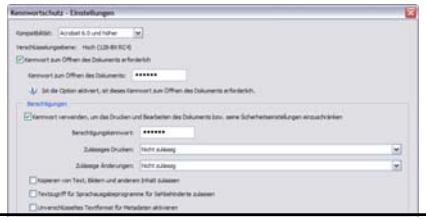
Sicherheit von PDF-Dateien

27.10.2005
Albrecht-Dürer-Schule,
Düsseldorf

SICHERHEIT VON PDF-DATEIEN

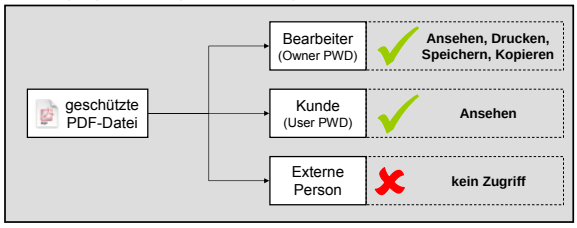
Berechtigungen/Nutzungsbeschränkungen zum

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



SICHERHEIT VON PDF-DATEIEN

Berechtigungen/Nutzungsbeschränkungen



SICHERHEIT VON PDF-DATEIEN

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 Bit = $2^{128} \approx 3.4 \times 10^{38}$ (ab Acrobat 5.0, vorher: 40 Bit)
⇨ **340282366920938463463374607431768211100**

SICHERHEIT VON PDF-DATEIEN

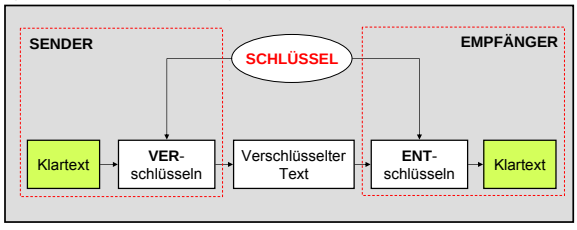
VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Schlüssel/Key
• Faustregel:
⇨ Verlängerung Schlüssel um 1 Bit
⇨ Verdoppelung der Resistenz gegen Angriffe mittels Ausprobieren

SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Symmetrische Verschlüsselung



SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Symmetrische Verschlüsselung

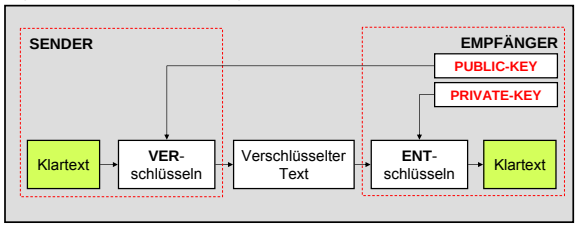
- Erzeugen von zwei etwa gleich langer Primzahlen ***p*** und ***q***
- Multiplizieren von ***p*** und ***q***, man erhält das Produkt ***N***
- Anwenden der Euler-Funktion ***φ(N)*** (= *(p-1)* • *(q-1)*) auf ***N***
- Berechnen von ***e*** und ***d*** (teilerfremd zu ***φ(N)***)
- ***e*** und ***N***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

SCHLÜSSEL	*p* und *q*	*N*	*φ(N)*	*e*	*d*

SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Asymmetrische Verschlüsselung



SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Symmetrische Verschlüsselung

SCHLÜSSEL	*p* und *q*	*N*	*φ(N)*	*e*	*d*

Asymmetrische Verschlüsselung

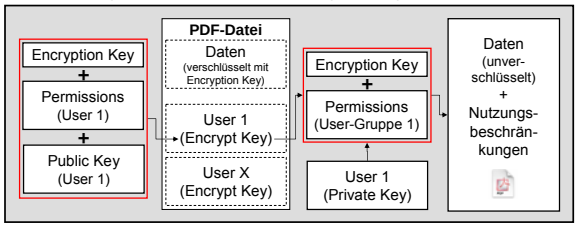
PUBLIC KEY	*p* und *q*	*N*	*e*

PRIVATE KEY	*p* und *q*	*(N)*	*φ(N)*	*d*

SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

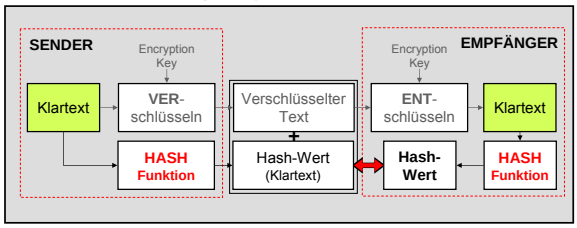
Einsatz von asymmetrischer Verschlüsselung: Self-Sign Sicherheit



SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

Die Hash-Funktion als Überprüfungsmechanismus



SICHERHEIT VON PDF-DATEIEN

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**

SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

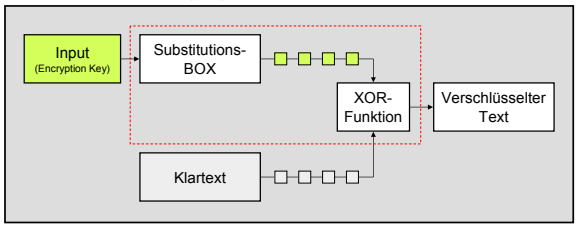
Wird eine PDF-Datei komplett verschlüsselt?

- 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

SICHERHEIT VON PDF-DATEIEN

VERSCHLÜSSELUNGSMETHODEN/ALGORITHMEN

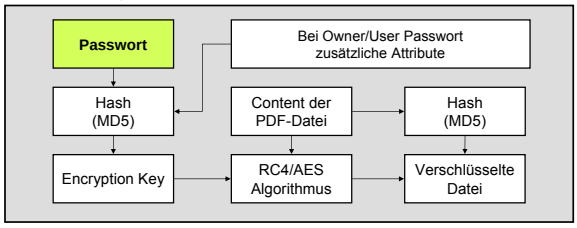
RC4/AES Verschlüsselungsalgorithmus



SICHERHEIT VON PDF-DATEIEN

STANDARD SECURITY HANDLER

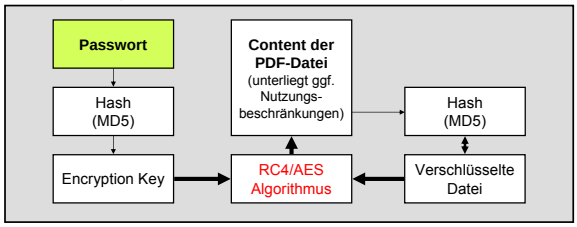
Verschlüsselung



SICHERHEIT VON PDF-DATEIEN

STANDARD SECURITY HANDLER

Entschlüsselung



SICHERHEIT VON PDF-DATEIEN

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

SICHERHEIT VON PDF-DATEIEN

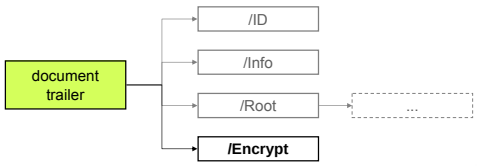
EINBETTUNG DER VERSCHLÜSSELUNG

Encryption

• ***/Encrypt*** steht im document trailer

⇨ dazu gehört das Encryption Dictionary

⇨ kein *Encrypt*, keine Verschlüsselung



SICHERHEIT VON PDF-DATEIEN

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
```

SICHERHEIT VON PDF-DATEIEN

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)

SICHERHEIT VON PDF-DATEIEN

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

SICHERHEIT VON PDF-DATEIEN

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

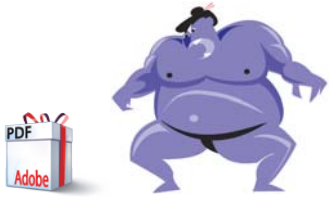
Neuerungen in Acrobat 7.0

- 128 Bit AES Verschlüsselung möglich
  (kann aber nur mit Acrobat/Viewer Version 7 geöffnet werden)

SICHERHEIT VON PDF-DATEIEN

© XQX GmbH, URL: http://www.adobe.de/events/acrobattour/popup8.html

Vielen Dank für Ihre Aufmerksamkeit!



www.alexjacob.info