

# Kriptografi pada Layanan TV Berbayar (Pay TV)

Dwitri Desvira 13510044  
Program Studi Teknik Informatika  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia  
13510044@std.stei.itb.ac.id

**Abstrak**—Layanan televisi berbayar merupakan layanan yang disediakan oleh suatu perusahaan yang menyediakan tayangan-tayangan dari berbagai negara. Tayangan-tayangan ini hanya dapat dinikmati oleh pelanggan yang telah menjadi anggota pada layanan tersebut. Pada layanan ini, pelanggan akan diberikan suatu *smart card* yang nantinya berfungsi untuk menangkap siaran yang dipancarkan oleh satelit.

Pada mulanya perkembangan *Pay TV* di Indonesia diawali oleh perusahaan bernama Indovision. Dalam *Pay TV* sistem penyiarnya terbagi dua, yaitu penyiaran melalui kabel dan penyiaran melalui satelit. Indovision merupakan perusahaan yang menggunakan sistem satelit dalam pendistribusian layanan televisi berbayar.

Mekanisme penyiaran satelit untuk *Pay TV* yaitu, dimulai ketika *provider* memancarkan siarannya ke satelit (*uplink*) lalu kemudian sinyal tersebut ditransfer dan dikirim lagi menuju ke bumi (*downlink*).

Agar pelanggan dapat menangkap siaran dari *provider*, setiap pelanggan memiliki sebuah *smart card* yang nantinya berfungsi untuk mendekripsikan siaran yang telah di *broadcast*.

**Kata Kunci**— *Pay TV*, *Smart card*, *Kriptografi*, *Satelite*

## I. PENDAHULUAN

Kehadiran televisi (TV) berbayar di Indonesia bukan merupakan hal yang baru lagi. Bagi masyarakat di kota besar TV berbayar atau yang biasa disebut *Pay TV* bukan sesuatu yang asing lagi. *Pay TV* merupakan layanan televisi berbayar yang disediakan oleh perusahaan tertentu yang siarannya hanya dapat dinikmati oleh pelanggan yang merupakan anggota dari layanan tersebut, dengan kata lain hanya diperuntukkan untuk pelanggan yang telah membayar.



Gambar 1. Salah satu layanan televisi berbayar

Pada umumnya, siaran pada televisi berbayar dipancarkan secara *broadcast*, namun hanya pelanggan yang membayarlah yang dapat menangkap siaran tersebut. Hal ini disebabkan sinyal *broadcast* yang dipancarkan telah dienkripsi dengan kunci yang unik. Untuk mengantisipasi siaran ini tidak dapat dinikmati oleh orang yang tidak memiliki hak, maka setiap pelanggan diberikan sebuah *smart card* yang mengandung kunci privat (*private key*) yang unik dalam konteks algoritma kriptografi kunci-publik. Selain *smart card*, pelanggan juga diberikan sebuah *card reader* yang dipasang pada pesawat tv yang nantinya berfungsi untuk membaca *smart card*. Setelah itu, pelanggan akan diberikan kunci simetri dalam bentuk terenkripsi dengan menggunakan kunci publik pelanggan. Selanjutnya, *smart card* yang dimiliki oleh pelanggan akan mendekripsi kunci simetri dengan kunci privat. Pada akhirnya, kunci simetri yang telah didapatkan akan digunakan untuk mendekripsi siaran *Pay TV* yang telah di *broadcast*.

## II. SEJARAH PAY TV

### A. Sejarah Umum

Perkembangan layanan televisi berbayar dapat dikatakan cukup pesat. Di Indonesia sendiri *Pay TV* merupakan hal yang tidak asing lagi. Tentu saja hal ini tidak lepas dari kemunculain pertama kali televisi berbayar. Dimulai saat Zenith meneliti kemungkinan adanya televisi berlangganan ketika televisi sendiri masih

dalam tahap penelitian dan pengembangan. Pada tahun 1940-an, *Zenith* memperkenalkan sebuah sistem televisi berbayar yang diberi nama *Phonevision* (mdr 0815) yang melayani pemutaran film-film dengan pemesanan melalui pesawat telepon. Awalnya televisi berlangganan sering diidentikkan dengan TV kabel, karena bermula pada tahun 1948 ketika warga Pennsylvania, Amerika Serikat kesulitan menerima siaran televisi karena terhalang perbukitan. Untuk mengatasi masalah ini, warga setempat memasang antenna untuk menangkap sinyal UHF yang dipakai dalam penyiaran program kemudian menarik kabel dari antena tersebut dan memasangnya ke rumah-rumah. Pada tahun 1972, *HBO (Home Box Office)* muncul dan memikat hati banyak kalangan, dan tentu saja dengan kemunculannya ini mata rantai televisi berlangganan makin kuat. Belum lagi tuntutan dan kebutuhan akan hiburan yang makin besar, membuat satelit pada era 1980-an menjadi primadona bagi perkembangan televisi berlangganan selanjutnya, sebut saja sistem *DBS (Direct Broadcast Satellite)* yang banyak diaplikasikan di berbagai negara. Sejarah dan perkembangan televisi berlangganan di Amerika memberikan peluang bagi terbukanya lahan komersial ini di wilayah lain seperti Eropa, Asia, dan Australia. Untuk kawasan regional Asia, Jepang pada tahun 1984 memperkenalkan sistem *DBS (Direct Broadcast Satellite)* yang pada akhirnya dipakai dalam industri televisi berlangganan.

### B. Sejarah di Indonesia

Seiring dengan perkembangan teknologi yang semakin pesat, kebutuhan masyarakat Indonesia terhadap hiburan yang berbasis teknologipun makin tinggi. Sama halnya dengan negara-negara lainnya, Indonesia juga telah mencicipi salah satu produk teknologi di industri pertelevisian, yaitu layanan televisi berbayar. TV berbayar ini menawarkan sistem pay-per-view melalui kabel atau DBS.

Di Indonesia, perusahaan televisi berlangganan pertama yang mengaplikasikan sistem DBS adalah Indovision. Indovision memulai operasi dengan menggunakan frekuensi C-Band melalui satelit Palapa C-2 pada awal tahun 1994, sampai akhirnya menggunakan perangkat S-Band melalui satelit INDOSTAR-1 atau lebih dikenal dengan nama CAKRAWARTA-1 pada akhir tahun 1997. Pada Mei 2009, Indovision meluncurkan Satelit INDOSTAR-2 guna menggantikan posisi Satelit INDOSTAR-1. Masih dengan menggunakan frekuensi S-Band, INDOSTAR-2 dioperasikan untuk mendukung transmisi teknologi penyiaran paling terbaru sehingga dimungkinkan untuk mendapat kapasitas 2 kali lipat dibandingkan satelit berikutnya.



Gambar 2. Logo dari Indovision

Setelah kemunculan Indovision untuk pertama kalinya, lalu muncul perusahaan-perusahaan lain seperti:

- PT MNC Sky Vision (Indovision & Top TV), satelit
- PT Indosat Mega Media (IM2/Indosat M2), kabel
- PT Link Net (First Media), kabel
- PT Mentari Multimedia (M2V), terrestrial
- PT Indonusa Telemedia (Telkom Vision), Kabel dan satelit
- PT Indonusa Telemedia (Yes TV), satelit
- PT Nusantara Vision (Okevision), satelit
- PT Karyamegah Adijaya (Aora), satelit
- PT Cipta Skynindo (Skynindo), satelit
- PT Telekomunikasi Indonesia (Groovia), IPTV

## III. MEDIA PAY TV

### A. Kabel / Wireless Cable

Di Indonesia, perusahaan yang menggunakan jaringan kabel dalam industri *Pay TV* adalah PT Telkom, yaitu menggunakan kabel broadband dalam pendistribusiannya.

#### Komponen utama sistem kabel

- *Headend*: berfungsi menangkap sinyal yang dibawa dari satelit maupun gelombang lain di udara yang kemudian akan didistribusikan kepada cable plant (jaringan kabel).
- *Trunk Cable*: berfungsi membawa sinyal, biasanya dilengkapi dengan *broadband amplifiers* setiap 2000 kaki agar dapat mempertinggi kekuatan sinyal.
- *Distribution of feeder cable*: berfungsi memperpanjang sinyal dari *trunk* menuju gardu induk sebelum disalurkan kepada masing-masing pelanggan.
- *Subscriber drop*: berfungsi menyalurkan sinyal dari gardu induk kepada masing-masing pelanggan.
- *Terminal equipment*: komponen yang diletakkan di setiap rumah pengguna layanan. Dapat berupa kabel modem, seperangkat televisi atau alat lain.

Pada sistem kabel dalam layanan televisi berbayar terdapat beberapa kekurangan. Sistem ini membutuhkan dana operasional yang sangat besar walaupun mekanisme

pendistribusiannya sederhana. Ketersediaan layanan ini sangat bergantung pada berapa banyak kabel yang dimiliki oleh *provider* dan wilayah mana saja yang akan menjadi target pemasarannya. Untuk keperluan peningkatan kualitas dan kapasitas, penggunaan serat optik merupakan pilihan yang tepat, karena potensi terkena gangguan terhadap kabel yang ditanam maupun yang digantung yang makin besar. Terlebih lagi media kabel konvensional dan serat optik ternyata masih mampu untuk disadap.

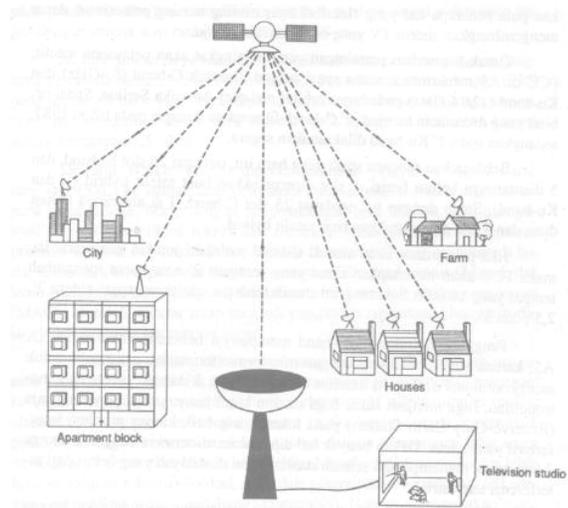
### B. Satelit / DBS (Direct Broadcasting Satellite)

DBS adalah siaran televisi melalui satelit langsung ke pesawat televisi (melalui antena), di Indonesia Indovision merupakan perusahaan yang menggunakan sistem satelit dalam pendistribusian layanan *Pay TV*.

Mekanisme penyiaran satelit untuk *Pay TV* yaitu, dimulai ketika *provider* memancarkan siarannya ke satelit (*uplink*) lalu kemudian sinyal tersebut ditransfer dan dikirim lagi menuju ke bumi (*downlink*). Di Indonesia kita bisa mengakses siaran-siaran TV dari seluruh dunia. Siaran tersebut pertama kali dipancarkan dari tempat produksi siaran dilakukan, kemudian dipancarkan kembali melalui satelit di Indonesia sampai akhirnya kita bisa menikmati ratusan tayangan dari berbagai negara di dunia. Pelanggan dapat menerima siaran itu dengan alat berupa penangkap sinyal satelit yang telah dihubungkan pada pesawat televisi pelanggan. Dengan kata lain, orang yang tidak memiliki alat tersebut tidak akan dapat menangkap siaran yang dipancarkan satelit.

#### Alat penangkap sinyal satelit

- *Satellite dish (Out Door Unit)*: komponen ini berbentuk seperti antena parabola dengan diameter sekitar 60-180 cm.
- *Decoder*: berfungsi mengakses layanan seperti penggantian saluran.
- *Smart card*: berfungsi untuk mengakses sistem.



Gambar 3. Mekanisme penyiaran melalui satelit

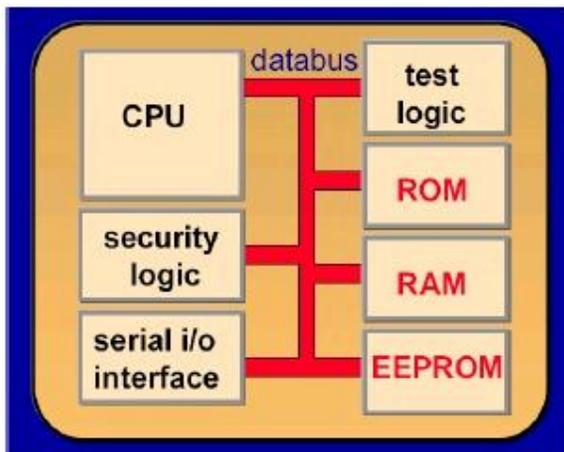
## IV. SMART CARD PADA PAY TV

### A. Smart card

*Smart card* merupakan sebuah kartu yang mengandung *embedded chip* komputer, baik tipe memori ataupun mikroprosesor, yang memiliki fungsi untuk melakukan transaksi dan menyimpan data. Data pada transaksi umumnya diasosiasikan dengan sebuah nilai atau informasi lalu disimpan pada chip dalam kartu. Pemrosesan data dilakukan melalui sebuah alat pembaca yang merupakan bagian dari sebuah sistem komputer.

*Smart card* pertama kali digunakan di Eropa tiga sebagai alat penyimpan nilai telepon untuk menghindari pencuri. Perkembangan *smart card* sangat pesat, sehingga aplikasinya dapat ditemukan di bidang apapun.

Di negara-negara maju, penggunaan *smart card* telah mendominasi semua aspek kehidupan, seperti berbelanja, menonton film, alat komunikasi, dan tanda pengenal. Hal ini mungkin disebabkan dari banyaknya keuntungan yang didapat dari penggunaan *smart card*, seperti lebih sedikit biaya yang dikeluarkan dan keamanan yang lebih terjamin.



Gambar 4. Skema dalam *smart card*

Penjelasan dari Gambar 4.

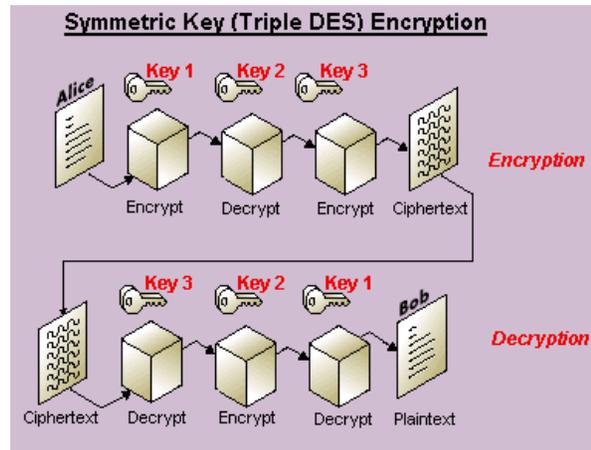
- CPU (Central Processing Unit) adalah jantung utama dari chip.
- Security logic digunakan untuk mendeteksi kondisi abnormal, seperti kondisi cahaya.
- Serial i/o interface berfungsi untuk berkomunikasi dengan benda diluar chip.
- Test logic berisi sekumpulan prosedur untuk melakukan self-test pada chip.
- ROM berisi sistem operasi dari kartu.
- RAM dapat dianalogikan seperti kertas coretan untuk CPU yang berguna untuk lalu lintas data dari dan ke CPU.
- EEPROM berisi data-data rahasia yang disimpan oleh kartu. Data-data rahasia iniantara lain, kunci-kunci kriptografi, kodePIN, template biometric dan kode aplikasi.
- Databus bertugas untuk menghubungkan seluruh elemen dari chip.

### B. Kriptografi Smart card

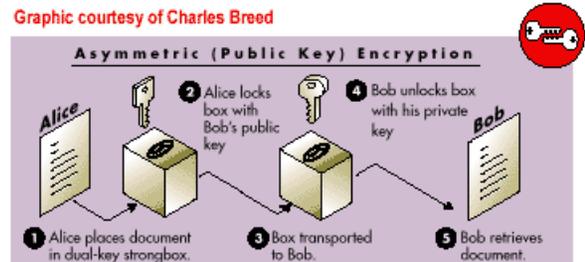
Kriptografi merupakan suatu ilmu yang dapat menjaga atau melindungi kerahasiaan suatu data. Dalam *smart card* terdapat data-data penting milik pemegang kartu yang harus dijaga kerahasiaannya. Aspek kerahasiaan dijaga dengan penggunaan enkripsi untuk melindungi informasi pada kartu. Ilmu kriptografi dimanfaatkan dalam beberapa hal, yaitu untuk :

1. Melakukan enkripsi data untuk melindungi keamanan data
2. Memastikan keaslian data, dengan cara mengenali jika data telah dimanipulasi
3. Memastikan data tetap unik dengan melakukan pengecekan bahwa data asli dan bukan merupakan kopi dari data yang asli. Untuk itu pengirim akan menyertakan tanda yang unik pada data asli.

Untuk mendapatkan sebuah chiperteks, data awal (plaintexts, dapat dibaca jelas) akan dienkripsi terlebih dahulu. Proses enkripsi ini membutuhkan algoritma enkripsi dan kunci. Algoritma tersebut terdiri dari dua, yaitu algoritma simetri dan asimetri. Biasanya untuk algoritma simetri digunakan Triple-DES dengan mode tiga kunci. Untuk lebih jelasnya dapat dilihat pada gambar dibawah ini.



Yang kedua algoritma asimetri dengan algoritma RSA sebagai algoritma yang paling umum. Untuk lebih jelasnya, skema algoritma tersebut dapat dilihat pada gambar di bawah ini.



### C. Smart card Pay TV

Pada layanan televisi berbayar, pelanggan akan diberikan sebuah *smart card* yang mengandung kunci privat (*private key*) yang unik dalam konteks algoritma kriptografi kunci-publik. Selanjutnya *smart card* akan mendekripsikan kunci simetri yang diberikan dengan kunci privat. Pada akhirnya kunci simetri yang didapat akan mendekripsikan siaran yang telah dipancarkan satelit dan pelanggan dapat menikmati tayangan-tayangan dari seluruh dunia.



Gambar 5. Peralatan pada layanan Top TV

## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Desember 2011

Dwitri Desvira (13510044)

## V. KESIMPULAN

*Pay TV* merupakan layanan yang diberikan oleh suatu perusahaan yang memberikan tayangan dari berbagai negara. Pelanggan yang dapat menikmati tayangan adalah pelanggan yang telah membayar kepada perusahaan tersebut secara berkala. Setiap pelanggan akan mendapatkan suatu kartu yang dikenal sebagai *smart card*, yang berfungsi untuk menangkap sinyal dari satelit.

Sistem penyiaran *Pay TV* ada dua, yaitu melalui kabel dan melalui satelit. Sistem kabel yaitu sistem yang menggunakan broadband kabel dalam pendistribusiannya. Sedangkan sistem satelit dimulai ketika *provider* memancarkan siarannya ke satelit (*uplink*) lalu kemudian sinyal tersebut ditransfer dan dikirim lagi menuju ke bumi (*downlink*).

Agar pelanggan dapat menangkap siaran dari *provide*, setiap pelanggan memiliki sebuah *smart card* yang nantinya berfungsi untuk mendekripsikan siaran yang telah di broadcast. Proses dekripsi pada *smart card* dimulai dengan mendekripsikan kunci simetri yang diberikan dengan kunci privat yang ada pada *smart card* pelanggan. Setelah mendapatkan kunci simetri, selanjutnya *smart card* akan mendekripsikan siaran yang telah disiarkan oleh penyedia layanan.

## REFERENCES

- [1] Munir, Rinaldi. *Matematika Diskrit*. Edisi Ketiga. 2005. Bandung. Penerbit Informatika.
- [2] Makalah -021 <http://www.scribd.com/doc/55801217/Makalah-021>. Tanggal akses : 11 Desember 2011
- [3] Wikipedia (2010) Televisi Berlangganan. [http://id.wikipedia.org/wiki/Televisi\\_berlangganan](http://id.wikipedia.org/wiki/Televisi_berlangganan). Tanggal akses : 11 Desember 2011
- [4] Kriptografi dalam kehidupan sehari-hari. [http://www.informatika.org/~rinaldi/Buku/Kriptografi/Bab-14\\_Kriptografi%20dalam%20Kehidupan%20Sehari-hari.pdf](http://www.informatika.org/~rinaldi/Buku/Kriptografi/Bab-14_Kriptografi%20dalam%20Kehidupan%20Sehari-hari.pdf). Tanggal akses : 11 Desember 2011
- [5] Pengembangan Teknologi Komunikasi. <http://edwi.dosen.upnyk.ac.id/PTK.9.05.pdf>. Tanggal akses : 11 Desember 2011
- [6] Aplikasi Kriptografi pada *Smart Card* di Indonesia. <http://www.informatika.org/~rinaldi/Kriptografi/2010-2011/Makalah2/Makalah2-IF3058-Sem2-2010-2011-017.pdf>. Tanggal akses : 11 Desember 2011