قرارداد های ارتباطی امن

سرفصل های درس:

فصل اول: ارتباطات امن

فصل دوم: معرفی قرارداد TCP/IP

فصل سوم: امنیت پست الکترونیکی

فصل چهارم: زیرساخت کلید عمومی (PKI)

فصل پنجم: پروتکل S/MIME

فصل ششم: آشنایی با پروتکل IPsec

فصل هفتم: SSL/TLS

فصل هشتم: تراکنش های الکترونیکی امن (SET)

فصل نهم: SSH

فصل اول: ارتباطات امن

- ارتباط بی سیم رادیویی (Wireless) چیست؟

به تکنولوژی ارتباطی اطلاق می شود که در آن از امواج رادیویی، مادون قرمز و مایکروویو ، به جای سیم و کابل، برای انتقال سیگنال بین دو دستگاه استفاده می شود.

فواید تکنولوژی (WIRELESS)

- تکنولوژی Wireless به کاربر امکان استفاده از دستگاه های متفاوت ، بدون نیاز به سیم یا کابل ، در حال حرکت را می دهد.
- تجهیزات Wireless به شما کمک می کند تا تمام اطلاعات را به راحتی برای مشتری خود به نمایش در بیاورید.
- تکنولوژی Wireless در حال گسترش است تا بتواند ضمن کاهش تکنولوژی هزینه ها، به شما امکان کار در هنگام حرکت را نیز بدهد.
- در مقایسه با شبکه های سیمی ، هزینه نگهداری شبکه های Wireless کمتر می باشد.
- شما می توانید از شبکه های Wirelessبرای انتقال اطلاعات از شبکه های روی دریاها، کوهها و ... استفاده کنید و این در حالی است که برای انجام کار مشابه توسط شبکه های سیمی، کاری مشکل در پیش خواهید داشت.

دسته بندی سیستم های WIRELESS

- سیستم های Wireless به سه دسته ی اصلی تقسیم می شوند:

۱.سیستم Wireless ثابت:

از امواج رادیویی استفاده می کند و خط دید مستقیم برای برقراری ارتباط لازم دارد. بر خلاف تلفن های همراه و یا دیگر دستگاههای Wireless، این سیستم ها از آنتن های ثابت استفاده می کنند و به طور کلی می توانند جانشین مناسبی برای شبکه های کابلی باشند و می توانند برای ارتباطات پرسرعت اینترنت و یا تلویزیون مورد استفاده قرار گیرند.امواج رادیویی وجود دارند که می توانند اطلاعات بیشتری را انتقال دهند و در نتیجه از هزینه ها می کاهند.

۲.سیستم Wireless مادون قرمز:

این سیستم از امواج مادون قرمز جهت انتقال سیگنالهایی محدود بهره می برد.این سیستم معمولا در دستگاه های کنترل از راه دور، تشخیص دهنده های حرکت، و دستگاه های بی سیم کامپیوترهای شخصی استفاده می شود.با پیشرفت حاصل در سالهای اخیر، این سیستم ها امکان اتصال کامپیوتر های نوت بوک و کامپیوتر های معمول به هم را نیز می دهند و شما به راحتی می توانید توسط این نوع از سیستم هایWireless ، شبکه های داخلی راه اندازی کنید.

۲.سیستم Wireless قابل حمل:

دستگاهی است که معمولا خارج از خانه، دفتر کار و یا در وسایل نقلیه مورد استفاده قرار می گیرند.نمونه های این سیستم عبارتند از : تلفن های همراه، نوت بوکها، دستگاه های پیغام گیر و PDA ها.این سیستم از مایکروویو و امواج رادیویی جهت انتقال اطلاعات استفاده می کند.

- نسل سوم شبکه های بیسیم ، سیستم های 3G ،کمک می کنند تا صدا و تصویر و داده را با کیفیت مناسب و به سرعت انتقال دهیم.
- در شبکه های موبایل نسل چهارم 4G ، رسیدن به نرخ بیت های بالا تا 1Gbpsبا قابلیت تحرک پذیری کامل مورد نظرمی باشد.

ارتباط رادیویی

- ارتباط رادیویی ، مخابره سیگنال ها با استفاده از مدولاسیون کردن امواج الکترومغناطیس در فرکانس های پایین تر از نور مرئی است.
- پرتو های الکترومغناطیس بوسیله نوسان سازی در میدان های الکترومغناطیس از میان هوا و خلاء گذر می کنند. اطلاعات با استفاده از روش های معین و از پیش تعیین شده و با تغییر بعضی از مشخصه های امواج منتشر شده ، مانند دامنه ، فرکانس،فاز یا پهنای پالس ، جابجا می شوند.
- زمانی که امواج رادیویی از رسانای الکتریکی عبور می کند ، میدان نوسانی یک جریان متناوب در رسانا ایجاد می کند . می توان این امواج را شناسایی و به صدا یا دیگر سیگنال های حامل اطلاعات تبدیل کرد .

ارتباطات ماهواره ای چیست؟

- ارتباطات ماهواره ای، نوعی از ارتباطات راه دور است که از طریق اقمار مصنوعی ارتباطی صورت می پذیرد.
- ایده ی اولیه استفاده از ماهواره برای ارتباط مخابراتی بین دو نقطه از کره زمین، اولین بار در سال ۱۹۴۵ توسط یک نویسنده بریتانیایی به نام "آرتورسی کلارک" مطرح شد.
- به علت محدودیت های فن آوری، عملی شدن این نظریه تا اواخر دهه ی ۵۰ یعنی ۱۹۵۷ طول کشید و در این سال، اولین ماهواره ساخت بشر، به نام "اسپوتنیک" توسط دانشمندان روسی ساخته و به فضا پرتاب شد.

سازمان های بین المللی ماهواره ای

- پیشرفت این فن آوری، به قدری سریع بود، که در سال ۱۹۶۴ **سازمان بین المللی مخابرات ماهواره های (اینتلست)** با شرکت ۱۳۹ کشور عضو تشکیل شد و مسؤلیت طراحی، ساخت و پرتاب ماهواره ها را در سه ناحیه اقیانوس هند، اطلس و آرام به عهده گرفت.
- هدف از تشکیل این سازمان برقراری ارتباطات بین المللی کشورها از طریق ماهواره بود.
- در حال حاضر این سازمان حدود ۲۰ ماهواره فعال داشته و ارتباطات بیش از ۱۷۰ کشور جهان را با یکدیگر برقرار می کند. با گسترش استفاده از ماهواره به تدریج سازمان های بین المللی و منطق های دیگری مانند "یوتلست"، "اینمارست"، "عربست" و "پان ام ست " نیز تشکیل شد و همراه توسعه کمی خدمات تلفن در سطح جهان، خدمات جدیدی از قبیل پخش برنامه های تلویزیونی، ویدیو کنفرانس، آموزش از راه دور، پزشکی از راه دور، اینترنت، دیتا و ... به وجود آمد.

انواع ماهواره ها

- ماهواره های فعال:

- این گونه از ماهواره ها، دارای فرستنده و گیرنده هستند و قادرند پیام های دریافتی را با موج دیگری مجددا به سوی کره زمین ارسال نمایند.

- ماهواره های غیرفعال:

این دسته از ماهواره ها از خود انرژی نداشته و کار آن ها صرفاً انعکاس امواج ارسالی از زمین ب هسوی کره زمین است. منعکس کننده های غیرفعال در مقابل سیگنال های با قدرت متفاوت و فرکانس های مختلف ، غیرفعال بوده و نیازمند آنتن بسیار بزرگ و فرستنده بسیار پرقدرت زمینی می باشند. این گونه از ماهواره ها در یک جا ثابت نبوده و به سادگی ردیابی نمی شوند.

کاربردهای ماهواره های ارتباطی

ماهواره های ارتباطی از لحاظ کاربرد های آ نها به سه نوع، طبقه بندی می شوند:

- **ماهواره های ارتباطی نقطه به نقطه:**

این نوع ماهواره فقط پیام را از یک فرستنده نیرومند، به یک دستگاه گیرنده نیرومند می رساند تا از آن جا برای استفاده عمومی پخش شود. مهم ترین موارد استفاده این قبیل ماهواره ها عبارتند از: توسعه ارتباطات تلفنی و تلگرافی، انتقال صفحات روزنامه ها، تقویت فرستنده های رادیویی و تقویت فرستنده های تلویزیونی.

- **ماهواره های توزیع کننده:**

این دسته از ماهواره ها، برنامه های تلویزیون را به طور مستقیم از فرستنده اصلی به فرستنده های محلّی منتقل می کنند. ماهواره های مولینا و ارلی برد که توسط شوروی و آمریکا به فضا فرستاده شدند، از این قبیل هستند.

- **ماهواره های پخش غیرمستقیم:**

این گونه از ماهواره ها برنام ههای تلویزیونی را در سراسر جهان، مستقیماً از فرستنده ها به دستگاه های گیرنده شخصی می رسانند.

انواع ماهواره های ارتباطی از نظر استقرار و گردش

ماهواره های ارتباطی از جهت چگونگی استقرار و گردش آنها در اطراف کره زمین به ماهواره های ثابت و مداری تقسیم می شوند:

- ماهواره های ثابت:

ماهواره هایی که با موشک های پرتاب کننده بسیار نیرومند در مدارهای استوایی زمینی قرار داده می شود و در فضا وضع ثابتی پیدا می کنند.

- ماهواره های مداری:

ماهواره هایی که در مدارهای بیضی شکل در فضا حرکت کرده و معمولاً هر ۱۲ ساعت یکبار در بالای مناطق معین قرار می گیرند.

پوشش ماهواره ها

- سطح زیر پوشش ماهواره از مهم ترین مسائل، در طراحی سیستم های ماهواره ای به شمار می رود. برای سطح پوشش ماهواره ها، چند نوع پوشش ممکن برای ماهواره های ثابت می توان در نظر گرفت:

۱. پوشش عمومی : سطح پوشش مفید در این حالت برابر ۱۹۵ میلیون کیلومتر مربع است.

۲. پوشش منطق های : سطح زیر پوشش آن از پوشش عمومی کمتراست.

- ۳. پوشش نیم کر های : بخشی از کره زمین(معمولاً نیم کره را شامل می شود) را پوشش می دهد.
- ۴. پوشش نقطه ای : پوشش فقط بر روی یک کشور و یا یک نقطه خاص متمرکز می شود.
- ۵. پوشش شکل داده شده : در این حالت، پرتو تشعشعی آنتن، برای زیر پوشش قرار دادن کشور یا محلی مشخص، به شکل همان کشور یا منطقه خواهد بود و حتی م یتواند یک کشور را از پوشش خود خارج کند.

سرویس های ماهواره ای

انواع خدمات اصلی که توسط اتحادیه بین الملل ارتباطات IIU برای ماهواره ها در نظر گرفته شده است را می توان به این صورت بیان کرد:

- **سرویس ارتباط ثابت ماهواره ای:**

ارتباط رادیویی بین ایستگا ههای زمینی در نقاط مشخص و معین از طریق یک یا چند ماهواره صورت می گیرد؛

- **سرویس ارتباط سیار ماهواره ای:**

بین ایستگا ههای زمینی سی‌ار با یک یا چند ایستگاه فضایی سیار یا بین ایستگا ههای فضایی سیار از این سرویس استفاده می کنند.

- **سرویس ماهواره ای پخش رادیو و تلویزیون:**

در سرویس ارتباط رادیویی، سیگنال صوتی یا تلویزیونی از ایستگاه های فضایی به طور مستقیم برای استفاده عمومی ارسال می شود و در واقع، عموم مردم می توانند با یک آنتن بسیار کوچک، سیگنال رادیو و تلویزیون را از ماهواره به طور مستقیم دریافت کنند.

- **سرویس ماهواره ای تعیین محل ایستگاه های فرستنده:**

این سرویس، سرویس ارتباط رادیویی برای تعیین ایستگاه های فرستنده رادیویی می باشد.

- **سرویس هدایت رادیویی ماهواره ای:**

این نوع سرویس، سرویس ارتباط رادیویی برای ارتباطات هدایت ایستگاه های سیار، مانند کشتی و هواپیما می باشد.

- **سرویس زمین شناسی ماهواره ای:**

سرویس ارتباط رادیویی است، که در آن گیرنده های حساس و غیرفعال روی ماهواره ها، اطلاعات مربوط به مشخصات و پدیده های غیر طبیعی زمینی را جمع آوری می کنند.

- **سرویس ماهواره ای GPS :**

سرویس ارتباط رادیویی برای هماهنگ کردن و استاندارد نگه داشتن فرکانس و وقت در نقاط مختلف جهان و سنکرون کردن سیستم ها با دقت بسیار زیاد می باشد.

- **سرویس ماهواره ای ارتباطات آماتوری:**

نوعی سرویس ارتباط رادیویی برای ایستگاه های فضایی است که به منظور خودآموزی ارتباطات داخلی برای بررسی ها و مطالعات فنّی؛ که توسط افراد آماتور صورت می گیرد، به این نام، نام گذاری شده است.

انواع لینک ماهواره ای

- **فضا–زمینی:**

ماهواره، اطلاعات را از اطراف گرفته و توسط اطلاعات موجود در داخل خود به پایانه های روی زمین رله می کند.

- **فضا–فضا :**

در این حالت، دو یا چند ماهواره در فضای بین خود، ارتباط برقرار می کنند.

- **زمین–فضا–زمین:**

در این حالت دو یا چند ایستگاه مستقر در سطح زمین می توانند از طریق ماهواره با یکدیگر در ارتباط باشند.

مخابرات های زمینی

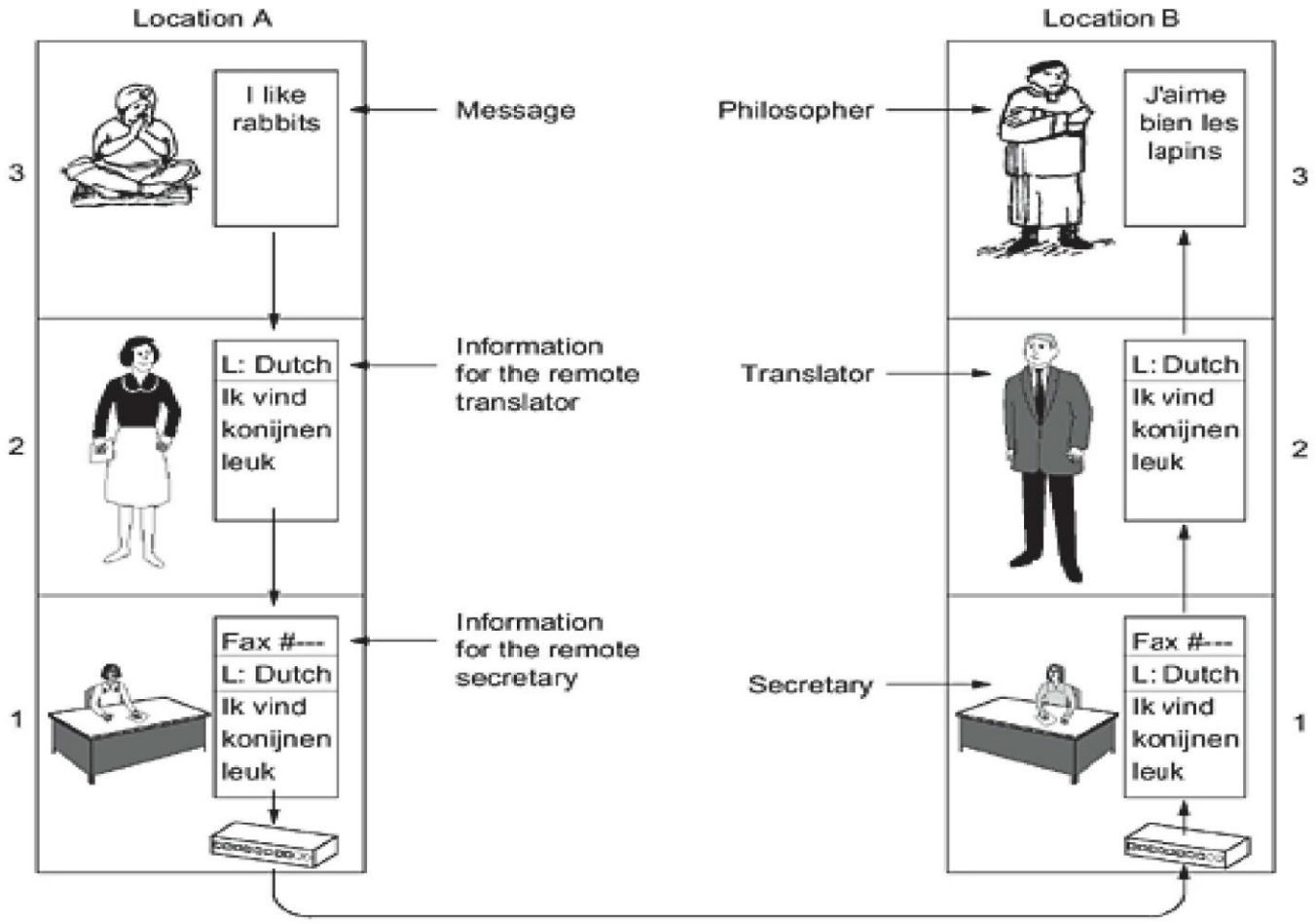
- کابل مسی
- فیبر نوری
- ایستگاه های زمینی

ایستگاه های زمینی

- ایستگاه های زمینی ماهواره معمولاً ازچند قسمت تشکیل شده اند: آنتن ، فرستنده ، گیرنده، سیستم های کنترل برقراری ارتباط ومنابع تغذیه مورد لزوم ایستگاه
- هریک ازاجزای فوق شامل قسمت های مختلفی اند که متناسب با نوع ایستگاه زمینی، حجم وتجهیزات آنها متفاوت خواهدبود.
- ایستگاههای زمینی سیستم های ماهواره ای مخابرات براساس نوع استفاده ازآنها عبارت اند از:

✓ ایستگاههای ثابت

✓ ایستگاههای سیار



TCP/IP

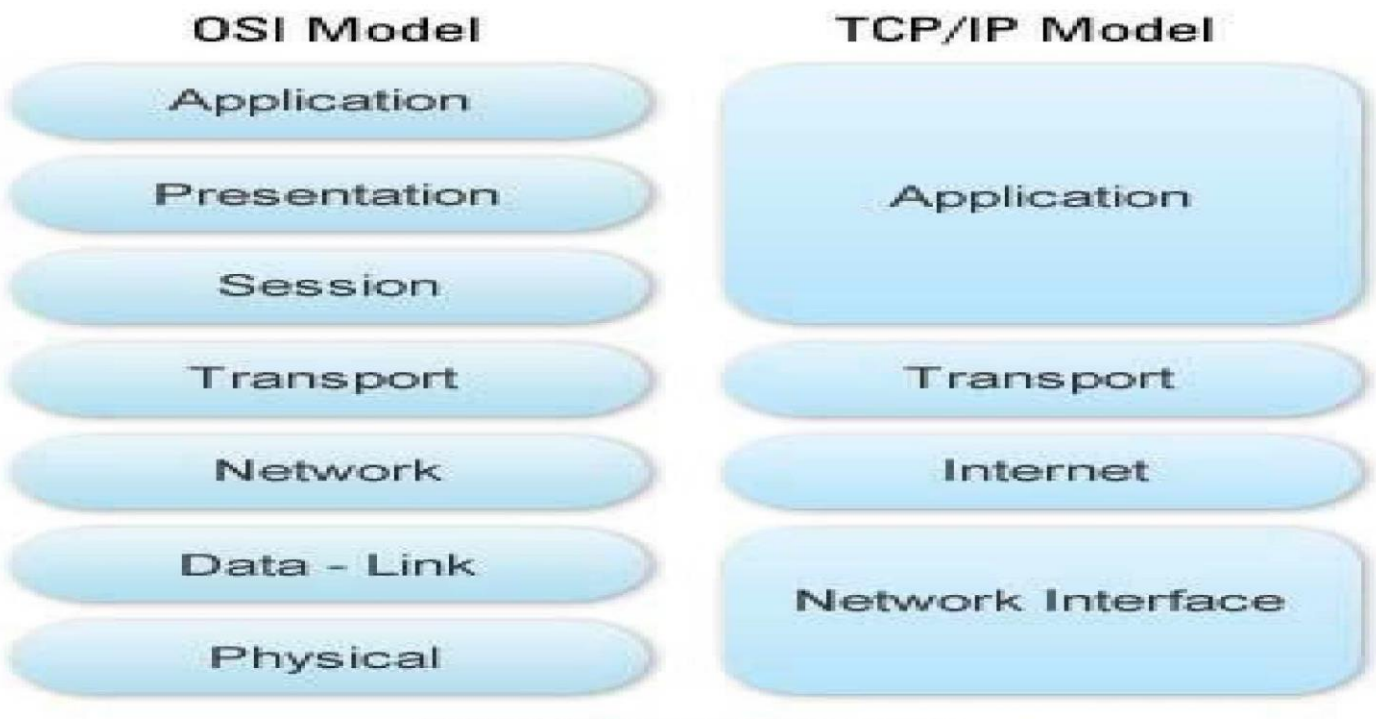
- **یک پروتکل اینترنتی مجموعه قوانینی هستند که چگونگی تبادل اطلاعات را در شبکه توصیف می کنند.**
- پروتکل، مجموعه قوانین لازم بمنظور قانونمند نمودن نحوه ارتباطات در شبکه های کامپیوتری است .

- **TCP/IP**

یکی از مهمترین پروتکل های استفاده شده در شبکه های کامپیوتری است . اینترنت بعنوان بزرگترین شبکه موجود، از پروتکل فوق بمنظور ارتباط دستگاه های متفاوت استفاده می نماید.

- مدل TCP/IP یا مدل مرجع اینترنتی ، یک توصیف خلاصه لایه TCP/IP برای ارتباطات و طراحی پروتکل شبکه کامپیوتراست.

- TCP/IP در سال ۱۹۷۰ بوسیله DARPA ساخته شده که برای پروتکل‌های اینترنت در حال توسعه مورد استفاده قرار گرفته است،



OSI & TCP/IP Models

OSI

(Open System Interconnection)

این مدل توسط IEEEایجاد شده و امکان بر قراری ارتباط بین دستگاهای ساخته شده توسط تولید کنندگان مختلف را فراهم می کند .

OSI در ۷ لایه تعریف شده است

لایه هفتم : Application Layer

این لایه با سیستم عامل و نرافزاراهای کاربردی در ارتباط است و کار آن عبارت است از:

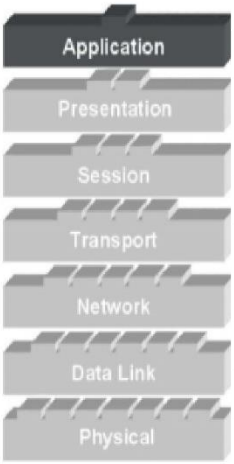
ارائه سرویس های شبکه به برنامه ها
برخی از پرتکل های معروف ای لایه عبارتند از:

Network Time Protocol (NTP)

Simple Network Management Protocol (SNMP)

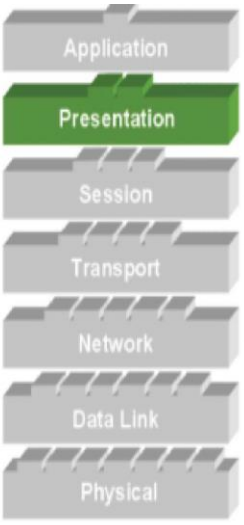
Telnet

File Transfer Protocol (FTP) , ...



DATA

◉ لایه ششم : Presentation Layer



این لایه اطلاعات مورد نیاز خود را از لایه بالایی دریافت کرده و آنر برای استفاده لایه های پایینی آماده کرده، و کارهای زیر را انجام می دهد:

ایجاد اطمینان لازم در رابطه با قابل استفاده بودن داده برای سیستم دریافت کننده

فرمت داده
ساختمان های داده
توافق در رابطه با گرامر انتقال داده برای لایه Application
رمزنگاری داده

DATA

◉ لایه پنجم : Session Layer

این لایه به کاربران در ماشینهای مختلف اجازه می‌دهد که جلساتی را بین خودشان برقرار کنند و خدمات گوناگونی مانند کنترل گفتگو و مدیریت نشانه و همگام‌سازی را نیز ارائه می‌دهد.

- مدیریت نشانه: به این معناست که دو طرف یک عمل بحرانی را در آن واحد انجام ندهند.
- همگام سازی: همگام سازی کمک می‌کند که در هنگام ارسال یک فایل بزرگ، پس از ازکار افتادن و بروز مشکل، انتقال دوباره از آخرین نقطه کنترلی، تکرار گردد.

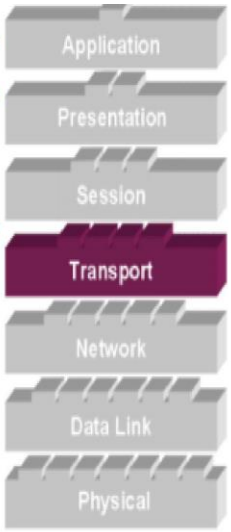
◉ لایه فوق مسئول ایجاد ، پشتیبانی و ارتباطات مربوطه با دستگاه دریافت کننده اطلاعات است و یه طور کلی کارهای زیر را انجام می دهد:

◉ ا یجاد ، مدیریت و خاتمه ارتباط برقرار شده بین برنامه ها

برخی از معروفترین پروتکل های این لایه عبارتند از :

HTTP, POP3, SMTP,...

◉ لایه چهارم : Transport Layer



◉ وظیفه اصلی این لایه دریافت داده از لایه بالاتر و در صورت نیاز شکستن آن به اندازه‌های کوچکتر، فرستادن آنها به لایه شبکه و اطمینان حاصل کردن از اینکه داده‌ها بطور صحیح به طرف مقابل می‌رسد.

◉ به طور کلی وظیفه این لایه به شرح زیر است :

حمل مطمئن داده
ایجاد ، مدیریت و خاتمه مدارات مجازی
تشخیص و برطرف نمودن خطاء

پروتکل های TCP، UDP و SPXدر این لایه قرار دارند.

Segments

لایه سوم : Network Layer

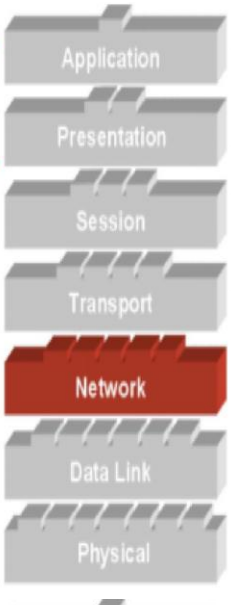
در لایه فوق روش ارسال داده ها برای دستگاه گیرنده تعیین خواهد شد. پروتکل های منطقی ، روتینگ و آدرس دهی در این لایه انجام خواهد شد.

- این لایه وظیفه کنترل زیر شبکه و همچنین چگونگی هدایت بسته‌های اطلاعاتی را از مبدأ به مقصد بر عهده دارد.

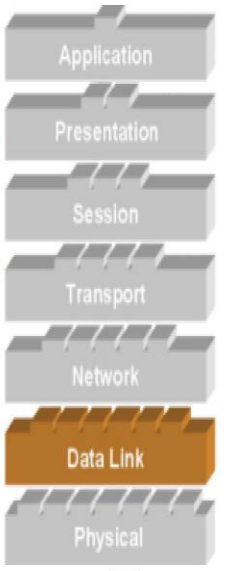
بطور کلی کارهای این لایه عبارتند از:

روتینگ
پاسخ به سوالات متعددی نظیر نحوه ارتباط سیستم های موجود در بخشهای مختلف شبکه
آدرس های مبداء ، مقصد ، Subnetو تشخیص مسیر لازم
پروتکل های IPو IPXدر این لایه استفاده می گردند.

(Packets)



مدل OSI



لایه دوم: Data Link Layer

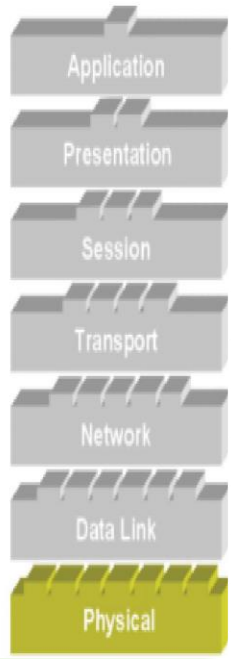
پروتکل های فیزیکی در این لایه به داده اضافه خواهند شد. در این لایه نوع شبکه و وضعیت بسته های اطلاعاتی نیز تعیین می گردند.

- وظیفه های این لایه عبارتند از :

انتقال مطمئن داده از طریق محیط انتقال
آدرس دهی فیزیکی و یا سخت افزاری (MAC)

فریم ها (Frames)در این لایه قرار دارند.

مدل OSI



لایه اول : Physical Layer

این لایه در ارتباط مستقیم با سخت افزار بوده و خصایص فیزیکی شبکه نظیر : اتصالات ، ولتاژ و زمان را مشخص می نماید.

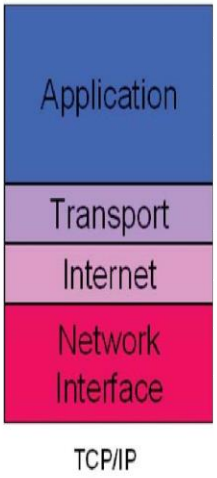
- وظیفه ارسال بیتهای خام(پردازش نشده) بر روی کانال ارتباطی و حصول اطمینان از ارسال درست بیت مورد نظر

کارهای این لایه عبارتند از:

کابل ها ، کانکتورها ، ولتاژها ، نرخ انتقال داده

ارسال اطلاعات به صورت مجموعه ای از بیت ها

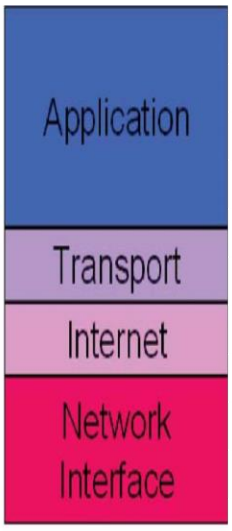
لایه کاربردی (APPLICATION) :



TCP/IP

- لایه Application ، بالاترین لایه در پشته TCP/IP است . تمامی برنامه و ابزارهای کاربردی در این لایه ، قادر به دستیابی به شبکه خواهند بود.
- پروتکل های موجود در این لایه بمنظور فرمت دهی و مبادله اطلاعات کاربران استفاده می گردند.
- HTTP - FTP - TELNET سه نمونه از پروتکل ها ی موجود در این لایه می باشند.
- پروتکل (HTTP(Hypertext Transfer Protocol بمنظور ارسال صفحات وب، استفاده می گردد .
- پروتکل(FTP(File Transfer Protocol برای ارسال و دریافت فایل، استفاده می گردد .
- TELNET برای ارتباط راه دور به سیستم هااستفاده میشود.

لایه TRANSPORT :



TCP/IP

- **لایه " انتقال "، قابلیت ایجاد نظم و ترتیب و تضمین ارتباط بین کامپیوترها و ارسال داده به لایه Application (لایه بالای خود) و یا لایه اینترنت (لایه پایین خود) را بر عهده دارد. این لایه دارای دو پروتکل اساسی است که نحوه توزیع داده را کنترل می نمایند.**
- TCP(Transmission Control Protocol)

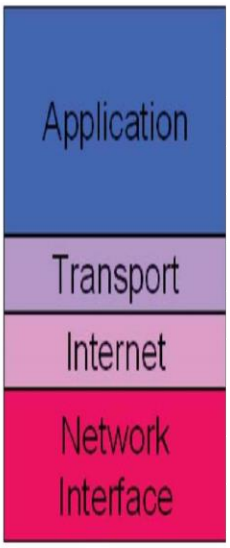
مسئول تضمین صحت انتقال اطلاعات است.(تاییدیه از گیرنده دریافت میشود)

Flow control در این پرتکل انجام میشود.(یکسان سازی سرعت انتقال درفرستنده و گیرنده)

- UDP(User Datagram Protocol)

در حین ارسال اطلاعات تاییدیه از گیرنده درخواست نمیشود.(قابل استفاده در زمانی که سرعت از دقت بیشتر اهمیت دارد مانند : ویدئو کنفرانس)

لایه اینترنت :



TCP/IP

- لایه "اینترنت"، مسئول آدرس دهی، بسته بندی و روتینگ داده ها (Packet -Switching) است.
- لایه فوق، شامل چهار پروتکل اساسی است:

۱. IP(Internet Protocol) : مسئول فرمت بندی و آدرس دهی داده ها بمنظور ارسال به مقصد مورد نظر است.

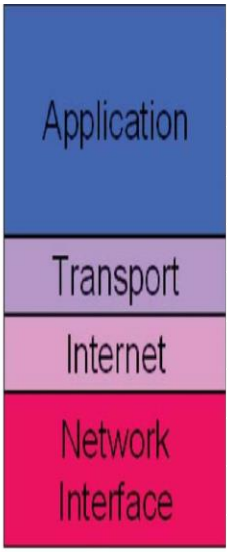
۲. ARP(Address Resoulation Protocol) :مسئول تشخیص آدرس MAC(Media Access Control) آداپتور شبکه است.
(یک عدد دوازده رقمی مبنای شانزده بوده که آدرسMAC ، نامیده می شود.)

۳. ICMP(Internet Control Message Protocol): مسئول ارائه توابع عیب یابی و گزارش خطاء در صورت عدم توزیع صحیح اطلاعات است.

۴. IGMP(Internet Group Managemant Protocol) : مسئول مدیریت Multicasting در TCP/IP میباشد.

TCP/IP

لایه NETWORK INTERFACE :



TCP/IP

- این لایه مسئول استقرار داده بر روی محیط فیزیکی شبکه و دریافت داده از محیط فیزیکی شبکه است .
- لایه فوق، شامل دستگاه های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است .
- لایه " اینترفیس شبکه "، شامل پروتکل های مبتنی بر نرم افزار مشابه لایه های قبل، نمی باشد. پروتکل های Ethernet و ATM(Asynchronous Transfer Mode)، نمونه هائی از پروتکل های موجود در این لایه می باشند .
- پروتکل های فوق، نحوه ارسال داده در شبکه را مشخص می نمایند.

مقایسه مدلهای OSI و TCP

- هر دو مدل به صورت پرتکل های مستقل هستند که بصورت پشته روی هم قرار گرفته اند.
- بر خلاف TCP ، در مدل مرجع OSI سعی بر اینست که سرویسها ، واسط ها و پروتکل ها در هر لایه متمایز بوده و به به این صورت عمل نمایند که هر لایه سرویسهایی را به لایه بالاتر میدهد.
  - سرویس میگوید آن لایه چه کار انجام میدهد.
  - واسط میگوید چگونه به این لایه دسترسی یابد.
  - پروتکل استفاده شده در هر لایه کاملا به خود لایه مربوط میشود و عملکرد لایه را توصیف میکند.
- در مدل OSI ابتدا مدل طراحی شد سپس پروتکل ها و عملکردها تعریف شدند . اما درمدل TCP ابتدا پروتکل ها بوجود آمدند .

لایه	OSI	TCP
شبکه	ارتباط های بدون اتصال و اتصال گرا پشتیبانی میشود	فقط ارتباط بدون اتصال انجام میشود
انتقال	فقط ارتباط اتصال گرا در اختیار است	ارتباط های بدون اتصال و اتصال گرا پشتیبانی میشود

نقاط ضعف مدل OSI

- در اکثر برنامه های کاربردی نیازی به لایه ارایه و جلسه نیست از طرفی دیگر لایه های ارتباط داده و شبکه خیلی پر هستند.
- این مدل بسیار پیچیده است و به سختی قابل پیاده سازی است و همچنین کارآمد نیست.

نقاط ضعف مدل TCP/IP

- این مدل مسائل سرویس ، رابط و پروتکل را از هم متمایز نمیکند.در نتیجه زمینه مناسبی برای طراحی شبکه جدید با استفاده از فناوری جدید را فراهم نمیکند.
- دارای طراحی خاص بوده که نمی تواند مدلهای دیگر را در برگیرد.(مثلا توصیف SNA توسط این مدل تقریبا ناممکن است)
- لایه رسمی به نام میزبان به شبکه در این مدل وجود ندارد و تنها رابطی بین لایه شبکه و لایه انتقال شده.
- لایه های فیزیکی و انتقال از هم متمایز نشده ، در صورتیکه هر یک وظیفه مستقل دارند.
- با وجود اینکه پروتکل های TCPو IP با دقت طراحی شده اند ولی پروتکل های دیگری در این مدل وجود دارند که یا ضعیف هستند و یا ساده(مانند TELNETکه برای ترمینالهای ساده طراحی شده)

- با توجه به باز بودن طرح TCP/IP، این پروتکل یک پروتکل ناامنی است.
- اگر نگرانی امنیتی داشته باشید جهت رفع این نگرانی و ایمن سازی ترافیک شبکه یا سیستم های مجری TCP/IPبهره گیری از فناوری های اضافی ضروری است.
- برای مثال، اگر می خواهید مطمئن باشید سایر افراد نتوانند داده های ارسالی به سرور وب شما را بخوانند استفاده از برنامه های SSLامنیت وب سایت را تضمین و ترافیک بین سرویس گیرنده و سرور وب شما را رمزگذاری می کند.

PGP:

- **سرویسهای محرمانگی و احراز اصالت برای پست الکترونیکی و فایل ها**

S/MIME:

- **سیستم توسعه یافته و چند منظوره پست الکترونیک امن است.**
- **سرویسهای رمز نگاری و امضای دیجیتال را فراهم میکند.**
- **این پروتکل اجازه میدهد پیام رمز شود ، امضاء گردد و یا ترکیبی از این دو اجرا شود.**

IPSEC:

- **ایجاد امنیت در سطح IP**
- **برای ایجاد VPN**
- **دسترسی امن هر یک از کارکنان شرکت از طریق ISP به منابع شرکت**
- **ارتباط امن بین چند شرکت**
- **ایجاد امنیت ساده برای سرویسهای دیگر(مانند تجارت الکترونیک و ...)**

SSL/TLS :

- **برای ایجاد امنیت در وب**
- **TLS نسخه استاندارد شده SSL است.**

SET :

- **تراکنش الکترونیکی امن**
- **مجموعه پروتکل های امنیتی و قالبهایی است که به کاربر اجازه میدهد تا از کارتهای اعتباری موجود در شبکه های گسترده بتواند استفاده کند.**

SSH :

- **پروتکل امنیتی برای ارتباطات راه دور(Remote) با رمز نگاری**
- **جایگزین مناسبی برای Telnet**

PGP

مقدمه

- پست الکترونیکی یکی از رایجترین و ارزانترین روشهای برقراری ارتباط است. روزانه میلیونها نامهٔ الکترونیکی از طریق این سرویس جابه جا می شود. پروتکلهای تبادل نامهٔ الکترونیکی از نخستین روزهای پیدایش شبکه و اینترنت ایجاد شدند، و به مرور زمان بهبود و توسعه یافتند. استفاده نیست؛ یعنی « امن » کنندگان پست الکترونیکی متوجه شدند که ارتباط از طریق این سرویس نامه های الکترونیکی در معرض خطراتی نظیر شنود، تغییر، یا جعل قرار دارند . بدین سبب نویسندگان پروتکلها سعی کردند تا با اعمال تغییراتی در پروتکلهای پیشین، و یا ایجاد پروتکلهای جدید، سرویس امنی برای تبادل نامه های الکترونیکی فراهم کنند.
- یکی از پروتکهای مشهوری که به طورکلی در این زمینه به کار گرفته شد PGPنام داشت.
- هدف این فصل بررسی پروتکل PGP، به طورعمده و بررسی سایر پروتکلهای نامه نگاری امن به طور مختصر است.
- PGPیکی از جالبترین تاریخچه های اختراعات رمزنگاری را به خود اختصاص داده است . مردی به تنهایی در برابر دولت ایالات متحده می ایستد تا به قیمت چندین سال از عمرش، از حریم خصوصی مردم دفاع کند، و سرانجام هم موفق می شود.

- •در سال ۱۹۷۶ ، یک متخصص رمزنگاری و طرفدار حریم خصوصی به نام Whitfield Diffie به همراه مهندس برقی به نام Martin Hellman نخستین الگوریتم رمزنگاری کلید عمومی را ابداع کردند. (این الگوریتم امروزه با نام Diffie-Hellman یا به اختصار DH نامیده می شود برای تبادل کلیدهای رمزنگاری به کار می رود).
- در سال ۱۹۷۷ ، سه محقق در دانشگاه MIT سه محقق با نام های ، Adi Shamir ،Rivest Ronو Len Adleman الگوریتم رمزنگاری کلید عمومی دیگری را ابداع نمودند(RSA).
- آژانس امنیت ملی آمریکا ، NSA،به MIT و این سه نفر هشدار داد که آنها بهتر است الگوریتم خود را منتشر نکنند.

اما MITو A,S,R توصیه nsaرا نادیده گرفتند و در جولای ۱۹۷۷ ، اختراع خود را درمجله Scientific American در مقاله ای تحت عنوان«New Directions in Cryptography» چاپ کردند.

از آنجا که انتشار جزئیات RSAبا توجه به هشدار NSA، با عجله انجام شد MITو ، R، S Aامتیاز اختراع (patentخود را در خارج از آمریکا از دست دادند. علت این بود که در (اغلب کشورها ثبت اختراع باید پیش از انتشار آن صورت بگیرد، حال آنکه در آمریکا مخترعین می توانند تا یک سال پس از انتشار برای ثبت اختراع اقدام کنند. همچنین بسیاری از کشورها به الگوریتمها امتیاز اختراع نمی دهند.

اختراع PGP

• در سال ۱۹۹۱ ، دولت آمریکا لایحهٔ ۲۶۶ را تقدیم مجلس سنا کرد.

یکی از بندهای این لایحه که برای پیشگیری و مبارزه با جنایات تنظیم شده بود، سازندگان نرم افزارهای رمزنگاری رامجبور می کرد که در محصولات خود یک « درِ پشتی » برای شنود توسط دولت تعبیه کنند

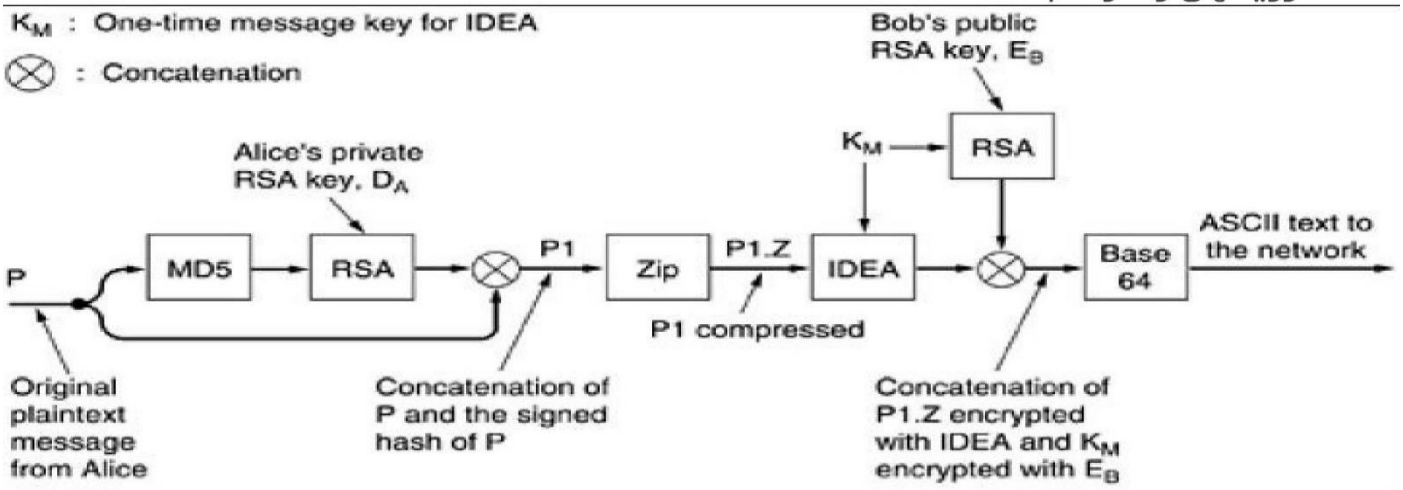
این لایحه انگیزه ای برای آقای فیلیپ ر. زیمرمن(PRZ) شد تا PGP را بنویسد.

- بعداً معلوم شد کهBass-O-Matic الگوریتم ضعیفی است، و ازIDEA به جای آن استفاده شد.
- PGP نسخهٔ ۲ و پس از آن ازIDEA استفاده می کنند.
- PGP نسخهٔ ۱ ازMD4 برای درهم سازی پیامها استفاده می کرد که مشخص شد ایراداتی دارد
- PRZ نسخه ۱ PGP را نوشت.او از RSAبه همراه الگوریتم رمزنگاری متقارنی به نام-Bass-O Matic که خود مبدع آن بود استفاده کرد.
- Ron Rivest این ایرادات را برطرف نمود وMD5 را عرضه نمود.
- PGP نسخهٔ ۲ به بعد ازMD5 استفاده می کند.
- PGP نسخه ۱ داده ها را برای انتقال ۷ بیتی uencodeمی کرد
- PGPنسخه ۲ به بعد از Base64 برای این منظور استفاده می شد.
- PGPنسخه ۱ از الگوریتم فشرده سازیLZHuf استفاده می کرد.
- PGPنسخه ۲ به بعد از الگوریتم فشرده سازی ZIP استفاده می کند.

نسخهٔ PGP / ویژگی	PGP نسخهٔ ۱	PGP نسخهٔ ۲ به بعد
الگوریتم متقارن	Bass-O-Matic	IDEA
الگوریتم درهم سازی	MD4	MD5
کد انتقال	uuencode	Base64
الگوریتم فشرده سازی	LZHuf	Zip

بررسی PGP(مروری بر الگوریتمها)

- PGP الگوریتمهای مختلف را به نحوی بسیار عالی پشت سر هم قرار داده تا تعداد زیادی سرویسهای را فراهم کند.



روند کار PGP

۱)کاربر متن مورد نظر خود را به PGP می دهد

۲) PGPبا استفاده ازMD5 متن نامه را درهم کرده و سپس با کلید خصوصی فرستنده، متن درهم شده را امضا می کند.

۳) امضا به متن آشکار الحاق می شود(p1).

۴)محتوای P1 با الگوریتم ZIP فشرده می شود (P1.Z)

۵) یک کلید نشست تصادفی تولید شده وP1.Z توسط الگوریتمIDEA و با استفاده از این کلید رمز می شود.

۶) کلید نشست با کلید عمومی گیرنده و استفاده از الگوریتمRSA رمز شده و به پیغام الحاق می شود.

۷)نتیجه با استفاده از Base64برای ارسال آماده میشود.

الحاق امضا پیش از رمزنگاری

- تنها گیرنده متوجه خواهد شد که چه کسی نامه را امضا کرده است.

- گیرنده به احتمال زیاد نسخهٔ غیر فشردهٔ نامه را نگه خواهد داشت . امضا پیش از فشرده سازی تولید می شود تا گیرنده نیازی به فشرده سازی مجدد برای بررسی امضا نداشته باشد . به علاوه، پیاده سازیهای مختلف ZIPممکن است خروجیهای متفاوتی داشته باشند وگیرنده نداند که از کدام پیاده سازی باید برای فشرده سازی استفاده کند.

فشرده سازی پیش از رمزنگاری

- حجم نامه کمتر شده و رمزنگاری آن سریعتر می شود.
- خصوصیات آماری نامه تغییر کرده و افزونگی آن کم می شود. نتیجتاً امکان رمزگشایی نامه توسط افراد ناخواسته کاهش می یابد.

استفاده از Base64

- نامه های الکترونیکی که برای انتقال از SMTPاستفاده می کنند، با محدودیتهایی روبرو هستند. مثلاً برای انتقال آنها باید از کد انتقال ۷ بیتیASCII استفاده کرد. این محدودیت مانع انتقال داد ه های باینری می شود.
- از آنجا که فرمت نامه های رمزنگاری شده باینری است،PGP از Base64برای حل این مشکل استفاده کرد.
- بر طبقBase64، RFC 3548 روشی برای کد کردن هر جریان بیتی به مجموعه ای از کاراکترهای حرفی – عددی است.

تبدیل مقادیر ۶۴ گانه به معادل Base ۶۴

Value	Code	Value	Code	Value	Code	Value	Code	Value	Code	Value	Code
0	A	11	L	22	W	33	h	44	s	55	3
1	B	12	M	23	X	34	i	45	t	56	4
2	C	13	N	24	Y	35	j	46	u	57	5
3	D	14	O	25	Z	36	k	47	v	58	6
4	E	15	P	26	a	37	l	48	w	59	7
5	F	16	Q	27	b	38	m	49	x	60	8
6	G	17	R	28	c	39	n	50	y	61	9
7	H	18	S	29	d	40	o	51	z	62	+
8	I	19	T	30	e	41	p	52	0	63	/
9	J	20	U	31	f	42	q	53	1		
10	K	21	V	32	g	43	r	54	2		

- به عنوان یک مثال فرض کنید بخواهیم رشتهٔ بیتی ۱۱۱۱۰۰۱۰۰۰۱۱۰۱۰۰۰۱۰۱۰۱۱۰ را به معادلBase64 آن تبدیل کنیم. ابتدا باید رشته به گروهای ۶ بیتی شکسته شود و سپس معادل هر گروه از جدول صفحه قبل استخراج گردد:

مقدار باینری	۰۱۰۱۱۰	۰۱۰۰۰۱	۱۰۰۰۱۱	۱۱۱۱۰۰
مقدار دسیمال	۲۲	۱۷	۳۵	۶۰
کد Base64 معادل	W	R	j	8

- همانطور که مشاهده می شود، کد Base64به جای هر ۶ بیت از یک سمبل ۸ بیتی استفاده می کند (هر کاراکتر معمولاً به ۸ بیت فضا برای ذخیره نیاز دارد). بنابراین کدBase64 حجم را در حدود ۳۳% افزایش میدهد.
- خوشبختانه PGPاین مشکل را نیز حل کرده است: بنا به محاسبات آماری، فشرده سازی Zip به صورت آماری حجم را در حدود ۵۰% کاهش می دهد. بنابراین با اعمال Zipو پس از آن Base64 حجم به 67%مقدار اصلی خود می رسد.

الگوریتمهای دیگر

- امروزه پیاده سازیهای متنوعی از PGPوجود دارند که گسترهٔ وسیعی از الگوریتمهای رمزنگاری را پوشش می دهند.
- به عنوان مثال:

کارکرد	الگوریتمهای مورد استفاده
امضای دیجیتال	DSS/RSA with MD5/SHA
رمزنگاری پیام	CAST/IDEA/3DES with RSA/DH (ElGamal)

مزایایی PGP

- PGP از چند جهت مورد توجه فراوان قرار گرفت. مهمترین دلیل توجه رسان ه ها به آن بود، که کنجکاوی مردم را برانگیخت و سبب شد تعداد زیادی آن را داونلود و از آن استفاده کنند . اما، صرف نظر از این علت ،« روانی » چند مزیت <<علمی » مهم نیز برای استفاده از PGPنیز وجود دارد.

- PGPاز بهترین الگوریتمهای رمزنگاری استفاده می کند، و همانطور که پیشتر اشاره شد، آنها را به بهترین شکل ممکن ترکیب کرده است.
- PGP وابسته به هیچ سیستم عامل خاصی نیست، و نسخه هایی از آن را می توان روی هر سیتم عاملی، از DOSو ویندوز گرفته تا یونیکس و لینوکس پیدا کرد . استفاده ازPGPهم کار بسیار ساده ای است.
- مستندات PGP بسیار جامع هستند.
- PGPمجانی و کد منبع آن در اختیار همگان است.
- اگر نیاز به پشتیبانی باشد، نسخهٔ بسیار ارزانی از آن قابل خر یداری است که به همراه پشتیبانی فنی ارائه می شود.

سرویس های PGP

- به کمک PGPمی توان بسیاری از سرویسهای امنیتی و غیر امنیتی را فراهم کرد:
- احراز هویت
- جامعیت
- محرمانگی
- فشرده سازی
- کد انتقا
- قطعه–قطعه سازی(segmentation) و سرهم بندی(reassembly) پیام ها

احراز هویت / جامعیت

- شکل بعد قسمت a فرآیند تولید امضای دیجیتال توسطPGP را نشان می دهد. توالی انجام کار به این کار به این صورت است که:

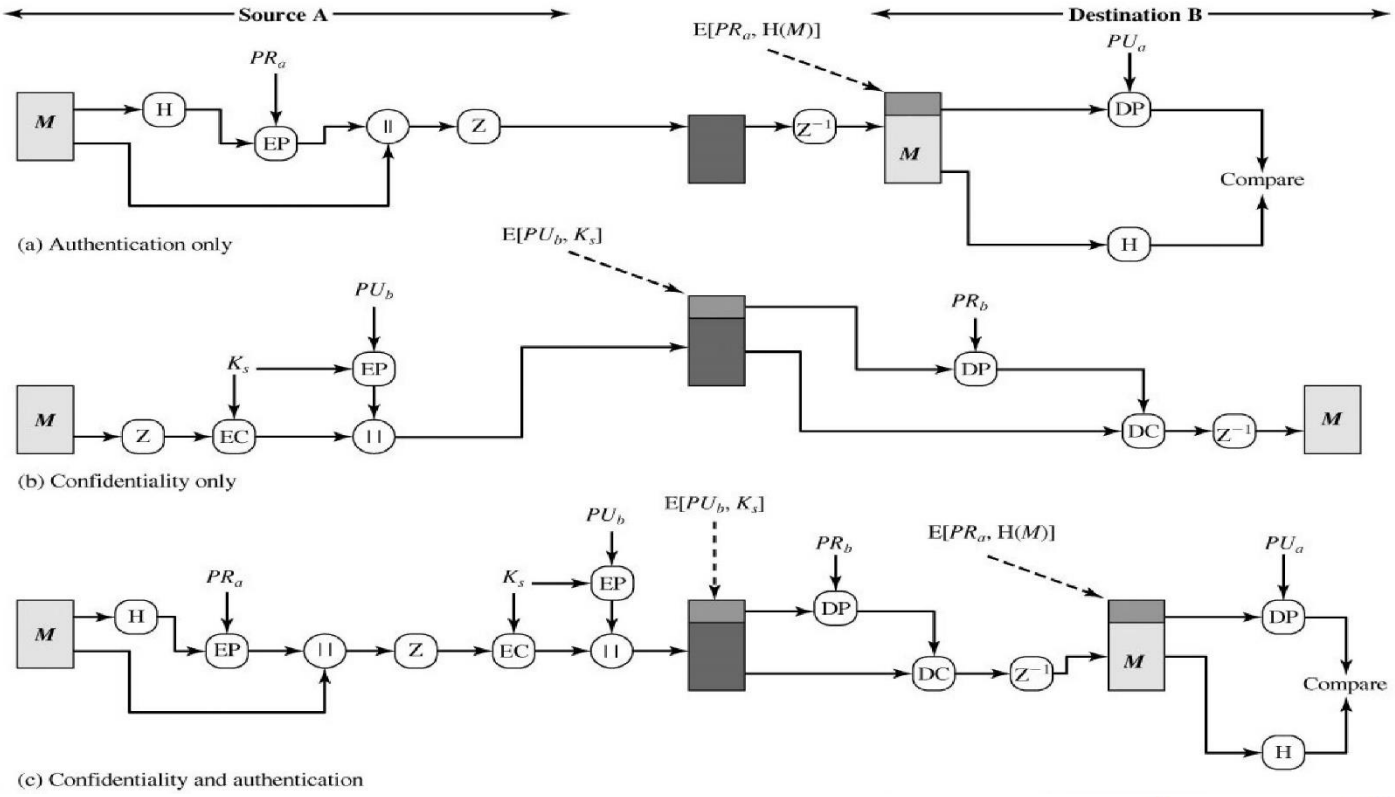
۱) فرستنده پیام را ایجاد میکند.

۲)SHA-1 برای تولید فشرده پیام ۱۶۰ بیتی به کار میرود.

۳) فشرده پیام توسط الگوریتمRSA و کلید خصوصی فرستنده امضا و نتیجه به پیام الحاق می شود.

۴) گیرنده از الگوریتمRSA و کلید عمومی فرستنده استفاده کرده تا فشرده پیام را از امضا استخراج کند.

۵) فشرده پیام رمزگشایی شده با فشردهٔ پیام دریافت شده مقایسه شده تا اصالت پیام احراز شود.



فشرده سازی

- ترکیب SHA-1 و RSAمکانیسم ایده آلی برای امضای دیجیتال فراهم می آورد.
- از آنجا که تا کنون روش مؤثری برای شکستن RSA کشف نشده است، گیرنده مطمئن خواهد بود که تنها صاحب کلید خصوصی متناظر میتوانسته امضا را تولید کند.
- به دلیل قدرتSHA-1در تولید فشرده پیامهای یکطرفه، گیرنده می تواند از جامعیت پیام اطمینان داشته باشد.
- به عنوان یک روش جایگزین می توان ازDSS/SHA-1 برای تولید امضا استفاده کرد.
- اگرچه امضاها اغلب به پیام یا فایل مربوطه الصاق می شوند اما PGPاز امضاهای مجزا هم پشتیبانی می کند. این ویژگی در چند جا مفید است:

- کاربر ممکن است بخواهد امضاها را در محلی مناسب نگهداری کند.
- امضاهای مجزای فایلهای اجرایی می توانند ویروسی شدن این فایلها را نشان دهد.
- وقتی لازم باشد که چند نفر یک پیام را امضا کنند، استفاده از امضاهای مجزا مفید خواهد بود. در غیر این صورت باید از امضاهای تودرتو استفاده کرد؛ یعنی نفر اول پیام را امضا می کند، نفر دوم پیام را به همراه امضای الحاق شدهٔ نفر اول امضا می کند، و قس علی هذا.

محرمانگی

- این سرویس از طریق رمزنگاری فراهم می شود. الگوریتمهای رمزنگاری مورد استفاده عبارتند از :
- 3DESو ، IDEA،CAST-128
- در هر سه مورد از سبک رمزنگاری CFB ۶۴ بیتی استفاده می شود.
- همان طور که پیشتر نیز اشاره شد، برای رمزنگاری پیام در PGP از کلید نشست استفاده می شود
- اگرچه در مستندات از این کلید به عنوان کلید نشست یاد شده است، اما از آن فقط یک مرتبه استفاده می شود. این کلید یکبار مصرف باید به نوعی به همراه پیام ارسال شود . برای محافظت ازآن، این کلید توسط کلید عمومی گیرنده رمز می شود .

- شکل قبلی قسمت b نحوهٔ فراهم شدن سرویس محرماگی را نشان می دهد:
- ۱) فرستنده یک عدد ۱۲۸ بیتی (یا ۱۶۸ بیتی) تصادفی را به عنوان کلید نشست این پیام تولید م یکند.

۲) پیام با الگوریتم CAST-128 یا 3DESیا IDEAو کلید نشست رمز می شود.

۳) کلید نشست با RSAو کلید عمومی گیرنده رمز و به پیام الحاق می شود.

۴) گیرنده پیام را دریافت کرده و کلید نشست آن را باRSAو کلید خصوصی خودرمزگشایی می کند.

۵) پیام با استفاده از کلید نشست رمزگشایی می شود.

نکته: PGPمی تواند به جایRSAاز الگوریتم تغییر یافتهٔ RSA با نامElGamal نیز استفاده کند.

- در شکل قبلی قسمت c نشان می دهد که دو سرویس محرمانگی و امضای دیجیتال چطور ممکن است بایکدیگر ترکیب شوند.

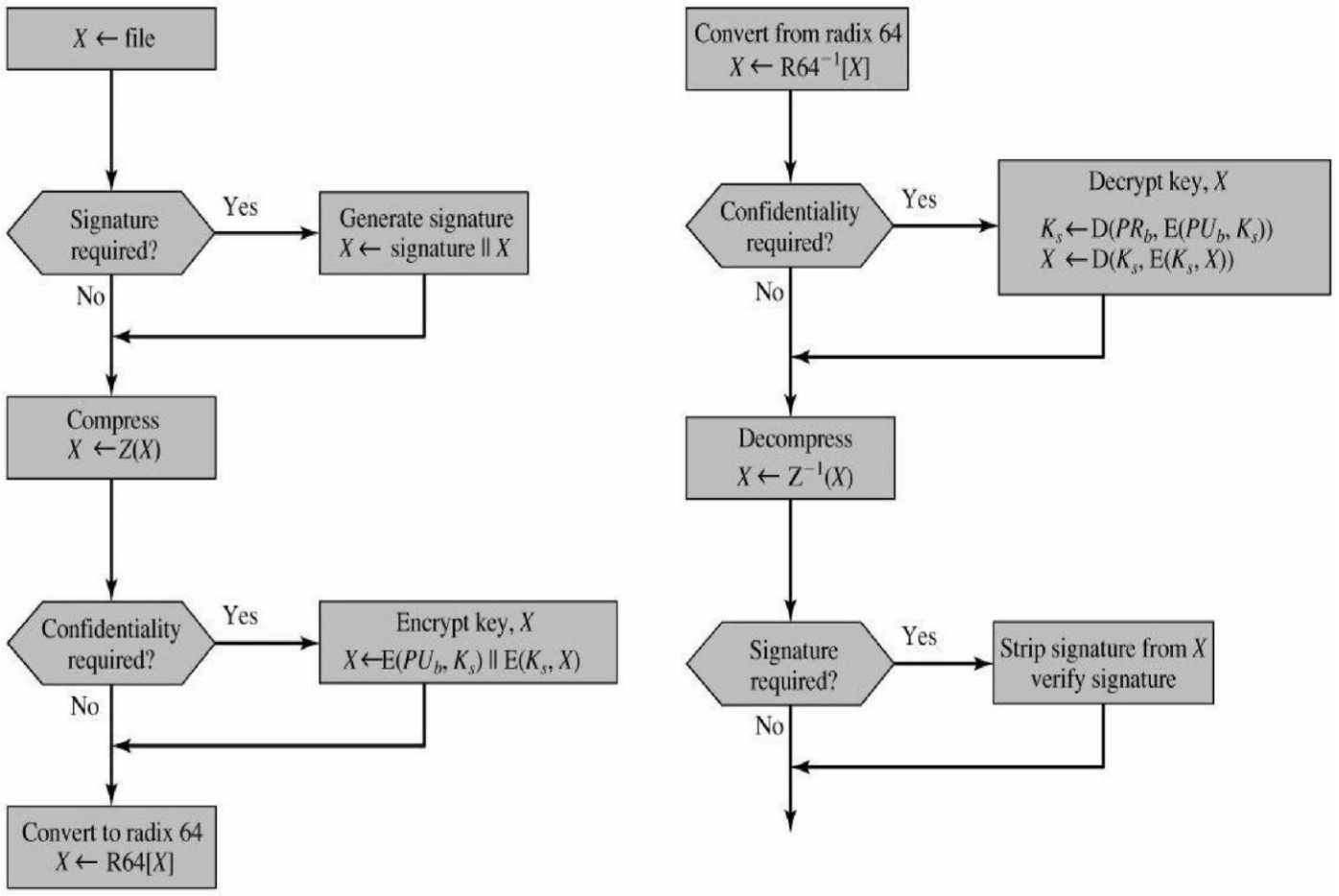
فشرده سازی

- پیام های PGPبه طور پیش فرض فشرده می شوند. پیشتر در بارهٔ ترتیب اعمال فشرده سازی وفواید آن صحبت شد. الگوریتم فشرده سازی مورد استفادهٔ PGP،ZIP نام دارد.
- ZIP توسط Jean-Richard Walesو lup Gailly،Mark Adler نوشته شده و کدآن مجانا در اختیار عموم قراردارد.
- این الگوریتم در سال ۱۹۷۷ توسط Abraham Lempelو Jacob Zivبهبود داده شد . از این نسخهٔ بهبود یافته اغلب با نامLZ77 یاد می شود.
- PGPاز این نسخه از الگوریتم ZIPیعنی LZ77استفاده می کند.
- در بخشهای بعد خواهیم دید که عدم استفاده از فشرده سازی درPGPمنجر به شکسته شدن این روش خواهد شد.

کد انتقال

- پیشتر اشاره شد کهPGPبرای حفظ سازگاری با نسخه های قدیمترSMTPاز کد انتقالBASE64استفاده می کند. شکل بعدی نحوهٔ استفاده از این سیستم کدینگ را نشان می دهد.

ارسال و دریافت پیام های PGP



(a) Generic transmission diagram (from A)

(b) Generic reception diagram (to B)

قطعه—قطعه سازی و سرهم بندی پیام

- اکثر سیستمهای پست الکترونیکی، حجم نامه ها را به مقدار مشخصی محدود می کنند . اگر حجم نامه ای از مقدار تعیین شده بیشتر باشد، آن نامه باید به چند قطعه تقسیم شود و هر قطعه به طور مجزا ارسال شود.

- PGPبرای حل این مسئله امکان قطعه قطعه سازی پیامها را فراهم کرده است. قطعه قطعه سازی پس از اتمام تمام مراحل قبلی انجام می پذیرد. تنها بخش اول حامل کلید نشست و امضای فرستنده ، خواهد بود. در سمت گیرندهPGPسرآیندهایe-mailرا استخراج کرده و تمام قطعات را سرهمبندی می کند. این فرآیند در شکل قبلی قسمت bنشان داده شده است.

بررسی پروتکل های ارتباطی امن PGP
زیرساخت کلید عمومی (PKI)

زیرساخت کلید عمومی (PKI)

زیر ساخت کلید عمومی (PKI) سیستمی برای پشتیبانی از امضای دیجیتالی و رمزگذاری اسناد برای اشخاص و سازمان هاست.

مفاهیم اصلی امنیت:

► ۱.۱. مقررات کنترل دسترسی

ابتدا هویت کاربر و سپس مجوز دسترسی او به اطلاعات باید بررسی شود. اجرای این دو امر به ترتیب توسط فرآیندهای تأیید هویت و عملکردهای تصمیم گیری کنترل دسترسی صورت می گیرد.

فرآیندهای تأیید هویت مسئول تصدیق و تأیید هویت کاربر هستند.

در واقع عملکرد کنترل دسترسی، متکی به این مرحله است.
در اینجا سه نوع متفاوت از اطلاعات مورد استفاده قرار می گیرد:

۱. **آنچه کاربر می داند :** (برای ارزیابی یک کاربر بر اساس رمز عبود یا یک راز مشترک است) و به دلایل زیر معمولاً ضعیف ترین راه حل برای تعیین هویت می باشد:

- توسط برنامه های کراکر می تواند از کامپیوتر دزدیده شود.
- هویت کاربر و رمز عبورها می تواند از طریق برنامه های sniffer از یکدگیر جدا شود.

۲. **آنچه کاربر دارد :** (کاربر یک نشانه رمز فیزیکی دارد. این روش معمولاً با روش قبلی ترکیب می شود به طوری که کاربر از حمله آگاه شود.)

۳. **آنچه کاربر هست:** (قوی ترین روش تعیین هویت است. زیرا دزدیدن نشانه رمز احراز هویت بسیار مشکل است.)از معایب این روش می توان به دو مورد اشاره کرد:

- محرمانه نیست.
- این روش بر خلاف رمزهای عبور و احراز هویت با کارت یک تطبیق دقیق را ایجاد نمی کند بلکه یک تطبیق نامشخص ایجاد کرده به این معنا که تعیین هویت مثبت و منفی غلط ممکن است پیش آید.

▶ ۲.۱. سیستم های توزیع شده و احراز هویت با رمز

فرض کنید شرکتی دارای چندین برنامه کاربردی است که توسط سیستم ها و سرورهای مختلف میزبانی می شوند، برای تعیین هویت کاربران به منظور اجازه دسترسی به این برنامه ها راه های متعددی وجود دارد که در اینجا به آن اشاره می کنیم :

۱. رمز عبورها متعدد که هر یک برای یک سیستم یا برنامه کاربردی به کار می روند.

۱. **رمز عبورها متعدد که هر یک برای یک سیستم یا برنامه کاربردی به کار می روند.**

این راه بسیار ساده است امّا به کارگیری آن برای کاربران پرزحمت خواهد بود و همواره مشکل فراموش کردن رمز عبورها وجود دارد.

---

۲. **رمز عبور مشابه که در هر سیستم تکرار می شود.**

این روش به شدت آسیب پذیر است زیرا اطلاع از یک رمز عبور که با حمله به ضعیف ترین سیستم به دست می آید می تواند باعث دسترسی به همه سیستم ها شود. مزایای این روش آن است که کاربران تنها مجبور به حفظ کردن یک رمز عبور خواهند بود.

---

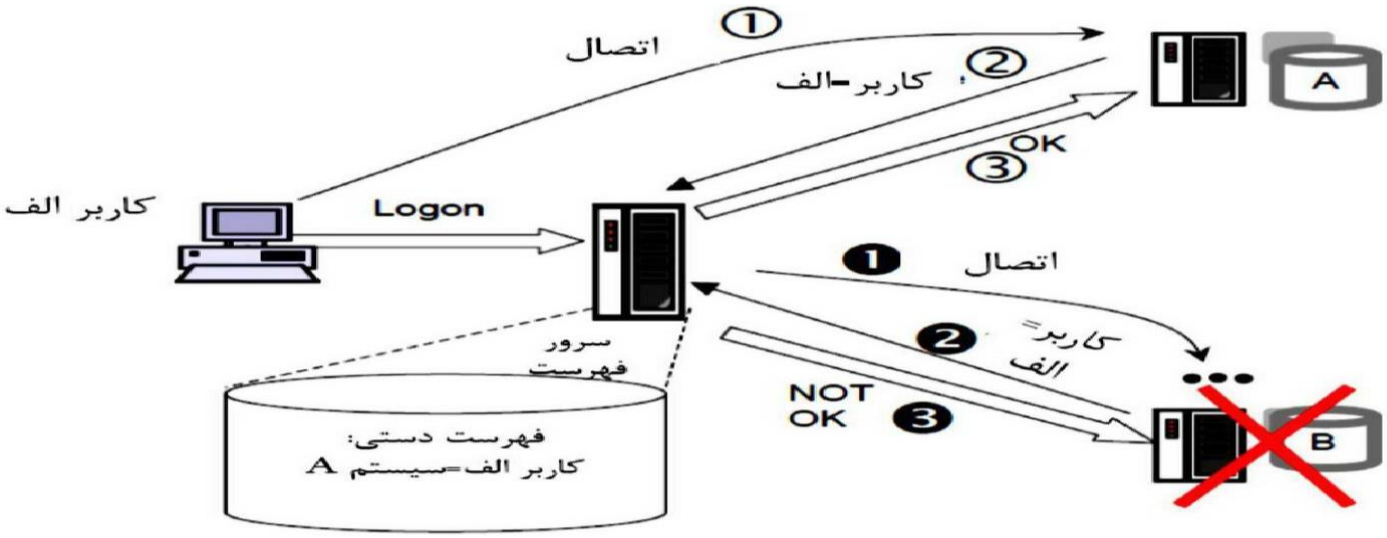
۳. **نرم افزار برای ورود به سیستم**

این سیستم قادر به ذخیره نام ها و رمزهای عبور کاربر برای هر سیستمی است که کاربر اجازه ورود به آنها را دارد. این نرم افزار فهرستی از برنامه های کاربردی مجاز را نشان داده و قادر به بازیابی جفت نام کاربری/رمز عبور مورد نیاز برای ورود به برنامه کاربردی است.

نقاط ضعف این نرم افزار آن است که پایگاه داده مربوط به رمز عبور که توسط رمزگذاری محافظت شده است و شبکه ارتباطی بین سرور Logon کننده و سایر برنامه های کاربردی است، بایستی یک شبکه ایمن باشد. قوی ترین کاربرد این روش به نامSSO معروف است.

۴. **سرور فهرست**

در این روش هر کاربر تنها یک رمز عبور دارد که در یک سیستم مرکزی ذخیره می شود. کاربر وارد سیستم مرکزی مورد اعتماد می شود تا هویت او را ارزیابی کند. وقتی کاربر وارد سیستم دوم می شود. سیستم دوم با اطلاع رسانی کاربر و رمز عبور صحت خود را به سیستم مرکزی اثبات می کند و درخواست پاسخ می نماید. اگر پاسخ مثبت باشد، کاربر سپس می تواند به سیستم دوم و برنامه های آن دسترسی یابد.



شکل ۱ – سرور فهرست

۳.۱. Hashing ◄

هشینگ روشی است که برای گرفتن اثر انگشت دیجیتالی برای یک پیام به کار می رود. این اثر انگشت می تواند به منظور **اعتبار سنجی**، **یکپارچگی** و **تمامیت پیام** به کار رود. امّا برای رمزگشایی پیام کاربرد ندارد. کد هش (hash) طول ثابتی دارد (معمولاً ۱۲۸ یا ۱۶۰ بیت) و به گونه ای است که کدی بی همتا محسوب می شود (یعنی پیام های متفاوت هش های متفاوت تولید می کنند).

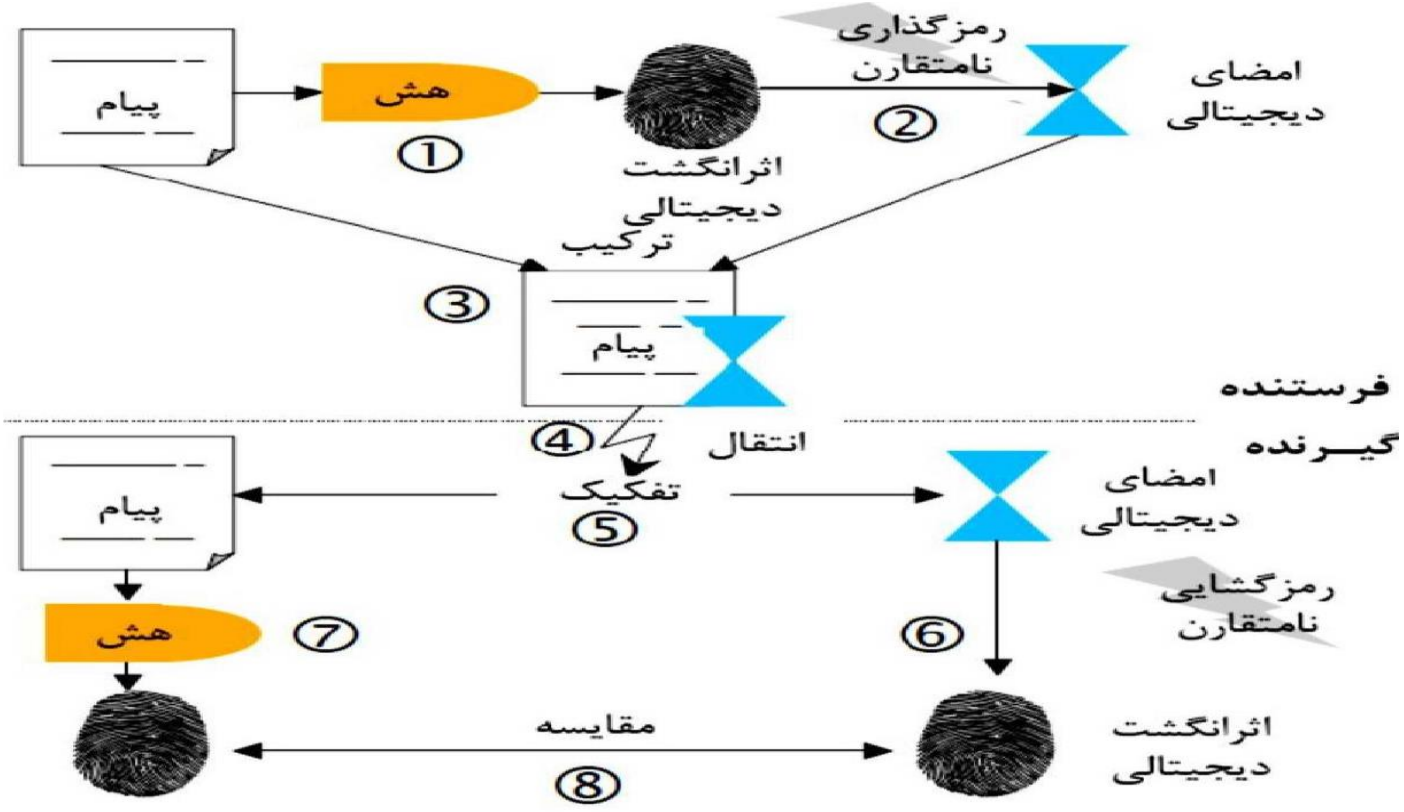
شکل ۴– هشینگ

الگوریتم های هشینگ،
توابع هش،
الگوریتم های هضم پیام،
رمزگذاری کنترلی،
اثر انگشت دیجیتالی،
چک تمامیت پیام (MIC)
و کد تشخیص دستکاری (MDC)
نیز نامیده می شوند.

برخی مثال ها شامل MD2، MD4، MD5 (که از ۱۲۸ بیت استفاده کرده و توسط Ron Rivest تولید شده است) و SHA1 که از ۱۶۰ بیت استفاده کرده و توسط مؤسسه ملی فناوری و علوم آمریکا اختراع شده است.

► ۴.۱. امضای دیجیتالی

برای گرفتن یک امضای دیجیتالی امن، چندین مرحله (که ترکیبی است از مفاهیم توضیح داده شده) بایستی به اجرا در بیاید.



شکل ۵- مکانیزم امضای دیجیتالی

شرح مراحل مختلف در شکل بالا از این قرار است :

۱. پیام هش می شود.

۲. به این ترتیب امضای دیجیتالی که با استفاده از کلید عمومی گیرنده رمزگذاری شده است، تولید می شود.

۳. پس از تولید امضای دیجیتالی، پیام با آن ترکیب می شود.

۴. پیام احراز هویت شده، ارسال می شود.

۵. پس از دریافت، پیام از امضای دیجیتالی جدا می شود.

۶. امضای دیجیتالی توسط کلید خصوصی گیرنده رمزگشایی می شود.

۷. پیام به صورت یک اثر انگشت دیجیتالی موقت هش می شود.

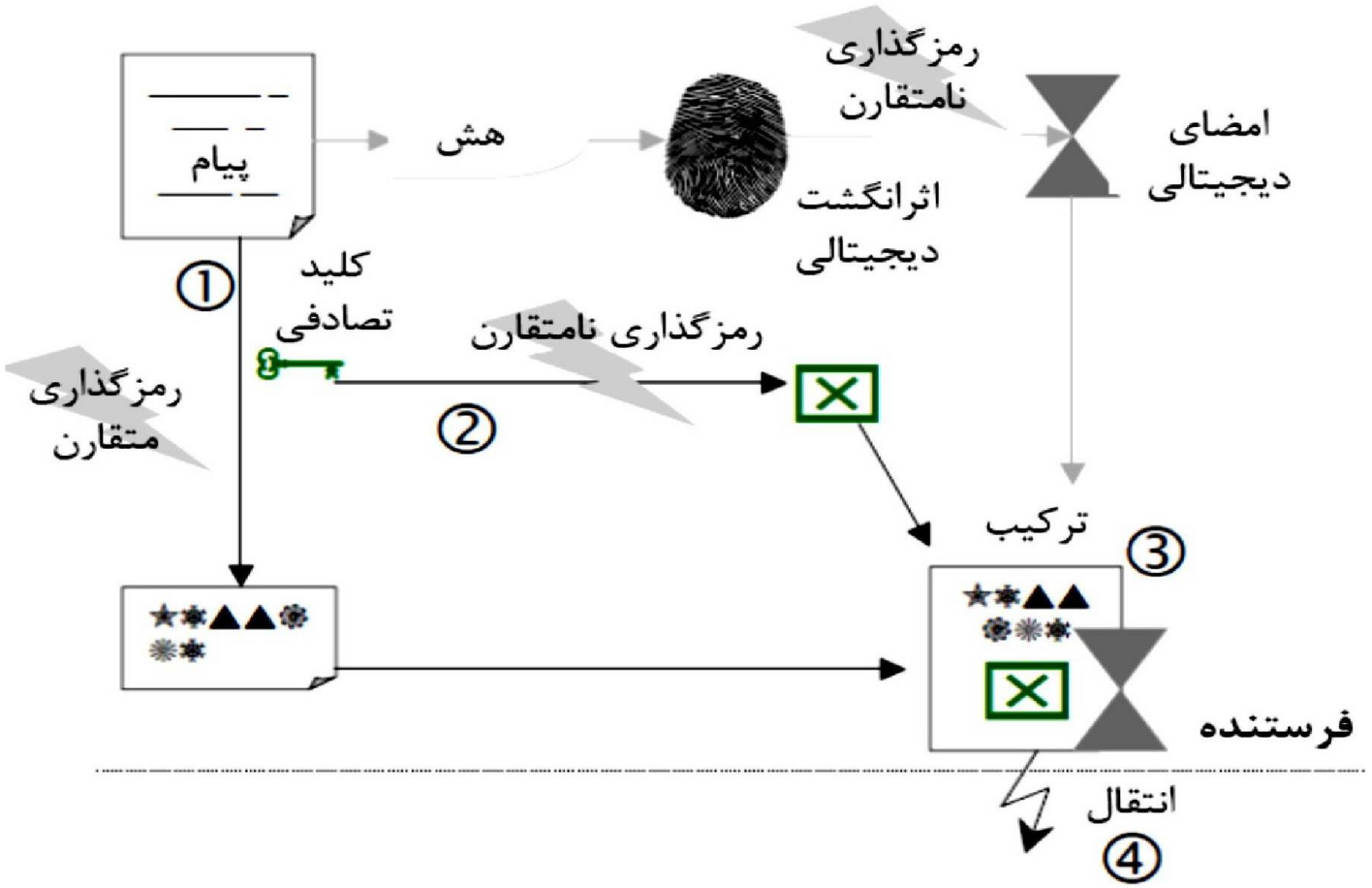
۸. پیام هش شده برای اعتبار سنجی اثر انگشت دریافت شده مورد استفاده قرار می گیرد.

هویت پیام در صورتی که در طول فرآیند انتقال، هیچ تغییری نکرده باشد (تمامیت)، تأیید می شود.

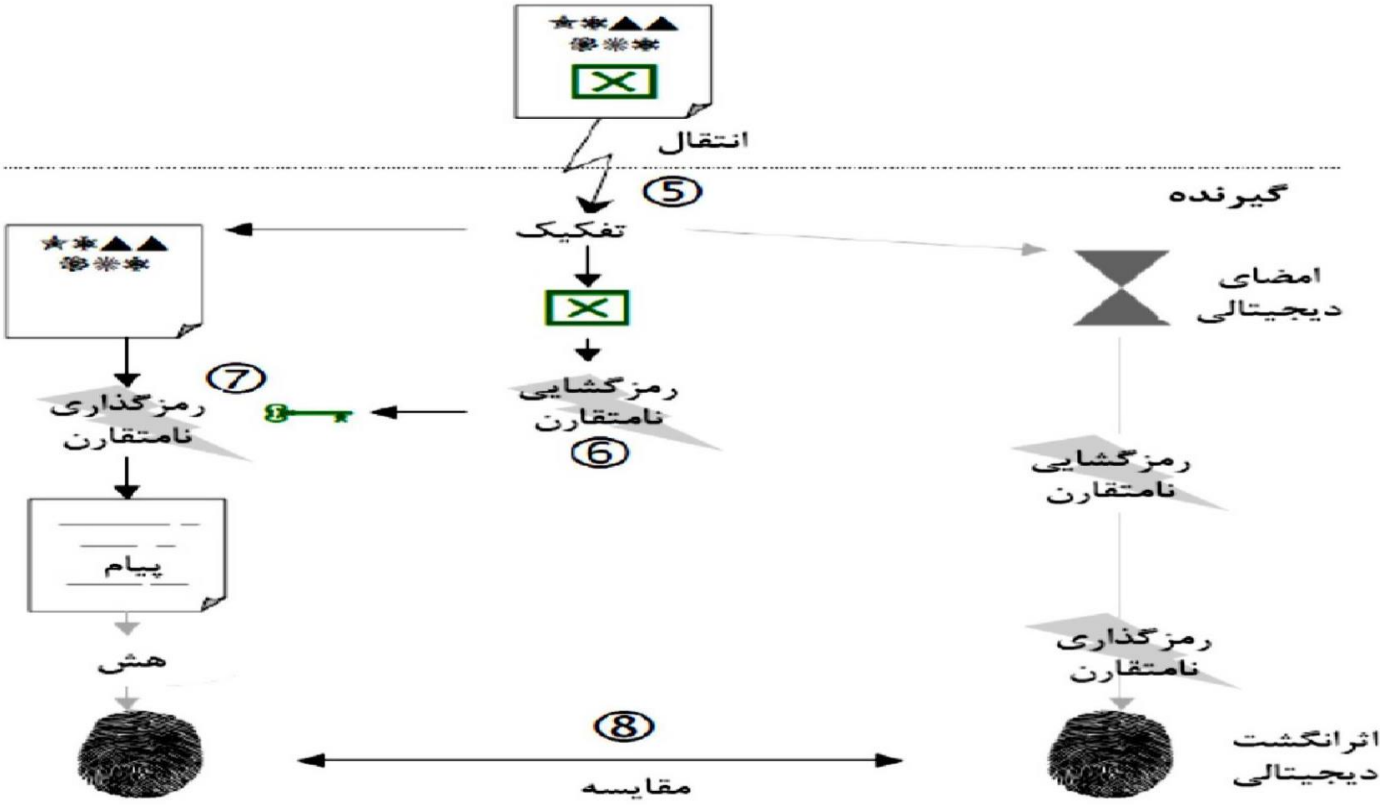
۵.۱. امضای دیجیتالی به همراه پیام رمزگذاری شده

امضای دیجیتالی در صورتی اعتبار پیام را تأیید می کند که این پیام در طول انتقال خراب نشده باشد (تمامیت).

برای اطمینان از محرمانه ماندن پیام مراحل دیگری بایستی انجام شود که در این قسمت به آن می پردازیم.



شکل ۶- امضای دیجیتالی با رمزگذاری پیام



شکل ۷- امضای دیجیتالی با رمزگشایی پیام

شرح مراحل مختلف در شکل های ۶ و ۷ از این قرار است :

۱. پیام با استفاده از یک کلید تصادفی رمزگذاری می شود.

۲. سپس این کلید تصادفی، با استفاده از کلید عمومی گیرنده، رمزگذاری می شود.

۳. کلید تصادفی رمزگذاری شده با امضای دیجیتالی و پیامی که رمزگذاری شده، تلفیق می شود.

۴. این بسته توسط شبکه به گیرنده ارسال می شود.

۵. پس از دریافت پیام رمزگذاری شده، کلید تصادفی و امضای دیجیتالی از یکدیگر جدا می شوند.

۶. کلید تصادفی با استفاده از کلید خصوصی گیرنده رمزگشایی می شود.

۷. پیام توسط کلید تصادفی رمزگشایی می شود.

۸. سپس پیام به یک اثر انگشت موقتی هش شده تا به منظور اعتبار سنجی اثرانگشت دریافت شده مورد استفاده قرار گیرد.

اگر پیام در طول فرآیند انتقال تغییر نکرده باشد احراز هویت آن به درستی انجام شده است.

۷.۱. خلاصه

سه نوع فرمت متفاوت پیام می تواند در سیستم رمزگذاری کلید عمومی به کار برده شود:

- پیام رمزگذاری شده: یک کلید متقارن برای رمزگذاری پیام و یک کلید عمومی برای رمزگذاری کلید متقارن به کار می رود.
- پیام امضاء شده: پیام به شکل اثر انگشت دیجیتالی هش می شود که با استفاده از کلید خصوصی به صورت یک امضای دیجیتالی رمزگذاری می گردد.
- پیام امضاء شده و رمزگذاری شده : ترکیبی از مفاهیم بالا که در آن پیام با استفاده از کلید خصوصی فرستنده امضاء شده و سپس توسط کلید عمومی رمزگذاری می شود.

OpenPGP و پیاده سازیهای PGP

با جا افتادن PGP، پیاده سازیهای متفاوت و گاه ناسازگاری از آن عرضه شد .
این «پروتکل» به حدی فراگیر شد که IETF تصمیم گرفت آن را استاندارد کند .
کمیته ای به نام OpenPGP Alliance این مسئولیت را بر عهده گرفت.
در سایت وب OpenPGP Alliance می خوانیم:

OpenPGP پرکاربردترین استاندارد رمزنگاری نامه در سراسر دنیاست.

این استاندارد توسط گروه کاری OpenPGP تحت عنوان **RFC2440** *پیشنهاد شده است.*
استاندارد OpenPGP از PGP اقتباس شده است؛

امروزه پیاده سازیهای زیادی از OpenPGP وجود دارد؛ مثلاً:

- PGP(تجاری)
- GNU Privacy Guard (GnuPG)
- Hushmail
- Veridis
- Authora
- EasyByte Cryptocx

استاندارد OpenPGP در سال ۱۹۹۸ بر اساس نسخهٔ PGP5 به وجود آمد.

PGP5 پیشتر PGP3 نامیده میشد.

در حقیقت نسل بعدی PGP 2.x محسوب می شود.

تمام پیاده سازیهای PGP از این استاندارد تبعیت می کنند،

بنابراین مشکل ناسازگاری خاصی میان پیاده سازیهای PGP وجود ندارد.

OpenPGP نسبت به PGP 2.x ویژگی های بسیار بیشتری دارد. جدول ۶ مقایسه ای از ویژگیهای این دو را نشان می دهد (ویژگی هایی که الزامی هستند با * نشان داده شده اند):

Feature	PGP 2.x (RFC 1991)	OpenPGP (RFC 2440)
Key format	V3 keys	V4 keys
Asymmetric algorithms	*RSA (encryption & signature)	RSA (encryption & signature)
		*DSA (signature)
		*Elgamal (encryption)
Symmetric algorithms	*IDEA	IDEA
		*Triple-DES
		CAST5
		Blowfish
		AES 128, 192, 256
		Twofish
Hash algorithms	*MD5	MD5
		*SHA-1
		RIPEMD-160
		SHA-256
		SHA-384
		SHA-512
Compression algorithms	ZIP	ZIP
		zlib
		BZip2

جدول ۲ مقایسه ویژگی های PGP 2.X و OpenPGP

کلیدهای V4 در OpenPGP نیز ویژگیهای زیادی نسبت به کلیدهای V3 دارند:

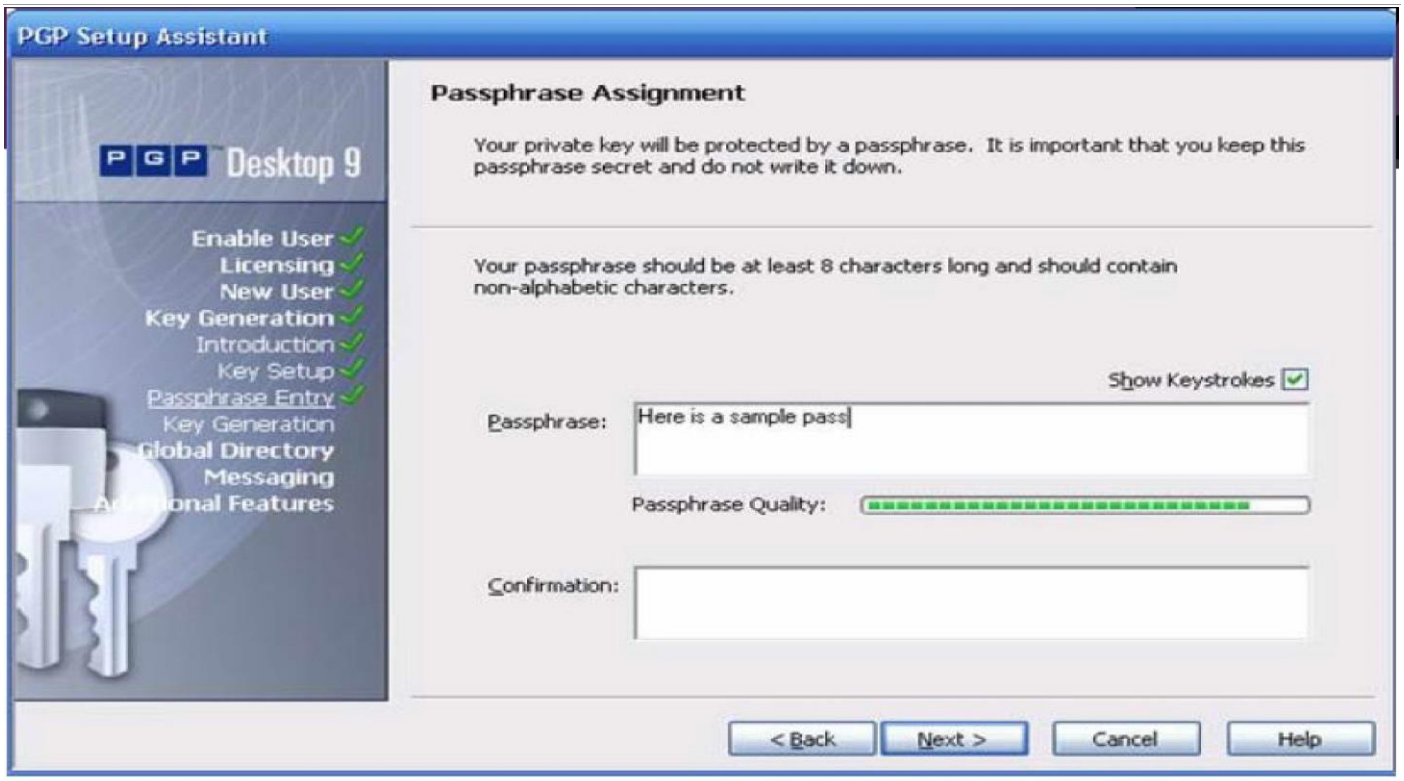
• یک کلید عمومی می تواند «زیرکلیدهایی» نیز داشته باشد ، که به کمک آنها می توان از کلیدهای مجزایی برای رمزنگاری و امضا استفاده کرد.

• امکان استفاده از چند الگوریتم وجود دارد، که پیاده سازی برخی از آنها به دلیل سازگاری با قبل الزامی است.

◄ بررسی نسخه ی PGP9 :

PGP9 آخرین نسخهٔ منتشر شدهٔ PGP تا به امروز است. این نرم افزار در چند نسخهٔ متفاوت عرضه شده است.

نخستین گام در استفاده از PGP9 (البته پس از طی مراحل registration !) وارد کردن گذرواژه ای برای رمز کردن کلید خصوصی است(شکل ۶). همانطور که این شکل نشان می دهد، PGP9 **تنها** گذرواژه های قوی را تأیید می کند.



شکل ۶ تنظیم گذرواژهٔ کلید خصوصی

نسخهٔ تجاری PGP

در گام بعد کلیدها و زیرکلیدها تولید می شوند.

یکی از امکانات PGP9 آن است که می تواند هنگام ارسال نامه ها از طریق SMTP، مداخله کرده و بنا به تنظیمات کاربر نامه ها را رمز و/یا امضا کند.

این ویژگی PGP Email Proxy نام دارد.

PGP9 می تواند از بخشی از دیسک به عنوان محلی برای ذخیرهٔ کلیدها استفاده کند.

این قسمت از دیسک توسط سرویس PGP از دستبرد مصون می ماند.

با وجود همهٔ این ویژگیها، PGP9 همان سرویسی را ارائه می دهد که نسخ ههای ساده، مجانی و خط فرمان PGP ارائه می کنند.

GPG

GPG (GnuPG یا GNU Privacy Guard) یکی از پیاده سازیهای معروف و مجانی OpenPGP است که تحت لیسانس GPL عرضه شده است.

دولت آلمان روی این پروژه سرمایه گذاری هنگفتی کرده است.

مزیت GPG بر PGP (علیرغم فقدان واسط گرافیکی) آن است که به علت استفاده از مجوز GPL، این نرم افزار برای همیشه مجانی خواهد بود.

اهمیت این مطلب وقتی آشکار می شود که کسی در آینده بخواهد پیامی را که امروز رمز شده، رمزگشایی کند. هیچ تضمینی نیست که PGP در آینده با همان شریط قبل به کاربران سرویس دهد (در حقیقت از زمان PGP9 به بعد این نرم افزار بسیار گرانتر شده است)؛ به علاوه دست به دست شدن مالکیت PGP که از گذشته وجود داشته نگرانی های زیادی را سبب شده است.

سایر پروتکل های E-Mail امن

در مقابل PGP می توان از دو پروتکل دیگر برای تبادل امن پیامها استفاده کرد:

PEM و **S/MIME**.

در این فصل این دو پروتکل بررسی می شوند.

PEM

PEM ((Privacy-Enhanced Mail) یکی از الگوریتمهایی است که برای امنیت e-mail ایجاد شد و چند شرکت بزرگ از آن پشتیبانی کردند،

اما به دلایلی که شرح آن خواهد رفت هرگز موفق نبود و امروزه از به ندرت از آن برای ارسال e-mail استفاده می شود (هر چند کاربردهای دیگری دارد).

زیمرمن در دهمین سالگرد ابداع PGP درباره PEM می نویسد:

هفته پیش از آنکه نخستین نسخهٔ PGP را منتشر کنم، از وجود استاندارد رمزنگاری e-mail دیگری با نام PEM مطلع شدم، که توسط چند شرکت بزرگ از جمله RSADSI پشتیبانی می شد. من به چند دلیل طراحی PEM را نمی پسندیدم.

اول آنکه PEM از DES ۵۶ بیتی برای رمزنگاری استفاده می کرد، که من آن را الگوریتم محکمی نمی دانستم.

همچنین PEM اصرار داشت که همهٔ پیامها امضا شوند،

و امضا را خارج از پیام رمزنگاری شده قرار می داد

، به طوریکه لازم نبود پیام رمزگشایی شود تا معلوم گردد چه کسی آن را امضا کرده است.

در این یادداشت، زیمرمن به مشکلات PEM اشاره می کند. البته مشکل دوم به مرور زمان حل شد، اما مشکل نخست کماکان پابرجا بود.

به علاوه RSADSI خود را بانی PEM معرفی می کرد و قصد داشت از مشتریان PEM پول بگیرد، اما مشتریان که به سبب مجوز RSA به نسخه ی مجانی الگوریتم دسترسی داشتند مخالفت کردند.

نتیجه این شد که PEM مهجور ماند و استفاده از آن به عنوان الگوریتم رمزنگاری e-mail بسیار محدود شد.

► تبدیلات PEM:

شکل زیر تبدیلات PEM را نشان می دهد. هر پیام بسته به نیاز کاربر از یک یا چند تا از این تبدیلات عبور می کند.

```
Transmit_Form = Encode(Encrypt(Canonicalize(Local_Form)))

Local_Form = DeCanonicalize(Decipher(Decode(Transmit_Form)))
```

- Local Form : نشان دهندهٔ پیام با استفاده از مجموعهٔ کاراکترهای بومی آن سیستم است.
- Canonicalize : پیام را برای ارسال با سیستم های استاندارد e-mail آماده می کند.
- Encrypt : پیام را رمزنگاری و/یا امضا می کند.
- Encode : پیام را از فرمت باینری به فرمت قابل چاپ تبدیل می کند.

عکس این تبدیلات (DeCanonalize، Decipher، Decode و Transmit Form) در سمت گیرنده صورت می گیرد تا پیام اصلی استخراج شود.

► PEM Encapsulation:

PEM از مکانیسم کپسوله سازی پیام RFC934 استفاده می کند .

هر پیام PEM بین دو EB (Encapsulation Boundary) محصور می گردد:

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----

********** PEM goes here ************

-----END PRIVACY-ENHANCED MESSAGE-----
```

RFC934 پیامها را به دو بخش تقسیم می کند: سرآیند پیام، و متن پیام:

```
-----BEGIN PRIVACY-ENHANCED MESSAGE-----

Encapsulated Header Portion

Blank Line

Encapsulated Text Portion

-----END PRIVACY-ENHANCED MESSAGE-----
```

بخشهای این پیام به ترتیب عبارتند از:

- BEGIN PRIVACY-ENHACED MESSAGE : این بخش پیام را آغاز می کند و Pre-EB نام دارد.
- Header : شامل اطلاعاتی در بارهٔ تبدیلات انجام گرفته روی پیام است.
- Blank Line : یک خط خالی که سرآیند و متن پیام را از هم جدا می کند.
- Text : نتیجهٔ اعمال تبدیلات به پیام اصلی.
- END PRIVACY-ENHANCED MESSAGE : این بخش پیام را خاتمه می دهد و Post-EB نام دارد.

S/MIME نسخه ی امن شده ی MIME است. بنابراین پیش از تشریح آن نیاز است که MIME تشریح شود.

خود MIME هم به علت رفع نواقص RFC822 به وجود آمد.

بنابراین در این بخش ابتدا RFC822 سپس MIME و در نهایت S/MIME تشریح خواهند شد.

S/MIME

► RFC 822 :

RFC822 قالب پیامهای ارسالی توسط سیستم پست الکترونیکی را بیان می کند.

هر پیام RFC822 از یک بخش پاکت(envelope) و یک بخش محتوا (contents) تشکیل می شود.

بخش محتوا به نوبهٔ خود شامل سرآیند و پیام اصلی است.

پاکت شامل تمام اطلاعات لازم برای ارسال و تحویل نامه است.

RFC822 در مورد این بخش از نامه توضیح بیشتری نمی دهد، چون این بخش بیشتر به اطلاعات رد و بدل شده میان سرورهای SMTP مربوط است.

- بخش محتوا بسیار آشناست، چون همه روزه با نامه های الکترونیکی سر و کار داریم و آنها را دیده ایم.
- تنها نکتهٔ مهم راجع به این بخش آن است که بخشهای سرآیند و متن پیام آن با یک خط خالی از هم جدا می شوند.
- مثال زیر، بر گرفته از RFC822 است وپیچیده ترین سرآیند ممکن برای یک پیام RFC822 به همراه یک متن پیام فرضی نشان می دهد:

```
Date       :  27 Aug 76 0932 PDT
From       :  Ken Davis <KDavis@This-Host.This-net>
Subject    :  Re: The Syntax in the RFC
Sender     :  KSecy@Other-Host
Reply-To   :  Sam.Irving@Reg.Organization
To         :  George Jones <Group@Some-Reg.An-Org>,
              Al.Neuman@MAD.Publisher
cc         :  Important folk:
                Tom Softwood <Balsa@Tree.Root>,
                "Sam Irving"@Other-Host;,
              Standard Distribution:
                /main/davis/people/standard@Other-Host,
                "<Jones>standard.dist.3"@Tops-20-Host>;
Comment    :  Sam is away on business. He asked me to handle
              his mail for him.  He'll be able to provide  a
              more  accurate  explanation  when  he  returns
              next week.
```

```
    In-Reply-To: <some.string@DBM.Group>, George's message
    X-Special-action:  This is a sample of user-defined field-
                names.  There could also be a field-name
                "Special-action", but its name might later be
                preempted
    Message-ID: 4231.629.XYzi-What@Other-Host

This is the most complicated RFC 822 header. The above blank lin
separates message header from message body. This example is take
from RFC 822 Appendix A.
```

- محدودیت های RFC822 :

- RFC822 لازم می دارد که تمام نامه ها باید از کدینگ ASCII7 استفاده کنند.

- **این محدودیت مانع ارسال فایلهای باینری یا نامه به زبانی غیر از انگلیسی می شود.**

در شبکه های نامه رسانی X.400 **(استاندارد مدل OSI که به جای SMTP استفاد ه می شود)** تبدیل کدینگ ASCII به EBCDIC دشوار است .

همچنین شبکه های X.400 که امکان انتقال فایلهای باینری را دارند نمی توانند این فایلها را به شبکه های مبتنی بر RFC822 تحویل دهند.

– مشکلاتی با برخی پیاده سازی های SMTP وجود دارد:

۱. طول خطوط به ۷۶ کاراکتر محدود است.

۲. نماد پایان خط در سیستمهای مختلف فرق دارد .

۳. مشکلات دیگری هم در کار با کارکترهای Tab و فواصل خالی وجود دارد.

بسیاری از این مشکلات با ارائهٔ دو RFC جدید یعنی RFC2821 (برای SMTP) و RFC2822 (برای قالب پیام) حل شدند.

MIME

MIME (Multipurpose Internet Mail Extensions) امکانات RFC2822 را توسعه می دهد.

MIME استاندارد گسترده ایست که RFC2045-2049 را به خود اختصاص داده است:

- ۲۰۴۵ : پیام هایی با بدنه اینترنتی
- ۲۰۴۶ : انواع رسانه ها
- ۲۰۴۹ : معیار هماهنگی نمونه ها

◄ مشخصات MIME :

MIME پنج سرآیند جدید تعریف می کند که می توان از آنها در بخش سرآیند پیامهای RFC2822 استفاده کرد. این ۵ سرآیند عبارتند از:

۱. MIME-Version : در حال حاضر تنها مقدار 1.0 را می پذیرد.

۲. Content-Type : به کمک آنها می توان از امکانات چند رسانه ای به هم راه پیامهای RFC2822 استفاده نمود. MIME هفت نوع Content-Type اصلی تعریف می کند، که هریک از آنها می توانند انواع مختلفی داشته باشند.

جدول زیر هفت نوع اصلی را به همراه چند زیر نوع نشان می دهد.

زیر نوعها قابل گسترش هستند، یعنی با ابداع قالبهای جدید می توان زیر نوع های جدیدی تعریف کرد.

هفت Content-Type اصلی با چند SubType نمونه...

Type	Subtype	Description
Text	Plain	Unformatted text; may be ASCII or ISO 8859.
	Enriched	Provides greater format flexibility.
Multipart	Mixed	The different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.
	Parallel	Differs from Mixed only in that no order is defined for delivering the parts to the receiver.
	Alternative	The different parts are alternative versions of the same information. They are ordered in increasing faithfulness to the original, and the recipient's mail system should display the "best" version to the user.
	Digest	Similar to Mixed, but the default type/subtype of each part is message/rfc822.

Message	rfc822	The body is itself an encapsulated message that conforms to RFC 822.
	Partial	Used to allow fragmentation of large mail items, in a way that is transparent to the recipient.
	External-body	Contains a pointer to an object that exists elsewhere.
Image	jpeg	The image is in JPEG format, JFIF encoding.
	gif	The image is in GIF format.
Video	mpeg	MPEG format.
Audio	Basic	Single-channel 8-bit ISDN mu-law encoding at a sample rate of 8 kHz.
Application	PostScript	Adobe Postscript.
	octet-stream	General binary data consisting of 8-bit bytes.

۳. Content-Transfer-Encoding : MIME شش کدینگ انتقال تعریف می کند.

این کدینگها تضمین می کنند که محتوای نامه هنگام انتقال توسط پست الکترونیکی بی تغییر بماند.

جدول زیر این کدینگها را نشان می دهد.

کدینگ های انتقال MIME

Transfer Encoding	Description
7bit	The data are all represented by short lines of ASCII characters.
8bit	The lines are short, but there may be non-ASCII characters (octets with the high-order bit set).
binary	Not only may non-ASCII characters be present but the lines are not necessarily short enough for SMTP transport.
quoted-printable	Encodes the data in such a way that if the data being encoded are mostly ASCII text, the encoded form of the data remains largely recognizable by humans.
base64	Encodes data by mapping 6-bit blocks of input to 8-bit blocks of output, all of which are printable ASCII characters.
x-token	A named nonstandard encoding.

۴. Content-Type : اگر محتوای MIME از چند بخش تشکیل شده باشد، از این شناسه برای تشخیص هر بخش به صورت یکتا استفاده می شود.

۵. Content-Description : گاه ممکن است یک پیام MIME شامل مواردی باشد که خوانندهٔ پیام قادر به تشخیص آنها نباشد. در این موارد از Content-Description استفاده می شود، که خوانندهٔ پیام به جای نشان ندادن محتوا، این Description را نشان می دهد (مشابه تگ های <alt> در HTML).

همان طور که جدول های فوق نشان می دهند، MIME قادر است همه نوع فایل را انتقال دهد و هیچ یک از محدودیتهای RFC822 را ندارد.

► امنیت و MIME:

RFC های ۲۶۳۲ تا ۲۶۳۴ سعی دارند MIME را گسترش داده و امنیت را به آن اضافه کنند . این نسخه از MIME ، S/MIME نام دارد((Secure MIME).

S/MIME چهار عملکرد را به MIME اضافه می کند:

۱. Enveloped Data : داده ها رمز می کند تا سرویس «محرمانگی» فراهم شود.

۲. Signed-Data : فشرده پیام را محاسبه و آن را با کلید خصوصی فرستنده امضا می کند . سپس پیام و امضا با Base64 کد می شوند. گیرنده فقط به شرطی می تواند از محتوای Signed-Data سر در بیاورد که از S/MIME بهره بگیرد.

۳. Clear-Signed Data : فشرده پیام را محاسبه و آن را با کلید خصوصی فرستنده امضا می کند. در این حالت فقط امضا Base64 می شود، که در نتیجه گیرنده خواهد توانست بدون S/MIME هم پیام را مشاهده کند، اما برای تطابق امضا به S/MIME احتیاج دارد.

۴. Signed and Enveloped Data : پیام را Sign یا Clear-Sign کرده و سپس آن را Envelope می کند.

► الگوریتم های S/MIME :

S/MIME از الگوریتمهای مختلفی برای امنیت استفاده می کند:

- DSS : الگوریتم توصیه شده برای امضای دیجیتال.
- Diffie-Hellman(ElGamal) : الگوریتم توصیه شده برای رمزنگاری کلید نشست.
- RSA : هم برای امضا و هم برای رمزنگاری می توان از آن استفاده کرد.

- 3DES یا RC2 ۴۰ بیتی : رمزنگاری پیام
- SHA-1 یا MD5 : استخراج فشرده پیام.

▶ **مقایسه S/MIME و PGP :**

هر دو PGP و S/MIME از الگوریتمهای رمزنگاری پیچیده ای برای انجام وظایف خود بهره می گیرند. در اینجا قصد نداریم این الگوریتمها را مقایسه کنیم؛ بلکه تنها PGP و S/MIME به طور کلی مقایسه خواهند شد.

یکی از مزایای S/MIME این است که این پروتکل بر اساس پروتکل MIME طراحی شده است، که امروزه استاندارد تبادل پیامهای الکترونیکی به شمار می رود.

▶ **مقایسه S/MIME و PGP :**

تفاوت عمده ی دیگرPGP و S/MIME در نحوهٔ مدیریت کلید این دو پروتکل است. در مراجع گوناگون از PGP به عنوان پرکاربردترین پروتکل نامه نگاری امن، و یا حتی به عنوان پرکابردترین پروتکل امنیتی یاد شده است.

امنیت PGP

برای بررسی امنیت هر الگوریتم یا پروتکل امنیتی می توان به «درخت های حمله» متوسل شد . این درختها بیانی رسمی و دقیق هستند که با مدل سازی تهدیدات امنیتی، امنیت سیستمها را در برابر حملات گوناگون تشریح می کنند. در این فصل ابتدا یک درخت حمله PGP را خواهیم دید. سپس آن دسته از حملاتی را که با موضوع این پژوهش مرتبطند انتخاب و بررسی می کنیم.

▶ **مثالی از یک درخت حملهٔ PGP :**

Bruce Schneier یکی از درخت های حمله ی PGP را طراحی کرده است. وی در رابطه با این درخت می گوید:

از آنجا که PGP پروتکل پیچیده ای است، درخت حملهٔ آن هم پیچیده شده و بنابراین ترجیح دادم آن را به شکل گرافیکی (درخت) نشان ندهم. PGP چندین ویژگی امنیتی را در خود جا داده است (نظیر محرمانگی، جامعیت، و غیره) ؛ در نتیجه، این درخت تنها یکی از

درختهای حملهٔ PGP را نشان می دهد. هدف حمله در این درخت «خواندن پیامی است که توسط PGP رمز شده است. » سایر اهداف ممکن عبارتند ا ز: «جعل امضای فردی دیگر» ، «تغییر امضای یک پیام» و «تغییر پیام رمز شده یا امضا شده ی PGP به گونه ای که این تغییر قابل مخفی بماند.»

درخت حملهٔ PGP آقای Schneier در شکل زیر نشان داده شده است.

درخت حمله PGP با هدف خواندن پیام رمز شده PGP

Goal: Read a message encrypted with PGP

1. Decrypt the message itself
   - 1.1. Break asymmetric-key encryption.
     - 1.1.1. Brute-force break asymmetric-key encryption.
     - 1.1.2. Mathematically break asymmetric-key encryption.
       - 1.1.2.1. Break RSA.
       - 1.1.2.2. Factor RSA modulus / calculate ElGamal discrete logarithm.
     - 1.1.3. Cryptanalyze asymmetric-key encryption.
       - 1.1.3.1. General cryptanalysis of RSA / ElGamal.
       - 1.1.3.2. Exploiting weaknesses in RSA / ElGamal.
   - 1.2. Break symmetric-key encryption.
     - 1.2.1. Brute-force break symmetric-key encryption.
     - 1.2.2. Cryptanalysis of symmetric-key encryption.
2. Determine symmetric key used to encrypt the message via other means.
   - 2.1. Fool sender into encrypting message using public key whose private key is known.
     - 2.1.1. Convince sender that a fake key (with known private key) is the key of the intended recipient (man in the middle attack).
     - 2.1.2. Convince sender to encrypt using more than one key– the real key of the recipient, and a key whose private key is known.
     - 2.1.3. Have the message encrypted with a different public key in the background, unbeknownst to the sender.
   - 2.2. Have the recipient sign the encrypted symmetric key.
   - 2.3. Monitor sender's computer memory.
   - 2.4. Monitor receiver's computer memory.
   - 2.5. Determine key from pseudorandom number generator.
     - 2.5.1. Determine state of randseed.bin when message was encrypted.
     - 2.5.2. Implant software (virus) that deterministically alters the state of

randseed.bin.

2.5.3. Implant software that directly affects the choice of symmetric key.

2.6. Implant virus that exposes the symmetric key.

3. Get recipient to (help) decrypt message.

3.1. Chosen ciphertext attack on symmetric key.

3.2. Chosen ciphertext attack on public key.

3.3. Send the original message to the recipient.

3.4. Monitor outgoing mail of recipient.

3.5. Spoof Reply-to: of From: field of original message.

3.6. Read message after it has been decrypted by recipient.

3.6.1. Copy message off user's hard drive or virtual memory.

3.6.2. Copy message off backup tapes.

3.6.3. Monitor network traffic.

3.6.4. Use electromagnetic snooping techniques to read message as is displayed on the screen (CRT monitors).

3.6.5. Recover message from printout.

4. Obtain private key of recipient.

4.1. Factor RSA modulus / calculate ElGamal discrete logarithm.

4.2. Get private key from recipient's key ring.

4.2.1. Obtain encrypted private key ring (AND)

4.2.1.1. Copy it from user's hard drive. (OR)

4.2.1.2. Copy it from disk backups. (OR)

4.2.1.3. Monitor network traffic. (OR)

4.2.1.4. Implant virus / worms to expose copy of the encrypted private key.

4.2.2. Decrypt private key.

4.2.2.1. Break IDEA encryption.

4.2.2.1.1. Brute-force break IDEA.

4.2.2.1.2. Cryptanalysis of IDEA.

4.2.2.2. Learn passphrase.

4.2.2.2.1. Monitor keyboard when user types passphrase.

4.2.2.2.2. Convince user to reveal passphrase.

4.2.2.2.3. Use keyboard-logging software to record passphrase when typed by user.

4.2.2.2.4. Guess passphrase.

4.3. Monitor recipient's memory.

4.4. Implant virus to expose private key.

4.5. Generate insecure public / private key pair for recipient.

دسته بندی حملات

با توجه به درخت حملهٔ PGP می توان حملات به پروتکل PGP را به چند دسته تقسیم نمود:

۱. حملاتی که مستلزم ناآگاهی کاربران است؛ نظیر استفاده کاربر از گذرواژه های ساده یا اغوای کاربران با استفاده از روشهای Social Engineering.

۲. حملاتی که مستلزم دسترسی فیزیکی مهاجم به کامپیوتر کاربر است؛ نظیر استفاده از حملاتی که مستلزم دسترسی فیزیکی مهاجم به کامپیوتر کاربر است؛ نظیر استفاده از Keylogger ها یا دزدیدن حلقهٔ کلید خصوصی.

۳. حملاتی که به الگوریتمهای سازندهٔ PGP صورت می گیرد، نظیر شکستن RSA، IDEA یا SHA-1.

۴. حملاتی که بر اثر ضعف در پیاده سازی پروتکل PGP اجرا می شوند، نظیر حمله هایی که به نسخه های مختلف GnuPG صورت گرفته است.

۵. حملاتی که مکانیسم مدیریت کلیدPGP (یعنی Web of Trust) را هدف قرار می دهند، یعنی به نحوی به کاربر می قبولانند که به کلید عمومی جعلی اطمینان کند.

۶. حملاتی که به PGP به عنوان یک سیستم (پروتکل) حمله می کنند.

▶ حمله به مکانیسم تولید عدد تصادفی:

کامپیوترها ماشینهایی قطعی (deterministic) هستند، و بنابراین نمی توانند اعداد تصادفی واقعی تولید کنند. به بیانی رسمی تر، هیچ FSM (Finite State Machine) ای نمی تواند عدد تصادفی تولید کند. در عوض، می توان الگوریتمهایی طراحی کرد که قادر باشند اعداد تصادفی مجازی (Pseudo-Random Numbers) تولید کنند. PRN ها باید یک سری خصوصیات داشته باشند:

۱. آنها باید تصادفی به نظر بیایند؛ یعنی هر نوع خصوصیت آماری آنها تصادفی باشد. مثلاً (به طور تقریبی) نصف طول دنباله صفر و نصف آن یک باشد، نیمی از دنباله های صفر به طول ۱ (0)، یک چهارم به طول ۲(00)، یک هشتم به طول ۳(000)و قس علی هذا باشد. دنبالهٔ صفرها ویک ها نباید قابل فشرده سازی باشد.

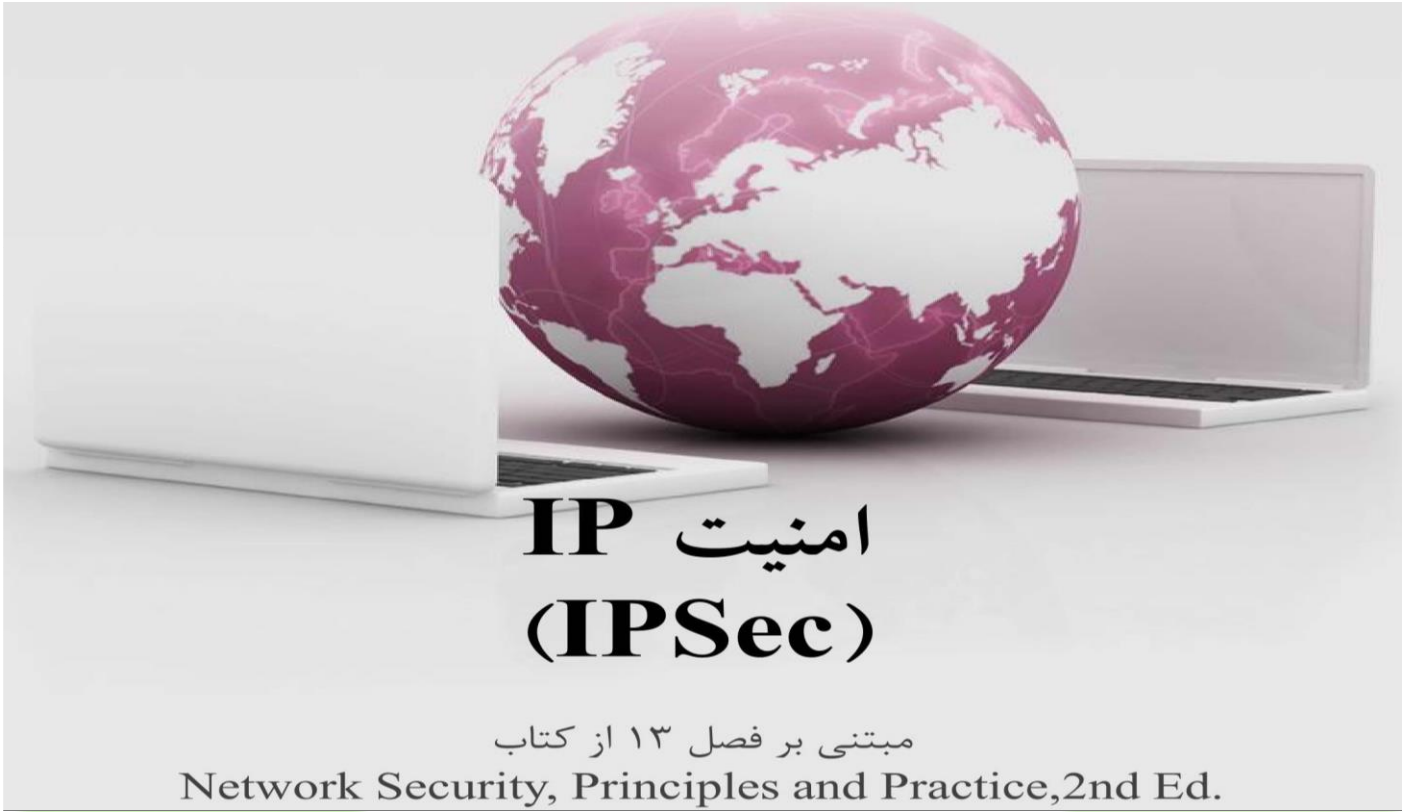
۲. آنها باید غیر قابل پیش بینی باشند؛ حتی با دانستن الگوریتم، نرم افزار، سخت افزار، و دنباله ای (به حد کافی) طولانی از بیتهای تولید شده تا کنون نباید توانست بیت بعدی را (از لحاظ محاسباتی) پیش بینی کرد.

۳. نباید بتوان آنها را مجدداً تولید کرد. اگر مولد عدد تصادفی در شرایط یکسان (در حد مطلوب) اجرا شود، دنباله های صفر و یک خروجی باید کاملاً متفاوت باشند.

الگوریتمهای مناسبی برای تولید PRN ها پیشنهاد شده است. در رابطه با PGP از دو طریق می توان به مولد PRN حمله کرد:

- دسترسی به randseed.bin (دسترسی فیزیکی)
- عدم به کارگیری صحیح الگوریتم PRNG (ضعف در پیاده سازی)

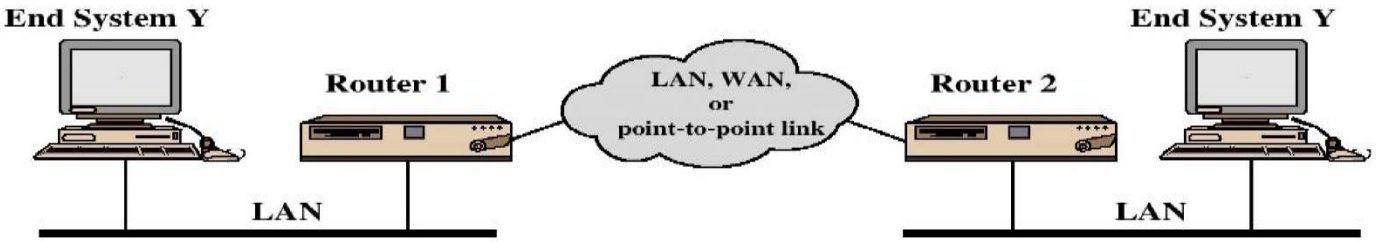
هر دو روش با فرض ما مبنی بر عدم دسترسی فیزیکی و عدم ضعف پیاده سازی در تناقض هستند.

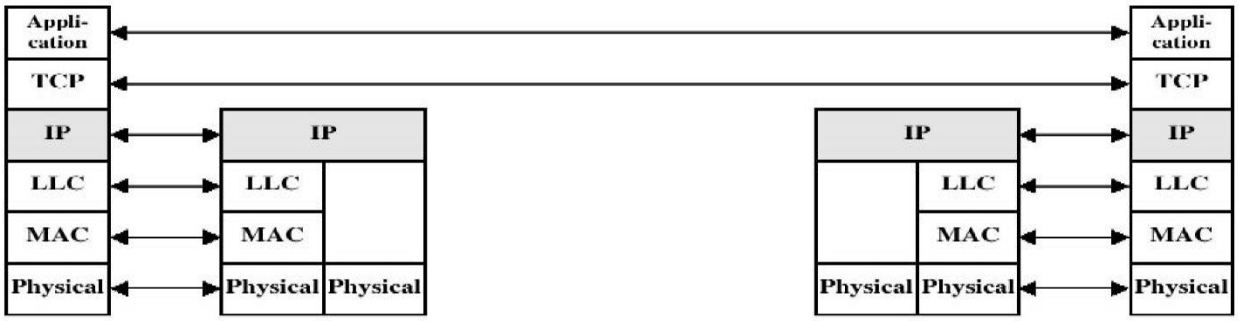


فهرست مطالب

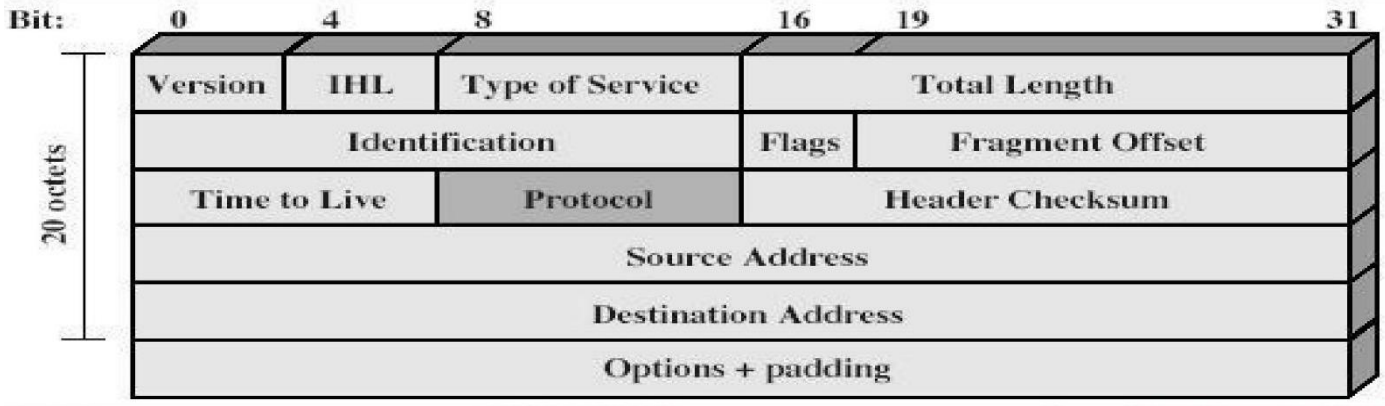
- مقدمه
- معماری IPSec
  - سرویس های IPSec
  - مجمع امنیتی(SA)
  - حالت‌های انتقال بسته‌ها
- AH
- ESP
- ترکیب SAها
- مدیریت کلید

مقدمه – مثالی از TCP/IP





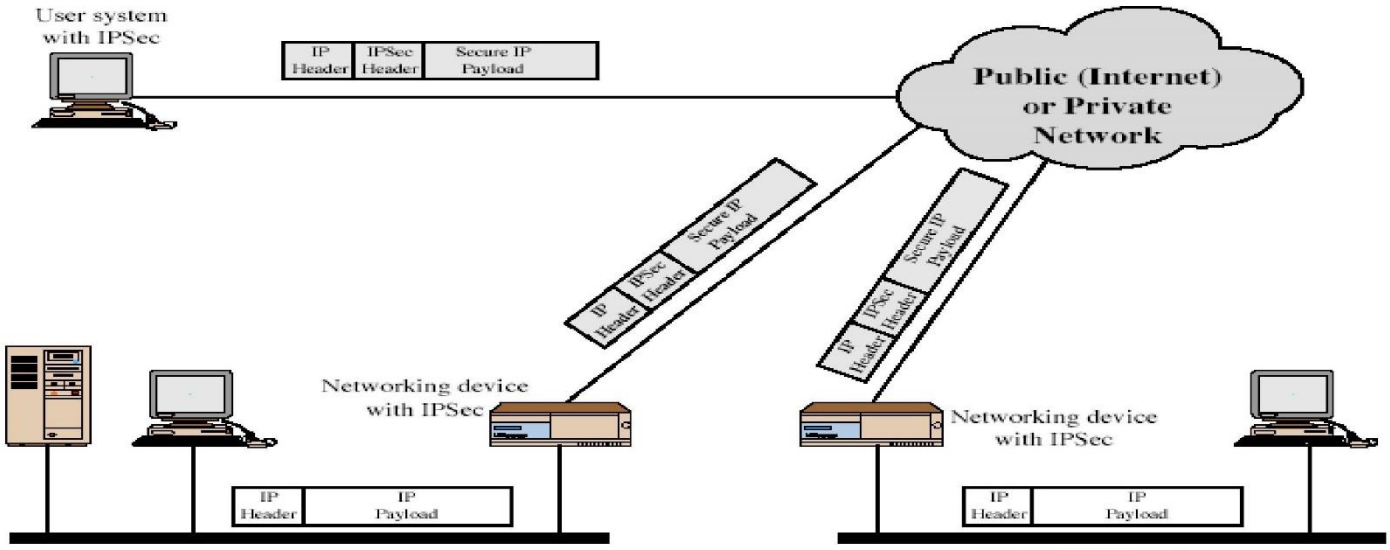
IPV4



مقدمه

- راه حل های امنیتی وابسته به کاربرد(تاکنون)
  - S/MIME و PGP : امنیت پست الکترونیکی
  - Kerberos : امنیت بین کاربر-کارگزار(احراز هویت)
  - SSL : ایجاد یک کانال امن در وب
- نیاز به امنیت در سطح IP
  - محرمانگی محتوای بسته های IP
  - هویت شناسی فرستنده و گیرنده بسته ها
- IPSec یک پروتکل تنها نیست بلکه مجموعه ای از الگوریتم های امنیتی و چارچوبی کلی فراهم می کند که به کمک آن ارتباط امنی برقرار کرد.
- سرویس های امنیتی فراهم شده توسط IPSec
  - هویت شناسی(به همراه کنترل جامعیت داده ها)
  - محرمانگی بسته ها
  - مدیریت کلید (تبادل امن کلید)
- نمونه کاربردهای IPSec
  - ایجاد VPN برای شعبه های مختلف یک سازمان از طریق اینترنت
  - دسترسی امن کارمندان شرکت به منابع شبکه از طریق اینترنت
  - امکان ارتباط امن بین چند سازمان
  - به وجود آوردن خدمات امنیتی برای کاربردهای دیگر(مثل تجارت الکترونیک)

IPSec



- مزایای استفاده از IPSec

— تامین امنیت قوی بین داخل و خارج LAN در صورت بکارگیری در راهیابها و حفاظ ها (Firewallها)

- عدم سربار رمزنگاری در نقاط انتهایی

— شفافیت از نظر کاربران

— شفافیت از دید برنامه های کاربردی لایه های بالاتر

— ایجاد ارتباط امن بین کارکنان سازمان از خارج به داخل

معماری IPSec: ویژگیها

- ویژگیها

— دارای توصیف نسبتا مشکل

— الزامی در IPv6 و اختیاری در IPv4

— در برگرفتن موارد زیر:

— پروتکل IPSec در سرآیند (Header)های توسعه یافته و بعد از سرآیند اصلی IP پیاده سازی میشود.

— مستندات IPSec بسیار حجیم بوده و به صورت زیر دسته بندی شده است:

- Architecture
- (ESP) Encapsulating Security Payload : رمزنگاری بسته ها (احراز هویت به صورت اختیاری)
- (AH) Authentication Header : تشخیص هویت بسته ها
- مدیریت کلید : تبادل امن کلیدها
- الگوریتم های رمزنگاری و هویت شناسی

معماری IPSec: سرویس ها

- سرویس های ارائه شده:
  - کنترل دسترسی
  - تضمین صحت داده ها در ارتباط Connectionless
  - احراز هویت منبع داده ها (Data Origin)
  - تشخیص بسته های دوباره ارسال شده و رد آنها (Replay Attack)
  - محرمانگی بسته‌ها
  - محرمانگی جریان ترافیک

معماری IPSec:
Association Security

- تعریف : مجمع امنیتی(Security Association) یک مفهوم کلیدی در مکانیزم های احراز هویت و محرمانگی برای IP بوده و یک رابطه یک طرفه بین فرستنده و گیرنده بسته ایجاد می کند.

- SA در IP به نوعی معادل Connection در TCP است

ویژگیها :

- **یک SA بصورت یکتا با ۳ پارامتر تعیین می شود:**
  - Security Parameters Index (SPI): یک رشته بیتی نسبت داده شده به SA
  - IP Destination Address : آدرس مقصد نهایی SA
  - Security Protocol Identifier : بیانگر تعلق SA به AH یا ESP

- پارامترهای SA
  - Sequence Number Counter
  - Sequence Counter Overflow
  - Anti Replay Windows
  - AH Information
  - ESP Information
  - SA Lifetime
  - IPSec Protocol Mode
  - Maximum Transmission Unit

معماری IPSec:
حالتهای انتقال بسته‌ها

– در هر دوی AH و ESP دو حالت انتقال وجود دارد:

- حالت انتقال(Transport Mode)

– تغییرات تنها روی محتوای بسته صورت می گیرد، بدون تغییر سرآیند IP

- حالت تونل (Tunnel Mode)

– اعمال تغییرات روی کل بسته IP(سرآیند+Payload) و فرستادن نتیجه به عنوان یک بسته جدید

- حالت انتقال

– در کاربردهای انتها به انتها(end-to-end) مثل کارگزار/کارفرما استفاده می‌شود

– ESP : رمزنگاری (ضروری) و صحت (اختیاری) Payload بسته

– AH : صحت Payload بسته و قسمتهای انتخاب شده سرآیند بسته

- حالت تونل

– مورد استفاده در ارتباط Gateway به Gateway

– هیچ مسیریاب (router) میانی قادر به تشخیص سرآیند داخلی نیست

Authentication Header (AH)

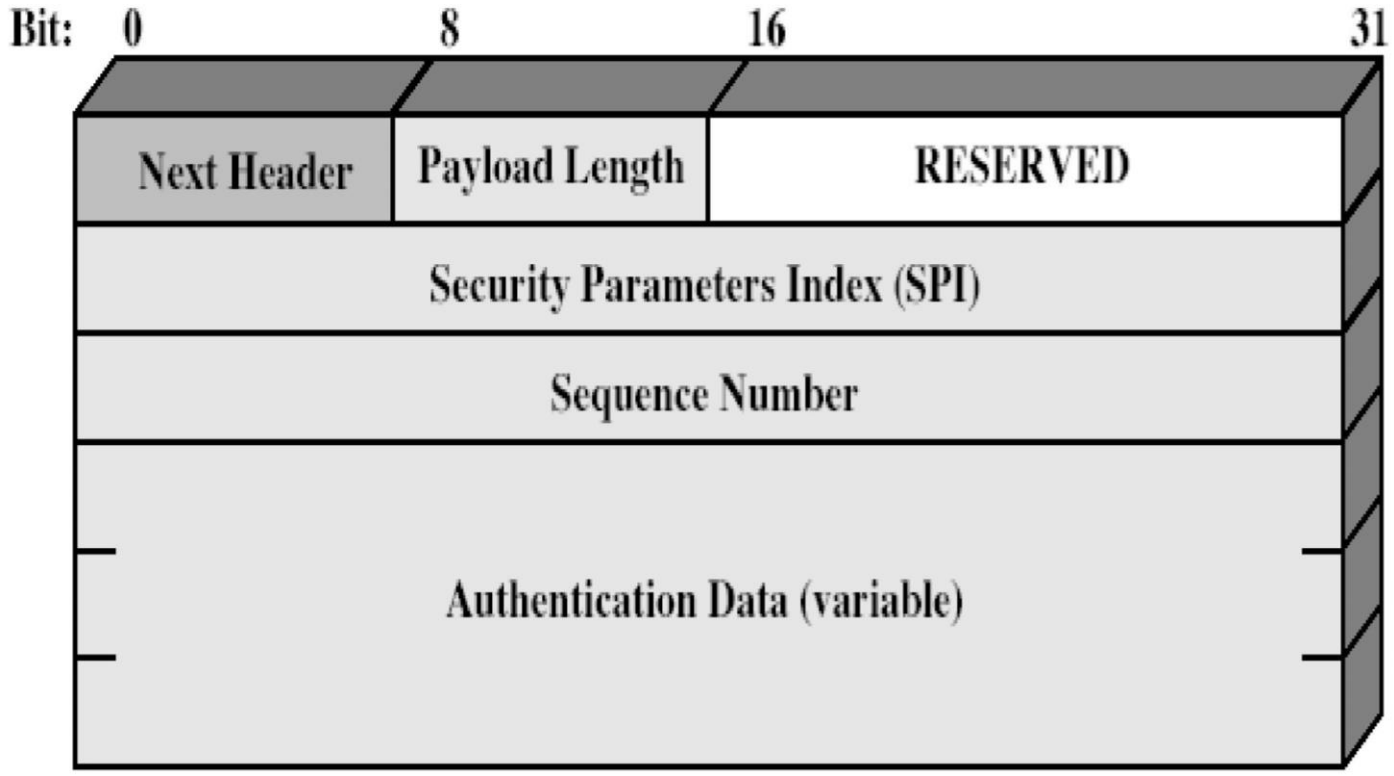
– تضمین صحت و احراز هویت بسته های IP

– تامین سرویس صحت داده‌ها با استفاده از MAC

- HMAC-MD5-96 یا HMAC-SHA-1-96

– طرفین نیاز به توافق روی یک کلید مشترک متقارن دارند

Authentication Header



AH

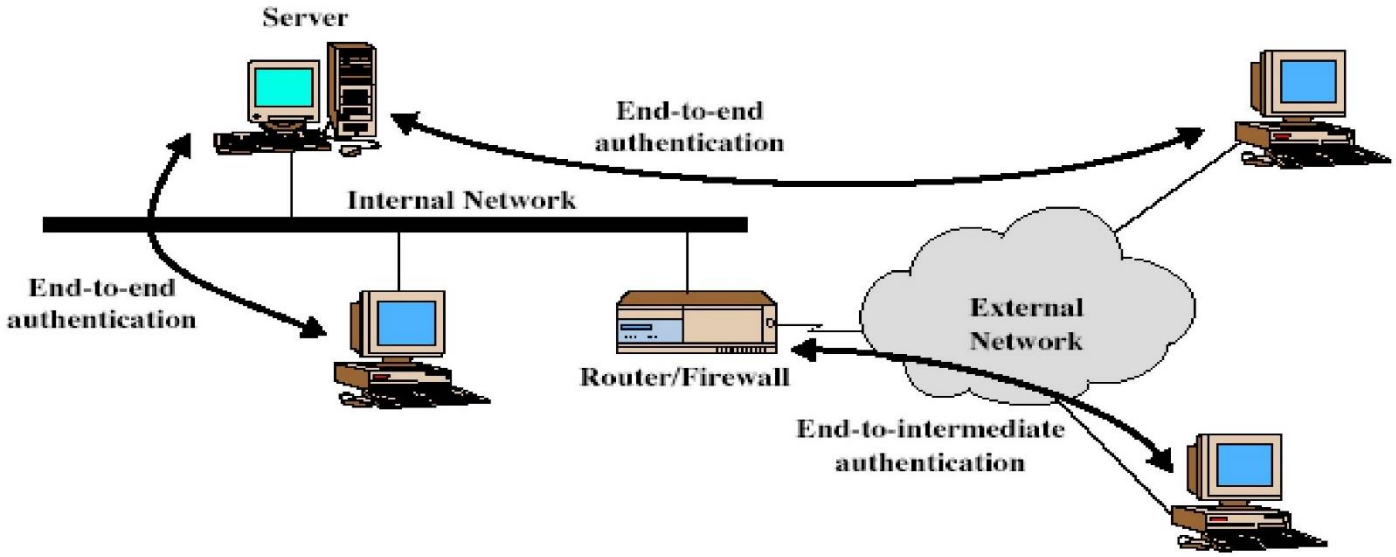
- فیلدهای AH :
  - Next Header(۸ بیت) : نوع سرآیند بعدی موجود در بسته
  - PayLoad Length(۸ بیت) : بیانگر طول AH
  - Reserved(16 بیت) : رزرو شده برای استفاده های آینده
  - Sec. Param. Index(۳۲بیت) : برای تعیین SPI مربوط به SA
  - Sequence Number(۳۲بیت) : شمارنده
  - Authentication Data(متغیر) : دربرگیرنده MAC یا ICV (Integrity Check Value)

- حالتهای انتقال و تونل در AH :

– حالت انتقال(Transport) : برای احراز هویت مستقیم بین کامپیوتر کاربر و کارگزار

– حالت تونل(Tunnel) : برای احراز هویت بین کاربر و حفاظ firewall)

End-to-end versus End-to-Intermediate Authentication



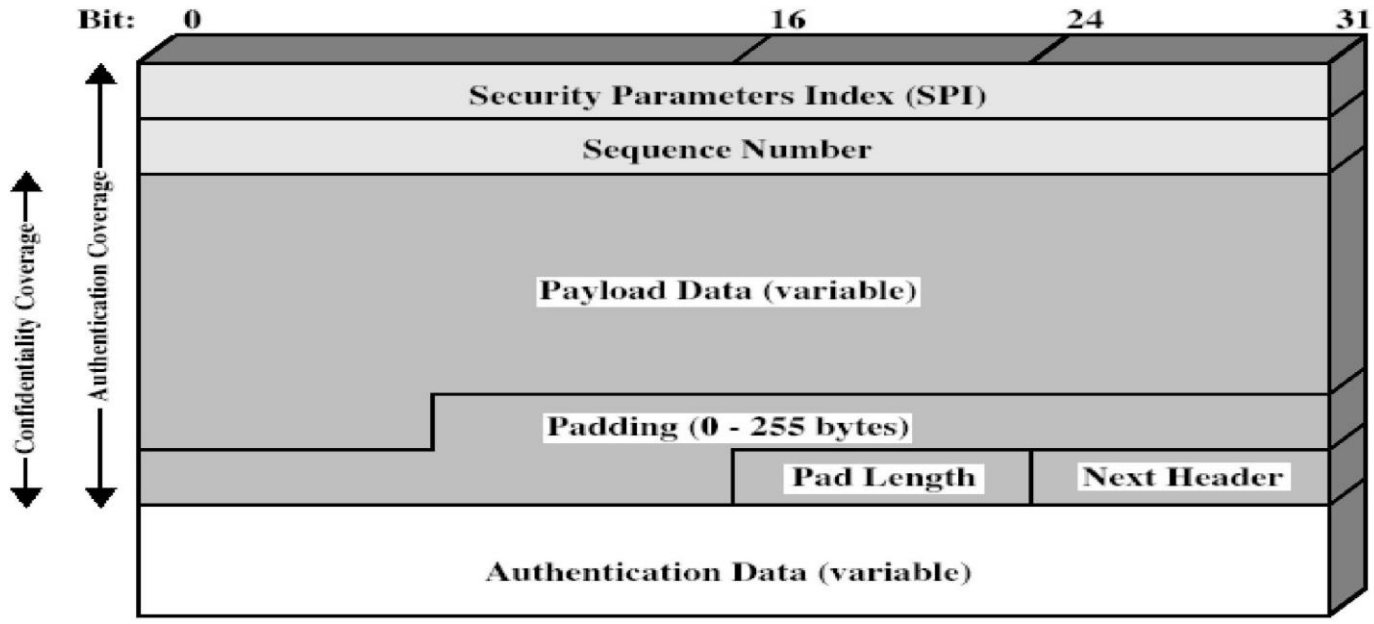
- روش مقابله با حمله تکرار(Replay)
  - اختصاص یک شمارنده با مقدار صفر به هر SA
  - افزایش شمارنده به ازای هر بسته جدید که با این SA فرستاده می شود
  - اگر شمارنده به مقدار $2^{32}-1$ برسد، باید از یک SA جدید با کلید جدید استفاده کرد

ESP

- ویژگیها
  - پشتیبانی از محرمانگی داده و تا حدی محرمانگی ترافیک
  - امکان استفاده از هویت شناسی(مشابه AH)
  - استفاده از الگوریتم DES در مد CBC(امکان استفاده از 3-DES, RC5, IDEA, 3-IDEA, CAST و Blowfish نیز وجود دارد)

- فیلدهای ESP
  - SPI : شناسه SA
  - Sequence Number : شمارنده برای جلوگیری از حمله تکرار مشابه AH
  - Payload : محتوای بسته که رمز می شود
  - Padding : بیتهای اضافی
  - Pad Length : طول فیلد بالا
  - Next Header : نوع داده موجود در Payload Data
  - Authentication Data : مقدار MAC محاسبه شده (بدون در نظر گرفتن خود فیلد)

Encapsulating Security Payload



- حالت انتقال
  - تضمین محرمانگی بین host ها
  - رمزنگاری بسته داده، دنباله ESP و اضافه شدن MAC درصورت انتخاب هویت شناسی توسط مبداء
  - تعیین مسیر توسط Router های میانی با استفاده از سرآیندهای اصلی(که رمز نشده اند)
  - چک کردن سرآیند IP توسط مقصد و واگشایی رمز باقیمانده پیغام
  - امکان آنالیز ترافیک

- حالت تونل

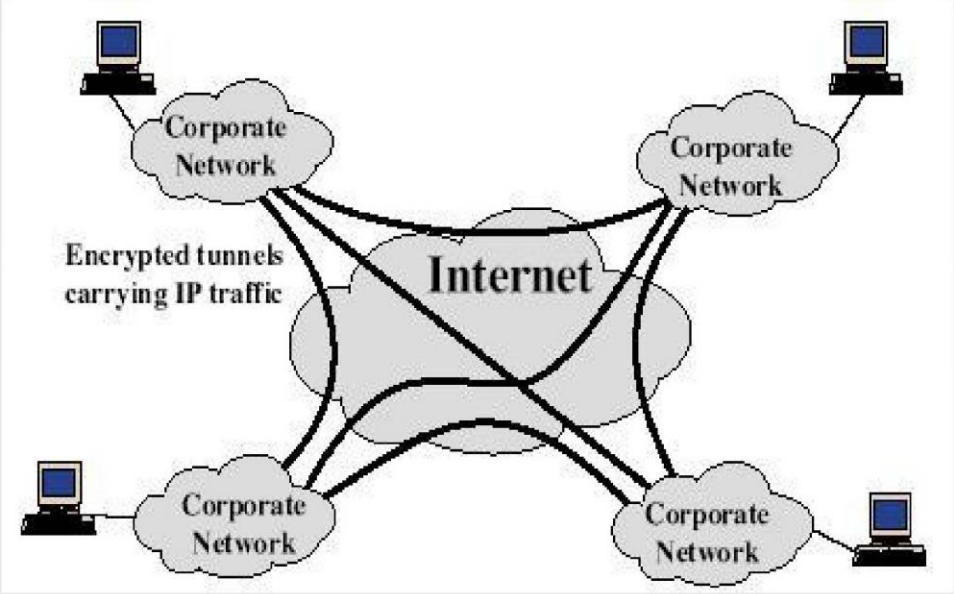
— اضافه شدن آدرس مبداء و مقصد دروازه های خروجی فرستنده و گیرنده سرآیند ESP و دنباله ESP و قسمت مربوط به MAC در صورت نیاز(برای هویت‌شناسی)

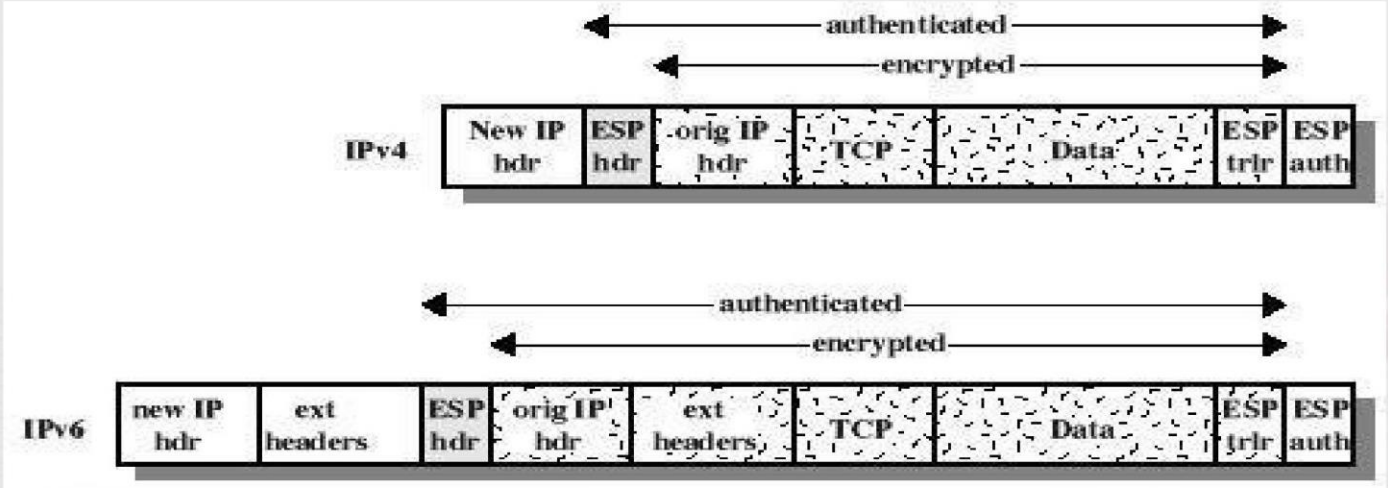
— انجام مسیریابی در Routerهای میانی از روی آدرس‌های جدید

— رسیدن بسته به فایروال شبکه مقصد و مسیریابی از روی آدرس IP قبلی تا گره نهایی

— حالت تونل IPSec یکی از روشهای ایجاد VPNها است

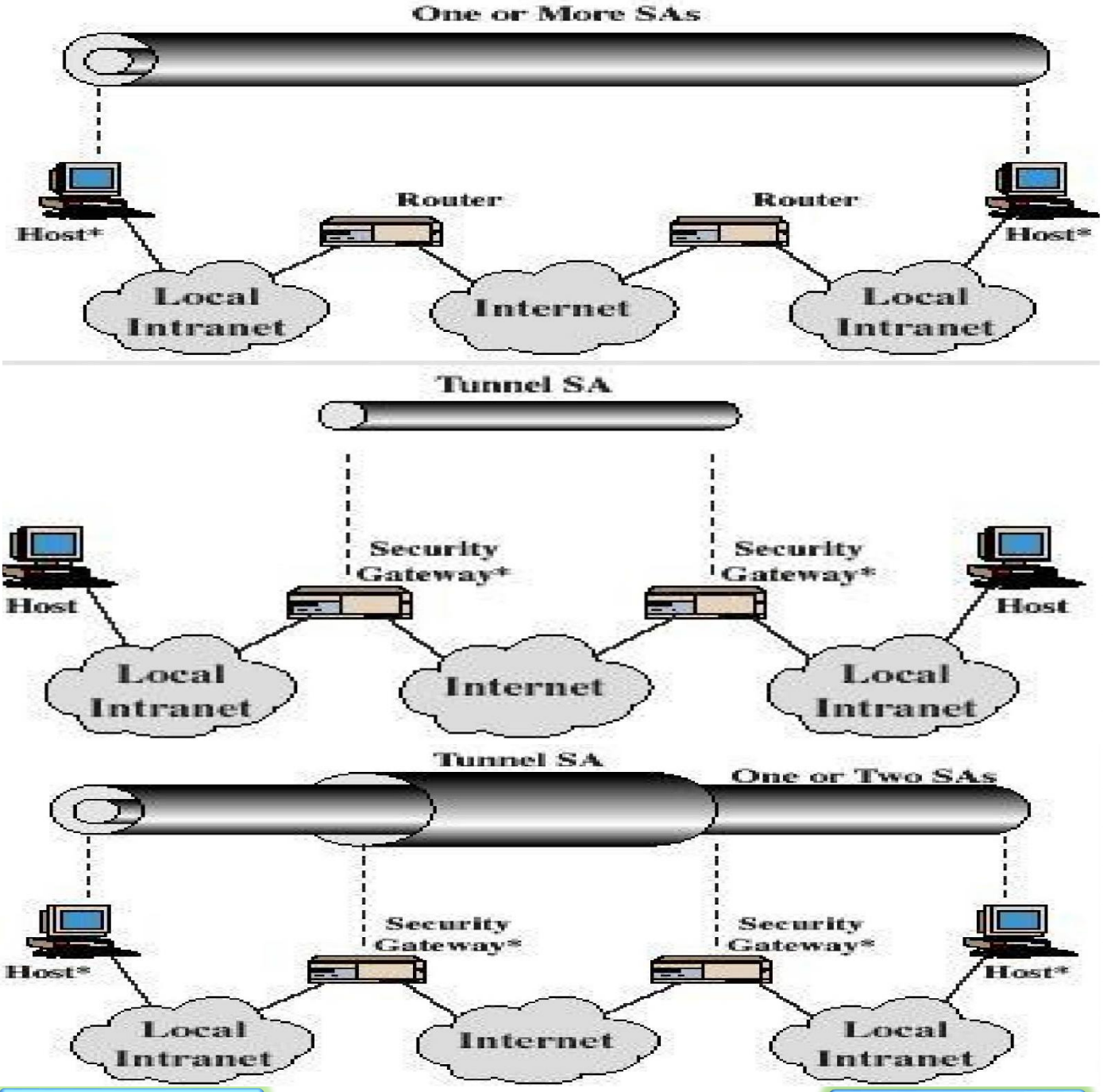
Tunnel Mode ESP

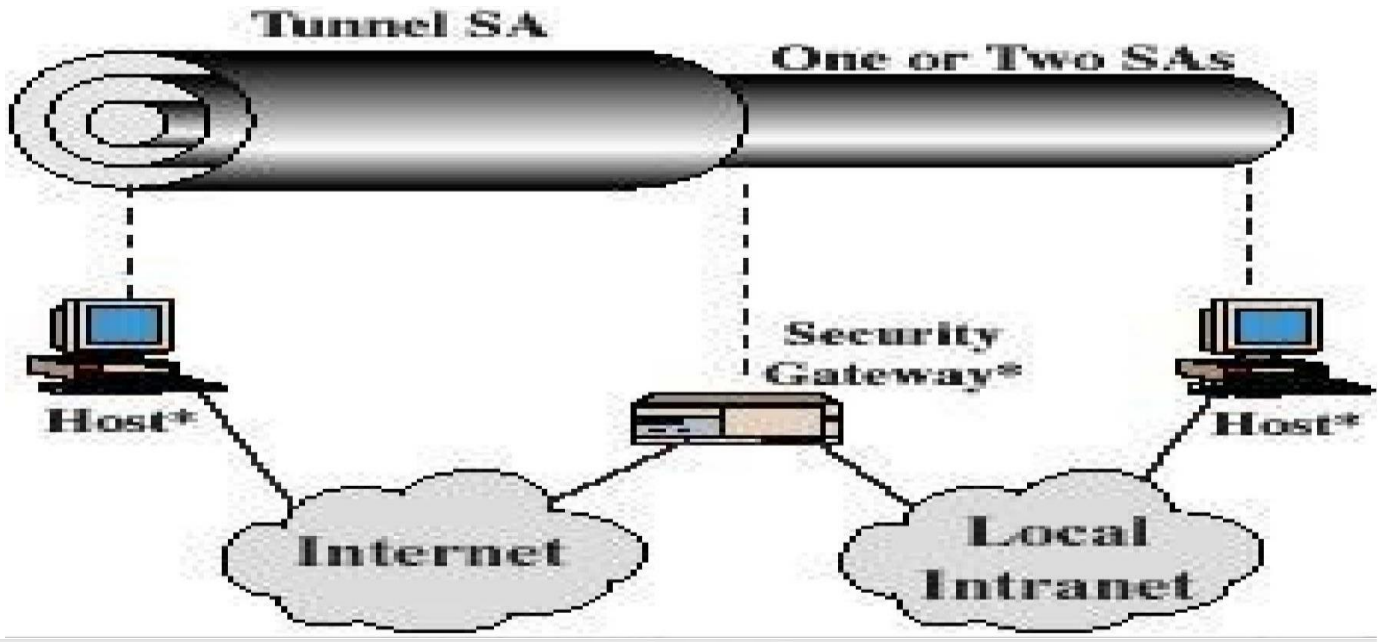


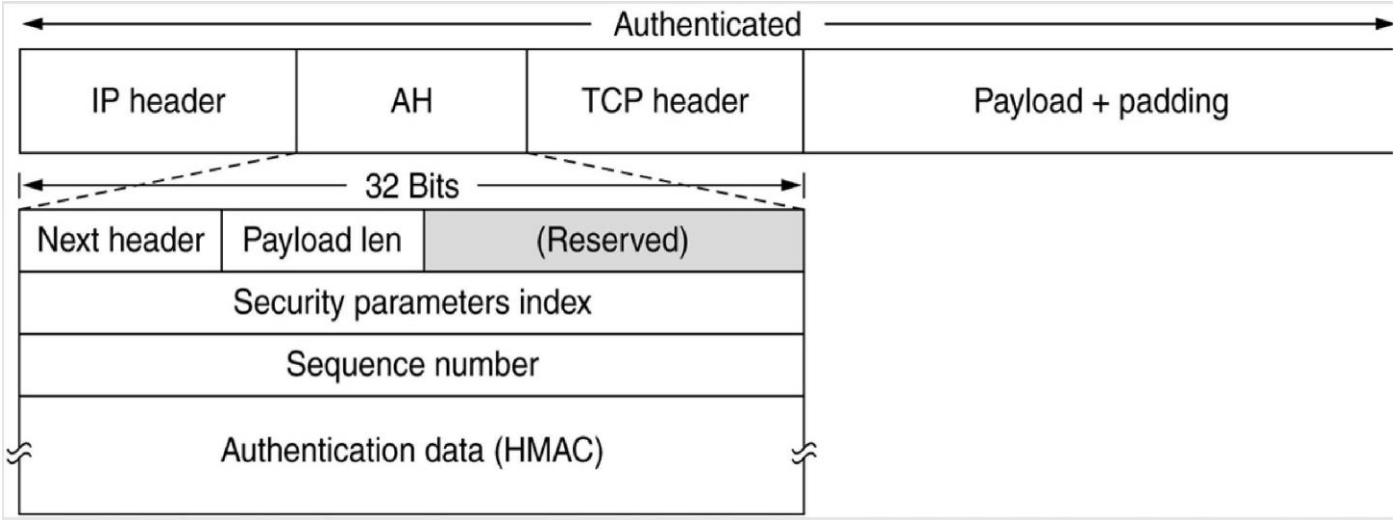


ترکیب SAها

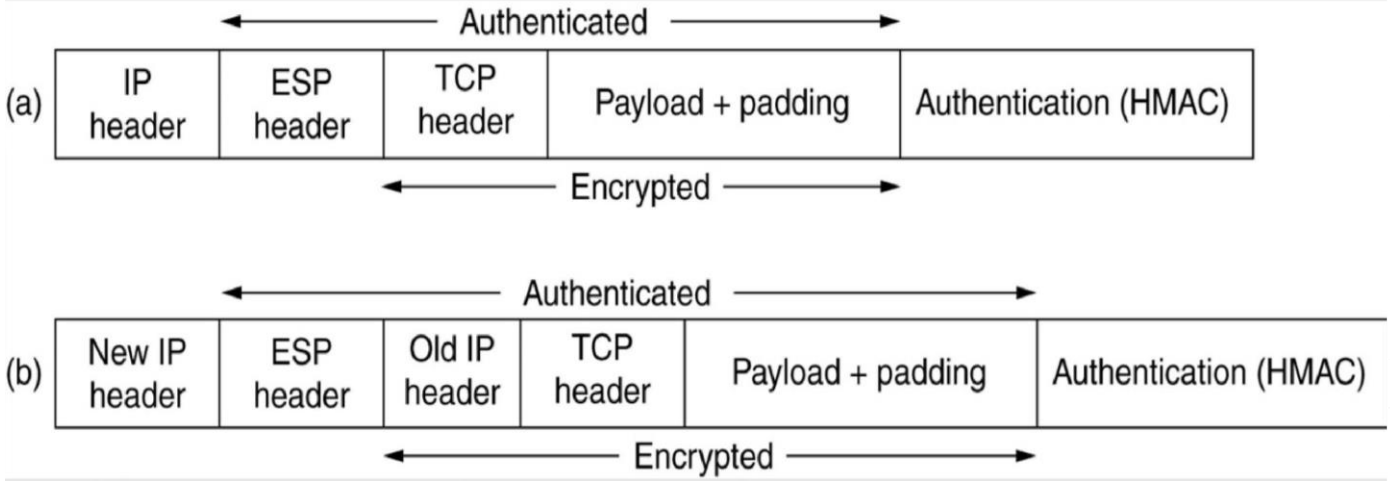
- با توجه به اینکه هر SA تنها یکی از سرویسهای AH یا ESP را پیاده سازی کرده است، برای استفاده از هر دو سرویس باید آنها را باهم ترکیب کرد
- ترکیبهای مختلف
  - پیاده سازی IPSec توسط host های متناظر
  - پیاده سازی IPSec توسط gateway ها
  - ترکیب دو حالت بالا







The IPsec authentication header in transport mode for IPv4.



(a) ESP in transport mode. (b) ESP in tunnel mode.

لایه سوکت های اَمن- SSL

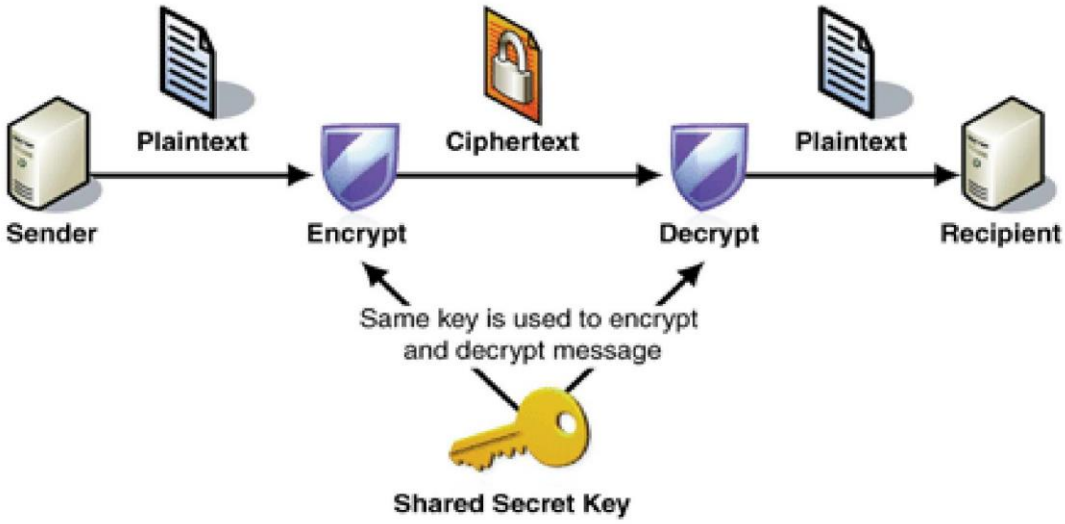
فهرست مطالب

- مقدمه
- معرفی پروتکل SSL
- شرح عملکرد پروتکل SSL
- نحوه بکارگیری پروتکل SSL
- معایب SSL

سه مشکل عمده در زمینه تبادل اطلاعات در شبکه:

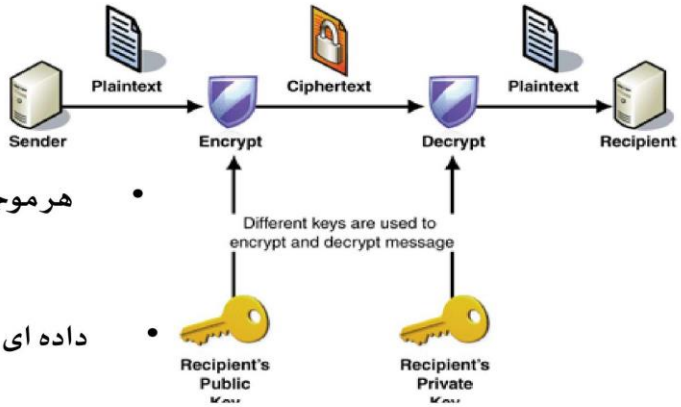
- محرمانگی داده ها (CONFIDENTIALITY)
- تمامیت داده ها (INTEGRITY)
- تائید هویت طرف های ارسال کننده و دریافت کننده (AUTHENTICATION)

رمزنگاری متقارن



- کلید رمزنگاری و رمزگشایی یکسان هستند
- سهولت پیاده سازی
- سرعت بالا

رمزنگاری نامتقارن



- هر موجودیت یک کلید خصوصی و یک کلید عمومی دارد.
- داده ای که با یکی از این دو رمز شود با دیگری رمزگشایی می شود.

- مشكل اصلي اين روش تطبيق كليد عمومي با موجوديت است؛
يعني بتوان اطمينان حاصل كرد كه **K** كليد عمومي موجوديت **X** است.

منظور از محرمانگي آن است كه اطلاعات ردوبدل شده توسط موجوديت هاي غيرمجاز قابل فهم نباشد.
محرمانگي از طريق رمزكردن اطلاعات ارسالي با يك كليد متقارن تصادفي به دست مي آيد.
الگوريتم هاي متقارن به لحاظ سرعت بيشتري كه دارند در رمزكردن حجم هاي بزرگ اطلاعات مورد استفاده قرار مي گيرند.
كليد متقارن تصادفي نيز با كليد عمومي گيرنده رمزميشود و همراه اطلاعات فرستاده مي شود گيرنده ابتدا با استفاده از كليد خصوصي اش، كليد متقارن تصادفي را مي يابد و سپس با استفاده از آن كل اطلاعات را رمزگشايي مي كند
منظور از تمامیت داده دریافت داده به همان صورت ارسال شده است.
در سمت فرستنده HASH پیغام ارسالی محاسبه شده و با کلید خصوصی رمزنگاری میشود و سپس به طرف گیرنده ارسال می شود.در سمت گیرنده پس از دریافت پیغام و رمزگشایی آن HASH مجدداً محاسبه می شود.
HASH دریافت شده از فرستنده نیز رمزگشایی می شود و با HASH محاسبه شده مقایسه می شود، اگر مطابقت داشت تمامیت داده ها احراز می شود.

معرفی و تاریخچه

- **SSL** یا **(SECURE SOCKET LAYER)** راه‌حلی جهت برقراری ارتباطات ایمن میان یك سرویس‌دهنده و یك سرویس‌گیرنده است که توسط شرکت **NETSCAPE** ارایه شده است.
- **SSL** پروتکلی است که پایین‌تر از لایه کاربرد و بالاتر از لایه انتقال قرار می‌گیرد.
- مزیت استفاده از این پروتکل بهره‌گیری از موارد امنیتی تعبیه شده نظیر **HTTP**، **IMAP**،**LDAP** و... می‌باشد که براساس آن الگوریتم‌های رمزنگاری بر روی داده‌های خام **(PLAIN TEXT)** آن برای امن کردن پروتکل‌های غیرامن لایه کاربردی که قرار است از یك کانال ارتباطی غیرامن مثل اینترنت عبور کنند، اعمال می‌شود و محرمانه ماندن داده‌ها را در طول کانال انتقال تضمین می‌کند.

عدم وجود مکانیزمی برای ارتباط امن درلایه انتقال

- **SSL1.0** اولین طراحی شرکت **NETSCAPE** * سال ۱۹۹۴ میلادی.
- **SSL3.0** توسط شرکت **NETSCAPE** طراحی و منتشر شد * اوایل سال ۱۹۹۶ میلادی.

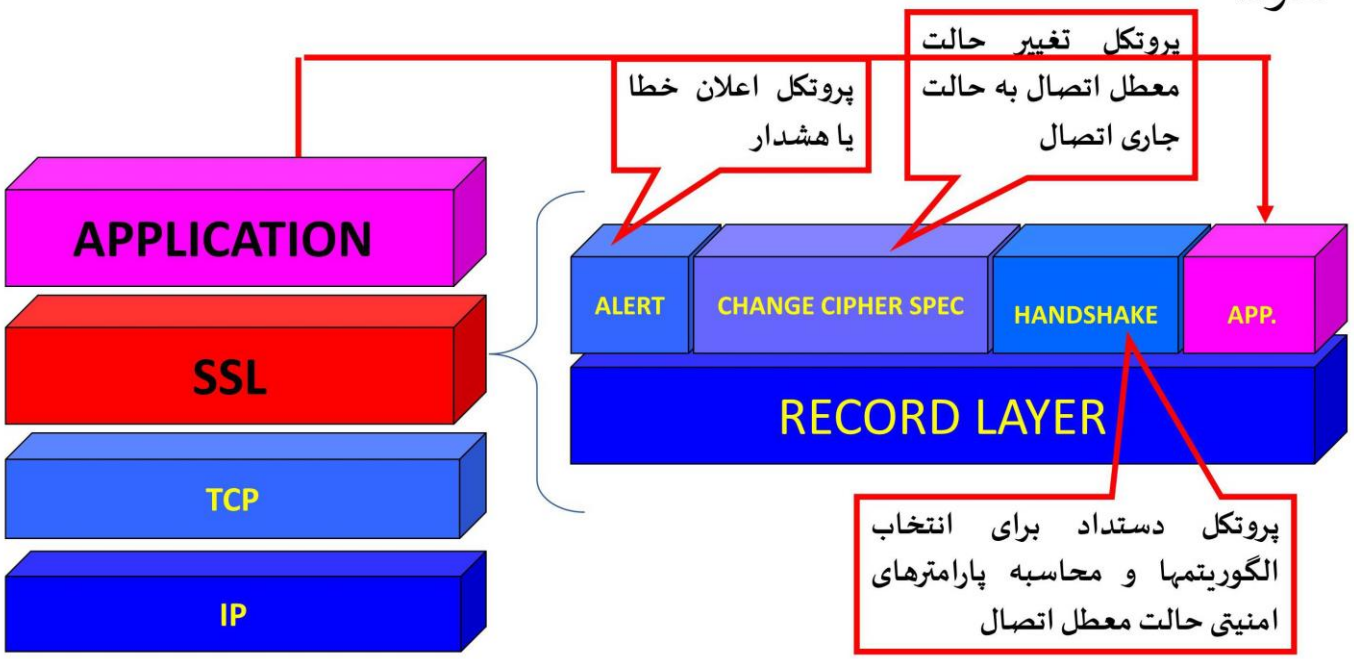
درابتدای ماه می سال ۱۹۹۶ میلادی، توسعه **SSL** تحت مسئولیت **IETF** درآمد.

- **TLS1.0** اولین نسخه استاندارد پروتکل **SSL** * اوایل سال ۱۹۹۹ میلادی.

تلاش برای ارتقای پروتکل **SSL** ادامه دارد.

SECURE SOCKET LAYER

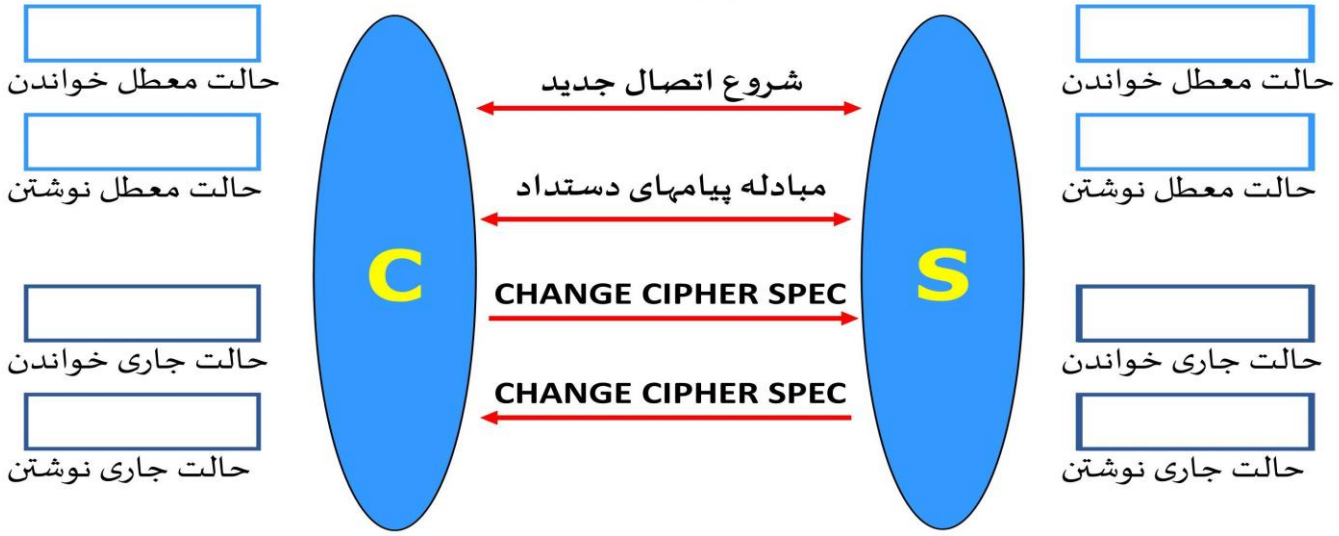
SSL یک لایه مجزاست که تنها برای برقراری امنیت به معماری اینترنت اضافه می شود.



پروتکل تغییر حالت معطل به حالت جاری

- در**SSL** چهارحالت اتصال وجود دارد:
- حالت خواندن و نوشتن معطل - **(Pending Read And Write States)**
- حالت خواندن و نوشتن جاری - **(Current Read And Write states)**

حالات چهارگانه اتصال

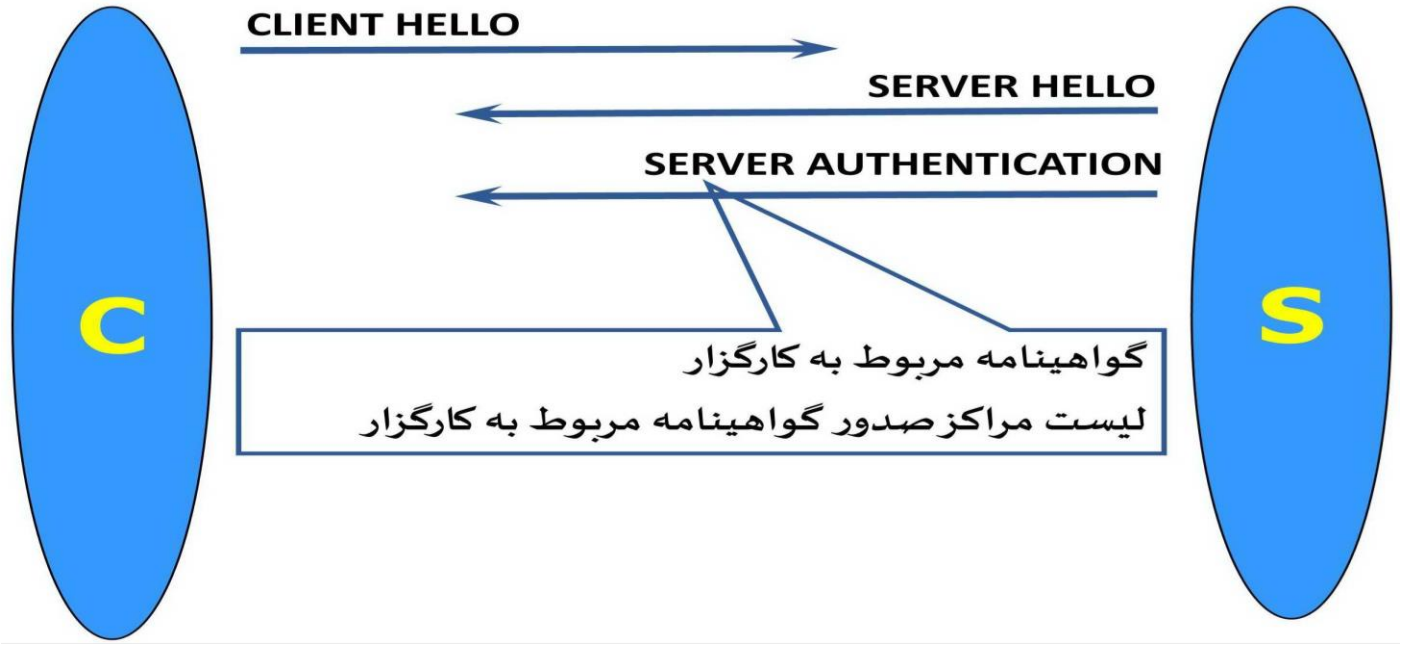


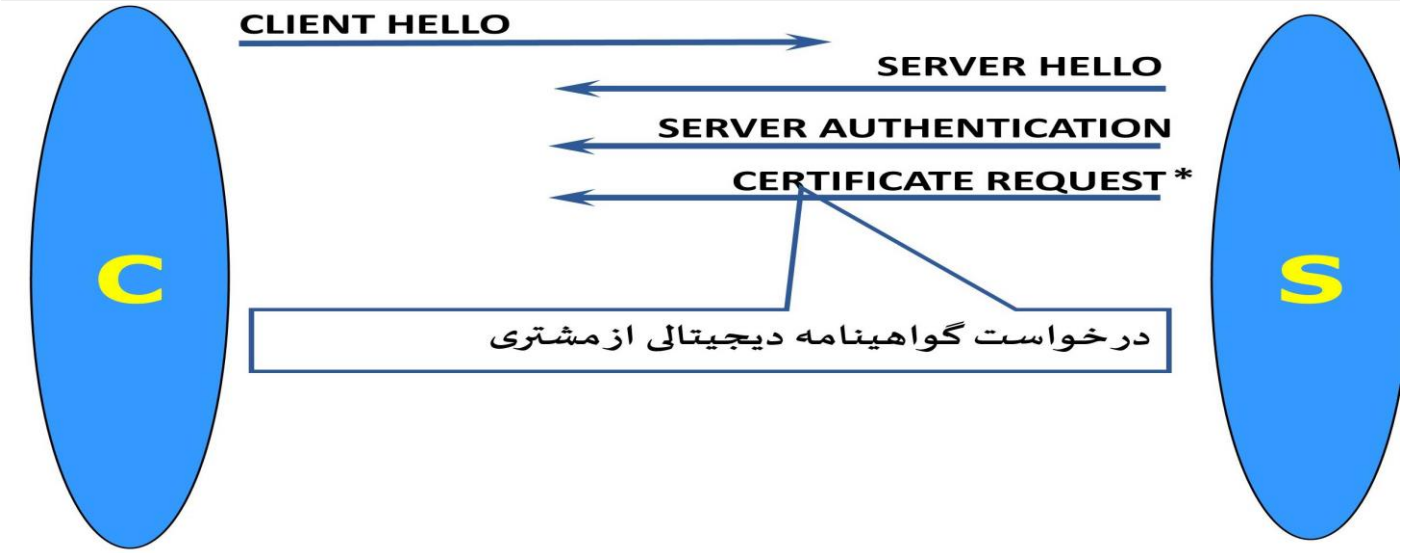
پروتکل دستداد

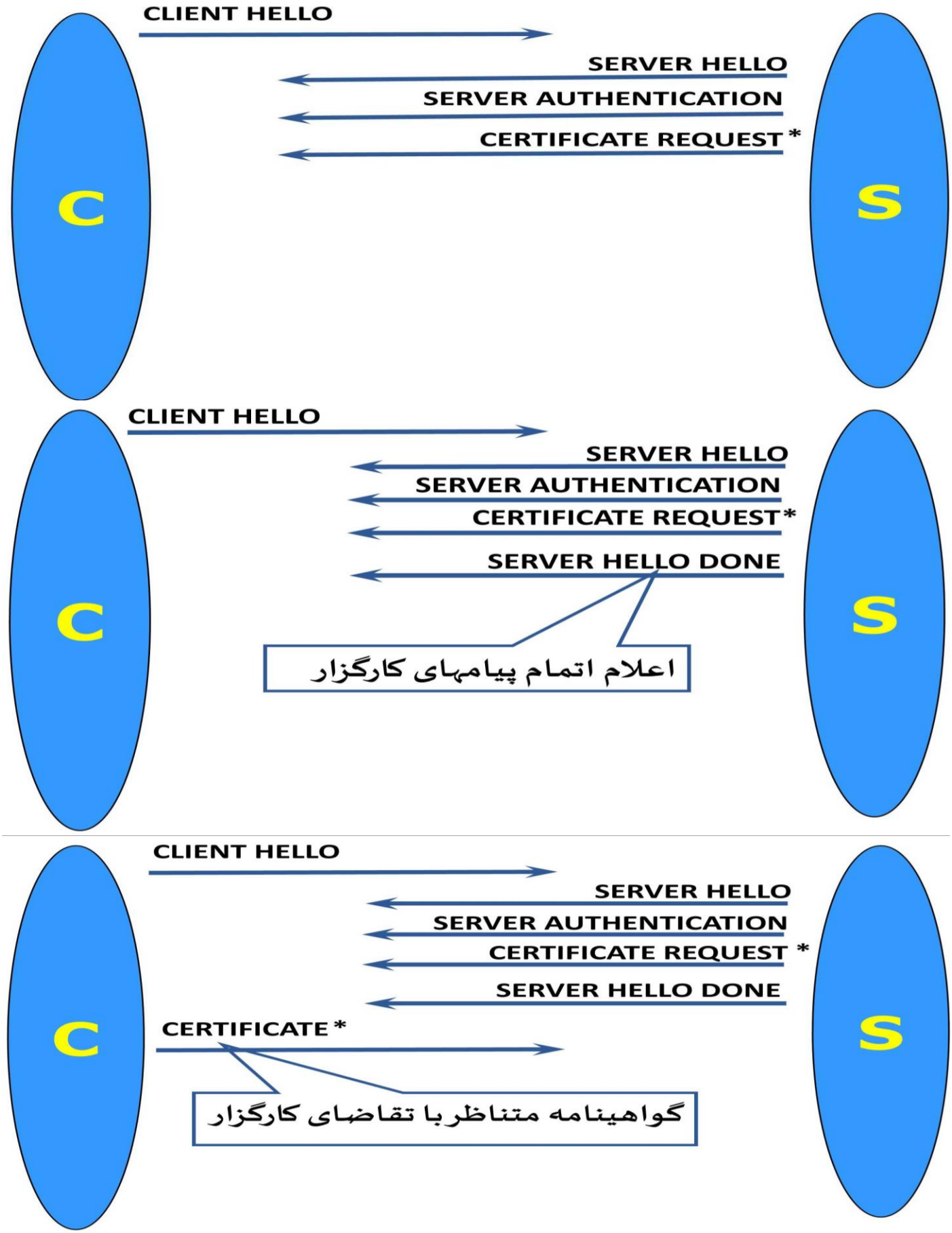
- توافق روی الگوریتمهای لازم برای جلسه
- تبادل پارامترهای رمزنگاری لازم برای توافق طرفین روی یک PRE-MASTER-SECRET
- مبادله گواهینامه به منظور احراز اصالت طرفین
- تولید پارامترهای امنیتی حالت معطل اتصال برای لایه ثبت
- ایجاد اطمینان از درستی محاسبات و مذاکرات

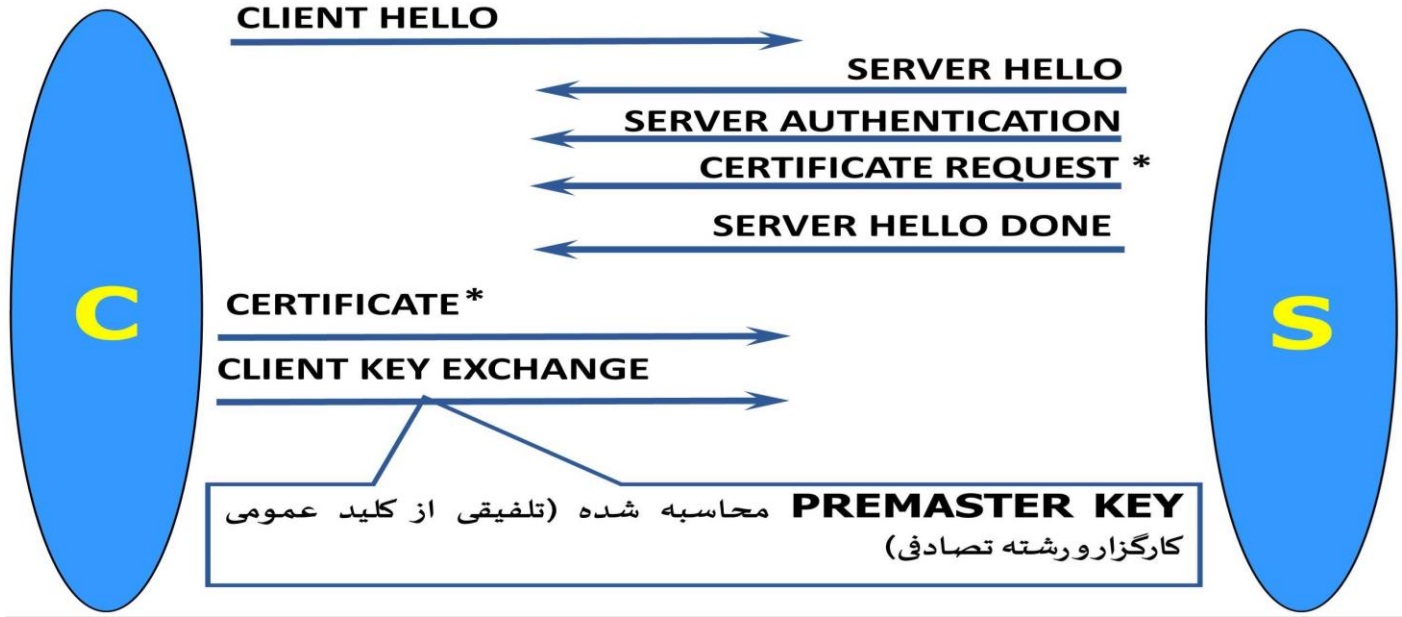
روند تبادل پیامها در یک دستداد کامل

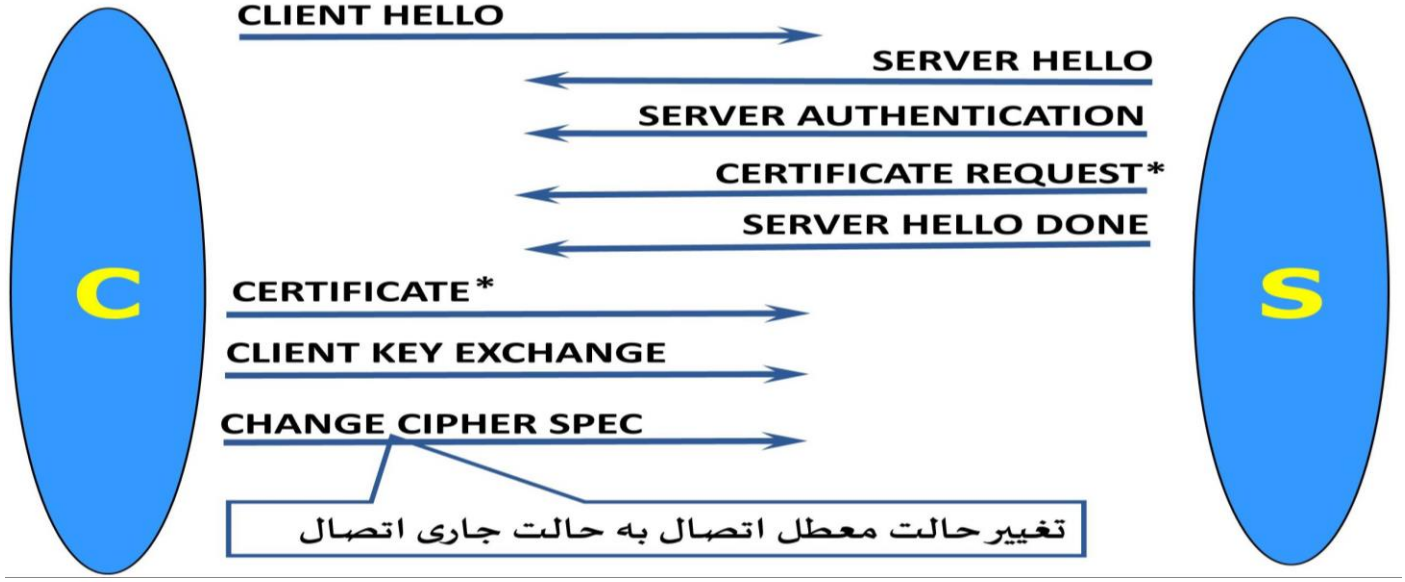

CLIENT HELLO
SERVER HELLO
C
S
نسخه انتخاب شده برای جلسه
عدد تصادفی ۳۲ بایتی کارگزار
شناسه جلسه
مجموعه پارامترهای رمز انتخاب شده برای جلسه
الگوریتم فشرده سازی انتخاب شده برای جلسه

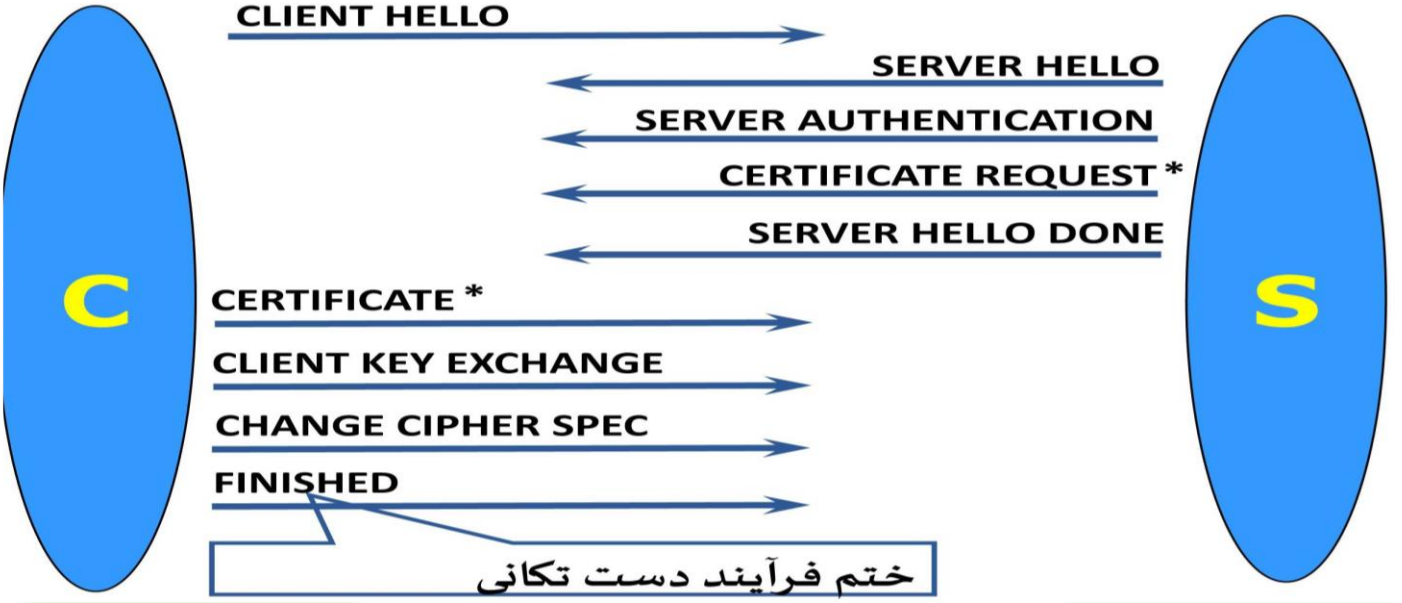

CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
C
S
گواهینامه مربوط به کارگزار
لیست مراکز صدور گواهینامه مربوط به کارگزار

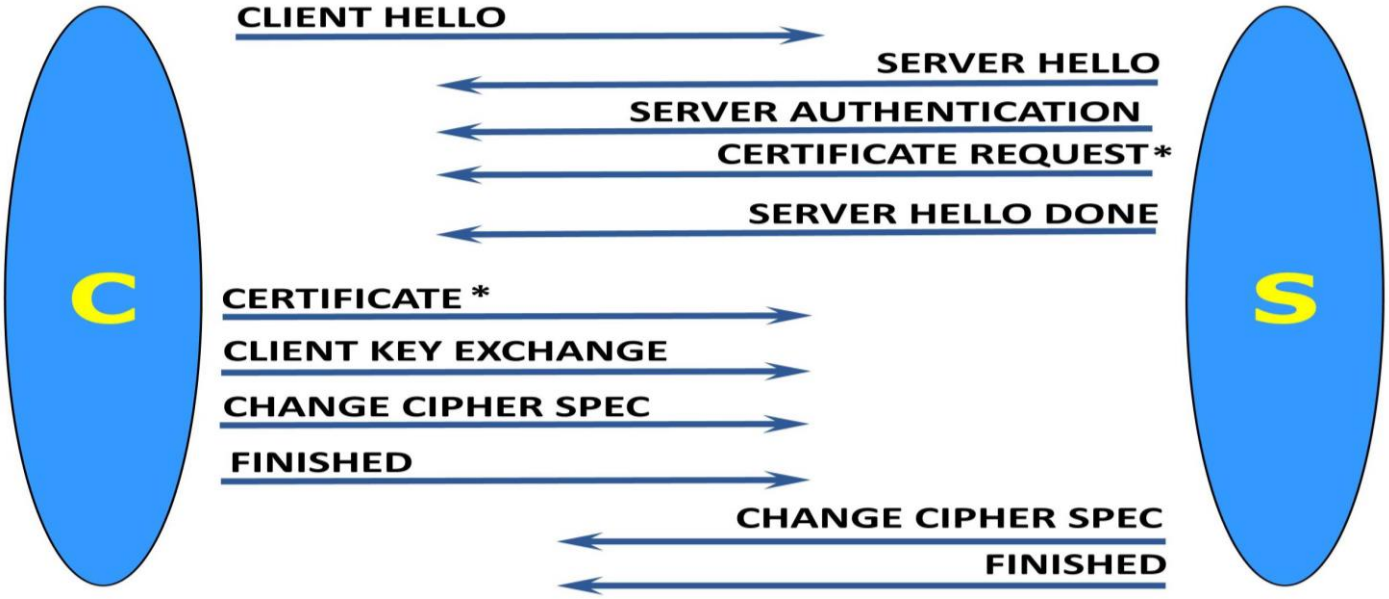

CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
CERTIFICATE REQUEST *
C
S
درخواست گواهینامه دیجیتالی از مشتری


CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
CERTIFICATE REQUEST *
C
S
CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
CERTIFICATE REQUEST*
SERVER HELLO DONE
C
S
اعلام اتمام پیامهای کارگزار
CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
CERTIFICATE REQUEST *
SERVER HELLO DONE
CERTIFICATE *
C
S
گواهینامه متناظربا تقاضای کارگزار


CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
CERTIFICATE REQUEST *
SERVER HELLO DONE
C
S
CERTIFICATE *
CLIENT KEY EXCHANGE
PREMASTER KEY محاسبه شده (تلفیقی از کلید عمومی
کارگزار و رشته تصادفی)


CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
CERTIFICATE REQUEST*
SERVER HELLO DONE
C
S
CERTIFICATE *
CLIENT KEY EXCHANGE
CHANGE CIPHER SPEC
تغییر حالت معطل اتصال به حالت جاری اتصال


CLIENT HELLO
SERVER HELLO
SERVER AUTHENTICATION
CERTIFICATE REQUEST *
SERVER HELLO DONE
C
S
CERTIFICATE *
CLIENT KEY EXCHANGE
CHANGE CIPHER SPEC
FINISHED
ختم فرآیند دست تکانی



ازسرگیری جلسه

- فرآیند تبادل کلید موجب کاهش سرعت برقراری جلسه است.

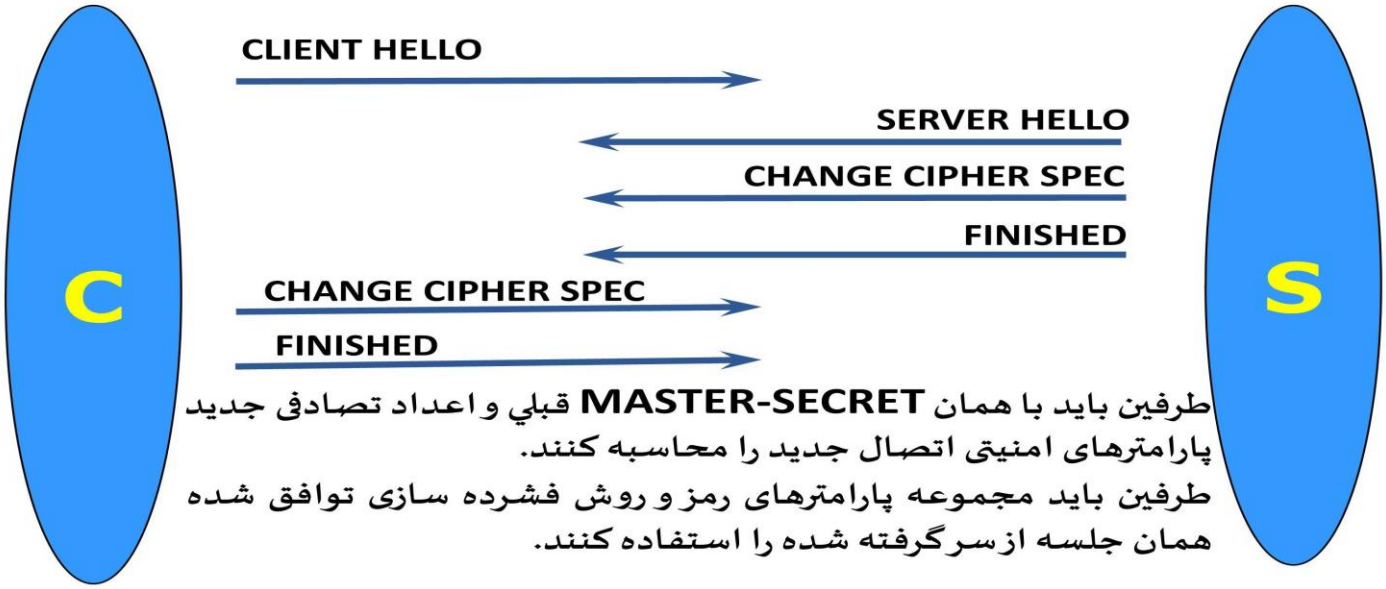
حذف فرآیند تبادل کلید

نگهداری MASTER-SECRET برای استفاده در اتصالات بعدی

- تفاوت اتصال و جلسه

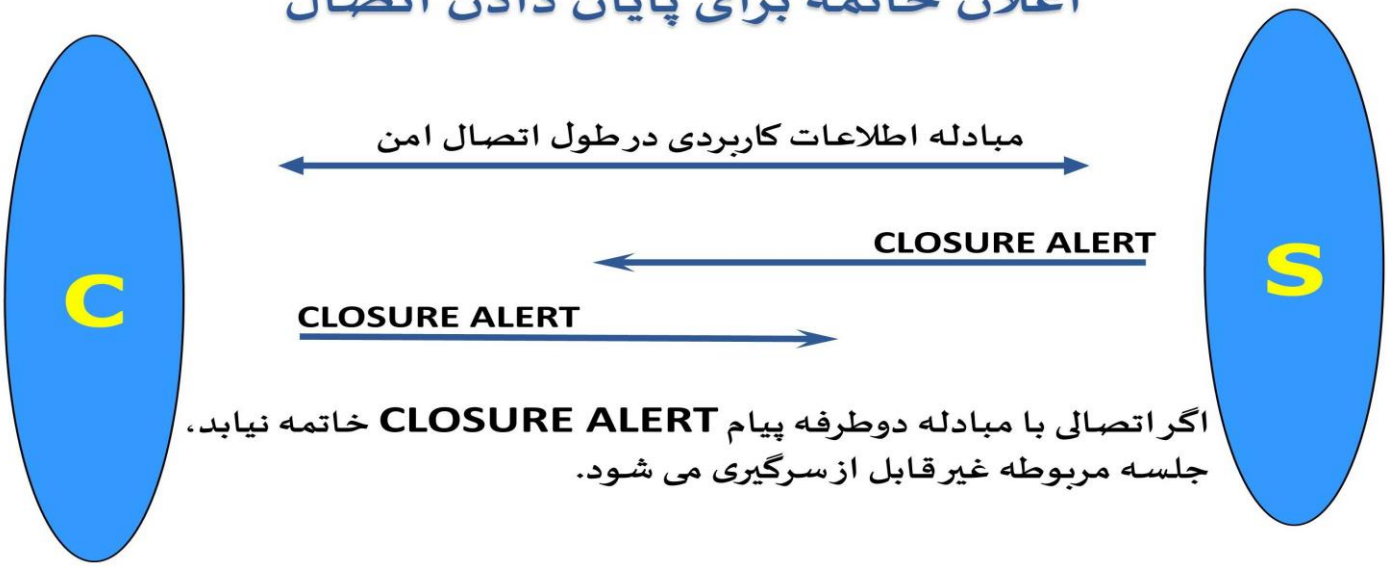
یک جلسه می تواند چندین اتصال را دربرداشته باشد.

روند تبادل پیام ها هنگام ازسرگیری جلسه



طرفین باید با همان MASTER-SECRET قبلي و اعداد تصادفی جدید پارامترهای امنیتی اتصال جدید را محاسبه کنند.
طرفین باید مجموعه پارامترهای رمز و روش فشرده سازی توافق شده همان جلسه ازسرگرفته شده را استفاده کنند.

اعلان خاتمه برای پایان دادن اتصال

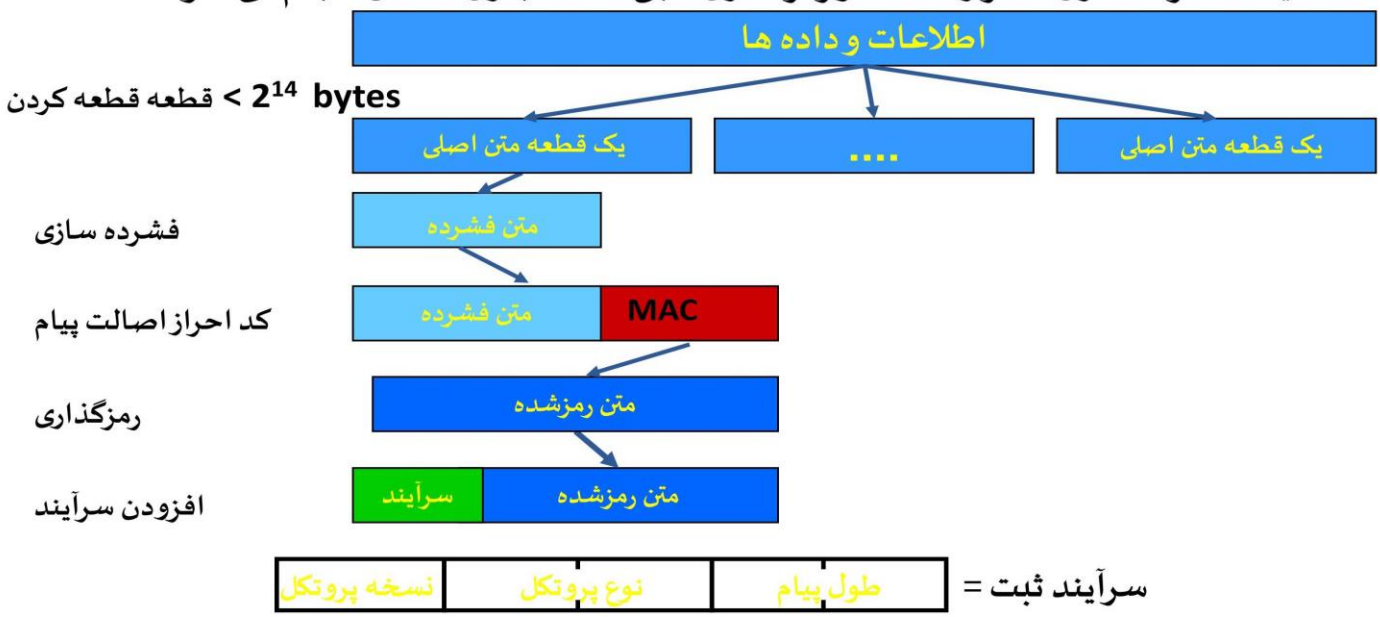


اگر اتصالی با مبادله دوطرفه پیام **CLOSURE ALERT** خاتمه نیابد، جلسه مربوطه غیرقابل از سرگیری می شود.

پروتکل ثبت

اطلاعات از چهار پروتکل لایه بالایی وارد لایه ثبت می شوند تا به شکل مناسب در آمده و به لایه انتقال فرستاده شوند.

عملیات فشرده سازی، احراز اصالت و رمزگذاری طبق حالت جاری اتصال انجام می شوند.



نحوه محاسبه کد احراز اصالت پیام (MAC)

MAC(data)=hash(secret_key + hash(secret_key+data+time_stamp))

ابتدا کلید سری به ابتدای داده و مهرزمان به انتهای داده ضمیمه شده و توسط الگوریتم درهم سازی که در ابتدا توافق کرده اند، چکیده آن استخراج می شود.نتیجه بدست آمده باردیگر به کلید سری ضمیمه شده و چکیده آن بدست می آید تا به عنوان کد احرازهویت درانتهای پیام درج شود.

پروتکل اعلان خطا

- پیام این پروتکل شامل دو بایت است.

شدت خطا

اگر خطا در حد هشدار باشد : مقدار بایت = ۱
در این حالت نشست می تواند ادامه یابد

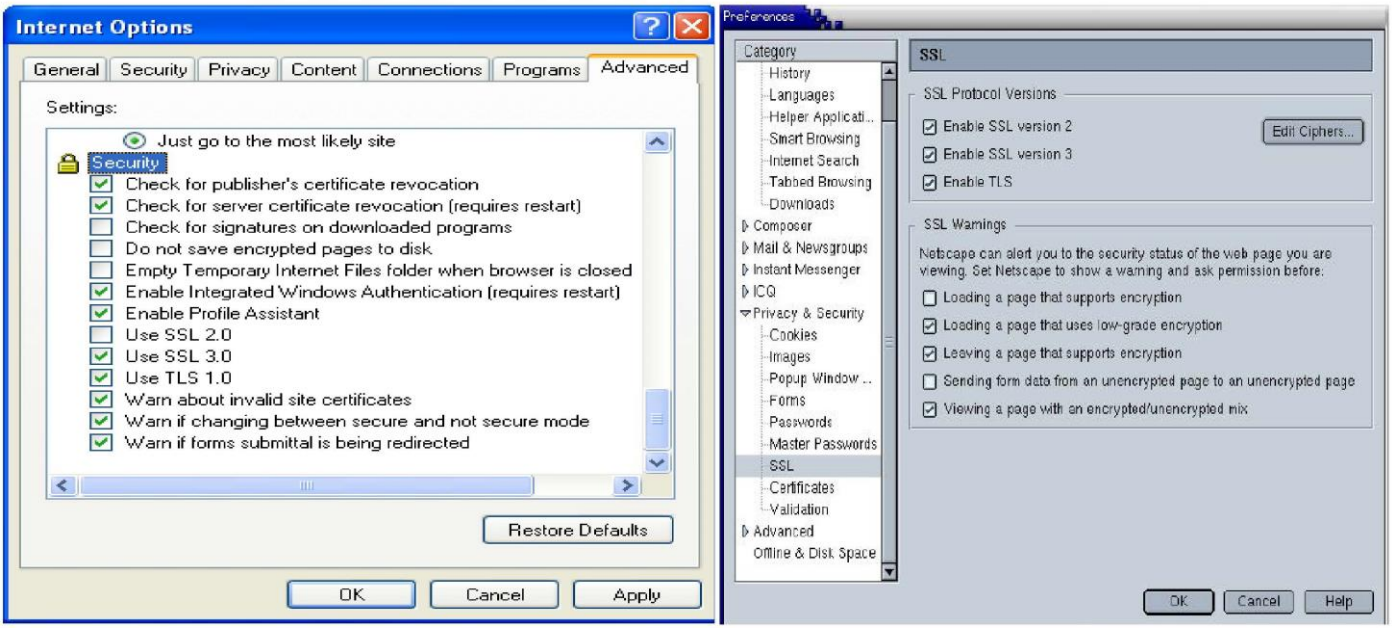
اگر خطا مهلک باشد: مقدار بایت = ۲
در این حالت نشست قطع خواهد شد

شرح خطا

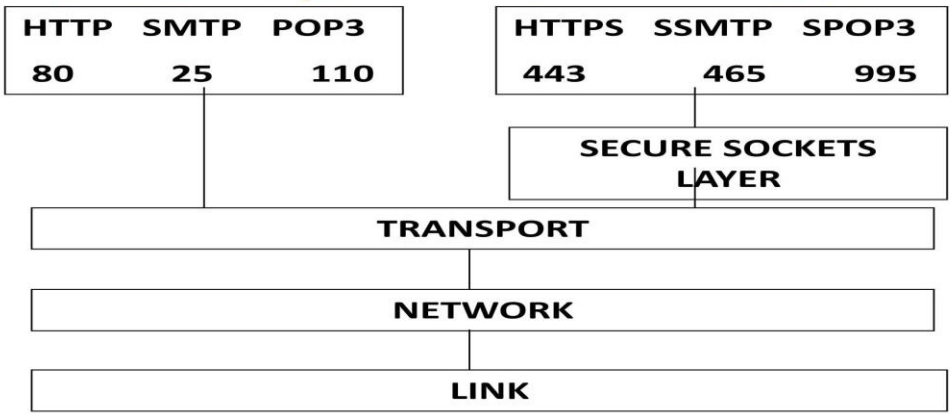
نمونه ای از خطاهای مهلک :دریافت پیام با کد نامعتبر **MAC** و دریافت قطعاتی از داده که به درستی از حالت فشرده خارج نمی شوند،عدم توافق بر سر پارامترهای امنیتی

نمونه هایی از خطاهای هشدار: عدم وجود گواهینامه،نامتبر بودن گواهینامه،و سایر پارامترهای مربوط به گواهینامه

نحوه فعال کردن استفاده از SSL در IE , NETSCAPE

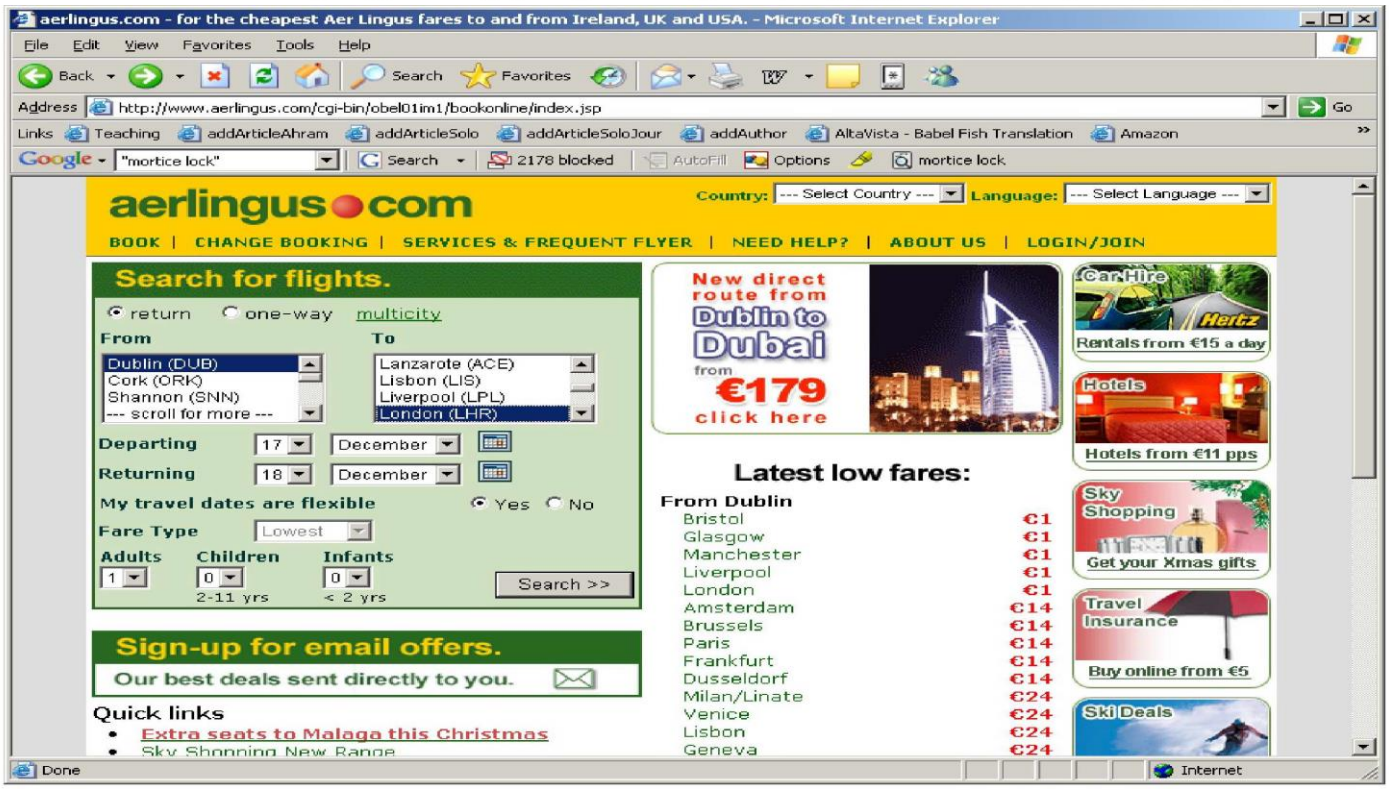


استفاده از پروتکل های لایه کاربرد بر روی SSL

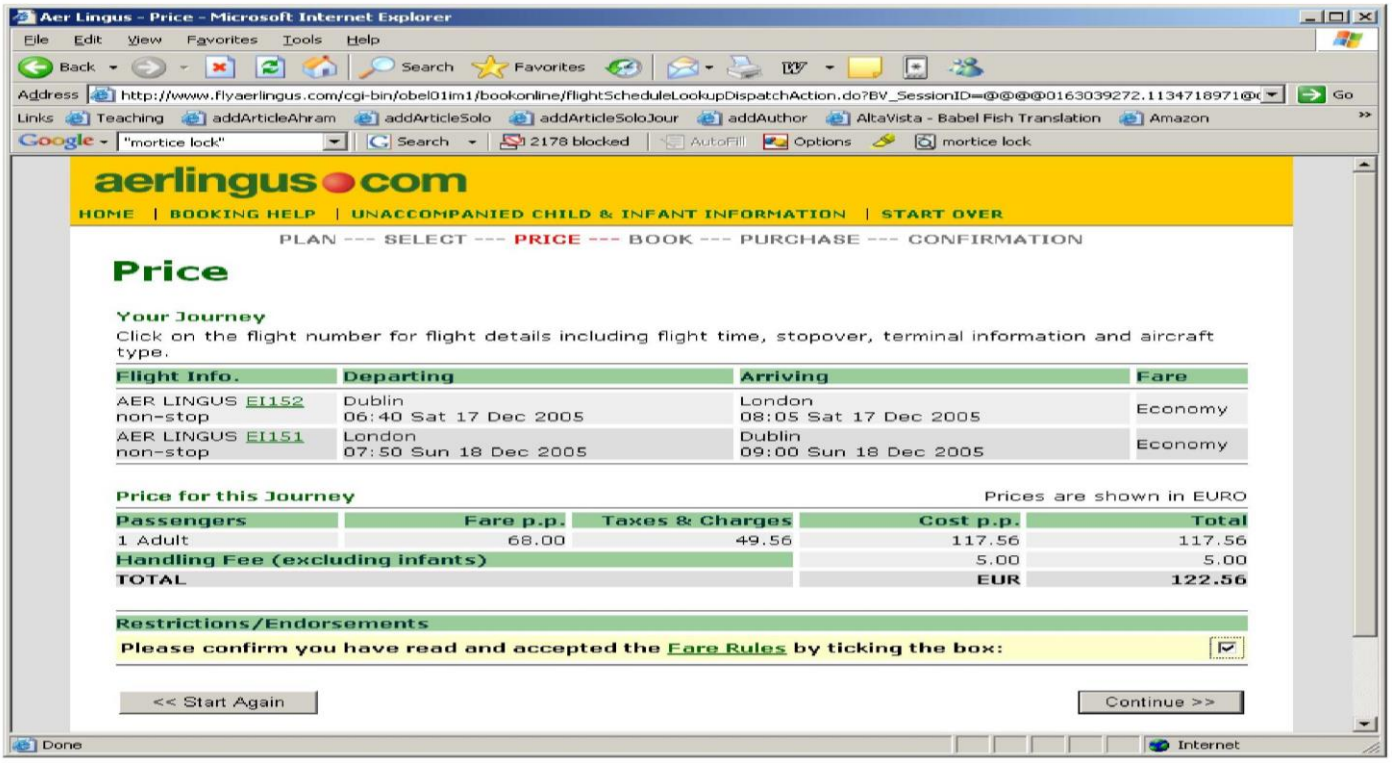


مثالی از بکارگیری SSL

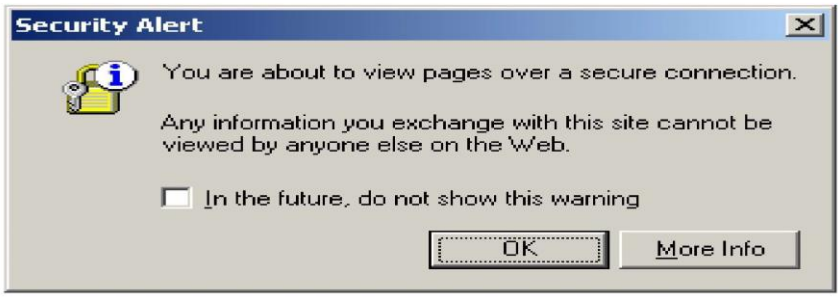
- خرید یک بلیط ازوب سایت شرکت هواپیمایی
- هنگام ورود به سایت اطلاعات پروازها به صورت عادی نمایش داده می شوند.



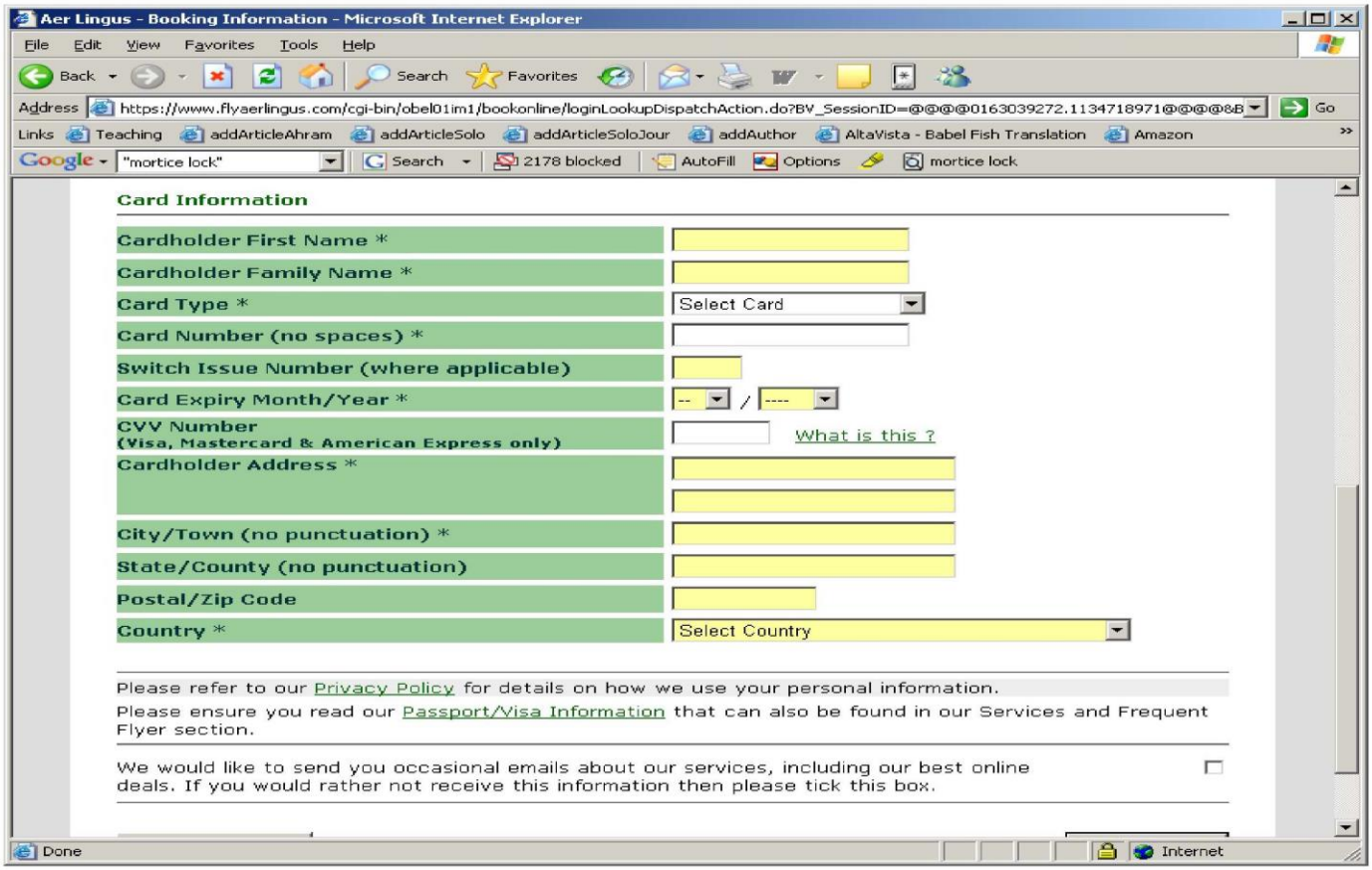
مشتری پروازها را مشاهده کرده و پرواز مورد نظر خود را انتخاب می کند



پیغام هشداری در مورد ادامه نشست با SSL در مرورگر مشتری ظاهر می شود



مشتری با تایید پیغام ادامه نشست را برروی پروتکل SSL ادامه می دهد.



HTTPS AND LOCK

هنگام تایید هشدارتوسط مشتری چه اتفاق می افتد

- شرکت هواپیمایی گواهینامه دیجیتال خود را برای مشتری ارسال می کند.
- مرورگر مشتری برای بررسی کلید عمومی شرکت هواپیمایی ، اعتبارگواهینامه دیجیتالی را ازطریق **CA** پیگیری می کند.
- پس ازموفقیت آمیزبودن مرحله قبل اطلاعات برروی **SSL** مبادله می شوند.

Transport Layer Security :TLS

- نسخه ای از**SSL** که درسال ۱۹۹۹ ارائه شده است (نسخه ۳,۱)
- درموارد زیربا **SSL** تفاوت دارد :
  - درصورت ارائه نشدن گواهینامه ، نشست خاتمه می یابد.
  - روش تولید رشته تصادفی **(NONCE)** تغییرکرده است.
  - روش تولید کد احرازهویت و اصالت پیام تغییرکرده است.
  - روش های رمزنگاری جدیدی به آن اضافه شده است.

معایب SSL

- نیازبه پهنای باند بیشتر
- کند بودن
- نیازبه استفاده ازپورت اختصاصی ۴۴۳ برای **HTTPS**
- عدم پشتیبانی از**UDP**
- پیچیدگی زیاد برای داده های جویباری و **VOIP**

SET SECURE ELECTRONIC TRANSACTION
تراکنش های الکترونیکی آمن

تعریف تجارت الکترونیک:

- تعامل سیستمهاي ارتباطی (COMMUNICATION) ، سیستمهای مدیریت اطلاعات (DATA MANAGEMENT)و امنیت (SECURITY) که به واسطه آنها امکان مبادله اطلاعات تجاری در رابطه با فروش محصولات و یا خدمات میسر می گردد.
- بنابراین تعریف اجزاء اصلی تجارت الکترونیک عبارتند از:

-1سیستمهای ارتباطی(COMMUNICATIONS)

-2سیستمهای مدیریت داده ها(DATA MANAGEMENT)

-3امنیت(SECURITY)

ابزارها در تجارت الکترونیکي

- ایمیل
- فروشگاه اینترنتی
- ابزار پیام سریع
- پول الکترونیکی

هفت اصل در نیازمندی تجاری

۱. اعتماد سازی اطلاعات مربوط به پرداخت و سفارش.

۲. تضمین یکپارچگی داده های در حال انتقال.

۳. اعتبار بخشیدن به این که خریدار یک کاربر قانونی شرکت کارت پرداخت است.

۴. اعتبار بخشیدن به این که فروشنده می تواند با موسسه مالی ارتباط و تراکنش داشته باشد

۵. ایجاد بالاترین امنیت در تراکنش ها و محافظت فنی از تمام کاربران.

۶. ایجاد پروتکلی مستقل از ساز و کار امنیتی انتقال .

۷. تسهیل و تشویق قابلیت همکاری نرم افزار و سرور در شبکه.

اهداف

۱. اعتبار بخشی به خریدار (cardholder)، فروشنده(merchant)، دریافت کننده (acquirer
۲. فراهم کردن اعتماد داده های پرداختی (اطلاعات امن می باشد و در اختیار سایرین قرار نمی گیرد. جلوگیری از استراق سمع)
۳. محافظت از یکپارچگی داده های پرداخت (عدم تغییر در هنگام عبور از مبداء به مقصد)
۴. تعریف الگوریتم ها و پروتکل های لازم جهت سرویس های امنیتی
۵. قابلیت تعامل (می بایست برنامه با تمام پلتفرم ها و نرم افزار ها قابلیت تعامل داشته باشد.)

روند خرید اینترنتی

۱. خریدار کالاهای مختلف را مشاهده می کند.
   - استفاده از مرورگر و مشاهده کاتالوگ آنلاین

   بعد از سفارش توسط خریدار، سرور وب فروشنده یک فرم بازبینی سفارش جهت تایید فروشنده به وی ارسال می کند. بعد از تایید وی پروتکل SET با خریدار اجازه می دهد تا پرداخت را انجام دهد. سپس به فروشنده می گوید که پرداخت انجام شده است.
   - مشاهده کاتالوگ عرضه شده توسط فروشنده روی سی دی

   به دلیل استفاده از پنهای باند بالا،گرافیک پایین وکاهش رزولوشن در روش قبل این روش به وجود آمده است. پس از سفارش خریدار یک پیام الکترونیکی با استفاده از پروتکل SET سفارش و دستور العمل پرداخت را به فروشنده ارسال می کند.
   - جستجو در کاتالوگ های کاغذی
۲. کالای مورد نظر را انتخاب می کند.
۳. مشاهده فرم سفارش توسط خریدار شامل مواردی چون لیست کالاهای انتخاب شده، قیمت آن ها، مالیات و هزینه جابجایی. این لیست یا توسط سرور فروشنده و به صورت آنلاین ساخته شده است و یا توسط نرم افزار در کامپیوتر خریدار تولید می شود.
۴. انتخاب نحوه پرداخت توسط خریدار.
۵. ارسال سفارش و نحوه پرداخت به فروشنده.
۶. درخواست تصدیق از موسسه مالی خریدار توسط فروشنده.
۷. تایید سفارش توسط فروشنده.
۸. ارسال کالا و یا انجام سفارش توسط فروشنده.
۹. درخواست مبلغ مورد نظر از موسسه مالی خریدار توسط فروشنده.

تعريفي از پروتكل SET

- یک مجموعه از پروتکل های امنیتی است که کاربران را قادر می سازد تا زیربنای پرداخت کارت اعتباری موجودشان را در یک شبکه باز مثل اینترنت به صورت امن به کار برند. SET با استفاده از رمز نگاری، پیام و اطلاعات رد و بدل شده مابین کاربران و سرور را رمز می نماید و به نحوی که حتی اگر مهاجم به اطلاعات رمز شده دسترسی نیز پیدا کند به هیچ وجه قادر به استخراج اطلاعات از پیام رمز شده نباشد.

مزایای استفاده از پروتکل SET

- پروتکل SET دارای سه مزیت می باشد که عبارتند از:
- محرمانگی، این کار توسط رمز نگاری صورت پذیرفته، که خواندن پیام ها را توسط بیگانگان غیرممکن می کند.
- درستی، بوسیله چکیده پیام و تایید امضا اطمینان می دهند پیام ها بدون تغییر رد وبدل می شوند.
- تایید بوسیله گواهی امضاء دیجیتال،که اطمینان می دهد ادعاهایی که افراد طرف معامله دارند قابل اثبات و اعمال انها غیرقابل انکار است.

سرویس های SET

- سرویس های SET شامل سه سرویس است:
- ۱-فراهم کردن کانال مخابراتی امن در بین تمام طرفین درگیر در یک تعامل
- ۲-فراهم کردن اعتماد با استفاده از گواهینامه های دیجیتالی X.509V3
- ۳-تضمین حریم، بخاطر اینکه اطلاعات تنها بین طرفین یک تعامل در هر زمان و در هر مکانی که لازم باشددر دسترس باشد.

تعریف آیتم های مختلف در SET

تعاملات در شراکت interaction of participants

در تراکنش های set روند خرید اینترنتی به وسیله خریدار شروع می شود.

خریدار Cardholder

خریدار از کارت پرداخت که توسط صادر کننده، صادر گردیده، جهت خرید استفاده می کند.

فروشنده Merchant

فروشنده طرف مقابل خریدار است که یا کالایی را می فروشد و یا سرویسی را انجام می دهد.

صادر کننده Issuer

یک موسسه مالی است که برای خریدار یک حساب باز کرده و به او یک کارت پرداخت می دهد.

دریافت کننده Acquirer

یک موسسه مالی است که برای فروشنده یک حساب باز کرده و پرداخت ها را در آن دریافت می کند.

تعاملات در شراکت interaction of participants

در تراکنش های set روند خرید اینترنتی به وسیله خریدار شروع می شود.

خریدار Cardholder

خریدار از کارت پرداخت که توسط صادر کننده، صادر گردیده، جهت خرید استفاده می کند.

فروشنده Merchant

فروشنده طرف مقابل خریدار است که یا کالایی را می فروشد و یا سرویسی را انجام می دهد.

مدخل پرداخت Payment gateway

یک دستگاه است که پیام های فروشنده شامل دستور العمل پرداخت از سمت خریدار را پردازش می کند و از گیرنده و یا نفر سومی دستور می گیرد.

عنوان تجاری Brand

موسسه های مالی آن را به وجود می آورند و با تبلیغ و تصویب قوانینی برای استفاده و پذیرش کارت های پرداخت، از آن جهت ارائه و خدمات کارت های پرداخت استفاده می کنند.

طرف سوم third parties

گاهی صادر کننده ها و دریافت کننده ها پردازش تراکنش ها را به پردازشگر سومی واگذار می کنند.

رمزنگاری

الف) متقارن symmetric

در این روش همان کلیدی که برنامه را رمز نگاری می کند، رمز گشایی هم می کند. سرعت آن بالاست. امنیت آن پایین است. الگوریتم رمز نگاری آن DES می باشد که مخفف Data Encryption Standard است. که توسط موسسه های مالی برای رمز نگاری شناسه هویت شخصی یا همان PIN که مخفف Personal Identification Numbers است، استفاده می گردد.

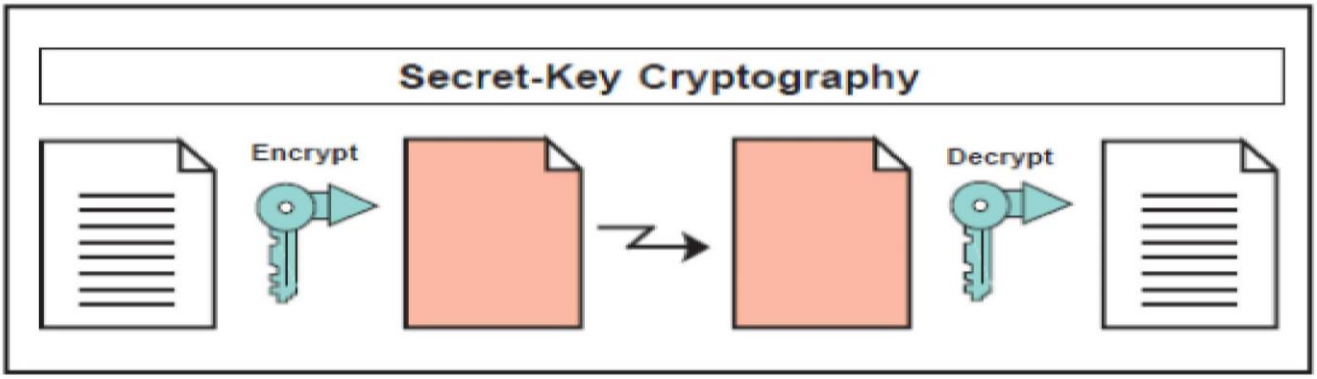


Figure 1: Secret-Key Cryptography

ب) رمزنگاری با کلید عمومی

در این روش کاربر از یک کلید عمومی public key و یک کلید خصوصی private key استفاده می کند. داده ای که با یک کلید قفل شود، به صورت انحصاری با آن یکی قابل باز شدن است. بنابراین وقتی پیغامی با کلید عمومی یک نفر باز شود، می توان مطمئن بود که داده از طرف او فرستاده شده است. همچنین اگر داده ای را با کلید عمومی یک فرد قفل کنیم، تنها فرد مقابل می تواند آن را باز کند. بهترین الگوریتم شناخته شده در این روش RSA است که مخفف اسم سه نفر می باشد. Rivest, Shamir, Adleman. کاربر تحت هیچ شرایطی کلید خصوصی اش را به کسی نمی دهد.

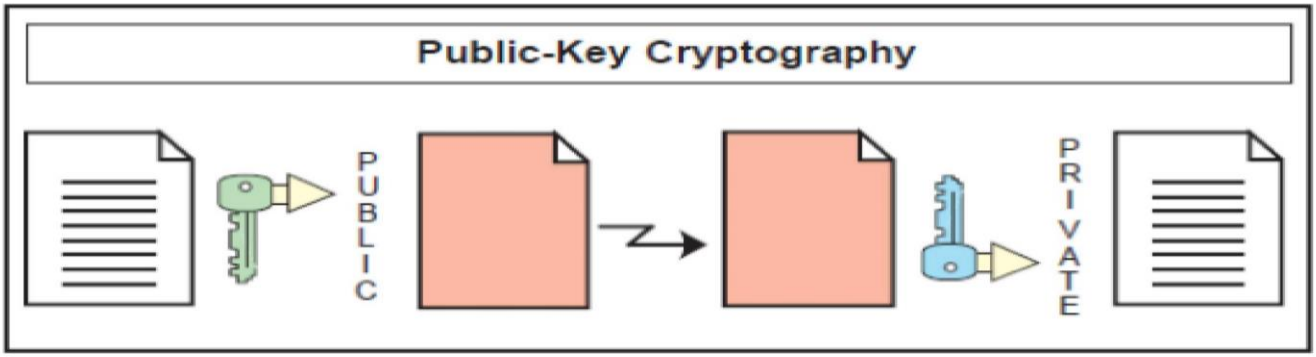


Figure 2: Public-Key Cryptography

چکیده پیام DIGEST MESSAGE:

چکیده پیام، مقدار منحصر به فرد است که از خود پیام تولید می شود. الگوریتم استفاده شده در SET به صورت یکطرفه می باشد که دارای چکیده پیامی به طول ۱۶۰ بیت می باشد. به وسیله این الگوریتم به واسطه جابجایی تنها یک بیت در پیام اصلی، به طور میانگین نصف بیت ها در چکیده پیام تغییر خواهند کرد. به ندرت پیش می آید که دو پیام مختلف دارای چکیده پیام شبیه هم باشند و همیشه با هم متفاوت اند.

امضای دیجیتال DIGITAL SIGNATURE:

تنها جهت اعتبار سنجی و یکپارچگی مورد استفاده قرار می گیرد.

کاربر چکیده پیام را تولید می کند و آن را با کلید خصوصی خود رمز می کند. سپس به گیرنده ارسال می کند. گیرنده چکیده پیام را با کلید عمومی فرستنده باز می کند، از طرفی خودش نیز چکیده پیام را محاسبه می کند. گیرنده چکیده پیام بدست آمده را با آن که فرستنده ارسال کرده، چک می کند. اگر یکی بود یعنی اینکه پیام در بین راه تغییر نکرده است.

گواهی نامهCERTIFICATE:

نحوه ساخت:

۱. چکیده پیام تولید می شود.
۲. چکیده به وسیله کلید خصوصی فرستنده رمز می شود که نتیجه آن امضای دیجیتال است.
۳. اصل پیام، امضای دیجیتال و گواهی نامه فرستنده (جهت اطمینان و بدست آوردن کلید عمومی فرستنده) به وسیله یک کلید متقارن که با الگوریتم تصادفی ایجاد شده است، رمز می شود. نتیجه آن پیام رمز شده یا Encrypted Message می باشد.
۴. کلید متقارن تصادفی به وسیله کلید عمومی گیرنده که از گواهی نامه وی بدست آمده رمز می شود. نتیجه آن نامه دیجیتال یا Digital Envelope می باشد.
۵. پیام خروجی شامل نامه دیجیتال و پیام رمز شده است که به گیرنده ارسال می شود.

نحوه باز کردن:

۱. گیرنده، نامه دیجیتال را به منظور بدست آوردن کلید متقارن تصادفی با استفاده از کلید خصوصی خود رمزگشایی می کند.
۲. پیام رمز شده به وسیله کلید متقارن که از مرحله قبل به دست آمد، رمز گشایی می شود.
۳. گیرنده امضای دیجیتال را به وسیله کلید عمومی فرستنده (که در گواهی نامه وی در پیام رمز شده موجود است را) به منظور به دست آوردن چکیده پیام رمز گشایی می کند.

۴. از طرفی خود نیز چکیده پیام را بدست آورده و آن را با خروجی مرحله ۳ مقایسه می کند. در صورتی که یکسان بود یعنی پیام را به دست آورده است.

دلیل استفاده از کلید متقارن سرعت بالاست.

در این روش محتوای پیام نیز از دید سایرین در امان می ماند.

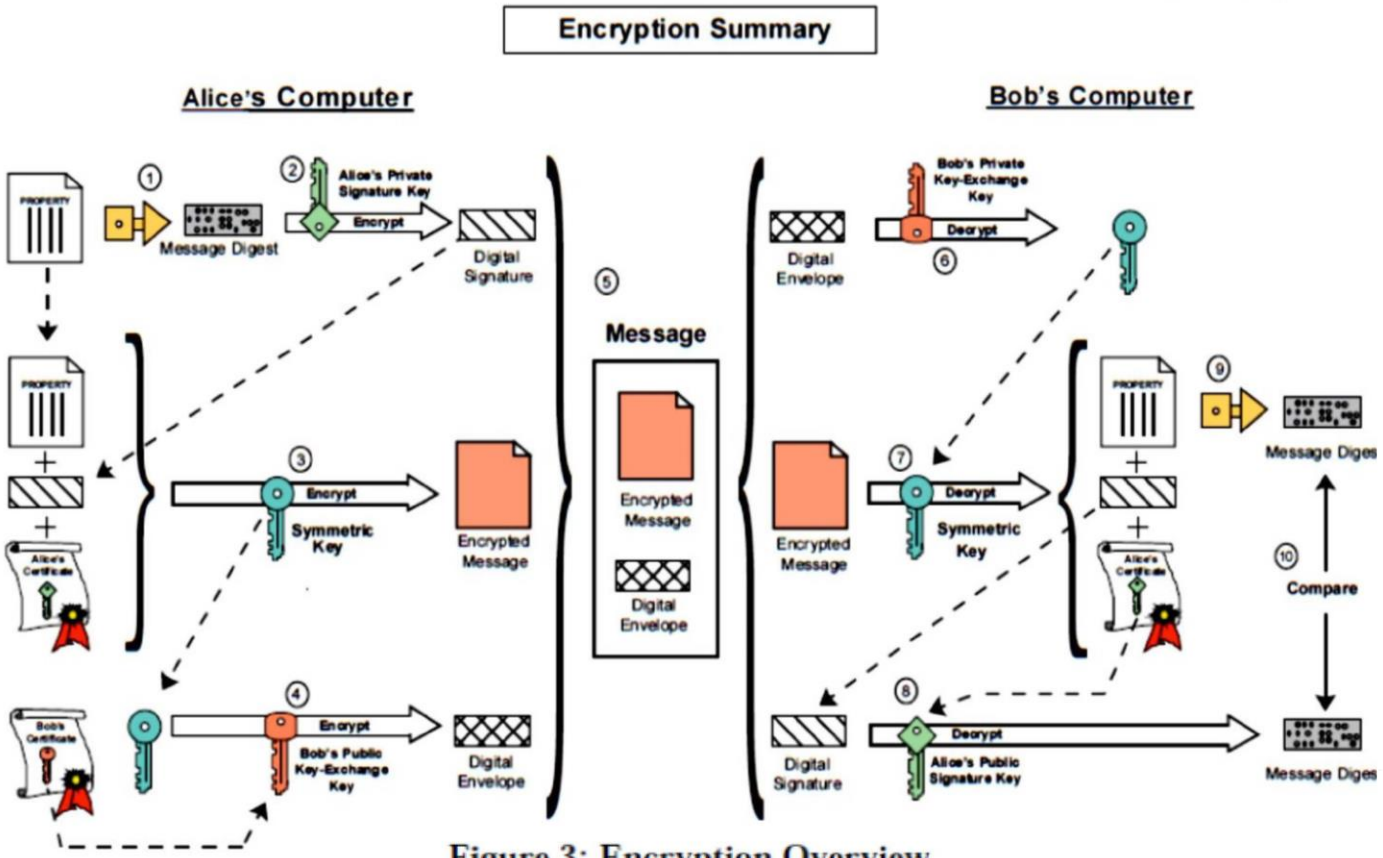


Figure 3: Encryption Overview

امضای دوگانه

وقتی باب از آلیس خرید می کند، می خواهد در صورت قبول سفارش باب توسط آلیس ، بانک پول را به حساب آلیس انتقال دهد. اما نه می خواهد که بانک از محتوای خرید با خبر شود و نه آلیس اطلاعات حساب باب را ببیند. باب تمام این کارها را با امضای دیجیتال هر دو پیام اما تنها با یک امضا انجام می دهد. این عملکرد باعث به وجود آمدن مفهوم امضای دوگانه می شود.

ساخت امضای دوگانه:

۱. محاسبه چکیده هر دو پیام به صورت جداگانه
۲. الحاق آن دو به یکدیگر
۳. محاسبه چکیده پیام جدید
۴. رمز نگاری این چکیده پیام با کلید خصوصی خریدار

آلیس درخواست باب را قبول می کند. سپس به بانک اعلام کرده و یک چکیده از پیام تقاضای باب را به بانک ارسال می کند. بانک بررسی می کند که پذیرش آلیس واقعاً برای درخواست باب بوده یا خیر. این کار توسط مقایسه چکیده پیام ارائه شده توسط آلیس و چکیده پیام باب در امضای دوگانه صورت می گیرد. او به صحت تقاضا در امضای دوگانه پی می برد در حالی که محتویات تقاضا را نمی بیند.

قوانین استفاده از کلید عمومی

این قوانین توسط دولت ها تصویب شده است:

- داده های رمز شده صرفا دارای ماهیت مالی باشند.
- محتویات به خوبی مشخص شده باشند.
- طول داده ها محدود باشند.
- رمزنگاری به آسانی جهت استفاده در سایر اهداف ممکن نباشد.

صدور گواهی نامه

گواهینامه خریدار: گواهینامه وی شامل شماره حساب و تاریخ انقضا نمی شود در عوض شامل اطلاعات حساب و مقدار راز است که تنها توسط نرم افزار خریدار که به وسیله یک الگوریتم یک طرفه هش کد شده است قابل شناخت است. با مشخص شدن شماره حساب، تاریخ انقضا و مقدار راز می توان به گواهی نامه رسید اما برعکس آن امکان پذیر نیست. در SET خریدار اطلاعات حساب و مقدار راز را در مدخل ورود وارد می نماید.

گواهینامه فروشنده: مشخص می کند که فروشنده با موسسه اعتباری در ارتباط بوده و می تواند کارت پرداخت مربوط به آن شرکت را قبول کند. این گواهینامه توسط موسسه اعتباری دریافت کننده تایید شده و تصدیق می کند که فروشنده با آن ها توافق تجاری دارد. یک فروشنده جهت کار در محیط SET می بایست حداقل یک جفت از این گواهی نامه ها را داشته باشد. هر فروشنده برای ارتباط با هر شرکت کارت پرداخت به دوتا از این گواهی نامه ها نیاز دارد.

گواهی نامه مدخل پرداخت: گواهی نامه مدخل پرداخت به وسیله دریافت کننده یا پردازنده آن ها برای سیستم هایی که پردازش تجویز و پیام ثبت شده را انجام می دهند، بدست می آید. گواهی نامه مدخل پرداخت توسط شرکت پرداخت برای دریافت کننده ها صادر می شود.

گواهی نامه دریافت کننده: می بایست دارای منبعی باشد که بتواند گواهی نامه هایی که به صورت مستقیم توسط خریدار درخواست می شود را قبول و پردازش کند. آن ها ترجیح می دهند که دارای علائم تجاری جهت انجام درخواست گواهی نامه ها باشند. چرا که به این صورت به دلیل عدم پردازش پیام SET نیازی به گواهی نامه ندارند.

گواهی نامه صادر کننده ها: دقیقاً مشابه دریافت کننده هاست.

سلسله مراتب اعتمادسازی

گواهی نامه های SET توسط یک سلسله مراتب اعتماد به ثبت می رسد. هر گواهی نامه به نهادی که آن را امضا کرده، لینک می شود و در صورت تایید به سمت بالا حرکت می کند. در انتها می بایست به ریشه یا همان root رسید.

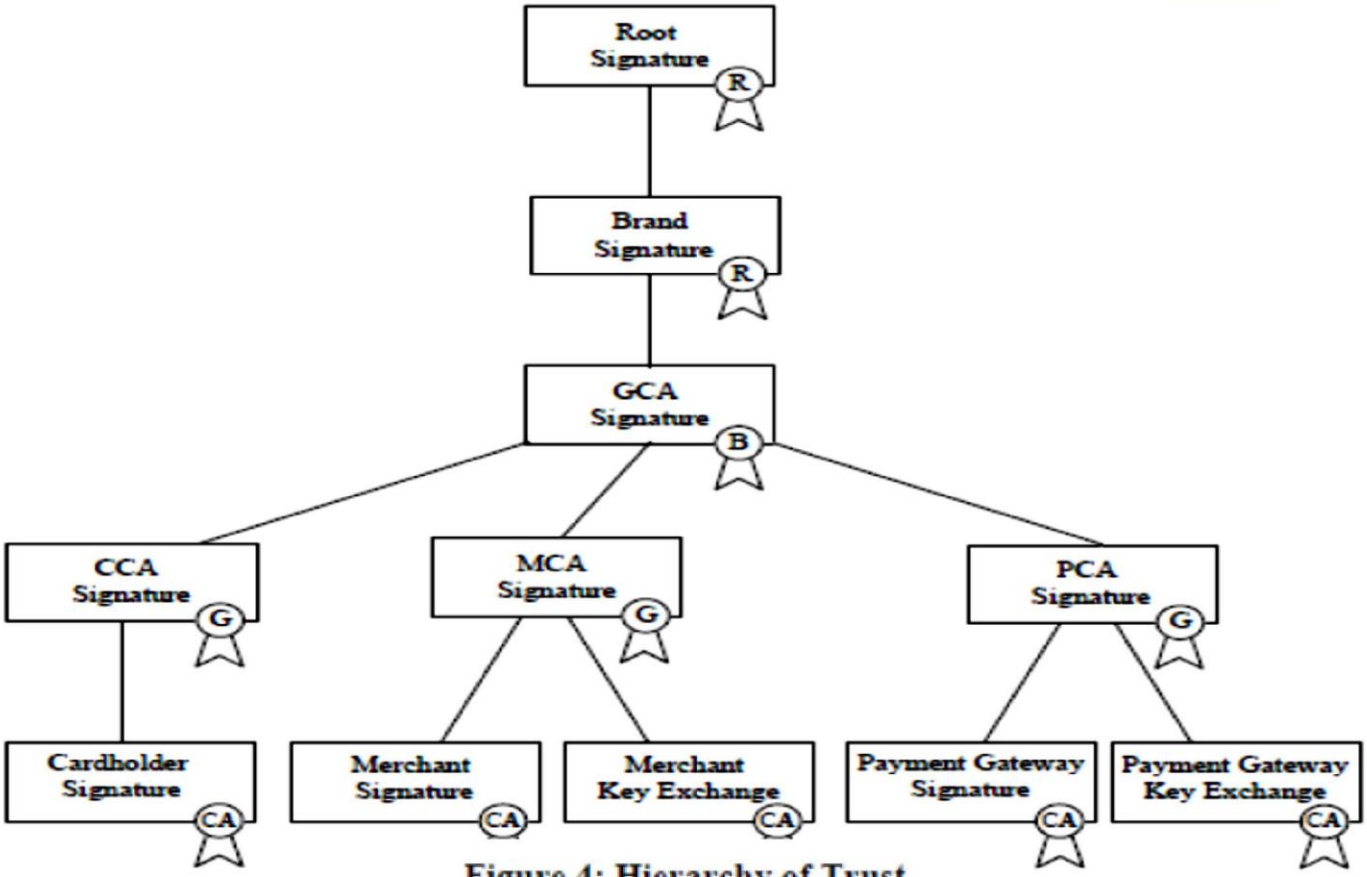


Figure 4: Hierarchy of Trust

کلید ریشه

کلید ریشه در گواهینامه امضا شده توسط وی موجود است. برنامه ها با ارسال یک درخواست اولیه به منبع، به گواهی نامه ای که شامل هش گواهینامه ریشه می شود، می گوید، من آن را دارم. در این روش در صورتی که برنامه گواهینامه آن را نداشت مرجع گواهینامه، به او یک درخواست ارسال می کند. اما به طور کلی در تمام سخت افزار ها و نرم افزار ها به صورت پیش فرض کلید عمومی ریشه وجود دارد.

تعویض کلید ریشه

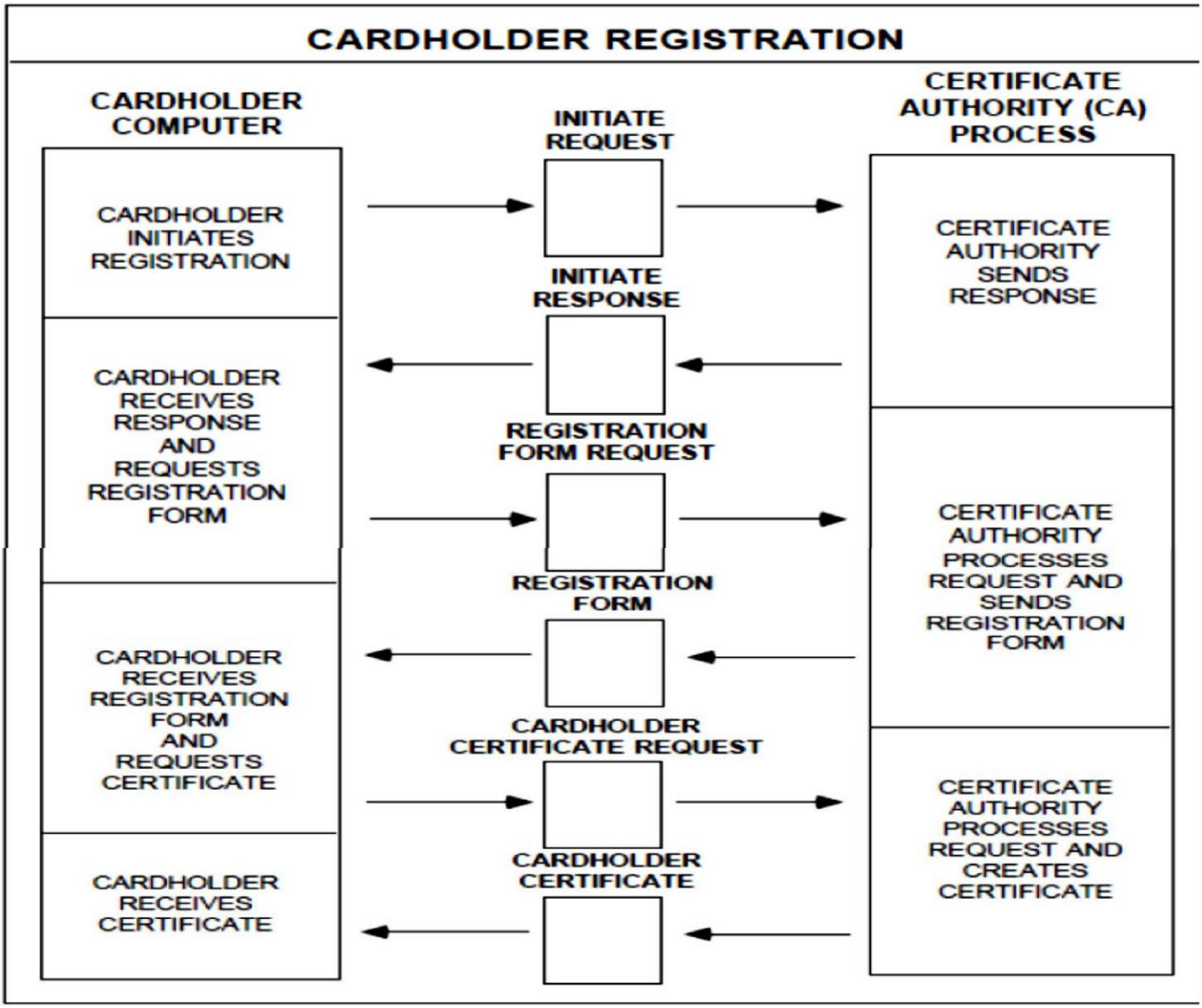
زمانی که کلید ریشه تولید می شود، جایگزین آن نیز تولید می شود. کلید جایگزین تا زمانی که به آن احتیاج نباشد، در جای امنی نگهداری می شود.

گواهی نامه ریشه امضا شده توسط آن و هش کلید جایگزین، با همدیگر توزیع می شوند. برنامه اخطار جایگزینی را همراه پیامی شامل گواهی امضا شده توسط ریشه جایگزین شده و هش کلید جایگزین بعدی می دهد و ...

روند پرداخت

شامل پنج مرحله ثبت نام خریدار، ثبت نام فروشنده، درخواست خرید، اجازه پرداخت و ثبت پرداخت.

ثبت نام خریدار



۱. نرم افزار خریدار درخواست شروع را به CA یا همان مرجع گواهینامه ارسال می کند.

۲. دریافت درخواست شروع.

۳. تولید پاسخ و امضای دیجتیال آن به وسیله چکیده پیام پاسخ و رمز کردن آن به وسیله کلید خصوصی CA.

۴. CAپاسخ را همراه گواهینامه اش به خریدار ارسال می کند.

۵. نرم افزار خریدار پاسخ شروع را دریافت می کند و صحت گواهینامه را با توجه به پیمایش زنجیره اعتماد یا همان trust chain تا ریشه بررسی می کند.

۶. نرم افزار خریدار، صحت امضای CA را با رمز گشایی آن با استفاده از کلید عمومی CA و مقایسه آن با نتیجه بدست آمده از چکیده پیام مشخص می کند.

۷. خریدار شماره حساب را وارد می کند.

۸. نرم افزار خریدار درخواست فرم ثبت نام را ایجاد می کند.

۹. نرم افزار خریدار، پیام را با استفاده از کلید متقارن شماره یک که به صورت تصادفی تولید شده است، رمز می کند. این کلید همراه شماره حساب خریدار با استفاده از توزیع کلید یا همان key-exchange متعلق به CA رمز می شود.

۱۰. نرم افزار خریدار درخواست فرم ثبت نام را به طور رمز شده به CA ارسال می کند.

- از این جا به بعد تنها سناریو را می نویسم. چراکه روند تبادلات مشخص است.

۱۱. CA فرم ثبت نام را با استفاده از کلید متقارن شماره یک رمز گشایی می کند.

۱۲. CA فرم ثبت نام را جهت صحت آن بررسی کرده و پیام فرم را با کلید خصوصی CA رمز می کند.

۱۳. CA فرم ثبت نام و گواهی نامه خودش را به خریدار ارسال می کند.

۱۴. نرم افزار خریدار صحت فرم ثبت نام دریافتی را با استفاده از زنجیره اعتماد بررسی می کند.

۱۵. نرم افزار خریدار صحت امضای CA را بررسی می کند.

۱۶. نرم افزار خریدار یک جفت کلید تولید می کند.

۱۷. خریدار فرم ثبت نام را تکمیل می کند.

۱۸. نرم افزار خریدار درخواست گواهینامه شامل اطلاعات ورودی در فرم ثبت نام را به صورت رمز شده تولید می کند.

۱۹. نرم افزار خریدار پیامی همراه درخواست کلید عمومی امضای خریدار و کلید متقارن شماره دو می سازد. سپس درخواست گواهینامه را رمز می کند.

۲۰. نرم افزار خریدار پیام را با استفاده از کلید متقارن شماره سه رمز می کند. این رمز را همراه با اطلاعات حساب خریدار با استفاده از کلید CA رمز می کند.

۲۱. نرم افزار خریدار پیام درخواست گواهینامه رمز شده را به CA ارسال می کند.

۲۲. CA کلید متقارن شماره سه و اطلاعات حساب کارت را بدست می آورد.

۲۳. CA امضای خریدار را بررسی می کند.

۲۴. CA درخواست گواهینامه را با استفاده از اطلاعات حساب خریدار از فرم ثبت نام بررسی می کند.

۲۵. به محض تایید،CA گواهی نامه خریدار را تولید و امضای دیجیتال می کند.

۲۶. CAپاسخ گواهینامه را تولید و آن را با کلید خصوصی خودش رمز می کند.

۲۷. CA با کلید متقارن شماره دو، پاسخ گواهینامه را رمز نگاری می کند.

۲۸. CA پاسخ را به خریدار ارسال می نماید.

۲۹. نرم افزار خریدار گواهینامه را با زنجیره اعتماد بررسی می کند.

۳۰. نرم افزار خریدار پاسخ را با استفاده از کلید متقارن شماره دو از مرحله ۱۹، رمز گشایی می کند.

۳۱. نرم افزار خریدار صحت امضای CA را بررسی می نماید.

۳۲. خریدار،گواهی نامه و اطلاعات را جهت تراکنش های آتی ذخیره می کند.

ثبت نام فروشنده

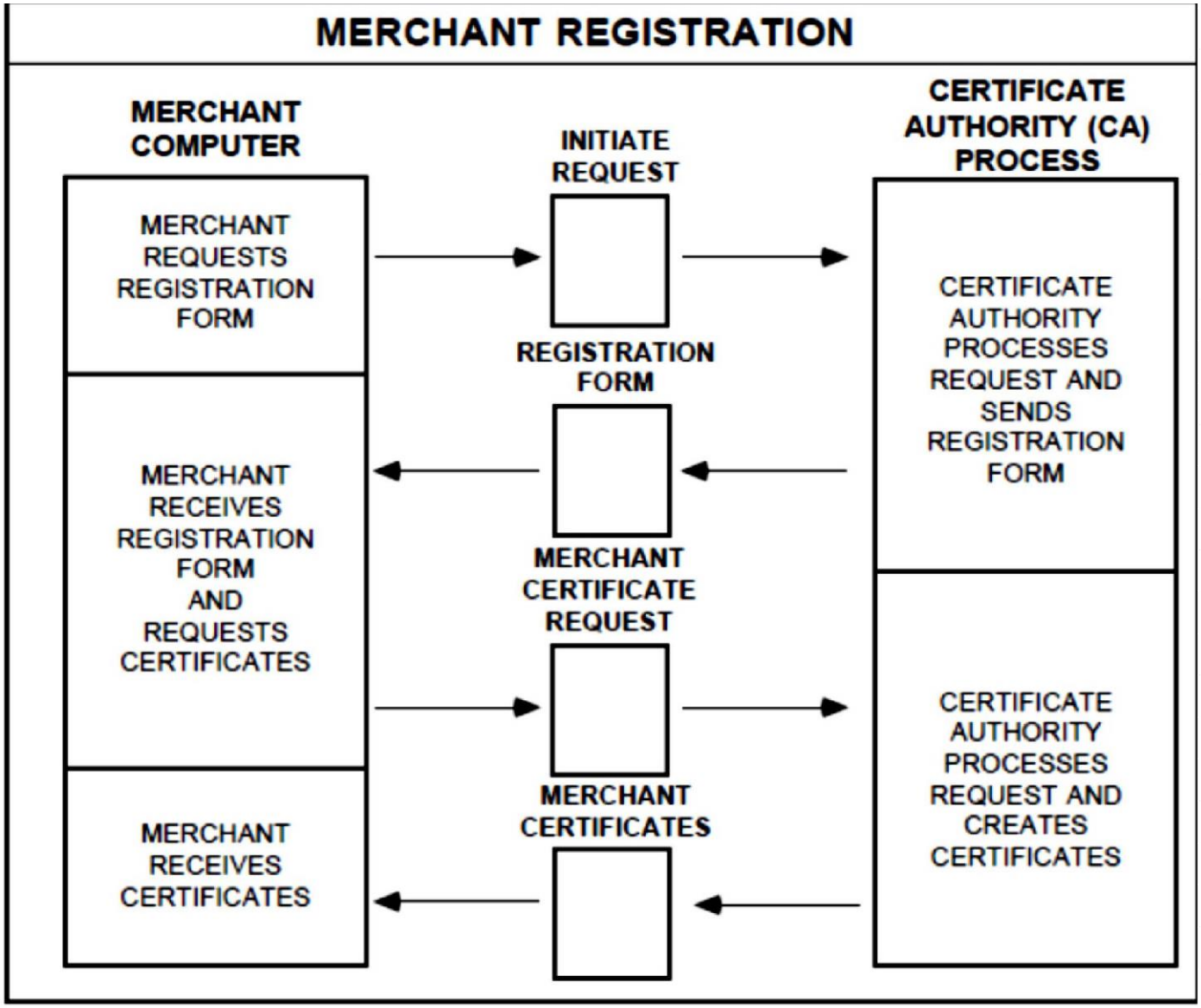


Figure 7: Merchant Registration

۱. نرم افزار فروشنده درخواست شروع را به CA ارسال می کند.

۲. CA درخواست شروع را دریافت می کند.

۳. CA یک فرم ثبت نام مناسب در نظر گرفته و آن را امضای دیجیتال می کند.

۴. CA یک فرم ثبت نام و یک گواهی نامه از خود را به فروشنده ارسال می نماید.

۵. نرم افزار فروشنده، فرم ثبت نام را دریافت و صحت آن را با زنجیره اعتماد مشخص می کند.

۶. نرم افزار فروشنده صحت امضای CAرا بررسی می کند.

۷. نرم افزار فروشنده یک جفت کلید می سازد.

۸. فروشنده فرم ثبت نام را تکمیل می کند.

۹. نرم افزار فروشنده درخواست گواهینامه را تولید می کینند.

۱۰. نرم افزار فروشنده با درخواست و کلید عمومی فروشنده، پیامی ایجاد کرده و آن را امضای دیجیتال می کند.

۱۱. نرم افزار فروشنده پیام را با استفاده از کلید متقارن شماره یک رمز می کند. این کلید همراه داده های حساب فروشنده رمز نگاری می شود.

۱۲. نرم افزار فروشنده پیام درخواست گواهی نامه را به صورت رمز شده به CA منتقل می کند.

۱۳. CA کلید متقارن شماره یک و داده های حساب فروشنده را رمز گشایی می کند. سپس پیام را با استفاده از کلید شماره یک رمز گشایی می کند.

۱۴. CA صحت امضای فروشنده را بررسی می نماید.

۱۵. CA درخواست گواهینامه را با استفاده از اطلاعات فروشنده تایید می کند.

۱۶. به محض تایید،CA گواهینامه را امضا می کند.

۱۷. CA پاسخ گواهینامه و امضای دیجتیال را می سازد.

۱۸. CA پاسخ را به فروشنده ارسال می نماید.

۱۹. نرم افزار فروشنده صحت گواهینامه را به وسیله زنجیره اعتماد تا کلید ریشه بررسی می کند.

۲۰. نرم افزار فروشنده صحت گواهینامه را بررسی می کند.

۲۱. نرم افزار فروشنده گواهینامه و اطلاعات حاصل از پاسخ را جهت استفاده در تراکنش های آتی ذخیره می کند.

درخواست پرداخت

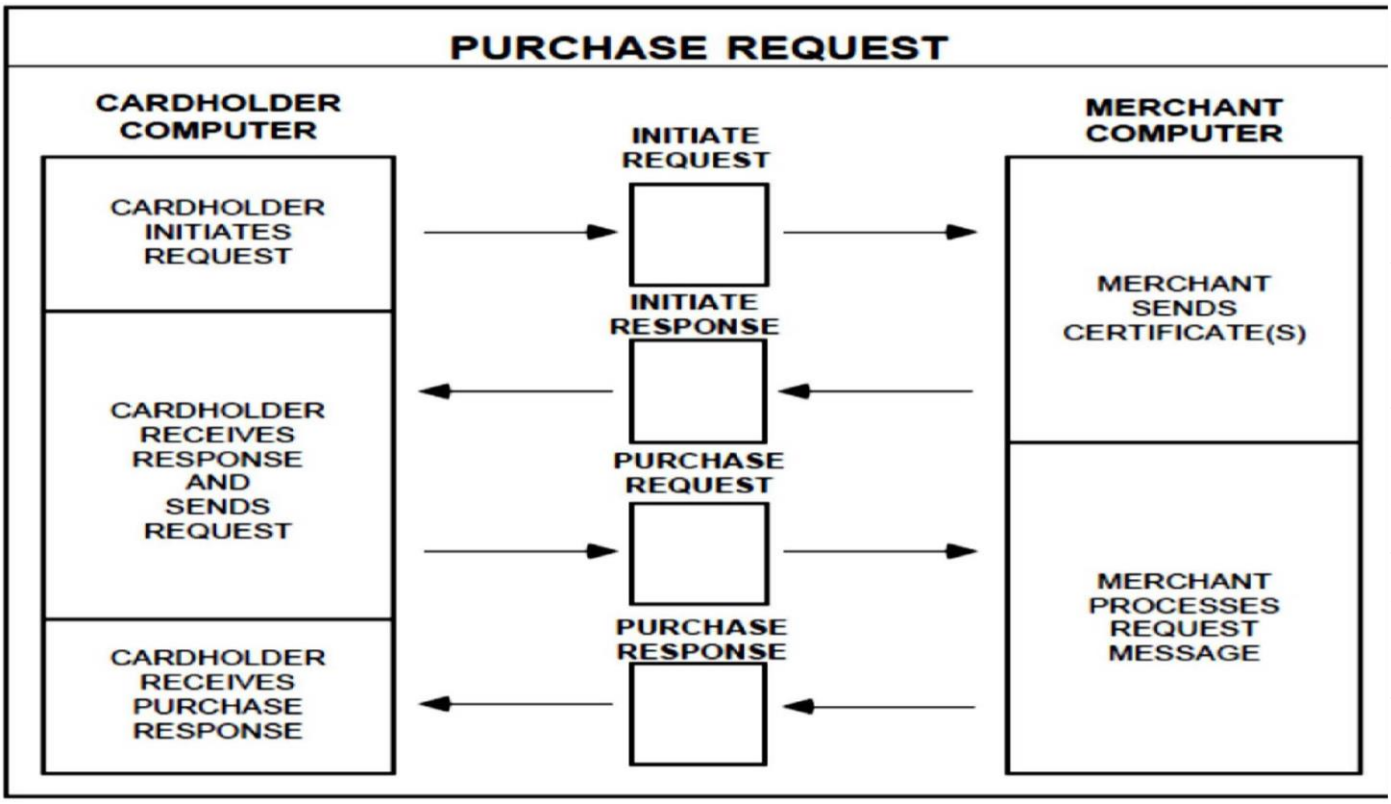


Figure 8: Purchase Request

۱. خریدار خرید می کند.

۲. نرم افزار خریدار یک درخواست شروع به فروشنده ارسال می نماید.

۳. نرم افزار فروشنده درخواست شروع را دریافت می کند.

۴. نرم افزار فروشنده پاسخ را تولید کرده و آن را امضای دیجیتال می کند.

۵. نرم افزار فروشنده پاسخ را به فروشنده و گواهی نامه کارت پرداخت را به خریدار ارسال می کند.

۶. نرم افزار خریدار پاسخ شروع را دریافت کرده و صحت گواهی نامه را با زنجیره اعتماد بررسی می کند.

۷. خریدار صحت امضای فروشنده را بررسی می کند.

۸. نرم افزار خریدار اطلاعات سفارش را با استفاده از اطلاعات مرحله خرید می سازد.

۹. خریدار دستور العمل پرداخت را کامل می نماید.

۱۰. نرم افزار خریدار یک امضای دوگانه را به وسیله هش کردن الحاق چکیده پیام های اطلاعات سفارش یا همان OI (Order information) و دستور العمل پرداخت یا همان PI (Payment Instructions) و رمز کردن نتایج هش دوگانه به وسیله کلید خصوصیِ امضا، تولید می کند.

۱۱. نرم افزار خریدار PI را با کلید متقارن شماره یک رمز می کند. این کلید همراه اطلاعات حساب خریدار به وسیله توزیع کلید مدخل پرداخت رمز می شود.

۱۲. نرم افزار خریدار OI و PI رمز شده را به فروشنده انتقال می دهد.

۱۳. نرم افزار فروشنده صحت گواهی نامه خریدار را با زنجیره اعتماد بررسی می کند.

۱۴. نرم افزار فروشنده صحت امضای دوگانه را بررسی می کند.

۱۵. فروشنده درخواستی شامل انتقال PI به مدخل پرداخت جهت مجوز را پردازش می کند.

۱۶. نرم افزار فروشنده پاسخ خرید شامل گواهی نامه امضای فروشنده را ساخته و آن را امضای دیجیتال می کند.

۱۷. نرم افزار فروشنده پاسخ خرید را به خریدار ارسال می کند.

۱۸. اگر تراکنش مجاز بود، فروشنده سفارش را برای خریدار تکمیل می نماید.

۱۹. نرم افزار خریدار صحت گواهی نامه امضای فروشنده را با زنجیره اعتماد بررسی می کند.

۲۰. نرم افزار خریدار صحت امضای دیجیتال فروشنده را بررسی می کند.

۲۱. نرم افزار خریدار پاسخ خرید را ذخیره می سازد.

اجازه پرداخت

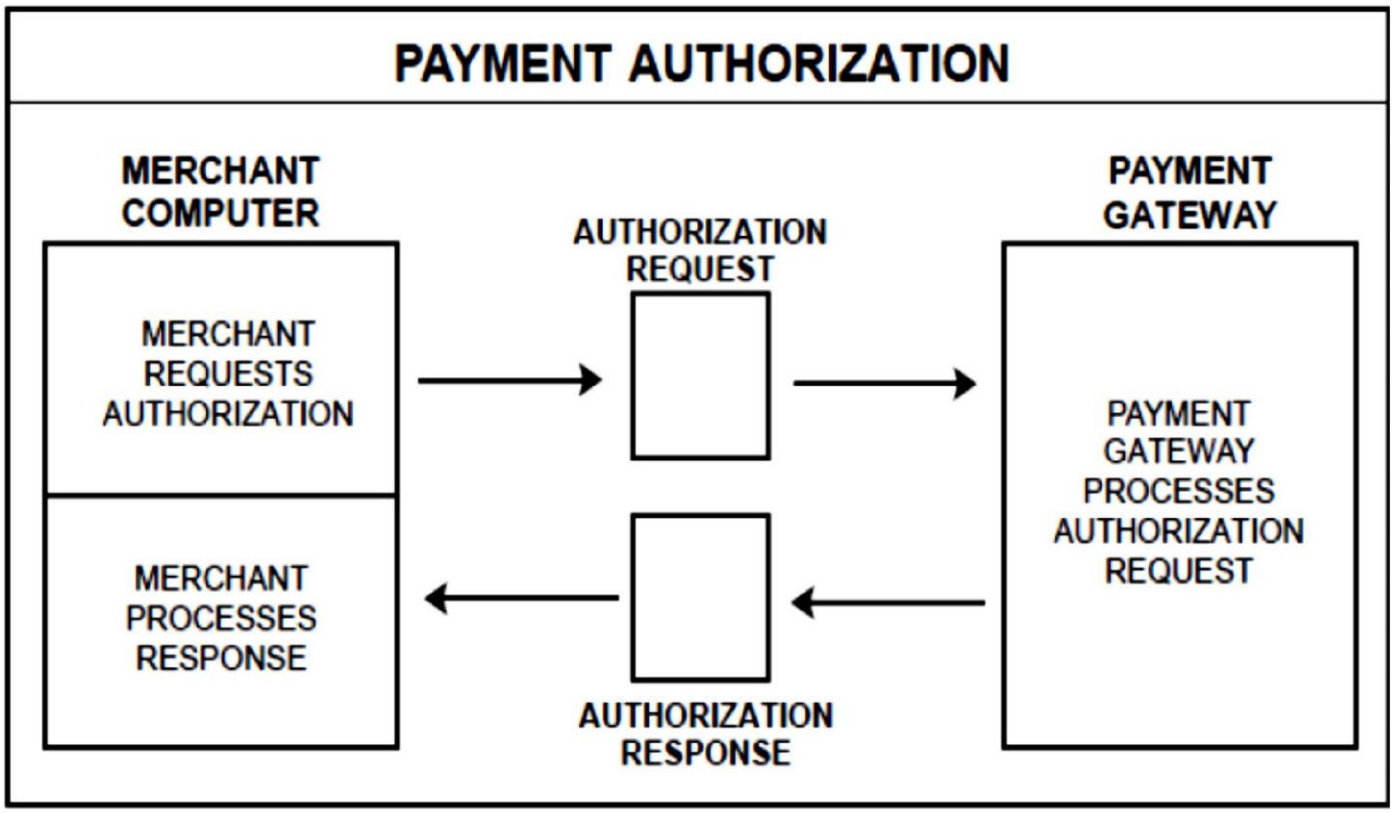


Figure 9: Payment Authorization

۱. نرم افزار فروشنده یک درخواست مجوز می سازد.
۲. نرم افزار فروشنده درخواست مجوز را امضای دیجیتال می کند.
۳. نرم افزار فروشنده درخواست مجوز را با تولید کلید متقارن تصادفی شماره دو رمز می کند. این کلید به وسیله توزیع کلید مدخل پرداخت رمزنگاری می شود.
۴. نرم افزار فروشنده درخواست مجوز رمز شده و PI رمز شده ی درخواست خرید خریدار را به مدخل پرداخت انتقال می دهد.
۵. مدخل پرداخت صحت گواهینامه فروشنده را به وسیله زنجیره اعتماد بررسی می کند.
۶. مدخل پرداخت کلید متقارن شماره دو را جهت رمزگشایی درخواست مجوز رمزگشایی می کند.
۷. مدخل پرداخت صحت امضای دیجیتال فروشنده را بررسی می کند.
۸. مدخل پرداخت صحت گواهینامه خریدار را با زنجیره اعتماد بررسی می کند.
۹. مدخل پرداخت کلید متقارن شماره یک و اطلاعات حساب خریدار را رمز گشایی می کند. سپس PI را با استفاده از کلید متقارن رمز گشایی می کند.
۱۰. مدخل پرداخت صحت امضای دوگانه PI مربوط به خریدار را بررسی می کند.
۱۱. مدخل پرداخت از هماهنگی بین درخواست مجوز فروشنده و PI خریدار مطمئن می شود.
۱۲. مدخل پرداخت درخواست مجوز را از میان شبکه مالی به موسسه مالی خریدار ارسال می نماید.
۱۳. مدخل پرداخت یک پیام پاسخ مجوز را ساخته و آن را با کلید خصوصی خود رمز نگاری می کند.
۱۴. مدخل پرداخت پاسخ مجوز را با کلید متقارن شماره سه که جدید است رمز کرده و سپس این کلید را به وسیله توزیع کلید فروشنده رمز می کند.
۱۵. مدخل پرداخت یک نشانه ثبت ساخته و آن را امضای دیجیتال می کند.
۱۶. مدخل پرداخت نشانه ثبت را با کلید متقارن شماره چهار رمز نگاری می کند. سپس این کلید همراه با اطلاعات حساب خریدار به وسیله توزیع کلید مدخل پرداخت رمز می شود.
۱۷. مدخل پرداخت پاسخ مجوز را به فروشنده ارسال می کند.
۱۸. نرم افزار فروشنده صحت گواهینامه پرداخت را با زنجیره اعتماد بررسی می کند.
۱۹. نرم افزار فروشنده کلید متقارن شماره سه را جهت رمز گشایی پاسخ مجوز رمز گشایی می کند.
۲۰. نرم افزار فروشنده صحت امضای دیجیتال مدخل پرداخت را بررسی می کند.
۲۱. نرم افزار فروشنده نشانه ثبت رمز شده را با نامه دیجتیال جهت پردازش های آتی ذخیره می کند.
۲۲. فروشنده روند درخواست خرید را تکمیل می کند.

ثبت پرداخت

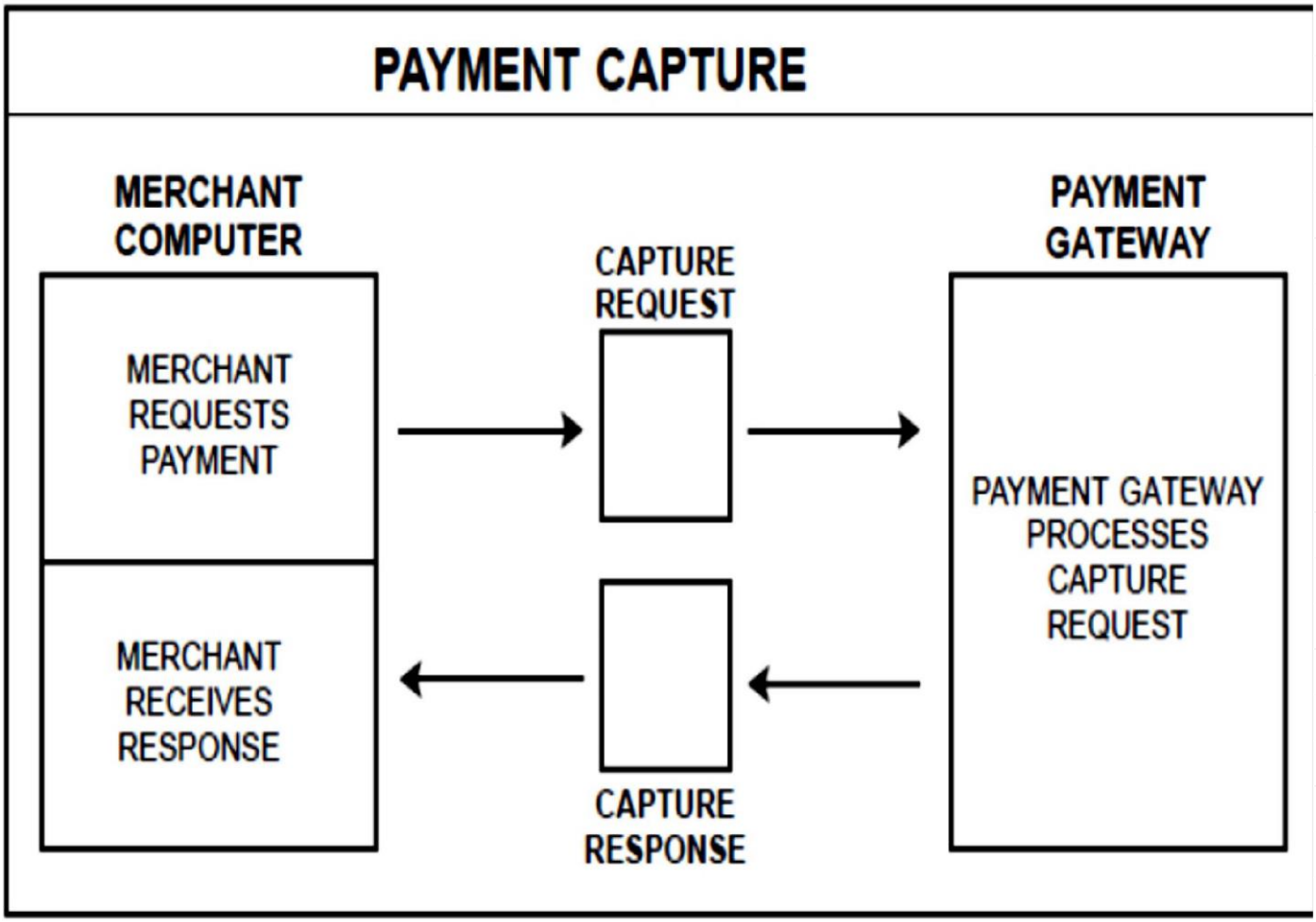


Figure 10: Payment Capture

۱. نرم افزار فروشنده درخواست ثبت را می سازد.

۲. نرم افزار فروشنده گواهی نامه فروشنده را در درخواست ثبت تعبیه می کند و آن را امضای دیجتیال می کند.

۳. نرم افزار فروشنده درخواست ثبت را به وسیله کلید متقارن شماره پنج رمز می کند. سپس این کلید را نیز رمز می کند.

۴. نرم افزار فروشنده درخواست ثبت رمز شده را همراه شناسه ثبت که قبل از پاسخ مجوز ذخیره شده بود، به مدخل پرداخت انتقال می دهد.

۵. مدخل پرداخت صحت گواهینامه فروش را با زنجیره اعتماد بررسی می کند.

۶. مدخل پرداخت کلید متقارن پنج را به منظور رمز گشایی درخواست ثبت، رمزگشایی می کند.

۷. مدخل پرداخت صحت امضای دیجتیال فروشنده را بررسی می کند.

۸. مدخل پرداخت کلید متقارن شماره چهار را به منظور رمزگشایی شناسه ثبت، رمزگشایی می کند.

۹. مدخل پرداخت از سازگاری بین درخواست ثبت فروشنده و شناسه ثبت اطمینان حاصل می نماید.

۱۰. مدخل پرداخت درخواست ثبت را از طریق شبکه مالی به موسسه مالی خریدار ارسال می کند.

۱۱. مدخل پرداخت پیام پاسخ ثبت شامل گواهینامه امضای مدخل پرداخت را امضای دیجتیال می کند.

۱۲. مدخل پرداخت پاسخ ثبت را به وسیله کلید متقارن شماره شش که جدید است،رمز نگاری می کند. سپس کلید متقارن شماره شش را با توزیع کلید فروشنده رمز می کند.

۱۳. مدخل پرداخت پاسخ ثبت فروشنده را به وی انتقال می دهد.

---

۱۴. نرم افزار فروشنده صحت گواهینامه مدخل پرداخت را با زنجیره اعتماد بررسی می کند.

۱۵. نرم افزار فروشنده کلید متقارن شماره شش را به منظور رمزگشایی پاسخ ثبت، رمز گشایی می کند.

۱۶. نرم افزار فروشنده صحت امضای دیجتیال مدخل پرداخت را بررسی می نماید.

THE END.!!!