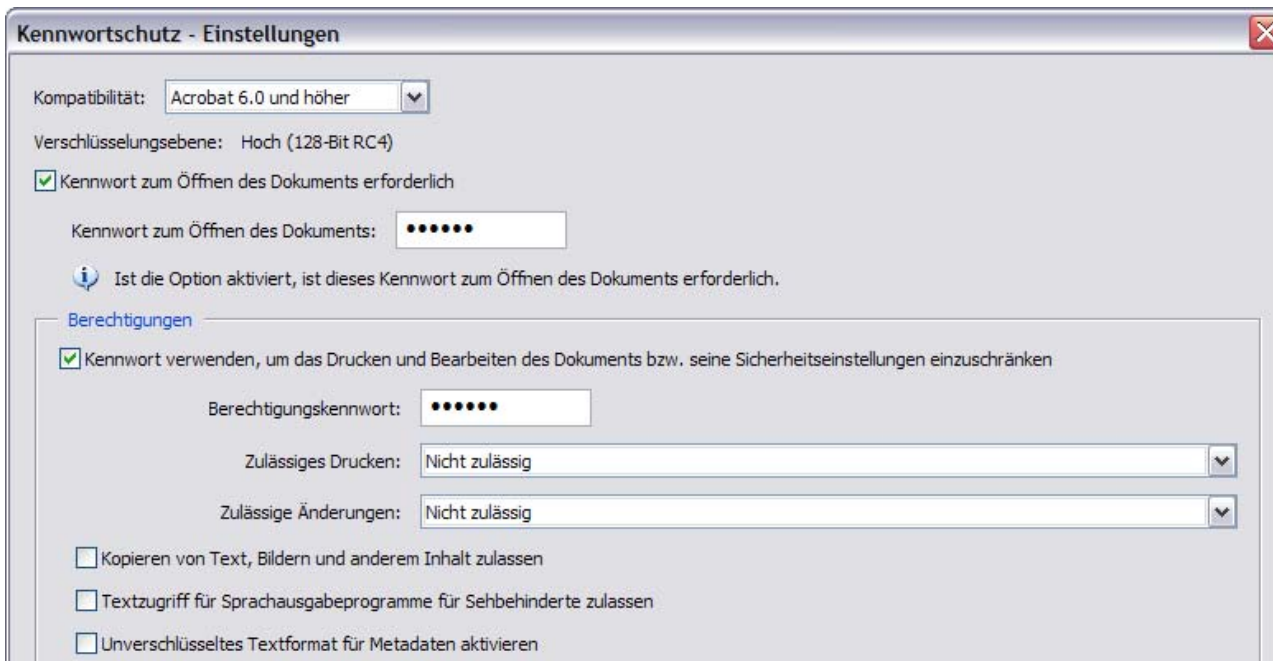


Sicherheit von PDF-Dateien



Berechtigungen/Nutzungsbeschränkungen zum

- Drucken
- Kopieren und Ändern von Inhalt bzw. des Dokumentes
- Auswählen von Text/Grafik
- Hinzufügen/Ändern von Anmerkungen und Formularfeldern




Kennwortschutz - Einstellungen

Kompatibilität: Acrobat 6.0 und höher

Verschlüsselungsebene: Hoch (128-Bit RC4)

Kennwort zum Öffnen des Dokuments erforderlich

Kennwort zum Öffnen des Dokuments:

 Ist die Option aktiviert, ist dieses Kennwort zum Öffnen des Dokuments erforderlich.

Berechtigungen

Kennwort verwenden, um das Drucken und Bearbeiten des Dokuments bzw. seine Sicherheitseinstellungen einzuschränken

Berechtigungskennwort:

Zulässiges Drucken: Nicht zulässig

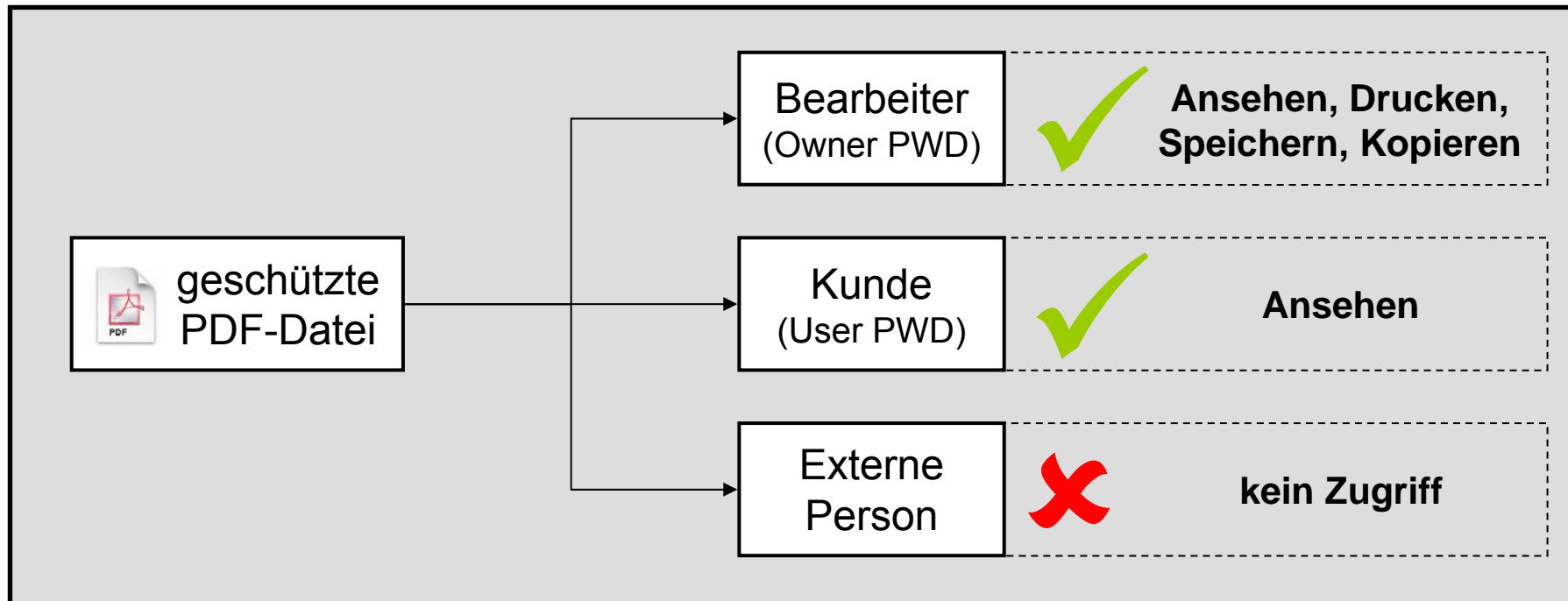
Zulässige Änderungen: Nicht zulässig

Kopieren von Text, Bildern und anderem Inhalt zulassen

Textzugriff für Sprachausgabeprogramme für Sehbehinderte zulassen

Unverschlüsseltes Textformat für Metadaten aktivieren

Berechtigungen/Nutzungsbeschränkungen



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Schlüssel/Key

- Passwörter in Acrobat max. 32 Zeichen
- Key wird über Hash-Funktion erstellt
 - ⇒ lautet bei Acrobat: *Encryption Key*
- Länge in Bit
 - ⇒ $128 \text{ Bit} = 2^{128} \approx 3.4 \times 10^{38}$ (ab Acrobat 5.0, vorher: 40 Bit)
 - ⇒ **34028236692093846346337460743176821100**



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Schlüssel/Key

- Faustregel:

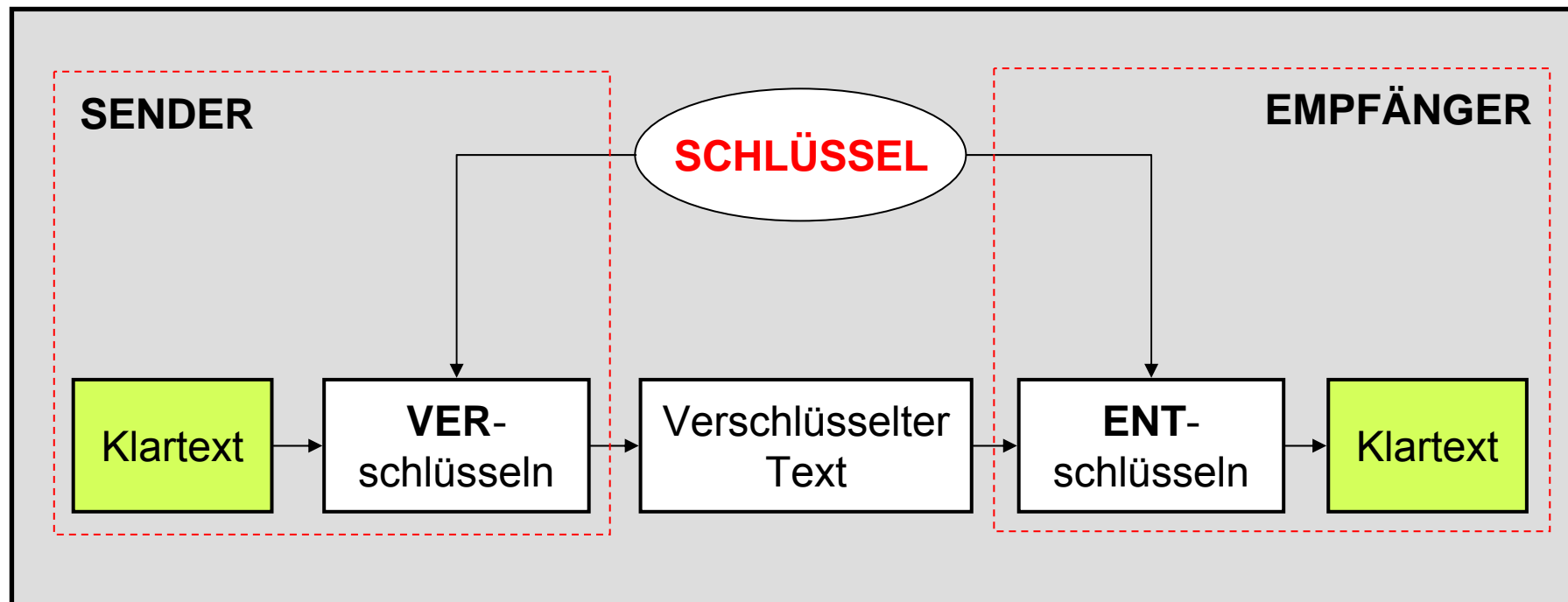
- ⇒ Verlängerung Schlüssel um 1 Bit

- ⇒ Verdoppelung der Resistenz gegen Angriffe mittels Ausprobieren



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Symmetrische Verschlüsselung



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Symmetrische Verschlüsselung

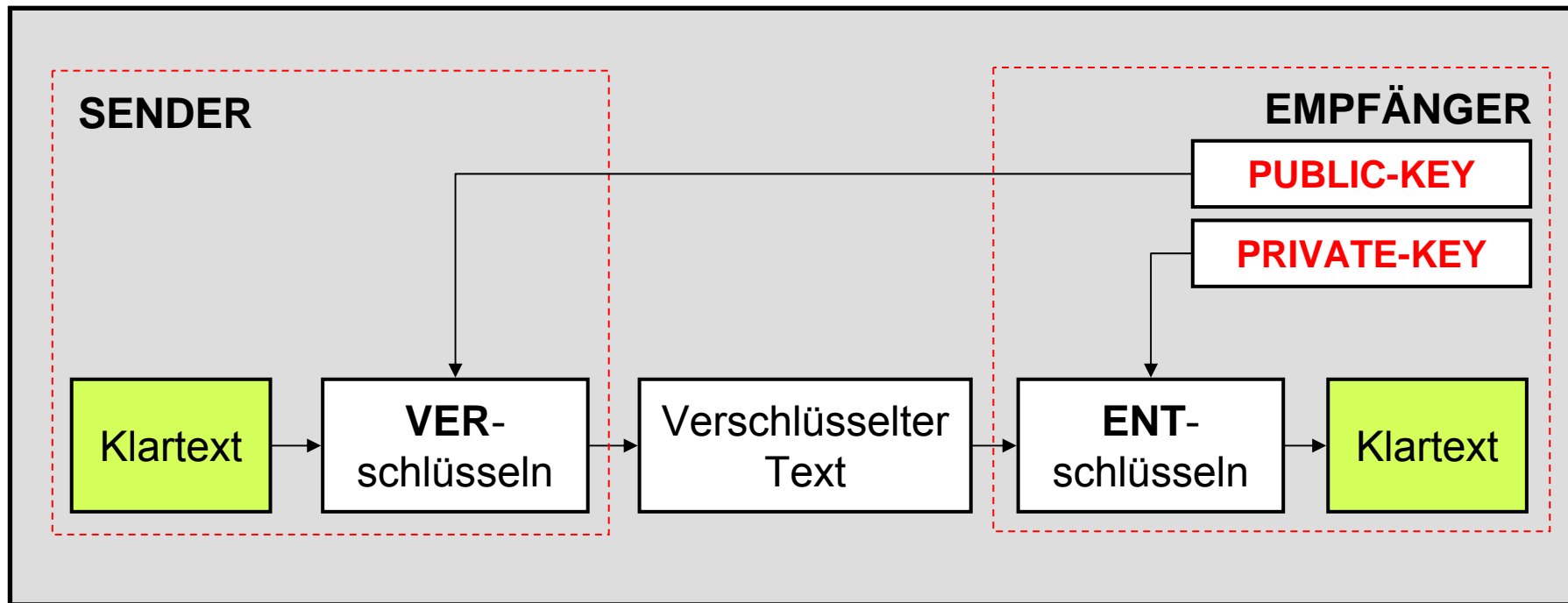
- Erzeugen von zwei etwa gleich langer Primzahlen p und q
- Multiplizieren von p und q , man erhält das Produkt N
- Anwenden der Euler-Funktion $\varphi(N)$ ($= (p-1) \cdot (q-1)$) auf N
- Berechnen von e und d (teilerfremd zu $\varphi(N)$)
- e und N werden zum Verschlüsseln benutzt
- d und $\varphi(N)$ werden zum Entschlüsseln benutzt
- Eine „Rückrechnung“ kann nicht über die gleiche Variable stattfinden (liegt an der benutzten Mathematik)

SCHLÜSSEL	p und q	N	$\varphi(N)$	e	d
-----------	-------------	-----	--------------	-----	-----



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Asymmetrische Verschlüsselung



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Symmetrische Verschlüsselung

SCHLÜSSEL	p und q	N	$\varphi(N)$	e	d
-----------	-------------	-----	--------------	-----	-----

Asymmetrische Verschlüsselung

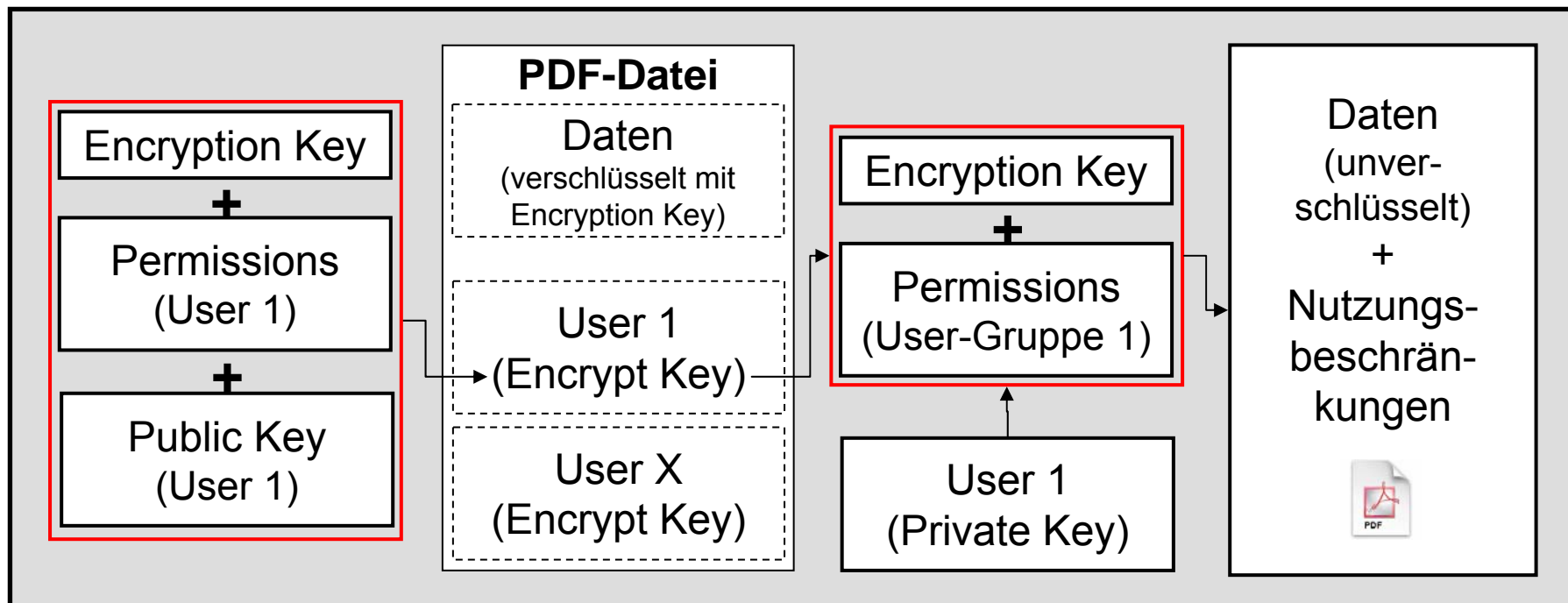
PUBLIC KEY	p und q	N	e
------------	-------------	-----	-----

PRIVATE KEY	p und q	(N)	$\varphi(N)$	d
-------------	-------------	-------	--------------	-----



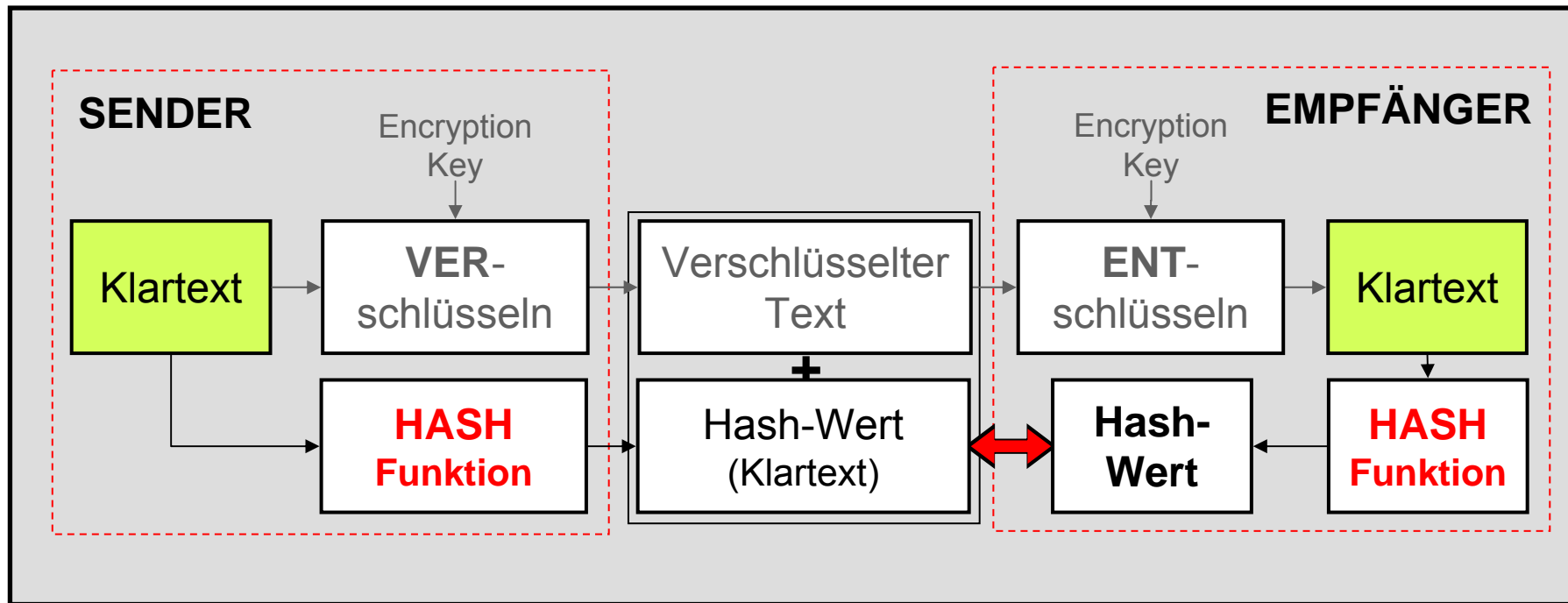
VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Einsatz von asymmetrischer Verschlüsselung: Self-Sign Sicherheit



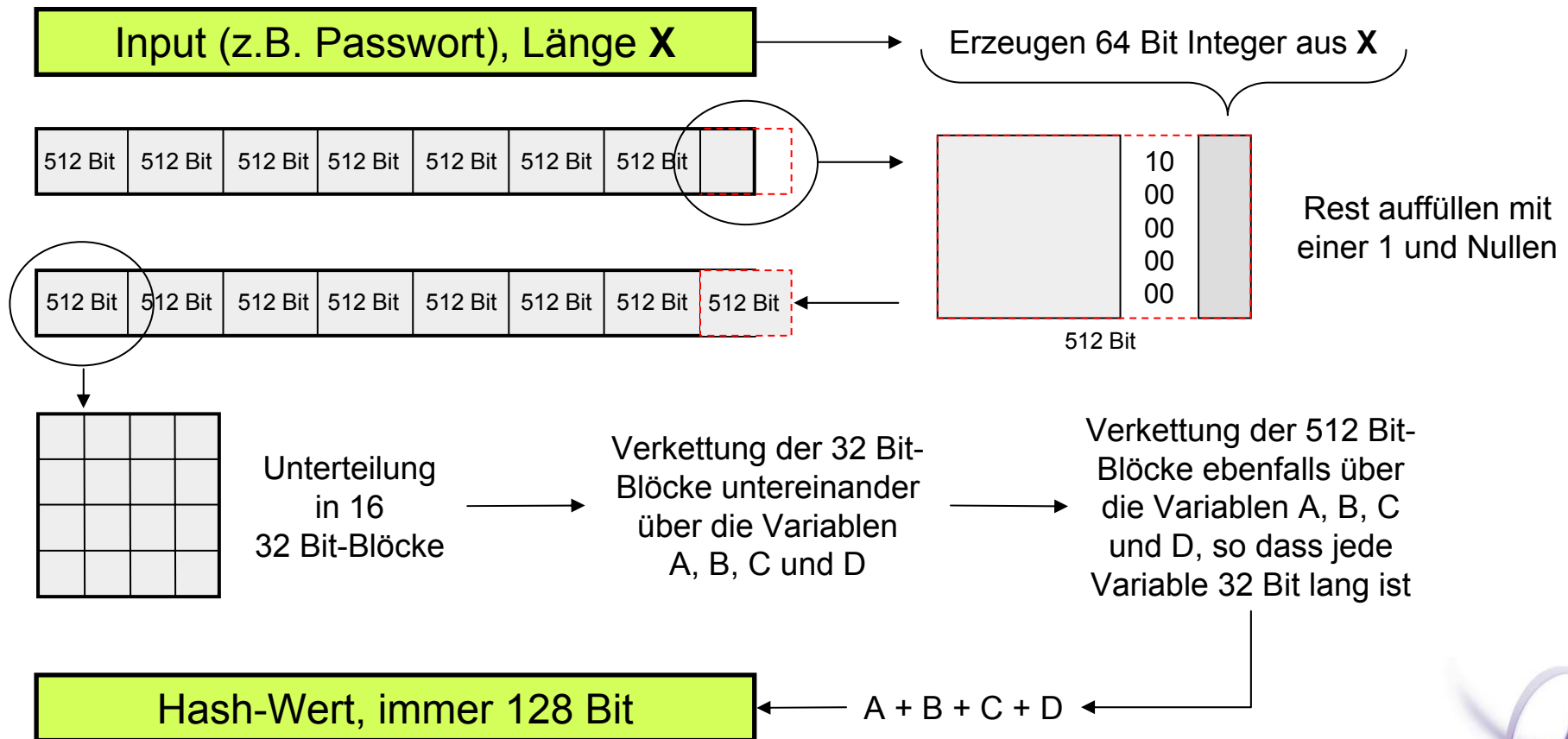
VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Die Hash-Funktion als Überprüfungsmechanismus



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Hash-Funktion (MD5 - Message Digest Algorithm 5)



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Erzeugung Hash-Wert

Die Erzeugung eines Hash-Wertes zeigt folgendes Beispiel:

Eingabe von: **PDFst@r2005!** erzeugt den
⇒ Hash-Wert: **8d4d753354e3d51aa43a2af82b2e6283**

Eingabe von: **PDFstar2005!** erzeugt den
⇒ Hash-Wert: **541c44a16895c4be2fb43073533df57f**



VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

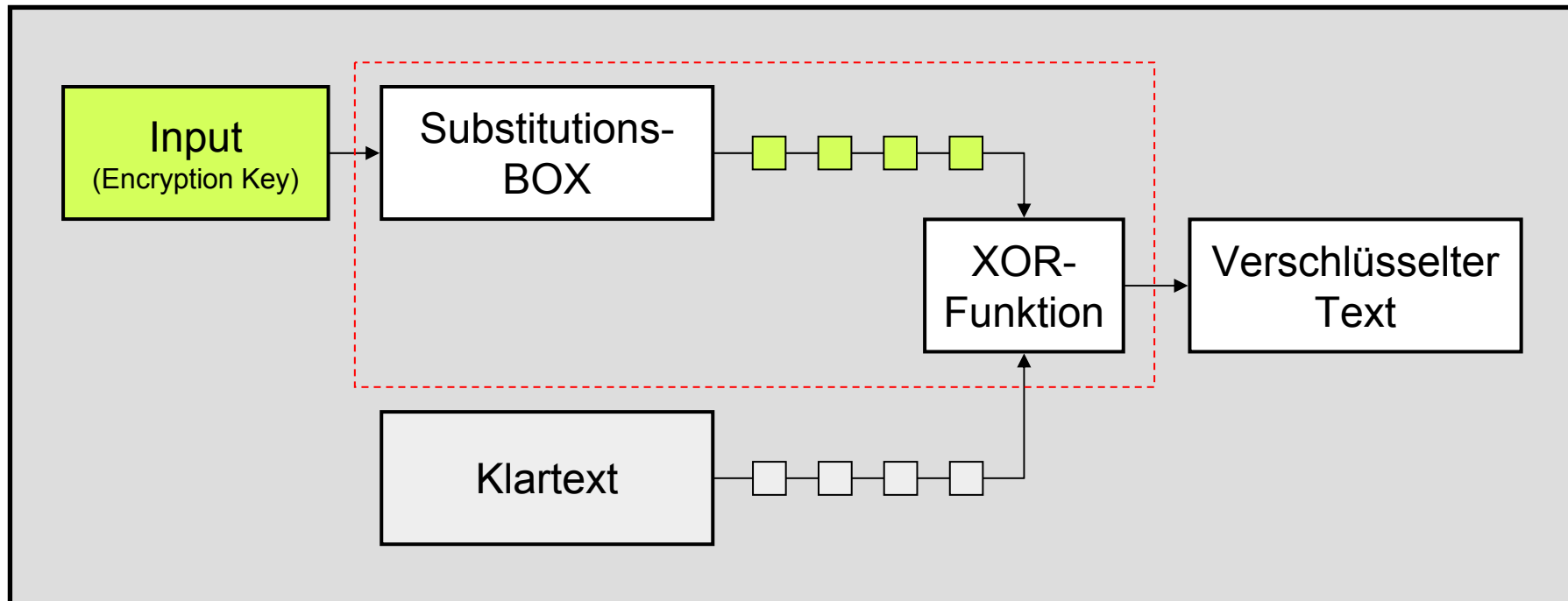
Wird eine PDF-Datei komplett verschlüsselt?

- nur der Inhalt von Strings (Text) und Streams (z.B. JPEG-Datenstrom), nicht aber die Objektverwaltung
 - ⇒ schnellen Zugriff auf Teile einer Datei, ohne erst die gesamte Datei entschlüsseln zu müssen
 - ⇒ Dokumenteninformationen/Lesezeichen werden kodiert
 - ⇒ Objekt- und Generationsnummer, sowie Berechtigungen gehen in eine Verschlüsselung mit ein



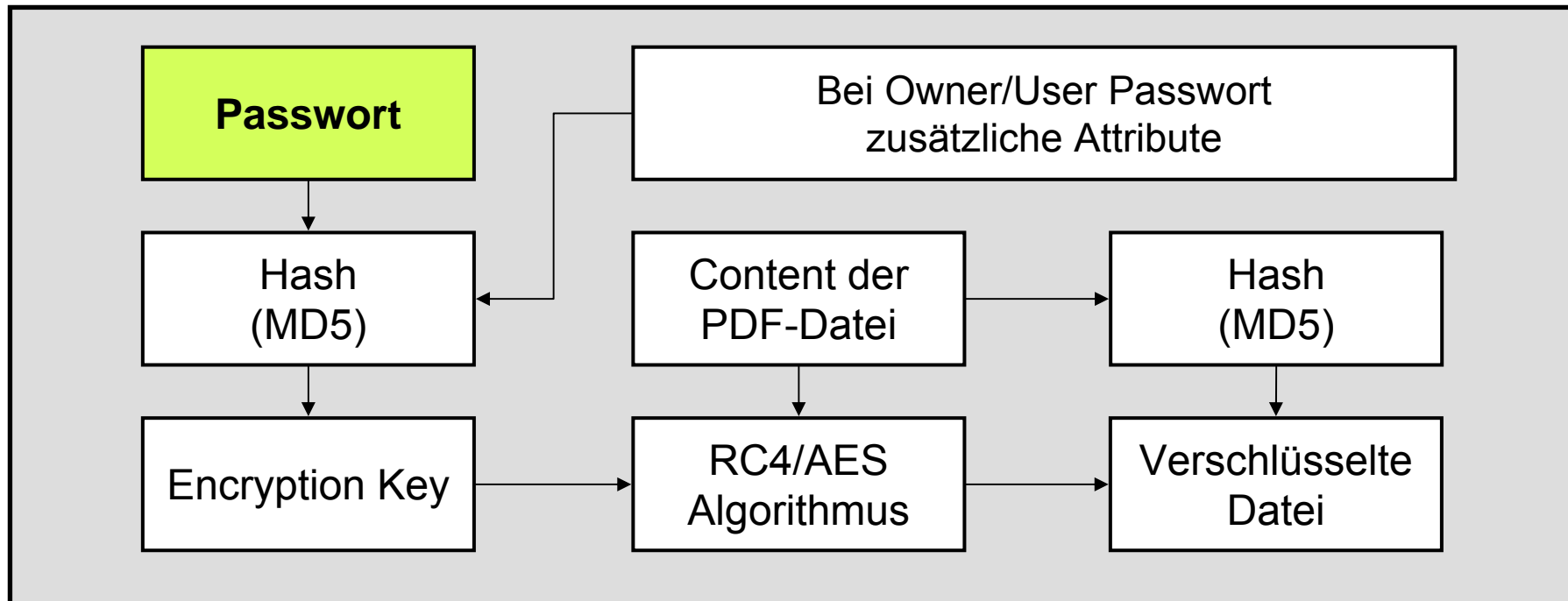
VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

RC4/AES Verschlüsselungsalgorithmus



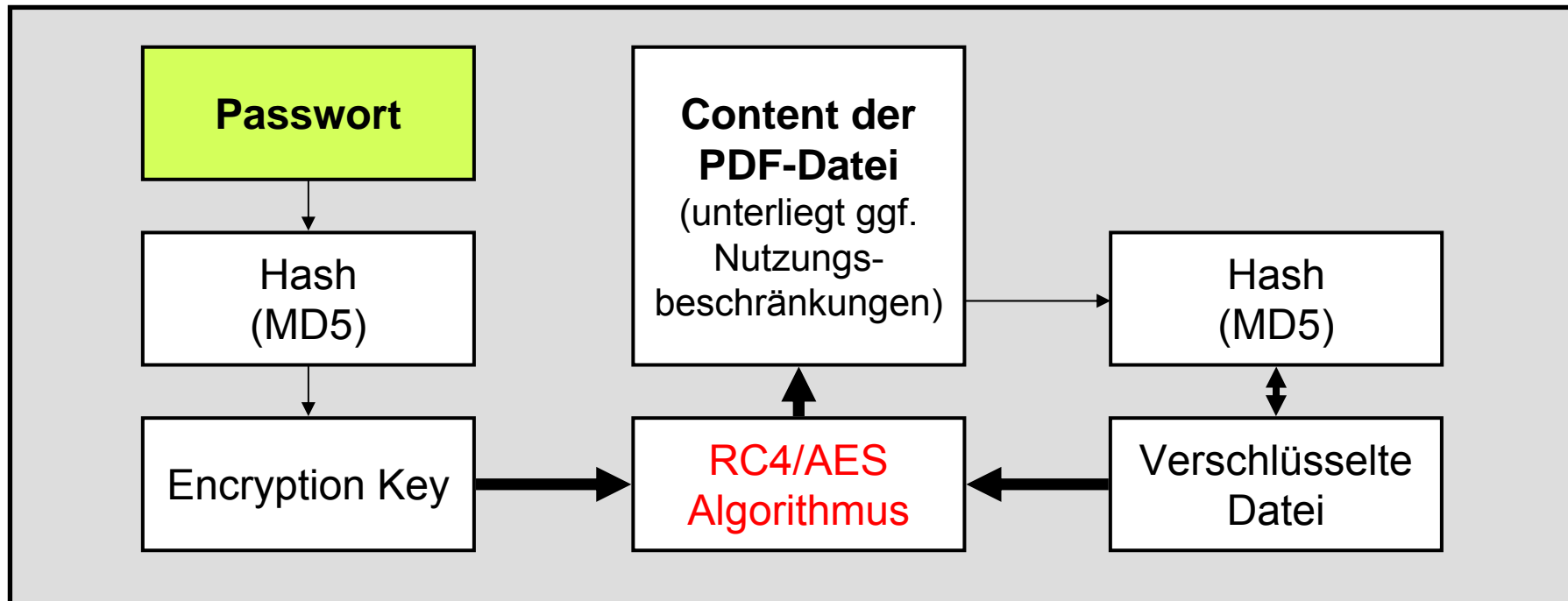
STANDARD SECURITY HANDLER

Verschlüsselung



STANDARD SECURITY HANDLER

Entschlüsselung



SECURITY HANDLER

Security Handler

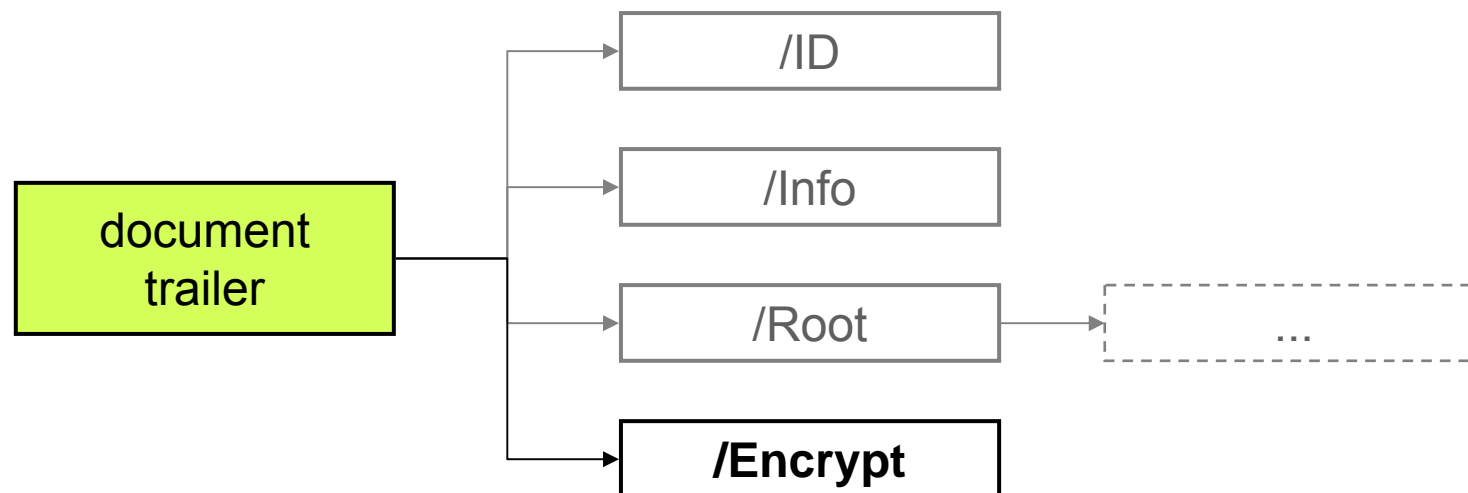
1. Entgegennahme/Abfrage eines Passwortes (User/Owner)
2. Umrechnen des Passwortes (Aufruf Hash-Funktion) in Encryption Key
3. RC4-/AES-Vorgang starten
4. Hash-Wert von Content erzeugen/mit gespeichertem Wert vergleichen



EINBETTUNG DER VERSCHLÜSSELUNG

Encryption

- ***/Encrypt*** steht im document trailer
 - ⇒ dazu gehört das Encryption Dictionary
 - ⇒ kein *Encrypt*, keine Verschlüsselung



EINBETTUNG DER VERSCHLÜSSELUNG

Standard Security Encryption Dictionary

- **Filter/SubFilter**: geben an, welcher Ver-/Entschlüsselungsmechanismus (Security Handler) benutzt wird
⇒ ab PDF 1.3 zur Unterstützung Public-Key-Infrastruktur (PKI)
- **V (Version)**: 0 bis 4, gibt an, auf welche Weise RC4 für die Verschlüsselung verwendet wird (Standard ist 3: 40-128 Bit)
- **Length**: Länge des Schlüssels (in Bit) als Vielfaches von 8, Default: 128
- **P (Permissions)**: Nutzungsbeschränkungen (32-stellige Binärzahl, jede Stelle hat bestimmte Bedeutung, wird als Dezimalzahl ausgegeben)
- **O und U**: Hash-Wert von Owner- und User-Passwort
- **EncryptMetadata** (true/false): Metadata-Informationen sind kodiert
Default: true, nur bei $V < 4$



EINBETTUNG DER VERSCHLÜSSELUNG

Beispiel

```
trailer                                % Trailer dictionary
<<
  /Size 95                             % Anzahl der Objekte in der Datei
  /Root 93 0 R                          % Der Dokumentenbaum hat die object ID 93
  /Encrypt 94 0 R                       % Das Encryption Dictionary hat die object ID 94
>>

94 0 obj                               % Encryption dictionary
<<
  /Filter /Standard                    % Standard Security Handler wird benutzt
  /R 3                                  % Revision 3 des Security Handlers
  /V 4                                  % Anwendung des RC4-Algorithmus (Variante 4)
  /Length 128                          % Länge des Encryption Key, hier 128 Bit
  /O (xxx...xxx)                       % Hashed Owner Password (32 byte)
  /U (xxx...xxx)                       % Hashed User Password (32 byte)
  /P 65472                              % Permissions als Dezimalzahl
>> endobj
```



ADVANCED PDF PASSWORD RECOVERY (APDFPR)

Funktion

- PDF-Dateien entschlüsseln, die mit User/Owner-Passwort geschützt sind
- Angriffsziel: Encryption Key
 - ⇒ Brute-Force (Werte generieren, hashen und vergleichen)
 - ⇒ Dictionary Attack (Einträge aus Wörterbüchern werden durchprobiert)

Anwendungsgebiet/ Beschränkungen

- APDFPR kann nur die Standardsicherheit von Acrobat verarbeiten
- 40 Bit-Verschlüsselung lässt sich knacken, 128 Bit-Verschlüsselung nicht
- Einige Dateien, die mit Acrobat 6.0 erstellt worden sind können nicht verarbeitet werden (ab PDF 1.5)



QUALITÄT DER ACROBAT-VERSCHLÜSSELUNG

- abhängig von der Qualität des Passwortes und
- Länge des Schlüssels (ab Acrobat 5.0: 128 Bit Standard, vorher: 40 Bit)
 - ⇒ Probleme bei Abwärtskompatibilität
 - ⇒ Angriffsziel für APDFPR
- Einhaltung der Nutzungsbeschränkungen
 - ⇒ lediglich der PDF-Viewer soll Funktionen deaktivieren
- Schutz vor erneutem Distillieren



ACROBAT IST SICHER, wenn...

- ...Passwort „sicher“ gewählt und geheim gehalten wird
- ...die Verschlüsselung mit 128 Bit erfolgt

- große Unternehmen: Public-Key-Infrastruktur
 - ⇒ LifeCycle Document Security

