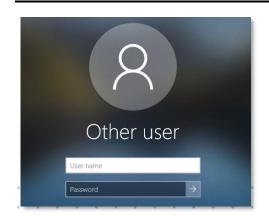
### 1.5.1 Kryptokonzepte

Datum:

Martin-Segitz-Schule ITT 10



BitLocker

Enter the password to unlock this drive

Press the Insert key to see the password as you type.

Kennwortschutz

kontrolliert den Zugriff auf das Benutzerkonto

Datenträgerschutz

Verschlüsselt alle Daten im Datenträger

**Grundprinzip von Hashfunktionen** 

heue Pin 2 Mashwert Speichern des Hashwerts

9635 Mashfunklim: 23

Pin angeben 23-23?

13=23? V Fehler: Kollision

Anforderung an Hashfunktionen:

- man kann Hashwert nicht zu Que West zurückrechnen

-Kollisionsresistena: gleicher Input führt stets zu anzigartigen, selben

- unabhangig von Eingangswert, hat der Hosh eine Aste lange

## 1.5.1 Kryptokonzepte

Datum:

Martin-Segitz-Schule ITT 10

# Unterschied zwischen Hashen und Verschlüsseln

shwert = Imput + Hashfunkt. Chiffie = Imput + Versell. Fiel. + Sellis

Bsp: - Pru summe - Datenverschlüsselung (Permanent speicher Checkesumme - Washmap - Westbagung nuerschlüsselung (WLAN)
- dizitale Signaturen

CIA: Starkt die Integrität von Daten Stärkt die Vertranlich Keit von Daten

#### Wie lassen sich Hashwerte knacken?

Rainbow-Table: fertige DB von bereits gehashten Input
- Brute Force (rohe Gewalt): reden Input ausproberen
- Dictionary: die 1000 - beliebtesten "PCJ

## Passwortkomplexität

Wie viele verschiedene Zahlen kann man mit dem jeweiligen Zahlensystem bei 8 Stellen bilden?

Dezimalsystem	Binärsystem	Hexadezimalsystem
108	2*	161

Wie viele Kombinationen gibt bei 8 Stellen und folgenden Situationen?

a-z	a-z, A-Z, 0-9	
26 <sup>8</sup>	62°	