رمزکننده های پهنای باند بالا

فهرست

مقدمه

برقراری ارتباط از راه‌دور، در تمام دوران تاریخ بشری، از آمال و آرزوهای بزرگ آدمی بوده است. برقراری ارتباط، از طریق ایجاد دود، توسط سرخپوستان، ارسال نامه‌ها، توسط کبوترهای نامه‌بر و چاپار، اختراع مورس و سپس تلفن، نمونه‌هایی است که بشر، در اعصار مختلف توانست، دامنه ارتباط خود را با پیرامونش توسعه دهد. در عصر رایانه‌ها و ماهواره‌ها، بشر می‌تواند در آن واحد، تصویر، صدا و دیگر اطلاعات مورد نیاز خود را در حداقل زمان، ارسال و یا دریافت کند. همزمان با ورود به قرن بیست و یکم و علی‌رغم توسعه و پیشرفت ارتباطات رادیویی و ماهواره‌ای و به دلیل انتشار روزافزون امواج الکترومغناطیسی، در فضای جو، توجه دست اندرکاران صنعت مخابرات و مراکز تحقیقاتی به ارتباطات با سیم و فناوری‌های روز، یعنی فیبرنوری چشمگیرتر شد، تا آنجا که، در خیلی از کشورها شبکه تلویزیونی کابلی (CABLE-TV) و ISDN، مجهز به سیستم پیشرفته انتقال فیبرنوری شده است.

تکنولوژی اطلاعات و ارتباطات و پیشرفت‌های چشمگیر بوجود آمده در این حوزه باعث شده تا دولت‌ها را وادار سازد ضمن توسعه و ارتقاء این تکنولوژی‌ها، ساز و کار نظارت و امنیت این نوع ارتباطات را در رئوس کارهای خود قرار دهد. با افزوده شدن بر تعداد خدمات ارائه شده و استفاده اغلب زیرساخت‌های کشور از شبکه‌های ارتباطی و رایانه ای از یکطرف و لزوم حفظ امنیت، ایمنی و پایداری این زیرساخت‌ها و ارتباط تنگاتنگ آن با امنیت ملی از سویی دیگر استفاده از روش‌هایی برای امن‌سازی داده‌های مبادله شده ضروری است. بی‌تردید رمزنگاری جزء لاینفک یک شبکه امن بوده و با استفاده از الگوریتم‌های مختلف رمزنگاری می‌توان میزان خطری که شبکه‌ها را تهدید می‌کند، به حداقل رسانید. لذا در این مجال نگاهی کوتاه به علم

اپتیک و ضرورت پیدایش آن و بررسی مفاهیم SDH[1] و رمز نگاری و در نهایت بررسی دستگاه‌های رمزکننده سخت افزاری پهنای باند بالا با ملاحظات پدافند غیر عامل پرداخته می شود.

[1] Synchronous Digital Hierarchy

فصل ۱

سیر تاریخی ارتباطات نوری

در اوایل استفاده از فیبر نوری، هر شرکت تلفن، یک سیستم TDM[۱] مربوط به خود داشت. پس از تجزیه شدن شرکت AT&T در سال ۱۹۸۴ شرکت‌های تلفن محلی مجبور بودند، حامل‌های فاصله‌های طولانی با سیستم‌های TDM مختلف را به هم متصل کنند. بنابراین نیاز به استانداردسازی سیستم‌های TDM کاملا محسوس بود. درسال ۱۹۸۵، Bellcor شروع به کار کردن روی استانداردهایی به نام SONET[۲] کرد. پس از مدتی CCITT[۳] نیز به این پروژه ملحق شد و حاصل کار، استاندارد SONET و توصیه‌نامه‌های موازی CCITT بود که SDH[٤] نامیده شدند و در حد بسیار کمی با SONET متفاوت می‌باشند.

---

[۱] Time Division Multiplexing

[۲] Synchronous Optical Network

[۳] International Telegraph and Telephone Consultative Committee (CCITT)

[۴] Synchronous Digital Hierarchy

استاندارد SONET

SONET برای ۴ هدف اصلی طراحی شد.

- ایجاد امکان اتصال شبکه‌های مختلف به یکدیگر
- یکپارچه‌سازی سیستم‌های دیجیتالی اروپا و آمریکا و ژاپن
- تسهیم‌کردن چندین کانال دیجیتالی

در آن زمان که SONET طراحی شد، پر سرعت‌ترین حامل دیجیتال که در آمریکا به صورت گسترده استفاده می‌شد T۳ با سرعت ۶۶.۷۳۶ Mbps بود. T۴ نیز تعریف شده بود ولی کاربرد چندانی نداشت و سرعت بالاتر از T۴ حتی تعریف نشده بود. بخشی از ماموریت SONET این بود که سرعت‌های GigaBits/sec وبالاتر را تعریف کند. همچنین یک راه استاندارد برای تسهیم کردن کانال‌های با سرعت کمتر به کانال SONET مورد نیاز بود.

- فراهم آوردن پشتیبانی لازم برای عملیات سرپرستی و نگهداری شبکه

اولین تصمیم برای SONET این بود که از سیستم TDM متداول استفاده شود. به این صورت که همه پهنای باند فیبر به عنوان یک کانال در نظر گرفته شود که شامل شیارهای زمانی[۱] است و در هر زمان زیرکانال مربوطه، پیام خود را روی کانال می‌فرستد. بنابراین سیستم SONET یک سیستم همزمان است. این سیستم با یک ساعت مرکزی کنترل می‌شود که دقت آن یک میلیاردیم ثانیه است. بیت‌ها روی خط

---

[۱] Time Slots

SONET در بازه‌های دقیقی فرستاده می‌شوند که توسط ساعت مرکزی کنترل می‌شود.

وقتی ایده سوئیچینگ بسته‌ای[1](که اساس کار شبکه‌های ATM است و براساس آن لازم نیست بسته‌ها همه به ترتیب و از یک مسیر به گیرنده برسند) مطرح شد، برای اینکه تفاوت آن با سیستم سنکرون SONET مشخص شود آن را Asynchronous Transfer Mode نامیدند. در سیستم SONET فرستنده و گیرنده به یک ساعت مشترک متصل شده‌اند در حالیکه در ATM چنین نیست.

استاندارد SDH

تکنولوژی SDH در ادامه‌ی تکنولوژی قدیمی‌ترPDH[2] به بازار ارائه گردید. تفاوت اصلی آن با تکنولوژی PDH در آن است که در PDH سطوح تسهیم‌کردن به صورت سلسله مراتبی و از قبل هماهنگ‌شده کار می‌کند. به این معنی که اگر لازم است یک بسته از یک سلسله مراتب پایین مثلا E۱ از داخل یک بسته با سلسله مراتب بالاتر مثلا E۴ خارج گردد، بسته E۴ باید به بسته‌های E۳ دی‌مالتی‌پلکس گردد و سپس بسته E۳ به E۲ و در ادامه بسته E۱ از داخل E۲ استخراج گردد و نمی‌توان E۱ را مستقیما از E۴ استحصال کرد و بیرون آورد. ولی در SDH می‌توان سلسله مراتب‌های پایین‌تر را از سلسله مراتب‌های چندین مرتبه بالاتر نیز یک مرتبه بیرون کشید و خارج کردن یک بسته ۲ مگابیتی از یک بسته ۱۵۵ مگابیتی در یک مرحله از دی‌مالتی‌پلکس‌کردن انجام می‌گردد. بدین ترتیب، SDH دارای قابلیت انعطاف‌پذیری بالایی است و سطح دسترسی به اطلاعات را بخوبی فراهم می‌کند.

درضمن مزیت دیگری که در تکنولوژی SDH وجود دارد این است که SDHتکنولوژی PDH را کاملا پشتیبانی می‌کند و شبکه‌های PDH به راحتی می‌توانند با شبکه های SDH ارتباط برقرار کنند. امروزه تکنولوژی SDH مانند

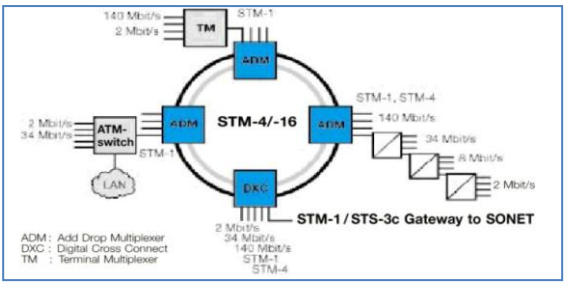
---

[1] Packet Switching

[2] Plesiochronous Digital Hierarchy

تکنولوژی PDH که در دهه‌های قبلی، تکنولوژی قالب انتقال بود درحال حاضر تکنولوژی قالب شبکه‌های انتقال در اکثر کشورها می‌باشد.

SDH نیز مانند SONET یک تکنولوژی تسهیمی تقسیم زمانی یا TDM است و عمل تسهیم در آن به روش سلسله مراتبی انجام می‌شود. در ضمن در این سیستم همیشه امکان افزودن و یا کاستن کانال‌ها وجود دارد. در مقایسه با سیستم قدیمی PDH در سیستم SDH استخراج یا جای‌دادن کانال‌های کم‌سرعت به جریان‌های پرسرعت، خیلی آسان‌تر انجام می‌گیرد و بدین ترتیب نیازی به دی‌مالتی‌پلکس و سپس مالتی‌پلکس دوباره نمی‌باشد.



نمای قیاسی از شبکه‌های ارتباطی مختلف

شکل فوق نمای قیاسی از ساختمان یک حلقه SDH با شاخه‌های گوناگون و سیگنال‌های وابسته به آن را نشان می‌دهد. همزمانی، مزیت انتقال سریع داده‌ها بدون نیاز به تاخیر زمانی را دارد. در این شبکه به پالس‌های زمانی خیلی دقیق نیاز می‌باشد و این پالس‌های زمانی بایستی در سرتاسر یک شبکه کامل توزیع شده باشند.

علاوه بر شبکه‌های PDH، SDH و ATM می‌توان به شبکه‌ی جدید OTN[۱] اشاره کرد که در آینده مورد استفاده قرار خواهد گرفت. دو استاندارد برایSDH

---

۱ Oracle Technology Network

وجود دارد؛ یکی CCITT (همان ITU[1] امروزی) و دیگری ANSI، که استانداردهای CCITT (STM-n علامت اختصار این استاندارد) کلی تر از ANSI (OC-n علامت اختصار این استاندارد) می‌باشند، یعنی ANSI قابل انتقال با استانداردهای CCITT می‌باشد.

۱ International Telecommunication Union(ITU)

فصل ۲

معرفی مفاهیم SDH

در مقابل سیستم‌های SDH که جهت انتقال سیگنال‌های با ظرفیت بالا استفاده می‌شود و شامل مراحل فریم‌بندی و تسهیم کردن همزمان می‌باشد، در سیستم‌های PDH، یک سیگنال رده‌بالا از ترکیب چندین سیگنال رده‌پائین خود تشکیل می‌شود و از معایب این سیستم این است که یک استاندارد کلی در جهان ندارد و دارای استانداردهای مختلفی است و همین امر موجب بروز اشکالات بزرگی از قبیل یکپارچه نبودن بایت‌های عملیاتی مختلف و مراحل متوالی مالتی پلکسینگ و دی مالتی پلکسینگ که منجر به نیاز به تجهیزات و هزینه های بیشتر می‌شود. از جمله مزایای تکنولوژی SDH موارد زیر را می‌توان نام برد:

- استفاده از تکنیک‌های تسهیمی همزمان، منجر به طراحی‌های کم هزینه‌تر در شبکه می‌شود.
- سیگنالSDH، ظرفیت انجام پروسه‌های مدیریتی و نگهداری شبکه را دارد.

- این تکنولوژی قابلیت انتقال سیگنال‌های مختلف، ازجمله سیگنال‌های مربوط به تکنولوژی‌های شبه‌همزمان قبلی و تکنولوژی‌های آینده، را دارد.
- با استفاده از یک واسط استاندارد، امکان ایجاد ارتباط بین تجهیزات تولیدکنندگان مختلف را فراهم می‌سازد.

استانداردهایی که توسط سازمانITU_T برای SDH معرفی شده‌اند نرخ بیت، ساختار، لایه فیزیکی، خصوصیات معماری اجزاء شبکه و معیارهای عملکرد شبکه در شبکه‌های SDH را بیان می‌کنند.

همزمان سازی[1] در SDH

برای انتقال دقیق اطلاعات روی شبکه SDH، زمانبندی بین ابزارهای شبکه از مسائل مهم می‌باشد. درآغاز پیدایش شبکه‌ها، متدهای زمانبندی غیرهمزمان[2] مورد استفاده قرار می‌گرفت. اما اکنون از روش‌های همزمان استفاده می‌شود.

برای زمانبندی همزمان در SDH پنج متد به‌کار می‌رود:

- زمانبندی داخلی با استفاده از اسیلاتور داخلی روی بورد با چرخش آزاد (پالس‌های ساعت Stratum ۳E یا Stratum ۳)
- زمانبندی خط[3]، مشتق شده از سیگنال SDHای که Scramble[4]ه شده و از اینترفیس پر سرعت دریافت می‌شود.

---

[1] Synchronization

[2] Asynchronous

[3] Line timing

[4] پروسه ای که جهت جلوگیری از از دست رفتن قدرت بازیابی پالس ساعت سیگنال در سمت گیرنده و فرستنده، به واسطه ارسال رشته‌های طولانی صفر و یک صورت می‌گیرد.

- زمانبندی سراسری[1]، که از یک ورودی نشأت می‌گیرد ولی سیگنال را در مسیر متفاوتی در خروجی پالس[2] می‌زند.
- زمانبندی حلقه‌ای[3]، که شبیه زمانبندی خط است ولی توسط تجهیزات خانگی مشتریان یا تجهیزات مالتی پلکسر پایانی (terminal multiplexer)، به غیر از ADMها مورد استفاده قرار می‌گیرد.
- زمانبندی خارجی[4]، که از یک منبع خارجی مانند یک سیستم GPS Stratum۱ یا یک پالس ساعت اتمی استفاده می‌کند.

سلسله مراتب انتقال در SDH

عبارت STM-N [5]، به مشخصه انتقال لینک سطح N، گفته می‌شود. برخلاف SONET که برای حامل‌های نوری‌اش عبارت OC-N و برای سطوح سیگنال الکتریکی STS-N را بکار می‌برد، سیستم SDH عبارت STM-N را برای هردو سیگنال الکتریکی و نوری بکار می‌گیرد.

واحد پایه انتقال در SDH، ۱۵۵.۵۲ Mbps می‌باشد که مربوط به STM-۱ است. برای دسترسی به نرخ بیت بیشتر، از حالت تسهیم سیگنال پایه(STM-۱) استفاده می‌شود. ریت‌های بالاترSDH، مضارب صحیحی از STM-۱ در رشته N*۴ می‌باشند. مقادیر استاندارد شده جهت نرخ بیت‌های بالاتر عبارتند از: (STM-۴)۶۲۲.۰۸۰Mb/s و (STM-۱۶)۲.۴۸۸۳۲Gb/s و (STM-۶۴)۹.۹۵۳۲۸۰Gb/s که به صورت

---

[1] Through timing
[2] Clock
[3] Loop timing
[4] External timing
[5] Synchronous Transport Module-N (STM-N)

STM-N(N=۱,۴,۱۶,۶۴) نشان داده می‌شوند. لازم به تذکر است که بیت ریت پایه در شبکه SONET، ۵۱.۸۴Mb/s می‌باشد که به آن STS-۱ گفته می‌شود. در شبکه SDH به این بیت ریت STM-۰ گفته می‌شود که البته استاندارد نبوده ولی در بعضی از سیستم‌ها استفاده می‌شود. این بیت ریت در تکنولوژی‌های رادیویی یا ماهواره‌ای با ظرفیت کم/متوسط مورد استفاده قرار می‌گیرد.

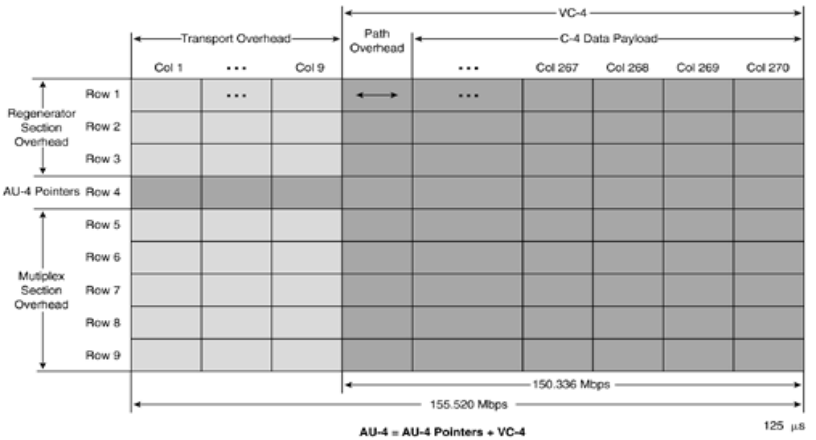
انطباق جزئی در سطح STM-۱ بین SONET و SDH وجود دارد. اما از لحاظ مدیریت کارآیی و آلارم‌ها بین شبکه‌های SONET و SDH هماهنگی نیست.

SDH Level	Line Rate (Mbps)	Payload Rate (Mbps)	Overhead Rate (Mbps)	SONET Equivalent
STM-۰	۵۱.۸۴۰	۵۰.۱۱۲	۱.۷۲۸	STS-۱
STM-۱	۱۵۵.۵۲۰	۱۵۰.۳۳۶	۵.۱۸۴	STS-۳
STM-۳	٤٦٦.٥٦٠	٤٥١.٠٠٨	۱۵.۵۵۲	STS-۹
STM-٤	٦٢٢.٠٨٠	٦٠١.٣٤٤	۲۰.۷۳٦	STS-۱۲
STM-٦	۹۳۳.۱۲۰	۹۰۲.۰۱٦	۳۱.۱۰٤	STS-۱۸
STM-۸	۱۲٤٤.۱٦۰	۱۲۰۲.٦۸۸	٤۱.٤۷۲	STS-۲٤
STM-۱۳	۱۸٦٦.۲٤۰	۱۸۰٤.۰۳۲	٦۲.۲۰۸	STS-۳٦
STM-۱٦	۲٤۸۸.۳۲۰	۲٤۰٥.۳۷٦	۸۲.۹٤٤	STS-٤۸
STM-۳۲	٤۹۷٦.٦٤۰	٤۸۱۰.۷٥۲	۱٦٥.۸۸۸	STS-۹٦
STM-٦٤	۹۹٥۳.۲۸۰	۹٦۲۱.٥۰٤	۳۳۱.۷۷٦	STS-۱۹۲
STM-۲٥٦	۳۹۸۱۳.۱۲۰	۳۸٤۸٦.۰۱٦	۱۳۲۷.۱۰٤	STS-۷٦۸

ساختار فریم SDH

SDH از ریت ۸۰۰۰ فریم در ثانیه تبعیت می‌کند. فریم STM-۱، فرمت پایه برای انتقال SDH می‌باشد.

ساختار فریم STM۱ جهت سادگی به صورت آرایه‌ای دو بعدی از بایت‌ها نمایش داده می‌شود که درون جدولی به ابعاد ۲۷۰ * ۹ قرار گرفته‌اند. یک ساختار نمونه در شکل ذیل نشان داده شده است.



ساختار فریم پایه SDH (STM_۱)

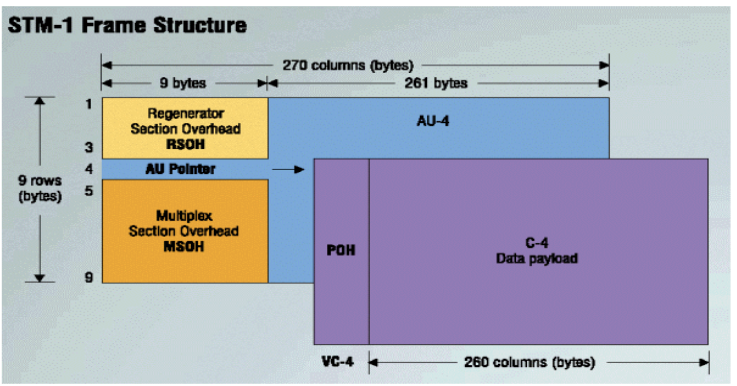
ابتدای فریم، بایتی با آدرس (۱،۱) می‌باشد و بایت انتهایی در موقعیت (۲۷۰ ، ۹) قرار گرفته است. عملیات انتقال بایت‌ها سطر به سطر از بایت اول تا آخرین بایت ادامه می‌یابد. طول زمانی این فریم ۱۲۵µs می‌باشد.

سرآیند بخش از دو ناحیه اصلی تشکیل شده است: سه سطر اول مربوط به سرآیند بخش‌بازساز (Regenerator Section Overhead –RSOH) بوده و سطرپنجم

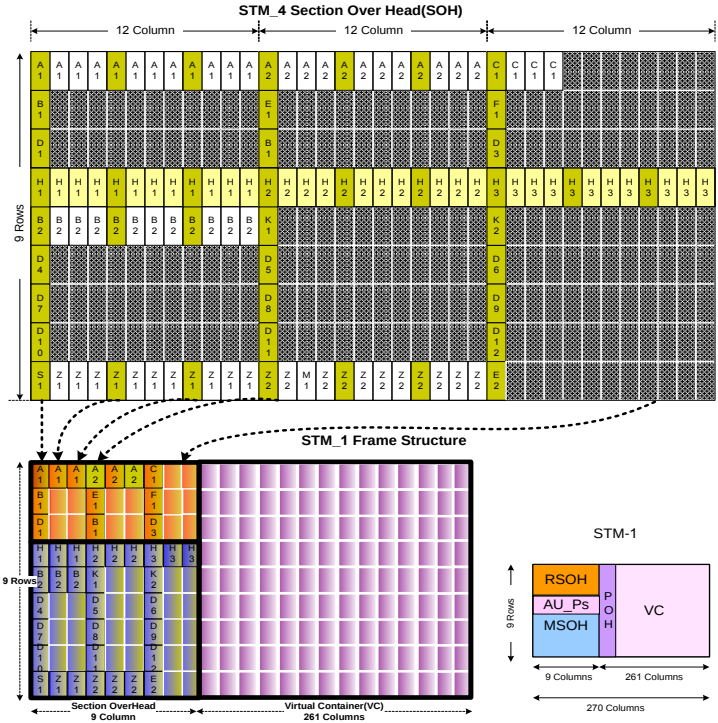
تا نهم مربوط به سرآیند بخش مالتی پلکس (Multiplexed Section Overhead-MSIH) می‌باشند.

ریت خطوط سنکرون STM-۱، ۱۵۵Mbps است و برای دسترسی به سرعت‌های بالاتر از روش‌های مالتی‌پلکس‌کردن استفاده می‌شود. خطوط STM-N استاندارد حاصله، نرخ N برابر خطوط STM۱ دارند که N نیز می‌تواند مقادیر ۱و۴و۱۶و۶۴ و۲۵۶ را بگیرد.

هر چه N بیشتر باشد درصد سرآیند نسبت به کل بسته بیشتر می‌شود. ولی نسبت سرآیند به Payload، ثابت باقی می‌ماند. سرآیند اضافه شده برای کنترل، پریتی، Stuffing و هشداردهی و سیگنالینگ بکار می‌رود.



ساختار یک فریم STM-۱



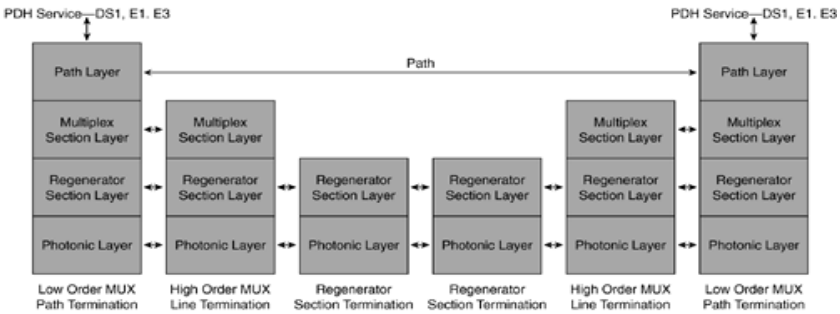
ساختار فریم ۴-STMو نحوه شکل‌گیری آن از طریق مالتی پلکس زمانی ۴ فریم ۱-STM

لایه‌های SDH

استاندارد SDH یک مدل لایه‌ای Client/server تعریف می‌کند که جهت مدیریت سرویس‌های انتقال، به چهار لایه تقسیم می‌شود. هر لایه با لایه متناظر خود با بکار بردن overheadهای ویژه، فرمت‌ها و پروتکل‌ها در ارتباط می‌باشد. این ساختار مشابه با مدل هفت لایه‌ای OSI می‌باشد که در ایجاد و تعریف شبکه‌ها بکار می‌رود.

این چهار لایه در شکل زیر نشان داده شده است :

- Path layer
- Multiplex section layer
- Regenerator section layer
- Photonic layer



شکل ۵ : مدل لایه‌ایSDH

لایه Path

Path یک کانکشن منطقی بین دو نقطه است که دریکی، فریم SDH با فرمت استاندارد برای نرخ خاصی فراهم می‌شود و در دیگری، فریم SDH با فرمت استاندارد از سیگنال دریافتی، پیاده می‌شود. در این لایه اطلاعات clientها، در یک فریم map/demap شده و سرآیند مسیر(POH) گذاشته و برداشته می‌شود. هشدارها و اطلاعات خطا در این لایه، وضعیت انتها به انتهای سیستم را نشان می‌دهد.

بخش Multiplex

بخش مالتی پلکس، یک ناحیه انتقال است به همراه تجهیزاتی که وسیله انتقال اطلاعات بین دوابزار شبکه‌ای (NE ۱) متوالی را فراهم می‌آورند. یکی از این ابزارهای شبکه، سیگنال line را تولید می‌کند و ابزاری دیگر این سیگنال را در انتهای دیگر خط، دریافت و پایان دهی۲ می‌کند.

سرآیند بخش مالتی پلکس (MSOH)، در این لایه گذاشته و برداشته می‌شود.

بخش Regenerator

بخش بازساز، در شبکه SDH، قسمتی از تسهیلات انتقال است که در برگیرنده نقاط پایان‌دهنده بین NEهای پایان‌دهنده و Regenerator یا فاصله بین دو Regenerator می‌باشد. بایت‌های سرآیند بخش بازساز (RSOH)، در این لایه گذاشته یا برداشته می‌شوند.

لایه Photonic

این لایه به صورت کلی با انتقال بیت‌ها از روی محیط فیزیکی فیبر سروکار دارد. عمل اصلی آن، مکالمات بین سیگنال‌هایSTM-N وانتقال پالس‌های نوری روی واسط فیبر می‌باشد. عملکردهای این لایه شامل موارد زیر می‌باشد: راه اندازی طول موج۳، شکل دهی پالس، مدولاسیون سطوح power.

---

۱ NE : Network Equipment
۲ terminate
۳ wavelength launching

معرفی تجهیزات مورد استفاده در شبکه‌های SDH

این ابزارها مشتمل‌اند بر ابزارهای بخش بازساز، ابزارهای بخش مالتی پلکس و ابزارهای پایان‌دهنده مسیر. این ابزارها با قرارگیری در کنار یکدیگر، توپولوژی‌های مختلفی را در شبکه SDH فراهم می‌آورند. نمونه‌ای از این ابزارها در ادامه معرفی می‌گردند.

بازساز[۱]

بازساز، ابزاری است که برای تقویت سیگنال‌های ضعیف شده بکار می‌رود و معمولاً در مواقعی بکار می‌رود که به دلیل فاصله زیاد بین مالتی‌پلکسرها، سطوح سیگنال در فیبر تضعیف می‌شود و دیگر قادر به درایو کردن دریافتگر۲ نمی‌باشد. به این ابزار repeater نیز گفته می‌شود.

تسهیم کننده ترمینال[۳]

تسهیم کننده ترمینال(TM)، یک المان پایان دهنده مسیر است که می‌تواند خطوط مختلف DS۱ وDS۳ وE۱ وE۳ وSTM-N را در یک نقطه متمرکز کند یا بر عکس.

به کمک این المان، سیگنال‌های PDH (شبکه‌های نیمه همزمان) مانند DS۱ و E۱ وE۳ را می‌توان روی Payloadهای متناظر در شبکه همزمان SDH نگاشت کرده

---

۱ Regenerator
۲ receiver
۳ Terminal Multiplexer

و پس از تبدیل الکتریکی به نوری، سیگنال STM-N منتجه را به خط تزریق نمود. عمل معکوس در زمان دریافت سیگنال انجام می‌شود. در عمل TM، یک ADM است که در مود ترمینال کار می‌کند و به این صورت اجازه می‌دهد کاربران با سرعت پایین به شبکه SDH دسترسی پیدا کنند.

تسهیم کننده Add/Drop[1]

ADM، یک پایان دهنده مسیر می‌باشد که می‌توان تعدادی سیگنال را روی یک سیگنال STM-N مالتی‌پلکس کند یا از روی آن دی‌مالتی‌پلکس کند. در یک سایت add/drop، فقط سیگنال‌هایی که دسترسی به آنها لازم است حذف یا اضافه می‌شوند. بقیه ترافیک بدون هیچ پردازش ویژه ای از داخل المان شبکه عبور می‌کند. علاوه بر آن ممکن است در ADM، سیگنالی پایان دهی شود یا دور بزنند.

سیستم اتصال متقاطع دیجیتال باند پهن[2]

سیستم اتصال متقاطع دیجیتال باند پهن(BDCS) ، می‌تواند یک تقاطع دوراهه را در سطوح E۳ وE۴ وSTM-N ایجاد کند. همچنین می‌تواند با سیگنال‌های سطوح بالاتر PDH یاSDH مانندE۳ و DS۳ وE۴ نیز اینترفیس برقرار کند. این المان می‌تواند برای برقراری ارتباط یک طرفه نیز بکار رود.

مهمترین تفاوت بین اتصال متقاطع وADM این است که اتصال متقاطع می‌تواند تعداد بیشتری STM-N را به یکدیگر متصل کند. BDCSها می‌تواند برای

---

۱ Add/Drop Multiplexer

۲ Broadband Digital Cross-Connect

آرایش‌دهی[۱]، ادغام[۲] و تفکیک STM۱ها یا برای مدیریت ترافیک باند وسیع بکار روند.

اتصال متقاطع دیجیتال باند وسیع[۳]

اتصال متقاطع دیجیتال باند وسیع (WDCS)، یک تقاطع دیجیتال است که سیگنال‌های سطح بالای SDH و E۳ را پایان دهی می‌کند. همچنین اتصالات متقاطع سطح پایین را نیز فراهم می‌آورد.

WDCS برای کاربردهای آرایش‌دهی سطح E۱ در جایگاه hub مناسب می‌باشد.

---

۱ grooming
۲ consolidation
۳ Wideband Digital Cross-Connect

فصل ۳

مروری بر مفاهیم رمزنگاری

تا چندی پیش برای تامین امنیت شبکه‌های داده، حفاظت فیزیکی و محدود کردن دسترسی افراد به شبکه‌ها کافی به‌نظر می‌رسید. اما امروزه برای برآورده کردن امنیت شبکه‌ها باید از روش‌های دیگری نیز بهره گرفت. محرمانگی[۱]، اطمینان از درستی داده‌ها[۲] و دسترسی دائم[۳] و در کنار آن احراز اصالت موجودیت‌ها[۴]، انکارناپذیری[۵] و کنترل دسترسی[۶]، به ترتیب از جمله اهداف پایه و فرعی هستند که باید در هنگام طراحی یک شبکه امن در نظر گرفته شوند. این اهداف قادرند از تهدیداتی همچون استراق سمع (دستبرد)[۷]، دستکاری[۱]، جعل[۲] و وقفه[۳] جلوگیری نمایند. علم

---

۱ Confidentiality
۲ Integrity
۳ Availability
٤ Authentication
٥ Non Repudiation
٦ Access Control
۷ Interception

رمزنگاری در راستای حل این مشکلات پا به عرصه وجود نهاده است. اگر منظور از پروتکل، یک فرایند چندسویه متشکل از زنجیره‌ای از قدم‌ها برای دستیابی به یک هدف معین در نظر گرفته شود، یک پروتکل رمزنگاری یک فرایند چندسویه برای نیل به یک هدف مرتبط با مقوله رمزنگاری (یکی از اهداف فوق) است.

در بین تهدیدات فوق، استراق سمع به عنوان حمله غیرفعال۴ و مابقی به عنوان حمله فعال۵ شناخته می‌شوند. در حمله غیرفعال محتوای پیام تغییر نمی‌کند ولی در حملات فعال از جمله ایفای نقش۶، تکرار۷، دستکاری و... صرفاً مشاهده پیام مطرح نیست و ممکن است که محتوای پیام تغییر کند.

هر پروتکل رمزنگاری توانایی پیش‌گیری از برخی تهدیدات مطرح شده را داشته و در نتیجه در هر زمان، بنا به تهدیدات موجود و همچنین شرایط محیط، باید از پروتکل‌های رمزنگاری مناسب استفاده نمود.

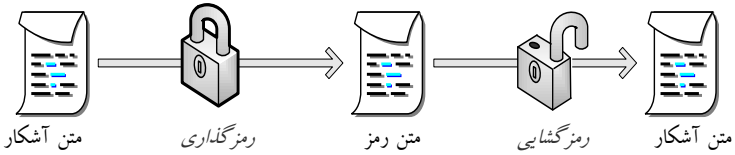
انواع سیستم‌های رمزنگاری

به‌طور کلی هر سیستم رمز۸ از اجزای مختلفی همچون یک فضای متن اصلی۹، یک فضای متن رمز شده۱۰، یک فضای کلید۱۱، مجموعه‌ای از تبدیل‌های

---

۱ Manipulation
۲ Fabrication
۳ Interruption
٤ Passive Attack
٥ Active Attack
٦ Masquerade
۷ Replay
۸ Cryptosystem
۹ Clear text
۱۰ Cipher text
۱۱ Key

رمزگذاری[1] و مجموعه‌ای از تبدیل‌های رمزگشایی[2] تشکیل شده است. مجموعه تبدیل‌های رمزنگاری و رمزگشایی، الگوریتم رمز نامیده می‌شود.



شکل ۵ : شمای کلی یک سیستم رمز

به‌طور کلی می‌توان سیستم‌های رمزنگاری را به دو دسته کلید متقارن[3] و کلید نامتقارن[4] تقسیم‌بندی نمود. در سیستم‌های رمز متقارن، تنها یک کلید وجود دارد که که تنها پارامتر مخفی سیستم رمز است که باید توسط کانال امنی میان رمزگذار و رمزگشا مبادله شود. به همین دلیل، ساختار این سیستم‌ها از سادگی نسبی برخوردار بوده و صحت و امنیت پیام را به طور همزمان تامین می‌نماید. تا قبل از دهه ۱۹۷۰ میلادی، سیستم‌های رمزنگاری از نوع سیستم‌های متقارن بودند ولی پس از آن به خاطر مشکلات به‌کارگیری آن‌ها، سیستم‌های نامتقارن به وجود آمدند و در کنار سیستم‌های متقارن به‌کار گرفته شدند. اساسی‌ترین مشکل سیستم‌های متقارن، نحوه تولید و مدیریت کلید در سیستم‌های با تعداد کاربر زیاد است. در سال ۱۹۷۶، دیفی و هلمن ایده رمزنگاری کلید عمومی را معرفی نمودند. بر اساس این ایده، عملیات رمزگذاری و رمزگشایی توسط دو کلید مجزا به نام‌های کلید عمومی و کلید خصوصی انجام می‌پذیرد. این دو کلید به‌گونه‌ای انتخاب می‌شوند که امکان محاسبه کلید عمومی از روی کلید خصوصی وجود داشته باشد ولی عمل عکس آن از نظر محاسباتی امکان‌پذیر نباشد. در این سیستم‌ها، امنیت و صحت پیام را می‌توان به

---

۱ Encryption
۲ Decryption
۳ Symmetric key
۴ Asymmetric key

صورت جداگانه تامین نمود. ایراد اساسی سیستم‌های نامتقارن نسبت به سیستم‌های متقارن، حجم محاسباتی بالای آن‌ها و درنتیجه سرعت کمتر آن‌ها است. به همین دلیل، اغلب برای رمز نمودن حجم زیادی از داده‌ها، از سیستم‌های متقارن استفاده می‌نمایند.

سیستم‌های رمز متقارن

از سیستم‌های رمز متقارن در متن‌های گوناگون با عنوان‌های مختلفی از جمله کلید خصوصی[۱]، کلید سرّی[۲]، یک کلیدی[۳] و تک کلیدی[۴] نام برده شده است. در این گونه از سیستم‌ها، کلیدهای رمزگذاری و رمزگشایی یکسان هستند یا به‌راحتی از یکدیگر نتیجه می‌شوند. در این سیستم‌ها، فرستنده توسط کلیدی که در اختیار دارد متن اصلی را با الگوریتمی مشخص رمز نموده و ارسال می‌کند. گیرنده نیز با همان کلید و الگوریتم رمزگشایی که عکس عمل رمزگذاری است، متن دریافتی را رمزگشایی می‌کند. از آن‌جایی‌که در این‌گونه از سیستم‌ها لازم است تنها فرستنده و گیرنده از مقدار کلید آگاه باشند، لذا کلید از طریق کانال امن میان آن‌دو مبادله می‌شود. در این سیستم‌ها مسیر انتقال پیام رمز شده و کلید می‌تواند متفاوت باشد. از ویژگی‌های رمزنگاری متقارن می‌توان به موارد زیر اشاره کرد:

- سیستم‌ها و الگوریتم‌های رمزنگاری متقارن از لحاظ عملکرد بسیار سریع هستند و امکان پیاده‌سازی سخت‌افزاری آن برای رمزنگاری بی‌درنگ داده‌ها تا نرخ‌های چندین گیگابیت بر ثانیه وجود دارد.

---

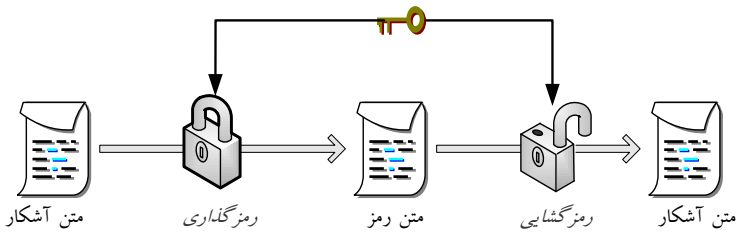
۱ Private Key
۲ Secret Key
۳ One Key
٤ Single Key

- در رمزنگاری متقارن، داده‌های متن اصلی در قالب بلوک‌هایی با طول ثابت و عموماً کوتاه (۶۴، ۱۲۸ یا ۲۵۶ بیتی) پردازش و رمز می‌شوند.
- امنیت کل داده‌ها به امنیت کلید گره خورده است و از آن‌جایی‌که کلیدهای رمزنگاری و رمزگشایی مشابه یکدیگرند، لذا طرفین ارتباط بایستی به روشی مطمئن بر روی کلید توافق نمایند (مثلاً از طریق ملاقات حضوری یا توسط شخص قابل اطمینان یا توسط سیستمی خودکار ولی مطمئن).
- هرگاه شخص یا سرویس‌دهنده‌ای بخواهد با تعداد زیادی از کاربران ارتباط امن و رمزنگاری شده داشته باشد، باید با تک‌تک آن‌ها کلیدی مجزا و مستقل را توافق کند. استفاده از کلیدی واحد توسط تمامی کاربران، امکان استراق سمع کاربران از اطلاعات یکدیگر را به‌وجود می‌آورد و درضمن سهل‌انگاری یا خیانت یکی از کاربران، امنیت تمامی آن‌ها را به‌خطر خواهد افکند.
- در شبکه‌ای که جمعاً n کاربر وجود دارد و دوبه‌دوی آن‌ها می‌خواهند با یکدیگر ارتباطی امن و رمزنگاری شده برقرار کنند، به تعریف و توافق $\frac{n(n-1)}{2}$ کلید سرّی و متقارن نیاز است.
- عموماً در تمام روش‌های رمزنگاری متقارن از توابع جانشینی[1] و توابع انتقالی[2] در طی چند مرحله استفاده می‌شود تا ارتباط بین ورودی و خروجی غیرقابل ردگیری باشد.

---

[1] Substitution
[2] Transposition

- بایستی الگوریتم به‌کار گرفته شده در سیستم‌های رمز متقارن دوطرفه باشند، یعنی باید تابع رمزگذاری تابعی معکوس‌پذیر باشد. معمولاً در این گونه از سیستم‌ها فرایند رمزگشایی و رمزنگاری تشابه کامل دارند و فقط مقادیر متغیرها و ثابت‌ها عوض می‌شوند ولی ذات ساختار الگوریتم رمزنگاری و رمزگشایی متحدالشکل و یکسان است.
- در سیستم‌های رمز متقارن بایستی طول کلید حداقل به‌اندازه‌ای باشد که قابل حدس زدن نباشد.



شکل ٦ : شمای کلی رمزنگاری متقارن

سیستم‌های رمز نامتقارن

در الگوریتم‌های رمزنگاری نامتقارن یا کلید عمومی، دو پارامتر به عنوان "کلید عمومی[۲]" و "کلید خصوصی[۳]" تعریف شده‌اند. با کلید عمومی می‌توان داده‌ها را رمز کرد ولی داده‌های رمز شده را نمی‌توان باز کرد. رمز داده‌ها فقط توسط کلید خصوصی باز می‌شود. پارامتر کلید عمومی در اختیار همگان قرار می‌گیرد و کلید

---

[۱] Round
[۲] Public Key
[۳] Private Key

خصوصی به صورت سری و محرمانه نزد صاحب آن نگهداری می‌شود. این روش رمز دارای خصوصیات زیر است:

- کلیدهای رمزگذاری ور مزگشایی متفاوت اما مرتبط هستند.
- رسیدن به کلید رمزگشایی از کلید رمزگذاری از لحاظ محاسباتی ناممکن می‌باشد.
- رمزگذاری امری همگانی می‌باشد و اساساً نیازی به به اشتراک گذاشتن اطلاعات محرمانه ندارد.
- رمزگشایی امری اختصاصی بوده و محرمانگی پیام‌ها محفوظ می‌ماند.
- کلیدهای عمومی و خصوصی عموماً اعدادی چندصد بیتی (تا چندهزار بیتی) هستند و الگوریتم‌های رمزنگاری قابل اعتماد نیز برمبنای تئوری اعداد بنا شده است.
- به کمک الگوریتم‌های کلید عمومی هرگاه n نفر بخواهند با یکدیگر ارتباطی امن داشته باشند، فقط به تعریف و توافق n جفت کلید نیاز است: به ازای هر نفر یک جفت کلید.
- روش‌های کلید عمومی دارای سرعت بسیار پایین هستند.

بر خلاف روش‌های متقارن که مبتنی بر جایگشت و جانشینی و استفاده از روش‌های غیرخطی معکوس‌پذیر هستند، روش‌های نامتقارن مبتنی بر توابع و مسائل ریاضی هستند و معمولاً امنیت آن‌ها وابسته به یک مسئله پیچیده ریاضی است. الگوریتم‌های RSA و الجمال نمونه‌های شناخته شده‌ای از رمزنگاری نامتقارن هستند که به‌ترتیب از دشوار بودن تجزیه حاصل‌ضرب دو عدد اول بزرگ و دشوار بودن محاسبه لگاریتم گسسته بهره می‌گیرند.

فصل ۴

معرفی سیستم رمز کننده خطوطSTM-n

پس از بیان مقدمات و مفاهیم در فصول قبلی، در این فصل به معرفی مقدماتی سیستم رمز کننده، نمونه کاربردهای این دستگاه، نمونه محصولات مشابه در این زمینه، تصویر کلی سیستم، بلوک دیاگرام سیستم، معرفی واحد های اصلی سیستم، پرداخته خواهد شد.

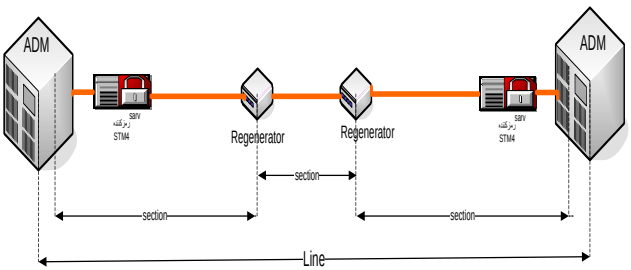
سخت‌افزار رمزکننده خطوط STM-n را می‌توان در لینک‌های Point to Point سنکرون SDH برای رمز کردن داده‌های مبادله شده میان خروجی فرستنده (پس از مالتی پلکسر) و ورودی گیرنده (قبل از دی‌مالتی پلکسر) به کار گرفت. این سخت‌افزار کلیه داده‌های خارج شده از فرستنده را با سرعت خط رمز نموده، برروی خط ارسال می‌کند و در طرف گیرنده نیز پس از رمزگشایی داده‌های دریافت شده، آن‌ها را دراختیار گیرنده قرار می‌دهد.

جایگاه‌های مورد استفاده سیستم

شبکه‌های پرسرعت امروزی بیشتر بر اساس تکنولوژی سنکرون SDH/SONET می‌باشند. کانکشن‌های OC-۳ و OC-۱۲ و OC-۴۸ با سرعت های انتقالی از ۱۵۵Mbps تا ۲.۴ Gbps در حوزه‌های کاربردی وسیعی مورد استفاده قرار می‌گیرند. نمونه این کاربردها کانکشن بین PBX[۱]ها، لینک‌های سیمی- لیزری، لینک‌های رادیویی بر اساس SONET می‌باشد.

دستگاه مورد نظر، مستقل از پروتکل لایه‌های بالاتر قابلیت رمز کردن یک لینک را دارا می‌باشد.

کاربرد این دستگاه در مود Line می‌باشد. شکل‌های ذیل نمونه کاربردهای این دستگاه را نشان می‌دهد:



شکل ۷ : نمونه کاربرد دستگاه بین دو Add/Drop Multiplexer

شکل ۸ : نمونه کاربرد دستگاه رمزکننده خطوط STM٤ در یک لینک Point-to-point

[۱] Private Branch Exchange

نمونه های مشابه محصول در بازار جهانی

جهت شناخت بازار بایستی محصولات مشابه نمونه‌های مختلفی از رمزکننده‌های لینک با سرعت‌ها و فرمت‌های مختلف بررسی و مقایسه گردد تا با تقویت دیدگاه، محصولی با کاربرد مناسب‌تر و قابلیت‌هایی در حد قیمت مورد نظر طراحی و تولید گردد.

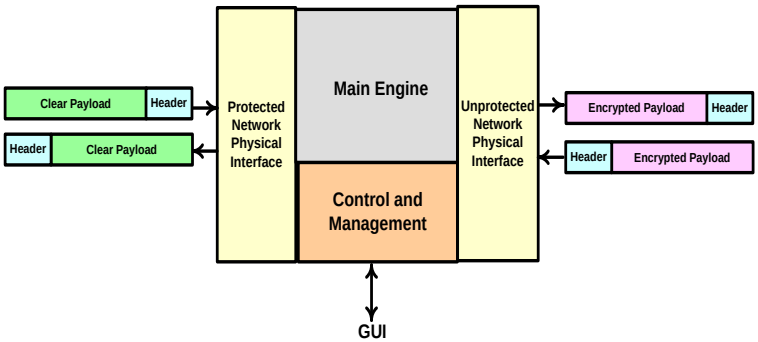
در جدول زیر نام محصولات رمزکننده خطوط SDH/SONET را نشان می‌دهد.

جدول ۱ : محصولات بررسی شده در زمینه رمزکننده خطوطSDH

	نام محصول و کارخانه سازنده
۱	Thales : Datacruptor SONET/SDH OC-۳/۱۲/٤۸
۲	CRYPTO AG: SONET/SDH Encryption HC-۸٥٤٤ STM-٤
۳	SafeEnterprise SONET Encryptor for OC۳, OC۱۲, OC٤۸, and OC۱۹۲ Networks
٤	InfoGaurd OC-۱۹۲/STM-٦٤ Encryptor
٥	LastMile AG CipherPilot ۲۰۰,۳۰۰,٤۰۰
٦	General Dynamics FASTLANE ATM/SONET Encryptor (KG-۷٥/KG۷٥A)

تصویر کلی و محدوده سیستم مورد نظر

بلوک دیاگرام کلی سیستم به شکل زیر می‌باشد:



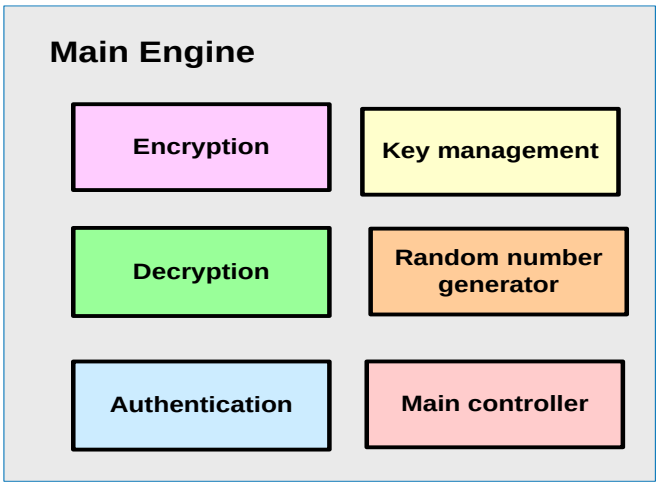
شکل ۹ : بلوک دیاگرام سیستم

دستگاه با استفاده از اتصالات فیبر نوری، به شبکه SDH متصل می‌شود و توانایی رمز کردن داده‌ها در حالت line (دو سر یک لینک) را دارد.

واحدهای اصلی تعریف شده در سیستم به شرح زیر می‌باشند :

- واحد ورودی/خروجی داده‌های رمز نشده (Plain text I/O Unit) مرتبط با شبکه حفاظت شده: در مود ورودی، این واحد داده‌های رمز نشده را از واحدهای قابل اعتماد دریافت کرده و با توجه به پروتکل امنیتی مورد نظر، رشته بیتی مناسب را جدا نموده و به همراه پیام‌های کنترلی مناسب جهت انتخاب الگوریتم رمز مناسب و کلید متناظر، به موتور پردازنده مرکزی می‌فرستد. در مود خروجی، این واحد داده‌ها را پس از رمزگشایی از موتور پردازنده مرکزی دریافت کرده و پس از تکمیل پردازش‌های نهایی با پروتکل مناسب به اینترفیس امن سخت‌افزار ارسال می‌کند.

- واحد ورودی/خروجی داده‌های رمز شده (Cipher text I/O Unit) مرتبط با شبکه حفاظت نشده: این واحد در مود ورودی، دیتای رمز شده را از اینترفیس فیزیکی واقع در قسمت ناامن شبکه دریافت می‌کند. برای باز کردن رمز بسته‌ها رشته دیتای استخراجی برای رمزگشایی به واحد مرکزی فرستاده می‌شود. در مود خروجی، داده‌های رمز شده از موتور پردازنده مرکزی دریافت شده و در این واحد پردازش‌های نهایی روی آن انجام می‌گیرد (نصب سرآیندهای لازم یا نصب نشانه‌های مناسب بر روی داده‌ها، یا درج اطلاعات کلید، با توجه به پروتکل‌های پذیرفته شده). این واحد داده‌ها را جهت انتقال در قسمت غیر قابل اعتماد شبکه به اینترفیس فیزیکی هدایت می‌کند.
- واحد مدیریت (Management Unit): این واحد، ارتباط امن مدیر سیستم را با سخت‌افزار فراهم می‌آورد. در عین حال داده‌های دریافتی از واحد مدیریت را تعبیر و تفسیر کرده و آن‌ها را با فرمت مناسب برای پیکربندی واحدهای مختلف، خصوصاً واحد پردازنده مرکزی، ارسال می‌کند. به طور مثال این اطلاعات می‌تواند مربوط به کلید مورد استفاده کاربر در عملیات رمز باشد.
- واحد کنترل کننده اصلی (Main Controller) : این واحد وظیفه تنظیم ارتباطات بین واحدهای مختلف و کنترل جریان داده‌ها را بر عهده خواهد داشت. فعالیت‌های کنترلی می‌تواند در سطوح مختلف و به صورت سلسله مراتبی در این واحد پیاده‌سازی شود.
- موتور پردازنده مرکزی (Main Engine): وظیفه موتور اصلی، انجام پردازش‌های لازم جهت پیاده‌سازی الگوریتم‌ها و پروتکل‌های رمزنگاری مورد نیاز است. این واحد در حقیقت هسته رمز سیستم محسوب می‌شود. بلوک دیاگرام موتور اصلی سیستم در شکل زیرنشان داده شده است.



شکل ۱۰ : بلوک دیاگرام موتور پردازنده مرکزی

بخش‌های فوق وظایف زیر را برعهده خواهند داشت:

- مولد اعداد تصادفی (Random Number Generator): این واحد وظیفه تولید اعداد تصادفی را برعهده دارد. داشتن خواص تصادفی لازم در تولید این اعداد لازم می‌دارد تا در طراحی این واحد مسایل تئوری و عملی مورد توجه واقع شوند.
- مدیریت کلید (Key Management): تولید، ذخیره‌سازی و بازیابی کلیدها از جمله وظایف این واحد است. علاوه بر آن پیاده‌سازی پروتکل تبادل کلید نیز در این واحد خواهد بود. این زیرسیستم تنظیم کلید ها با کنترل مدیر سیستم و به روز رسانی آنها بر اساس زمانبندی های تعریف شده و تولید کلید های جدید و تغییر کلید در نشست های بین دو دستگاه و مدیریت کلید نشست های مدیریتی را بر عهده دارد.
- واحد رمز گذار: پیاده‌سازی الگوریتم های رمز و اعمال آنها بر رشته داده های دریافتی از جمله وظایف این واحد محسوب می‌شود.

- واحد رمزگشا : این واحد مسوول رمزگشایی رشته داده دریافتی با الگوریتم‌های مورد نظر می‌باشد.
- واحد احراز اصالت : برای برقراری یک ارتباط امن، لازم است پروتکلی برای احراز اصالت دستگاه مقابل و همچنین احراز اصالت مدیر یا کاربر دستگاه وجود داشته باشد. در این راستا متدهایی نظیر توابع درهم برای این کاربرد پیاده‌سازی خواهند شد.
- واحد کنترل کننده: در پیاده‌سازی ساختار کلی یک رمزکننده سخت‌افزاری با استفاده از واحدهای پایه‌ای معرفی شده، لازم است تا ارتباطات لازم بین این واحدها به‌طور مناسبی برقرار شود. وظیفه این واحد،پیاده‌سازی پروتکل‌های امنیتی و ارتباطی لازم بر اساس به‌کارگیری واحدهای پایه‌ای موجود می‌باشد.