Kodowanie i szyfrowanie sygnałów fonicznych i wizyjnych

Technika rejestracji sygnałów

1

Zastosowanie szyfrowania

- Ochrona prywatności w zastosowaniach typu VoIP (Voice & Video over IP – telefonia Internetowa, telekonferencje)
- Ochrona danych wrażliwych – dokumentacja medyczna, biometria
- Ochrona praw autorskich (i innych praw majątkowych) – telewizja cyfrowa (DVB), wideo na żądanie (VOD, platformy streamingowe), filmy DVD, BD, UHD-BD

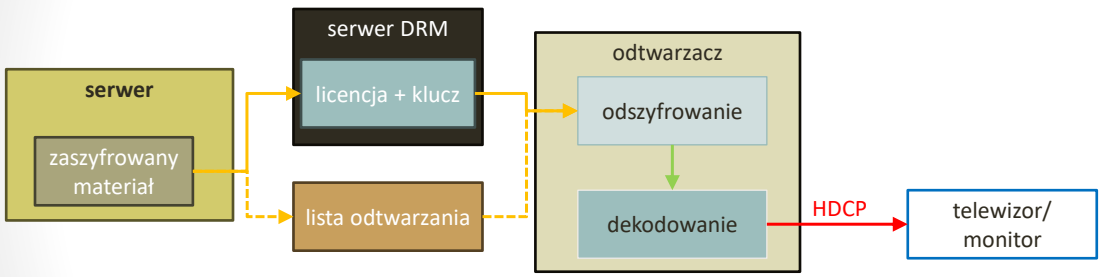
2

System DRM (Digital Right Management)

- Szyfrowanie materiału multimedialnego w celu uniemożliwienia dostępu bez prawidłowego klucza
- Podczas próby odtworzenia wyświetlany jest monit o dostarczenie licencji, która zawiera w sobie klucz deszyfrujący
- Różne rodzaje licencji: pojedyncze odtworzenie, pojedyncza kopia, 1 generacja kopii, ograniczenia geograficzne, ograniczenia czasowe
- Odtwarzacz weryfikuje licencję i deszyfruje strumień multimedialny

3

System DRM (Digital Right Management)



4

Google Widevine

- system ochrony treści premium w ramach dystrybucji cyfrowej
  - wykorzystywany m.in. przez Google Play, YouTube, Netflix, Disney+, Amazon Prime Video, HBO Max, Hulu, Peacock, Discovery+, Paramount+
  - korzysta z
    - Encrypted Media Extensions
    - ISO/IEC 23001-7 (szyfrowanie w kontenerze ISO base media file format)
    - ISO/IEC 23001-9 (szyfrowanie w kontenerze MPEG2)

5

Google Widevine

- obsługiwany przez większość urządzeń obecnych na rynku

	LG	Panasonic	PHILIPS	SAMSUNG	SHARP AQUOS	SONY BRAVIA
Operating System	WebOS	FirefoxOS	AndroidTV	Tizen	AndroidTV	AndroidTV
Cloud License Service	✔	✔	✔	✔	✔	✔
Hardware DRM (Level 1)	✔	✔	✔	✔	✔	✔
DASH	✔	✔	✔	✔	✔	✔
HTML5	✔	✔	✔	✔	✔	✔
VP9 Profile0 (8bit)	✔	✔	✔	✔	✔	✔
VP9 Profile2 (10bit)	✔	2017	2017	2017	2017	2017

źródło: https://developers.google.com/widevine/drm/overview?hl=pl

6

Encrypted Media Extensions

- JavaScriptowe API przeglądarki, które umożliwia odtwarzanie w HTML-u zaszyfrowanego audio i wideo.
- interfejs pośredniczącym między odtwarzaczem webowym a systemem ochrony treści (DRM).
- nie definiuje konkretnego DRM, protokołu licencjonowania ani polityki biznesowej.
- zastępuje używane kiedyś wtyczki przeglądarkowe.

7

MPEG Common Encryption (MPEG-CENC) – ISO 23001-7

- definiuje wspólny, niezależny od DRM format szyfrowania mediów w plikach i strumieniach opartych na ISO Base Media File Format (MP4).
- stosuje szyfrowanie AES-128 do próbek albo określonych fragmentów próbek strumienia AV.
- każda zaszyfrowana póbka jest powiązany z identyfikatorem klucza, na podstawie którego odtwarzacz może poprosić właściwy serwer licencyjny o klucz deszyfrujący.
- pozwala na obsługę zaszyfrowanej treści przez różne systemy DRM (np. Widevine, PlayReady albo FairPlay)

8

„Dziura analogowa”

- Brak kontroli na wyjściach analogowych odtwarzacza
- Nowsze rozwiązania (urządzenia) eliminują „dziurę analogową” poprzez stosowanie tylko połączeń cyfrowych, wyposażonych w szyfrowane interfejsy (np. HDMI wraz z HDCP)
- Sygnał analogowy odtwarzany jest przy znacznie zdegradowanej jakości

9

Przykłady technologii zabezpieczania danych przez nieautoryzowanym dostępem

- SCMS
- Macrovision
- CSS
- AACS
- HDCP

10

SCMS – Serial Management System

- uzupełnienie połączenia SPDIF o zabezpieczenie przed nielegalnym wykonywaniem cyfrowych kopii
- powstał, żeby zabezpieczyć format DAT (*Digital Audio Tape*) przed robieniem cyfrowych kopii
  - stosowany także w MiniDisc-ach i DCC (*Digital Compact Casette*)
  - pierwotnie (1987 r.) planowany był system polegający na wykrywaniu obecności sygnałów w okolicy 3840Hz; brak tych częstotliwości oznaczałby, że materiał jest zabezpieczony
  - przyjęty w 1992 roku
- rozwijany dla potrzeb telewizji w postaci m.in. broadcast flag

11

SCMS – Serial Management System

- **profesjonalny sprzęt pozbawiony był zabezpieczenia SCMS**
- w praktyce polega na odpowiednim ustawieniu dwóch bitów w kodzie SPDIF:
  - 00 – brak zabezpieczenia przed kopiowaniem
  - 10 – zakaz kopiowania
  - 11 – możliwość wykonania jednej kopii, ale bez możliwości skopiowania tej kopii
- działanie (za http://www.minidisc.org/)

źródło	**kopia**
analogowe	11
CD	10
cyfrowe, 00	11 lub 00 (zależnie od modelu)
cyfrowe, 11	10
cyfrowe, 10	brak możliwości zapisu

12

Macrovision Video Copy Protection

- opracowany w połowie lat 80-tych XX wieku w celu zabezpieczenia materiałów wideo przed kopiowaniem
- polega na
  - wstawianiu dodatkowych impulsów synchronizacji w sygnale wygaszania ramki, co zakłóca pracę układów AGC w magnetowidach
  - modulowaniu impulsów przekazujących informacje o kolorze (w systemie NTSC)
- objawiał się okresowymi zmianami jasności i nasycenia obrazu, zrywaniem synchronizacji itp.
- do obejścia za pomocą praktycznie dowolnego wzmacniacza sygnału wizyjnego

13

Macrovision Video Copy Protection

14

Macrovision Video Copy Protection

- na płytach DVD funkcjonował jako **APS** (Analog Protection System) lub jako **Copyguard**
- polegał na ustawieniu odpowiedniej flagi w plikach VOB
  - po opłaceniu praw licencyjnych
- do obejścia przy pomocy praktycznie każdego oprogramowania do kopiowania płyt DVD-Video

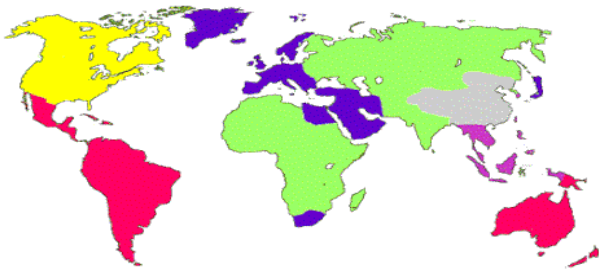
15

Broadcast flag

- dotyczy przekazów cyfrowych
  - obecny we wszystkich odbiornikach standardu ATSC (USA) od 2005 roku
  - w Europie brak standardu
- informuje, czy istnieje możliwość nagrywania danego programu, a także
  - czy można ominąć reklamy
  - czy można zapisać program w wysokiej jakości
  - czy można wykonać kopię z nagranego programu
  - itp.

18

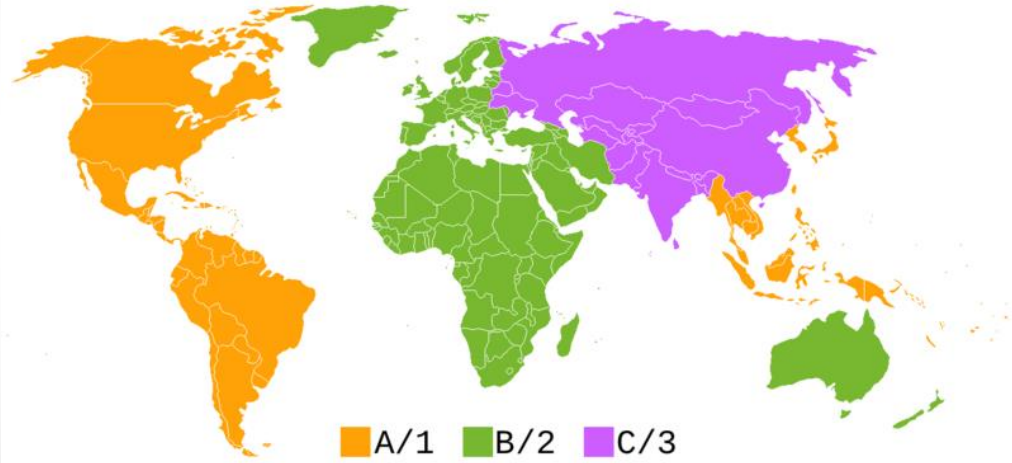
Kodowanie regionalne (DVD)



Region 0	bez ograniczeń
Region 1	USA, Kanada
Region 2	Europa, bliski wschód, Południowa Afryka, Japonia
Region 3	Południowo-wschodnia Azja, Taiwan
Region 4	Ameryka środkowa i południowa, Meksyk, Australia, Nowa Zelandia
Region 5	Rosja, większość krajów Afryki, Indie, Pakistan
Region 6	Chiny
Region 7	linie lotnicze

19

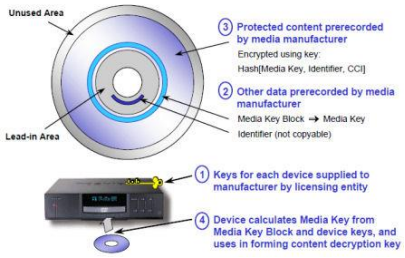
Kodowanie regionalne (Blu-ray)



20

CSS – Content Scramble System

- opracowany w 1996 roku
- zabezpiecza materiały zapisane na płycie DVD-Video oraz DVD-Audio
  - wymaga „współpracy” nośnika, napędu i oprogramowania do odtwarzania
  - klucz o długości 40 bitów
- obecny wyłącznie na tłoczonych płytach

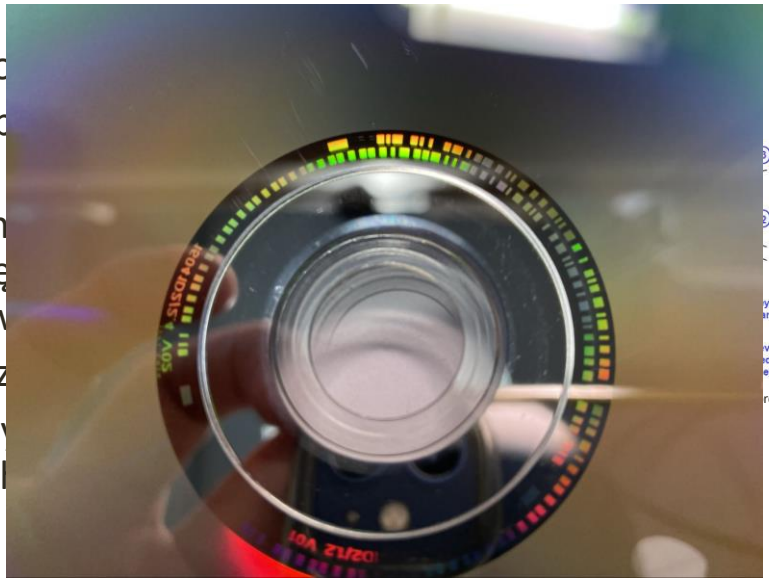


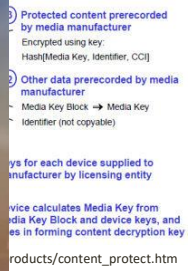
http://www.manifest-tech.com/ce_products/content_protect.htm

21

CSS – Content Scramble System

- opraco
- zabezp
  płycie
  - wym
    napę
    odtw
  - klucz
- obecn
  płytac





22

CSS – Content Scramble System

- uniemożliwia skopiowanie danych z płyty DVD na dysk twardy
- stosowanie CSS wymaga uiszczenia opłat licencyjnych
- powiązany z kodowanie regionalnym
- złamany w 1999 roku przez Norwega - Jona Lecha Johansen (w niecałe dwa lata po pojawieniu się DVD-Video)
  - soft o nazwie *DeCSS*

23

AACS – Advanced Access Content System

- odpowiednik CSS dla płyt Blu-ray i HD-DVD
- specyfikacja opublikowana w 2005 roku, pierwsze płyty HD-DVD i Blu-ray pojawiły się w I. połowie 2006 roku
- zabezpieczenie złamane w grudniu 2006 roku przez „muslix64” (soft o nazwie *BackupHDDVD*)

24

AACS – Advanced Access Content System

- podstawowe różnice w stosunku do CSS
  - materiał zakodowany za pomocą „title keys” o długości 128 bitów z użyciem AES (Advanced Encryption Standard)
  - każdy odtwarzacz posiada unikalny zestaw kluczy – *decryption keys* (w CSS grupa odtwarzaczy)
    - teoretycznie można wyeliminować nawet pojedyncze odtwarzacze

25

AACS – Advanced Access Content System

- wprowadza ograniczenie rozdzielczości na wyjściach analogowych do 960x540 pikseli
- teoretycznie umożliwia zarządzanie procesem wykonywania kopii
- obecnie wersja AACS2 dla potrzeb formatu Ultra HD Blu-ray

26

BD+

- kolejne zabezpieczenie oferowane przez format Blu-ray
  - jego istnienie przyczyniło się do zwycięstwa formatu BD nad HD-DVD
- rodzaj wirtualnej maszyny, za pomocą której można uruchamiać programy zawarte na płycie Blu-ray w celu
  - sprawdzenia poprawności kluczy
  - sprawdzenia czy odtwarzacz jest bezpieczny
  - kontrolować wyświetlane treści
- złamane w listopadzie 2007 roku przez twórców AnyDVD HD

27

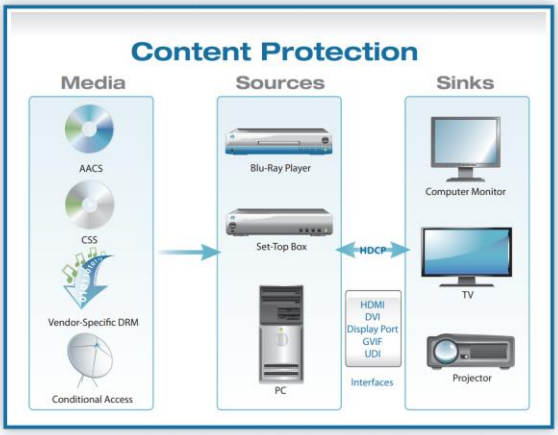
BD ROM Mark

- ostatnie z zabezpieczeń na płycie Blu-ray
- polega na wytłoczeniu na płycie dodatkowych danych (znaku wodnego) identyfikujących źródło i współpracujących z AACS
  - dane są wykorzystywane przez odtwarzacz do sprawdzenia, czy płyta jest oryginalna
  - danych nie da się skopiować
- ma zapobiegać masowemu kopiowaniu pirackich płyt

28

HDCP - High-bandwidth Digital Content Protection

- zabezpiecza przed nieautoryzowaną transmisją danych między urządzeniami AV
- opracowane przez Intela
- korzystanie z HDCP wymaga opłacenia licencji
- dotyczy także transmisji bezprzewodowych

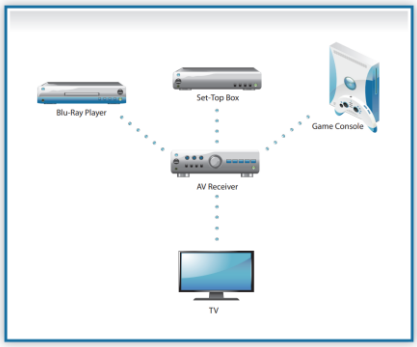


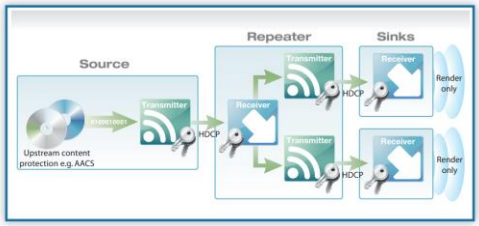
Źródło (także dla następnych slajdów o HDCP): https://www.digital-cp.com/sites/default/files/resources/HDCP_deciphered_070808.pdf

29

HDCP - High-bandwidth Digital Content Protection

- wyróżnia się trzy typy urządzeń
  - źródło (source)
  - repeater
  - odbiornik (sink)
- polega na wymianie kluczy między urządzeniem źródłowym (np. odtwarzacz Blu-ray) i odbiornikiem (np. telewizor LCD)
  - brak obsługi HDCP przez dane urządzenie (odbiorcze) uniemożliwia przesłanie obrazu i/lub dźwięku (lub ograniczenie jakości)

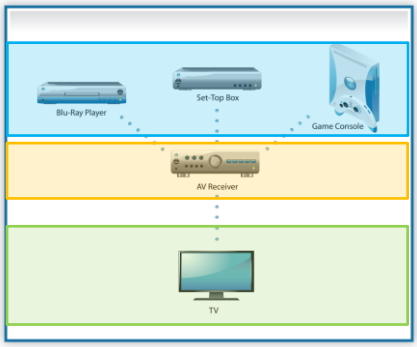


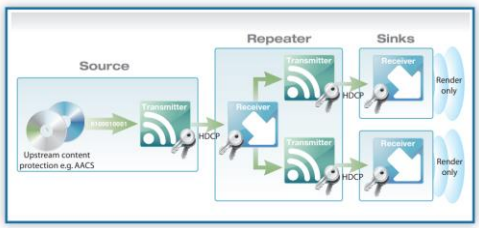


31

HDCP - High-bandwidth Digital Content Protection

- wyróżnia się trzy typy urządzeń
  - źródło (source)
  - repeater
  - odbiornik (sink)
- polega na wymianie kluczy między urządzeniem źródłowym (np. odtwarzacz Blu-ray) i odbiornikiem (np. telewizor LCD)
  - brak obsługi HDCP przez dane urządzenie (odbiorcze) uniemożliwia przesłanie obrazu i/lub dźwięku (lub ograniczenie jakości)





32

HDCP - High-bandwidth Digital Content Protection

- każdy „nadajnik” i „odbiornik” posiada
  - 40 unikatowych 56-bitowych kluczy (*Device Private Keys*)
  - 20-bitowy *Key Selection Vector* – rodzaj numeru identyfikacyjnego
    - powyższe dostarczane są przez DCP (*Digital Content Protection*) po podpisaniu licencji
- autentykacja rozpoczyna się od wymiany KSV i ustalenia wspólnego klucza, który będzie używany do szyfrowania danych w ramach danej sesji
- co 128 klatek lub co 2 sekundy następuje sprawdzenie czy transmisja przebiega poprawnie

33

HDCP - High-bandwidth Digital Content Protection

- złamany w 2001 (przed praktyczną implementacją w jakimkolwiek urządzeniu) przez naukowców-kryptologów
  - w 2010 upubliczniono odtworzony poprzez kryptoanalizę klucz główny HDCP, efektywnie niszcząc cały system
- obecnie rozwijane wersje 2.x (najnowsza 2.3)
  - wykorzystują inne kodowanie (m.in. AES 128 z 3072-bitowym kluczem RSA dla nadajnika i 1024-bitowymi kluczami RSA dla odbiornika)
  - sprawdzają czas transmisji sygnału między źródłem i odbiornikiem (musi być poniżej 20ms)
  - wymagane do transmisji 4k
  - również złamane

34

HDCP - High-bandwidth Digital Content Protection

What is the smallest number of Device Key sets that can be purchased? **2026**

The quantities and prices for key orders are listed below:

Description	Cost (USD)
HDCP 1.x Transmitter or Receiver Key - Qty of 10,000	$3,000 USD
HDCP 1.x Transmitter or Receiver Key - Qty of 100,000	$7,500 USD
HDCP 1.x Transmitter or Receiver Key - Qty of 1,000,000	$15,000 USD
HDCP 2.x Annual Source Key Fee - Up to 100/year	$500 USD
HDCP 2.x Annual Source Key Fee - Up to 1K per year	$1,000 USD
HDCP 2.x Annual Source Key Fee - Up to 10K per year	$2,000 USD
HDCP 2.x Annual Source Key Fee - Up to 100K per year	$5,000 USD
HDCP 2.x Annual Source Key Fee - Up to 1M per year	$10,000 USD
HDCP 2.x Annual Source Key Fee - For quantities over 1M per year	$20,000 USD
HDCP 2.x Receiver Key - Qty of 10,000	$3,000 USD
HDCP 2.x Receiver Key - Qty of 100,000	$7,500 USD
HDCP 2.x Receiver Key - Qty of 1,000,000	$15,000 USD

źródło: https://www.digital-cp.com/faqs

35