Verschlüsselungsverfahren

für Medien – Rundfunk / TV

16.01.09

Matthias Bach

Gliederung

- Historie
- Die Syster Verschlüsselung
- Weitere analoge Verschlüsselungsverfahren
- DVB Standard
- Conditional Access Systeme
- Die Smartcard
- Steuercodes (EMM / ECM)
- Common Scrambling Algorithmus

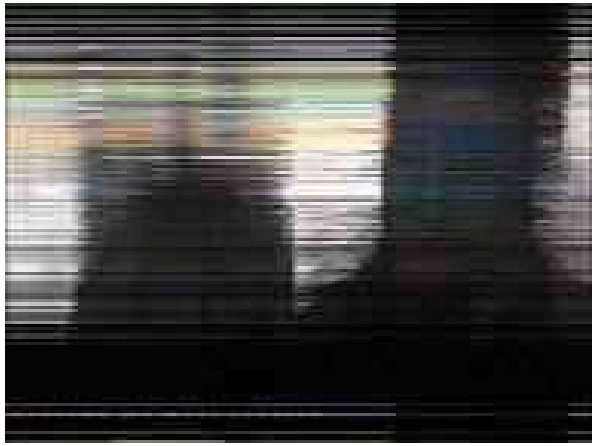
Gliederung

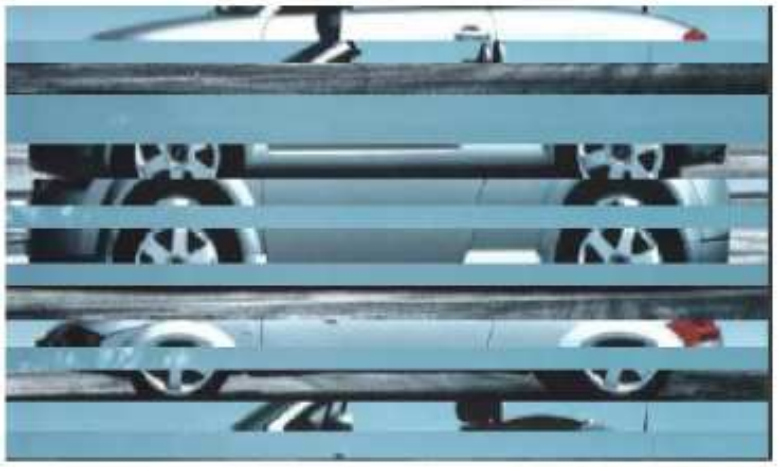
- Irdeto Verschlüsselung
- Loggen von Datenstreams
- Irdeto II. Verschlüsselung
- Seca Verschlüsselung
- Weitere Informationen
- Register der Abkürzungen
- Quellenverzeichnis

Verschlüsselung Anfang der 90er

- In Deutschland nur 1 verschlüsselter TV Sender (TeleClub, der später zu Premiere wurde)
- Analog mit verschlüsseltem Bild, Ton unverschlüsselt
- Früher in PayView3 codiert, ab Mitte der 90er in Syster (Nagravision)
- Syster = Zufällige Vertauschung aufeinander-folgender Bildzeilen
- Syster wurde schnell kompromittiert

Syster





Matthias Bach

Syster

- Vertauschen der Zeilen im TV Bild nach einem bestimmten Muster (Line Shuffeling, auch Nokia LS)
- Bei Syster 625 (PAL) die vertauscht werden
- Beispielbild mit 16 Zeilenblöcken erlaubt :

$$2^{n-1} = 2^{16-1} = 2^{15} = 32768$$

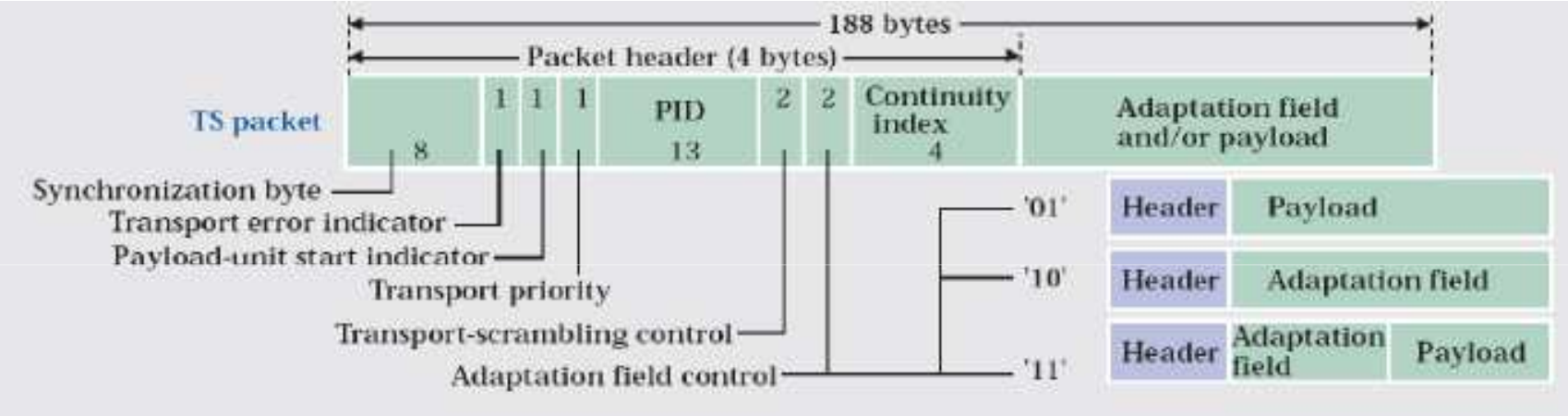
  - 32768 Permutationen

Weitere analoge Verfahren

- Videocrypt I. / II.
- Eurocrypt M / S
- Discret 12
- Smartcrypt
- PayView3 / Satpac
- Nokia Line Shuffeling
- Luxcrypt (L-Crypt)

Analoge Verfahren

DVB Standard



- Daten werden in Blöcke (Container) zerlegt (TS)
- Jeder TS Block ist 188 Byte groß
- Payload = Nutzdaten (TV Bild und Ton)

DVB-Standard

- Die ersten 4 Byte fungieren als :
  - Synchronisations Byte
  - Meldebit für Fehler
  - Kennzeichnung des Paketes
  - Ob die Payload verschlüsselt ist (Transport Scrambling Control)

Conditional Access System (CAS)

- Schnittstelle zwischen codiertem DVB Datenstrom und Smartcard*
- Teilweise embedded in Receivern oder als Modul per PCMCIA Einschub
- Mit Smartcard Reader
- Beinhaltet das „Verschlüsselungssystem“ auf Kundenseite

Conditional Access System (CAS)

Conditional Access System (CAS)

- Irdeto / BetaCrypt
- Viaccess
- Nagravision
- Conax
- NDS Videoguard
- Seca Mediaguard
- Biss
- Griffin

Conditional Access System (CAS)

- Ziel des CAS: 8 Byte langes, gültiges Control Word (CW) generieren
- CW entschlüsselt die Payload (im TS Paket)
- CW wird im Common Scrambling Algorithmus (CSA) verschlüsselt (bis heute nicht kompromittiert)
- Wird der CSA bekannt, sind alle Verfahren, Module etc. kompromittiert und wertlos.

Smartcard

- Asynchrone Ausführung
- Mikroprozessor und EEPROM
- Auf die Daten im EEPROM kann nur über den Mikroprozessor zugegriffen werden

Smartcard

- Zugriffe von extern dadurch nicht möglich
- Mikroprozessor enthält kryptographische RSA- und DES Einheiten (eingehende, chiffrierte Daten werden so entschlüsselt und im EEPROM abgelegt)

- ***Die Smartcard dient bei CA Systemen als Dekodierkarte für die in den Steuercodes enthaltenen Daten***

Steuercodes

- Werden mit dem eingehenden Datenstrom gesendet
- Anbieter kann z. B. neue Schlüssel an Karten der Kunden verteilen (per Satellit, Kabel usw.)
- Z. B. Karten können per Steuercodes aktiviert / abgeschaltet werden
- Steuercodes werden differenziert in :
  - Entitlement Management Messages (EMM)
  - Entitlement Control Messages (ECM)

Steuercodes

- Diese Steuercodes übermitteln das codierte CW zum CSA Descrambler
- Wäre das Control Word in Klartext, könnte es bei modifizierten Endgeräten geloggt werden
- System wäre somit kompromittiert
- Weitere Steuercodes dienen zur Fernkonfiguration des CAS oder der Smartcard

Smartcard

- Smartcards enthalten mehrere Schlüssel:
  - Signierten Plain Master Key (PMK)
  - Service Keys (Üblich sind 10 versch. Service Keys)
- Mit einem gültigen Service Key entschlüsselt der Mikroprozessor das CW für den CSA Descrambler.
- Mehrere Service Keys für verschiedene Services notwendig (Programmpakete, Pay-Per-View usw.)

Steuercodes: EMM

- EMMs adressieren einzelne Decoder oder Decoder-gruppen
- EMMs aktivieren oder sperren Smartcards
- EMMs erteilen Berechtigungen für Angebote (Sender etc.)
- Mit EMMs werde neue Service Keys auf die Smartcard geschrieben

Steuercodes: EMM

- EMMs werden über logische Kanäle (PIDs) übertragen
- PIDs von EMMs werden in einer Conditional Access Table (CAT) verwaltet, die jeder Decoder beim einschalten aufbaut
- Die CAT Einträge werden auch über PIDs übertragen (PID 0x01h)
- EMMs sind verschlüsselt und werden mittels des PMK dechiffriert

Steuercodes: EMM

- PMK liegt fest im EEPROM der Smartcard
- EMMs in Klartext könnten mitgeloggt werden.
- Dadurch könnte man gesperrte Karten wieder freischalten oder
- Karten mit neuen Service Keys ausstatten

Steuercodes: ECM

- ECMs enthalten z.B. das aktuell gültige CW für den CSA Descrambler
- Nummer des Service Keys, mit dem das aktuelle CW entschlüsselt werden muss
- Timestamp
- ECMs werden ebenfalls über PIDs übermittelt
- Die PIDs der ECMs werden auch in der CAT verwaltet

Common Scrambling Algorithmus

- Standard Verschlüsselungsverfahren bei DVB konformen Übertragungen
- CSA = XOR Verknüpfung der zu verschlüsselnden Datenbytes mit einer Pseudozufallszahlenfolge
- Pseudozufallszahlenfolge wird von einer Finite State Machine (FSM) erzeugt.
- Das Control Word legt den Startzustand des FSM fest

Irdeto

- Premiere Verschlüsselungssystem bis 2006
- Verschlüsselung des ORF bis 2008
- Aktuell in Nutzung bei Canal Digitaal NL, Nova Hellas u.a.
- 8 Byte CW = 64 Bit = 2^{64} Möglichkeiten (Bruteforce mit 1µs pro Versuch = 500.000 Jahre)
- Smartcards mit Ländercode ausgestattet (GER = Premiere / TEL = Dt. Telekom)

Irdeto

- Irdeto Karten im Auslieferungszustand NUR mit Seriennummer und Hex-Master-Key (HMK) im EEPROM
- HMK 10 Bytes lang, Hex-Serial 3 Bytes lang
- Hex Serial zur eindeutigen Identifikation der Karte
- Für eine weitere Funktion der Karte sind diverse Codes vom Anbieter notwendig
- Werden per Sat / Kabel etc. geliefert

Irdeto

1. Karte einlegen
2. Karte erhält per Sat/Kabel einen Master Key (MK)
   MK 8 Bytes lang => Notwendig zur Karten-aktivierung
3. MK wird auf der Karte mit dem HMK verrechnet
   Ergebnis: Plain Master Key (PMK – 8 Bytes lang)
4. Provider-ID (3 Bytes lang) wird auf die Karte übertragen (ID des Anbieters [Premiere etc.])

Irdeto

- Provider-ID notwendig, um die Karte für die weiteren Operationen gezielt anzusprechen
- 2 Bytes der Provider ID = Provider Gruppe
- PMK gilt für eine ganze Provider Gruppe
- Dadurch können maximal 256 Karten gezielt angesprochen werden
- Abhilfe mit Binärmaske CB-20 Nano
- Auf Karte nun HS, HMK, MK, PMK, Provider-ID

Irdeto

Geloggte Masterkeys bei Irdeto

Auswertung eines Irdeto EMM-Streams erzeugt von Master-LOG V3.83

==========

Pay-TV Provider: Prem World Sat C-Cards
PID: 1000

Bereich: Master-Keys <12>

HEX-Sr	PR	Pro-ID	MasterKey	Date
7EEBE8	10	21EBFE	00D723537F74FDCB1B	0772
7EEBEA	10	21EBFC	00CFDFA1245B69762E	0772
7EEBEC	10	21EBFA	001614DABC6DF5E81B	0772
7EEBF4	10	21EBF3	0029262F60166C3E1A	0772
7EEBF7	10	21EBF0	0047D328B7F1B8615E	0772
7EEBFB	10	21EBEC	001A3557B0ADF4C826	0772
7EEC06	10	21EBE1	00184749C2280AE56B	0772
7EEC08	10	21EBDF	00D259168D3171371D	0772
7EEC0B	10	21EBDC	005A57C214E822B697	0772
7EEC10	10	21EBD7	00C94824DB08863863	0772
7EEC11	10	21EBD6	0074AA10C82FDE9DC9	0772
7EEC12	10	21EBD5	0083B85CDA8B456702	0772

Irdeto

- Nun folgen die eigentlichen Keys
- Keys sind mit Provider Gruppe adressiert
- Datenstrom (ID 2D58xx) zur Visualisierung geloggt
- Key wird mit aktuellem Datum und PMK verrechnet
- Ergebnis Plainkey (8 Bytes & 1 Byte für Keynummer)
- Im Beispiel: Key 08
- Key Updates erfolgen vom Anbieter in bestimmten Zeitabständen

Irdeto

Geloggter EMM Stream bei Irdeto

Auswertung eines Irdeto EMM-Streams erzeugt von Master-LOG V3.83

==========

Pay-TV Provider: Prem World Sat C-Cards
PID: 1000

Bereich: Keys der eigenen CardGroup <1>

Pr CGroup Key Date D-ID Type ChID
10 2D58xx 08=>083EDFF8CF9E7C52F1 0772 0771 1009 7D27

→ Plainkey: B2520188062 44CFD (PMK:BEA7C566DC6C8AB2)

Irdeto – Nano Codes

- Nano Codes = 2 Bytes lange Befehle
- Werden im EMM Datenstrom übertragen
- 1. Byte Instruktion / 2. Byte Länge des Folgestring
- Folgestring z.B. Datum, Neue Provider-ID, Set Key
- CB20 Nano für individuelle Adressierung von Karten
- Andere Nanos sind meist für Smartcard Verwaltung notwendig

Irdeto II.

- Weiterentwicklung von Irdeto
- Kommunikation zwischen Smartcard und CAM wird verschlüsselt
- Mittels CAM-Key
- Loggen der Daten somit nicht mehr möglich
- Noch heute im Einsatz, Irdeto I. wird nicht mehr eingesetzt
- Weiterer Nachfolger in Arbeit

Seca

- Verschlüsselung z.B. in Frankreich, Spanien, Polen
- Ebenfalls 8 Byte langes CW (vgl. Irdeto)
- CW wird aus PK und Secondary Key (SK) durch Verrechnung entschlüsselt (= plain)
- PKs und SKs werden in Management Keys (MK) und Operation Keys (OK) aufgeteilt
- MK-01 ist vergleichbar mit dem PMK bei Irdeto
- Programmable Provider User Adress (PPUA) ist ähnlich der Provider-ID bei Irdeto

Weitere Informationen

- Seca wurde ebenfalls zu Seca II. weiterentwickelt
- Sehr gängig sind Cryptoworks, Conax, Videoguard
- Entwicklung geht ständig voran
- Bis auf Videoguard wurden bereits alle Systeme kompromittiert
- Derzeit sicher ist nur Cryptoworks und Griffin

Abkürzungen

- CAS = Conditional Access System
- CSA = Common Scrambling Algorithmus
- TS = Transport Stream (Datenpaket)
- CW = Control Word
- EMM = Entitlement Management Message
- ECM = Entitlement Control Message
- PMK = Plain Master Key
- SK = Service Key
- CAT = Conditional Access Table

Abkürzungen

- PK = Plain Key
- PID = Logischer Übertragungskanal für EMM/ECM
- Prov. ID = Provider ID von Irdeto
- HS = Hex Seriennummer
- HMK = Hex Master Key
- SK = Secondary Key
- MK = Management Key
- OK = Operation Key
- PPUA = Programmable Provider User Adress

Quellenangaben

- Wikipedia (Grundbegriffe CAS, CSA, Irdeto, etc.)
- Hochschule Bremen – Labor für Computertechnik 04/05
- www.iswitch.ch/ma.pdf
- www.cl.cam.ac.uk/~mgk25/nagra.pdf
- www.tjaekel.de/dvb.htm
- TU-Darmstadt – Fachbereich Informatik (für CSA)
- www.isat.info
- http://thoic.com

Ende

Vielen Dank für Ihre Aufmerksamkeit