

Multimediadatensicherheit am Beispiel DVB

Medientechnologie IL

Andreas Unterweger

Vertiefung Medieninformatik
Studiengang ITS
FH Salzburg

Sommersemester 2018

- Ziele
 - Schutz von Multimediadaten (z.B. Kopierschutz)
 - Rückverfolgbarkeit (z.B. Traitor Tracing)
- Methoden (Auswahl)
 - **Verschlüsselung**
 - Wasserzeichen
 - Steganographie
 - Fingerprinting
- Schwerpunkt Kopierschutz
 - Unberechtigte Kopien verhindern (oder zumindest erschweren)
 - Datenkopien im Regelfall unbrauchbar (nicht abspielbar)
 - Beispiel: Content Scramble System (CSS) für DVDs

- Domäne

- Vor der Kompression (engl. *pre-compression*)
- Während der Kompression (engl. *in-compression*)
- Nach der Kompression (engl. *post-compression*)



- Formatkonformität

- Kompatibel (Dekodierung durch regulären Decoder möglich)
- Inkompatibel (Dekodierung durch regulären Decoder nicht möglich)

- Längenerhaltung

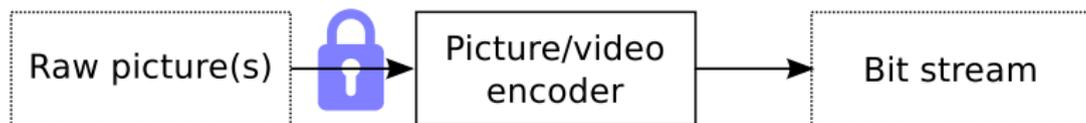
- Längenerhaltend (Länge bleibt nach Verschlüsselung gleich)
- Nicht längenerhaltend (Länge ändert sich nach Verschlüsselung)

- Umfang
 - Vollständig (alles wird verschlüsselt)
 - Selektiv (teilweise Verschlüsselung)
 - Region of Interest (nur bestimmte Bildbereiche werden verschlüsselt)



Verschlüsselung vor der Kompression

- Beispiele
 - AES-Verschlüsselung von Pixelblöcken
 - Permutation von Pixeln innerhalb einer Region
- Vorteile
 - Kompressionsunabhängig
 - Schnell (da keine Dekodierung erforderlich)
- Nachteile
 - Robustheit gegen Kompression erforderlich (alternativ Kommunikation mit Encoder, um verschlüsselte Regionen verlustfrei zu komprimieren)
 - Reduktion der Kompressionseffizienz



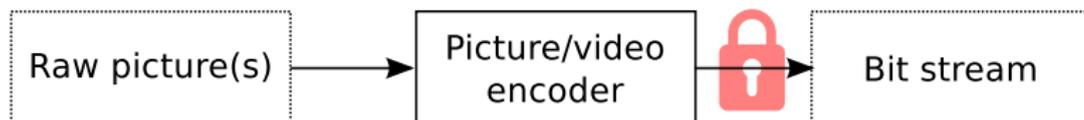
Verschlüsselung während der Kompression

- Beispiele
 - Verschlüsselung der AC-Koeffizienten-Vorzeichen
 - Verschlüsselung von MV-Komponenten-Vorzeichen
- Vorteile
 - Einfach implementierbar (volle Kontrolle über Encoder)
 - Einfluss auf Kompressionseffizienz
- Nachteile
 - Modifikation des Encoders notwendig
 - Verzögerung des Kodiervorganges



Verschlüsselung nach der Kompression

- Beispiele
 - JPEG: Änderung der Reihenfolge von Huffman-Codewörtern
 - H.264: Änderung der Reihenfolge von Codewörtern (ohne Details)
- Vorteile
 - Keine Modifikationen im Bildbereich notwendig
 - Schnelle Verarbeitung auf Bitstrombasis möglich
- Nachteile
 - Formatspezifisch
 - (Teilweise) Dekodierung eventuell notwendig



- Bereiche, die unverschlüsselt bleiben sollen, werden verändert
- Beispiel: Ein Block in H.264-kodiertem Frame verändert



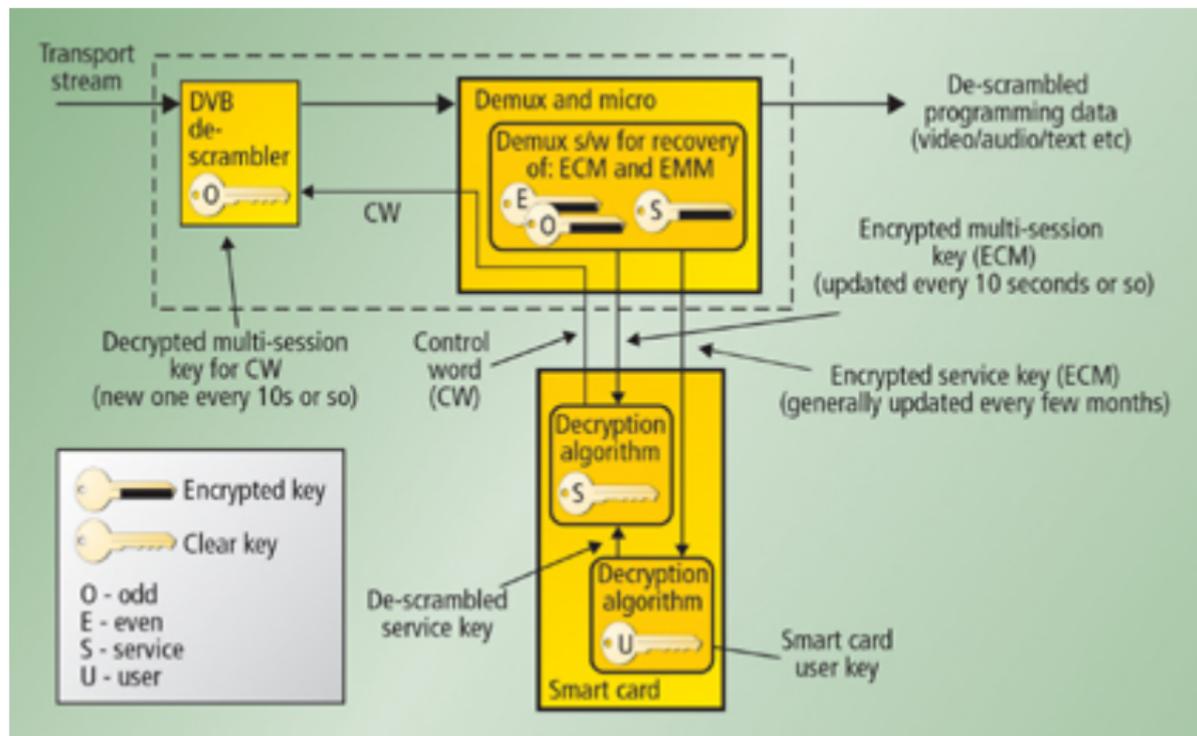
- Örtlicher vs. zeitlicher Drift
- Beispiel von vorhin mit Folgeframes (Framenummern 2, 3, 5 und 10)



- Ursachen
 - Datendekorrelation (durch Transformation) innerhalb eines Blockes
 - Intraprediktion innerhalb von Einzelbildern
 - Interprediktion über mehrere Bilder hinweg
- Domänenspezifität
 - Vor der Kompression: Kein Problem
 - Während der Kompression: Kontrollierbar
 - Nach der Kompression: Großes Problem
- Umfangsspezifität
 - Vollständig: Kein Problem
 - Selektiv: Kein Problem (sogar Vorteil)
 - Region of Interest: Großes Problem

- Digital Video Broadcasting (DVB)
 - Verschiedene Varianten für verschiedene Übertragungswege
 - Bekannte Varianten: DVB-S(2(X)), DVB-C(2), DVB-T(2)
 - Basis: MPEG-TS (mit Spezialanforderungen)
- DVB-Verschlüsselung
 - Verschlüsselung des TS- oder PES-Paket-Payloads (wahlweise)
 - Schlüssel teilweise geheim → benötigt Smart Card oder Äquivalent
 - Verschiedene Algorithmen spezifiziert
 - Teile der Algorithmen geheim (inkl. herstellerspezifische Details)
- Verschlüsselungseigenschaften
 - Nach Kompression (Bitstrom wird verschlüsselt)
 - Nicht formatkonform (Multimediatdaten verschlüsselt nicht dekodierbar)
 - Längenerhaltend (vereinfacht)

Beispiel DVB-Verschlüsselung: Übersicht II



Quelle: Massel, M.: Conditional access. <http://broadcastengineering.com/mag/conditional-access> (abgerufen am 4.3.2014), 2014.

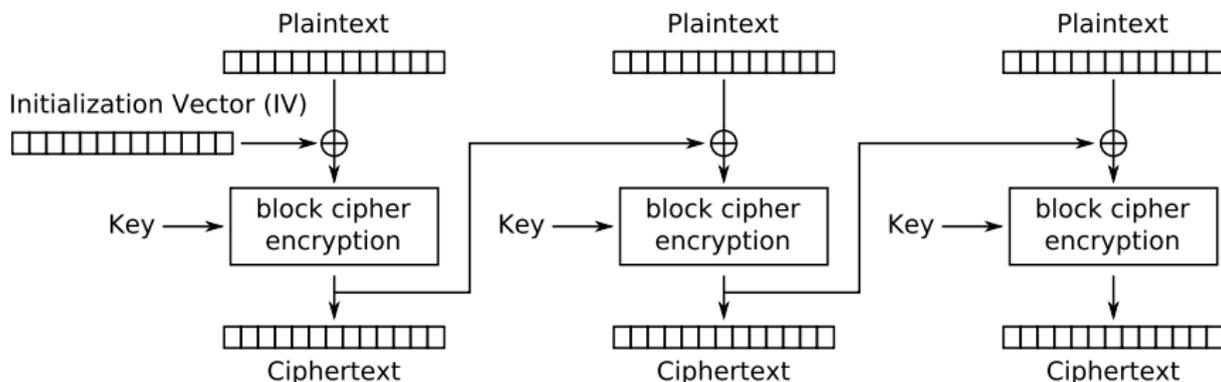
- Entschlüsselung
 - Eigene Descrambler-Komponente entschlüsselt Daten
 - Control Words (CW) steuern Entschlüsselung
 - DVB-Standards definieren Entschlüsselung via CW
 - Abwechselnde Schlüssel (gerade/ungerade (even/odd))
 - Datenpakete müssen even/odd-Markierung enthalten
 - Unverschlüsselte Pakete werden nicht entschlüsselt
- Entitlement Control Messages (ECM)
 - Enthalten (verschlüsselte) programmspezifische Schlüssel
 - Werden von Smart Card verarbeitet → liefert CW
 - Ermittlung von CW aus ECM-Inhalt geheim
- PMT enthält Information zu ECM-PIDs (**unverschlüsselt**)

- Entitlement Management Messages (EMM)
 - Definieren Zugriffsrechte für Benutzer(-gruppe)
 - Enthalten Service-Schlüssel (z.B. für Conax-Service)
 - Schalten Smart Card frei → erlauben Entschlüsselung
 - Nachträglicher Rechteentzug möglich
- Conditional Access Table (CAT)
 - Enthält EMM-PIDs für Krypto-Services (z.B. für Conax)
 - Fixe PID 1
 - **Unverschlüsselt**
- Verschlüsselungsalgorithmus
 - CW sind je 64 Bit lang
 - Bekannter Teil ist zumeist AES mit 128 Bit Schlüssellänge
 - AES wird im Cipher-Block-Chaining(CBC)-Modus verwendet

Beispiel DVB-Verschlüsselung: Details III

- CBC-Modus

- Gleicher Klartext führt zu unterschiedlichem Schlüsseltext
- Schlüsseltext von Block hängt von Vorgängern ab
- Initialisierungsvektor (IV) für ersten Block benötigt



Cipher Block Chaining (CBC) mode encryption

Quelle: http://en.wikipedia.org/wiki/File:CBC_encryption.svg

Beispiel DVB-Verschlüsselung: Details IV



*Not always present

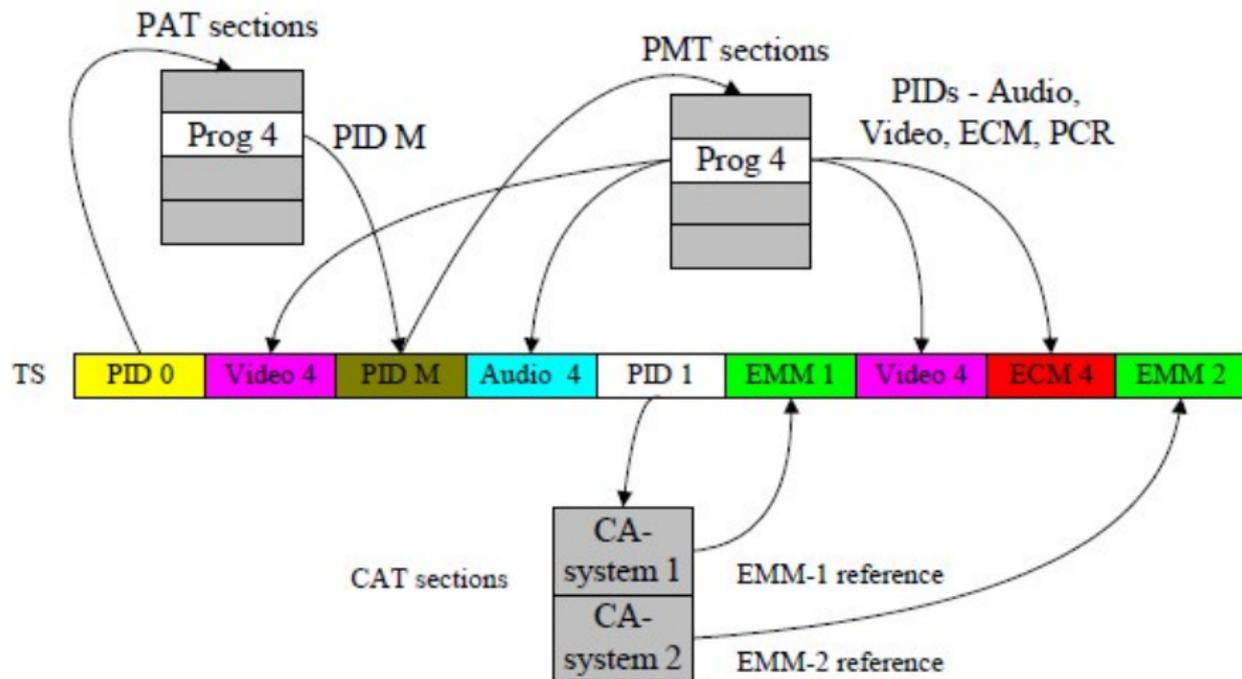


*Not always present

Quelle: ETSI: Digital Video Broadcasting (DVB); Content Scrambling Algorithms for DVB-IPTV Services using MPEG2 Transport Streams (ETSI TS 103 127 V1.1.1), 2013. Auch verfügbar

unter:http://www.etsi.org/deliver/etsi_ts/103100_103199/103127/01.01.01_60/ts_103127v010101p.pdf

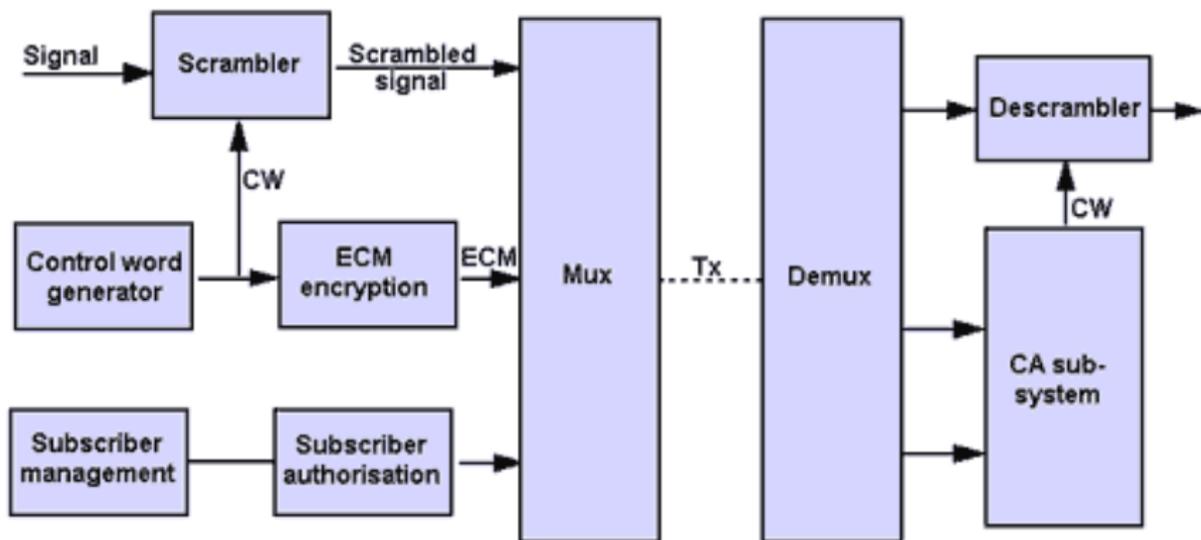
Beispiel DVB-Verschlüsselung: TS-Beispiel



Quelle: <http://kcchao.wikidot.com/program-service-information>

Beispiel DVB-Verschlüsselung: Gesamtüberblick I

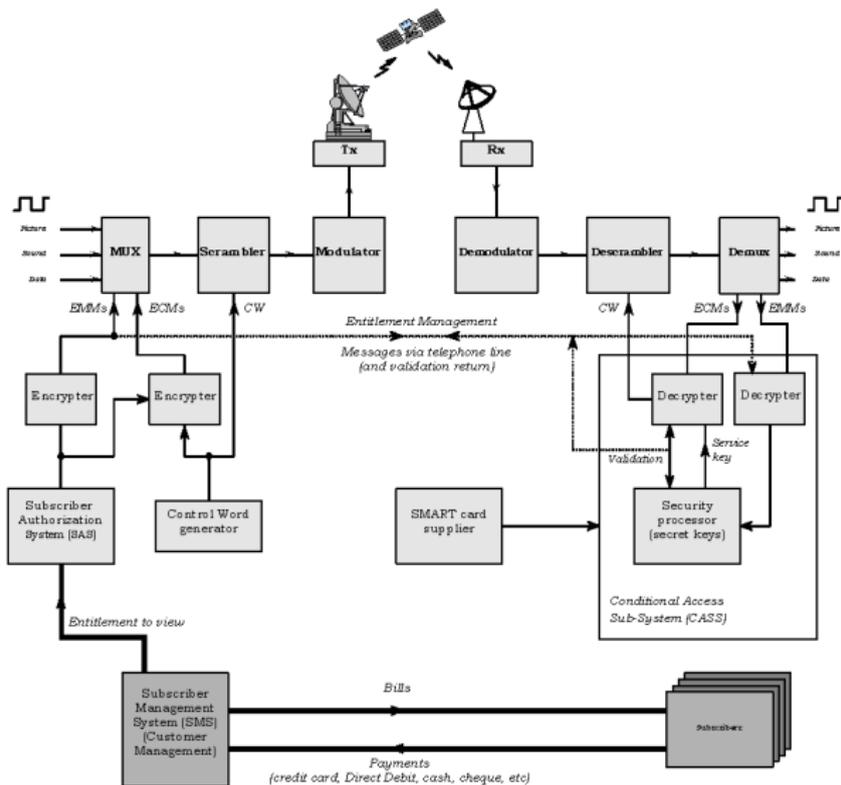
- Gesamtsystem inkl. Verschlüsselung auf Senderseite:



Quelle: ThinkQuest: Conditional Access TV.

http://library.thinkquest.org/07aug/01676/relevance_entertainment_conditionalaccesstv.html (abgerufen am 4.3.2014), 2007.

Beispiel DVB-Verschlüsselung: Gesamtüberblick II



Quelle: Duran, J. E.: Ohne Titel. <http://www.une.edu.ve/~jduran/Dvb.htm> (abgerufen am 5.3.2014), 1996.

Fragen?