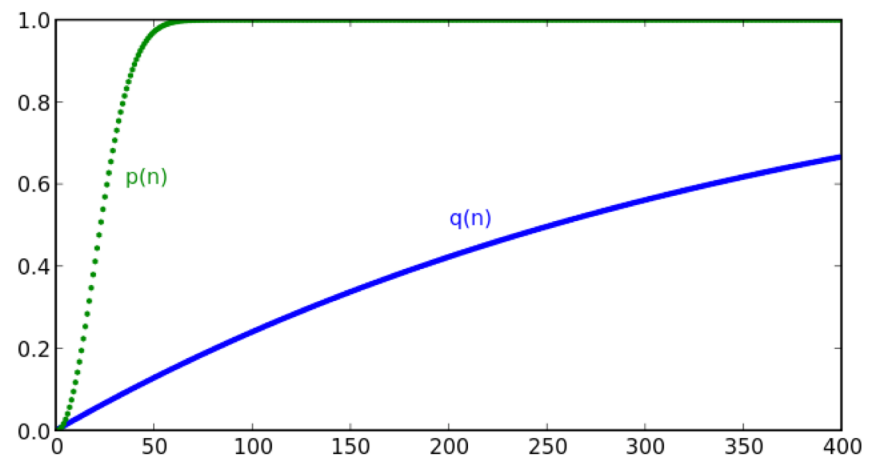
Krypt. Hashfunktion

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 $p, q > 0.5$?



Krypt. Hashfunktion

Geburtstagsparadox

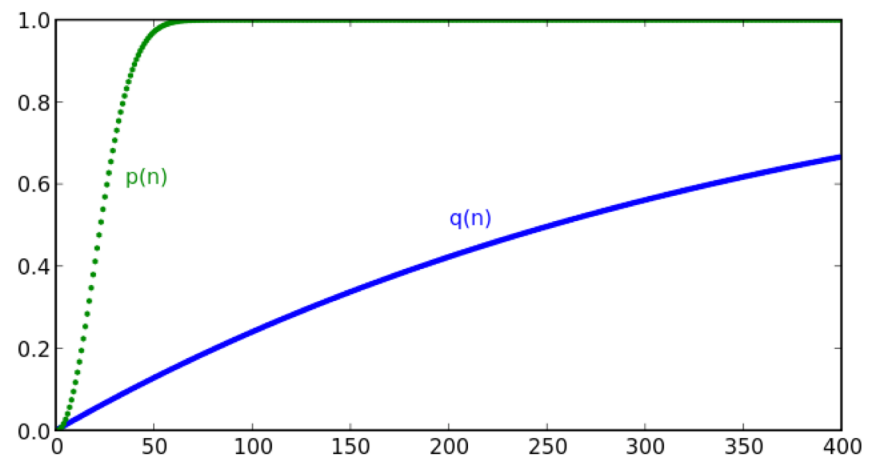
$p(n)$ → Wahrscheinlichkeit dafür, dass mind. 2 Personen am gleichen Tag Geburtstag haben.

$$n = 23$$

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

$$n = 253$$

Wie muss groß muss n sein,
damit $p, q > 0.5$?



Krypt. Hashfunktion

Verwendung

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