دانشکده مهندسی برق

پایان نامه برای دریافت درجه کارشناسی ارشد در رشته

مهندسی فنآوررری اطلاعات- مخابرات امن

عنوان:

طراحی و شبیه‌سازی حملات جانبی زمانی و توانی و کاربردهای آن در کارت‌های هوشمند

دانشجو :

علی بهرامی

استاد راهنما:

دکتر وحید طباطباوکیلی

تابستان ۸۷

تاییدیهٔ هیأت داوران

هیـأت داوران پـس از مطالعـــه پـایـان نـامـه و شـرکـت در جلسـهٔ دفـاع از پـایـان نـامـــه بـا عنـــوان **" طراحی و شبیه سازی حملات جانبی زمانی و توانی و کاربردهای آن در کارت‌هـای هوشـمند"** توسط آقای **علی بهرامی** کفایت تحقیق انجام شده را برای اخذ درجه کارشناسی ارشـد در رشتـه **فـن-آوری اطلاعات** ، گرایش **مخابرات امن** مورد تأیید قرار می دهد.

اسامی هیات داوران بشرح زیر می باشد:

۱- **دکتر وحید طباطباوکیلی**	مرتبه علمی: **دانشیار**	دانشگاه: **علم و صنعت**
۲- **دکتر مجید نادری**	مرتبه علمی: **دانشیار**	دانشگاه: **علم و صنعت**
۳- **دکتر هادی شهریار شاه‌حسینی**	مرتبه علمی: **استادیار**	دانشگاه: **علم و صنعت**
۴- **دکتر حسن طاهری**	مرتبه علمی: **دانشیار**	دانشگاه: **امیرکبیر**

بسمه تعالی

اینجانـــب .....بـــه شـــماره دانـــشجویی.....

دانشجوی رشته .....مقطع تحصیلی .....

بدین وسیله صحت و درستی نتایج موجود در این پایان نامه را تایید نموده و گواهی می نمایم که در این نتایج هیچ گونه دخل و تصرفی صورت نگرفته باشد. همچنین متعهد می گردم کـه کلیـه نتایج عملی موجود در این پایان نامه حاصل کار اینجانب بوده و متعلق به هـیچ یـک از محققـین قبلی نمی باشد. چنانچه خلاف موارد فوق حتی بصورت جزئـی و در هـر زمـان مـشخص گـردد دانشگاه علم و صنعت ایران حق دارد که این پایان نامه را باطل نماید. در این صـورت تعهـد مـی نمایم که تبعات قانونی این مسئله و همچنین کلیه خسارات ناشی از آن به عهده اینجانب باشد.

نام و نام خانوادگی

امضاء و تاریخ

تقدیر و تشکر:

با سپاس از استاد ارجمند جناب آقای دکتر طباطباوکیلی که با راهنمائیهای ارزنده خود، مرا در اجرای این پروژه یاری نمودند.

همچنین از اساتید محترم جناب آقای دکتر نادری، دکتر شاه‌حسینی و دکتر طاهری که داوری این پایان-نامه را بر عهده داشتند، سپاسگزارم.

با تشکر از مرکز تحقیقات مخابرات ایران بخاطر حمایتهای مادی و معنوی این پروژه

تقدیم به زیباترین واژه زندگی

مادر عزیزم

و تقدیم به روح پدر بزرگوارم

چکیده

حملات مبتنی بر کانال جانبی یک سری جدید از تهدیدات علیه الگوریتم‌های رمزنگاری و سیستم‌های امنیتی هستند. این حملات برخلاف حملات کلاسیک، به ضعف‌های محاسباتی الگوریتم‌ها کاری نداشته و از ضعف‌های پیاده‌سازی استفاده می‌نمایند.

در این حملات از اطلاعات کانال جانبی مانند زمان اجرا، توان مصرفی وسیله رمزنگار، تشعشعات مغناطیسی، دفعات مراجعه به حافظه‌های *cache* و ... استفاده نموده و امنیت سیستم را مورد تهدید قرار می‌دهند.

در این پایان‌نامه ابتدا به معرفی حملات زمانی، توانی ساده و تفاضلی، حمله مبتنی بر *cache* و حمله مبتنی بر الگو پرداخته، سپس حملات زمانی و توانی تفاضلی را روی الگوریتم *AES* اجرا نموده‌ایم. در ادامه با ترکیب حملات زمانی و توانی، حمله جدیدی به نام حمله انرژی را معرفی نموده و با کمک شبیه‌سازی‌ها، در فصل پنجم نشان می‌دهیم که حمله انرژی از دو حمله دیگر قوی‌تر است.

در فصل آخر روشهای مقابله با این حملات را معرفی کرده و یک روش امن را برای پیاده‌سازی الگوریتم *AES* پیشنهاد می‌نمائیم. در این روش از جدول‌های *lookup* و روش ماسک‌گذاری بصورت همزمان استفاده شده که علاوه بر ایجاد امنیت در مقابل حملات کانال جانبی، سرعت اجرای الگوریتم نیز نسبت به سایر روش‌های مقابله، افزایش می‌یابد.

کلمات کلیدی : حملات کانال جانبی، حمله زمانی، حمله توانی، حمله انرژی، حمله مبتنی بر حافظه *cache* ، حمله مبتنی بر الگو، ماسک گذاری، الگوریتم رمزنگاری *AES*

فهرست مطالب

پیشگفتار:

در عصر اطلاعات و ارتباطات، امنیت همه شبکه‌هائی که با داده‌ها سروکار دارند (مانند شبکه‌های مخابراتی و کامپیوتری)، بسیار مهم بوده و بدون ایجاد امنیت، نمی‌توان از همه مزایای این شبکه‌ها استفاده کرد. همانطور که می‌دانیم اهداف اصلی ایمنی شبکه‌ها عبارتند از فراهم کردن محرمانگی، درستی داده‌ها، دسترسی به اطلاعات مجاز.

برای برآورده کردن اهداف ذکر شده، مکانیزم‌های مختلفی مطرح شده‌اند. رمزنگاری یکی از مهمترین مکانیزم‌هائی است که در انتقال و ذخیره داده‌ها بکار می‌رود. همزمان با توسعه علم رمزنگاری و ارائه الگوریتم‌های نوین رمز کردن، حملات جدید و قوی‌تری نیز علیه سیستم‌های رمزنگار مطرح می‌شوند.

یک سیستم رمزنگاری را حداقل از دو دیدگاه می‌توان مورد نظر قرار داد، از یک نظر، می‌توان آنرا یک موضوع کاملا"ریاضی‌وار و محاسباتی، مانند یک نگاشت که یک ورودی را به یک خروجی تبدیل کرده و ممکن است یک کلید را بعنوان پارامترورودی داشته‌باشد، در نظر گرفت. از منظری دیگر، این الگوریتم، در صورت مفید بودن، باید توسط یک برنامه روی یک پردازنده، در یک محیط ویژه اجرا شود، بنابراین خواص ویژه‌ای را تولید می‌کند.

بر اساس این دو دیدگاه، حملات مطرح شده علیه الگوریتم‌های رمزنگاری را می‌توان به دو دسته کلی حملات کلاسیک و حملات مبتنی بر کانال جانبی تقسیم نمود. اولین دیدگاه در حملات و تحلیل‌های سنتی و دیدگاه دوم در حملات مبتنی بر کانال جانبی، بکار می‌رود. بعبارت دیگر در حملات کلاسیک از ضعفهای محاسباتی الگوریتم‌ها و خواص آماری داده‌های تولیدی توسط الگوریتم استفاده شده، اما مهاجم در حملات کانال جانبی، به ضعفهای محاسباتی کاری نداشته و روی ضعفهای پیاده‌سازی متمرکز می‌شود.

حملات مبتنی بر کانال جانبی، یک مجموعه جدید از تهدیدات علیه وسایل رمزنگاری هستند که علیرغم پیاده‌سازی آسان و ساده آنها، بسیار قوی بوده و یک تهدید اساسی برای الگوریتم‌های رمزنگاری می‌باشند. بنابراین باید مقاومت انواع پیاده‌سازی‌های محتلف یک الگوریتم رمزنگاری را در برابر این حملات ارزیابی نمود. یکی از مهمترین وظایف یک کارشناس رمز، شناسایی این حملات و روشهای مقابله با آنها و استفاده از یک یا ترکیبی از این روشهای مقابله است.

این حملات هنگامی قابل اجرا هستند که، بین اندازه یکی از کمیت‌های فیزیکی تولید شده توسط سیستم رمزنگار و حالت داخلی وسیله رمزنگار، همبستگی وجود داشته و این حالت داخلی نیز به کلید مخفی یا پیام‌های رمزشده و رمزنشده وابسته باشد.

در این حملات از اطلاعات نشتی سیستم رمزنگار استفاده می‌کنند. اطلاعات جانبی، همان کمیتهای فیزیکی می‌باشند، مانند توان مصرفی سیستم رمزنگار، زمان اجرای یک الگوریتم رمزنگاری، تعداد دفعات مراجعه به حافظه *cache* ، تشعشعات مغناطیسی و ... . اطلاعات کانال جانبی معمولا" براحتی قابل گردآوری بوده و بنابراین ضروری است که عملکرد این حملات، هنگام ارزیابی امنیت یک سیستم، بدقت مورد تحلیل قرار گیرد.

حملات جانبی را با توجه به نوع اطلاعات جانبی مورد استفاده، به چندین دسته تقسیم می‌نمایند، مانند: حملات زمانی، توانی، الکترومغناطیسی، حملات برپایه حافظه *cache* ، حملات مبتنی بر الگو[1]، و .... .

در فصل اول این پایان‌نامه، مقدمه‌ای ذکر شده که در آن بطور مختصر، حملات کانال جانبی مطرح و انواع دسته‌بندی‌های مختلف بکار رفته در مورد آنها، بیان شده‌است. در فصل‌های دوم و سوم به ترتیب به معرفی حملات زمانی و توانی پرداخته و اصول تئوری آنها را بیان نموده و نمونه‌هائی از حملات اجرا شده را ذکر کرده‌ایم. فصل چهارم به معرفی حملات مبتنی بر *cache* و مبتنی بر الگو اختصاص یافته است. این دو حمله، در سال‌های اخیر معرفی گشته و هر کدام، کاربردهای ویژه‌ای دارند.

[1] *Template Attack*

در فصل پنجم، نتایج حاصل از شبیه‌سازی اجرای حملات زمانی و توانی تفاضلی روی الگوریتم *AES* بیان شده است. علاوه بر این در فصل پنجم، یک حمله جدید را که ترکیبی از حملات زمانی و توانی است، معرفی و قدرت آنرا با حملات توانی و زمانی مقایسه گشته‌است. شبیه‌سازی‌ها نشان می‌دهد، این حمله که آنرا به عنوان حمله انرژی نام‌گذاری نموده‌ایم، قویتر از حملات زمانی و توانی است.

در فصل ششم، به بررسی انواع روشهای مقابله با حملات جانبی پرداخته و یک روش را برای پیاده‌سازی امن الگوریتم *AES* مطرح نموده‌ایم. در این روش علاوه بر این که امنیت مورد نظر در مقابل این حملات بدست آمده، سرعت اجرا نیز نسبت به سایر پیاده‌سازی‌های امن، بهبود یافته است. فصل هفتم نیز به بیان نتایج پرداخته و در آن، پیشنهاداتی برای اجرا در آینده ذکر شده است.

فصل ۱- مقدمه:

۱-۱ نگاهی به حملات مبتنی بر کانال جانبی:

در میان حملات مختلفی که روی الگوریتم‌های مختلف رمزنگاری انجام می‌شوند، حملات مبتنی بر کانال جانبی دارای پیاده‌سازی و اجرای ساده‌ای هستند. این حملات یک سری جدید از تهدیدات علیه وسایل رمزنگاری را معرفی کرده و در نتیجه باید مقاومت انواع پیاده‌سازی‌های محتلف یک الگوریتم رمزنگاری را در برابر این حملات ارزیابی کرد. یکی از مهمترین وظایف یک کارشناس رمز، شناسایی این حملات و روشهای مقابله با آنها و استفاده از یک یا ترکیبی از این روشهای مقابله است.

این پروژه به معرفی و بررسی حملات مبتنی برکانال جانبی و روشها وتکنیک‌های مختلف بکار رفته در آنها، اثرات مخرب این حملات و شیوه‌های مقابله با آنها می‌پردازد.

بحث امنیت همواره یک موضوع بسیار مهم در سیستم‌های محاسباتی و انتقال داده بوده وتحقیقات وسیع و هزینه‌های فراوانی در این زمینه شده‌است.

الگوریتم‌های رمزنگاری از قبیل: رمزهای متقارن، کلید عمومی و توابع هش[1] ، تشکیل‌دهنده یک دسته از ساختارهای اولیه[2] هستند که می‌توانند به عنوان واحدهایی برای ایجاد فرآیندهای خاص امنیتی، مانند تشخیص هویت بین دو موجودی، ایجاد محرمانگی، تضمین صحت داده انتقالی و... بکار روند.

[1] *Hash*
[2] *Primitive*

در عمل فرآیندهای امنیتی تنها به بیان توابع مورد نیاز می‌پردازند و به نحوه اجرای این توابع کاری ندارند. مثلا" تصریح یک پروتکل امنیتی، معمولا" مستقل از این است که الگوریتم رمزنگاری با سخت‌افزار پیاده‌سازی می‌شود یا نرم افزار، یا داده‌های پردازش‌شده در حین اجرای الگوریتم در یک *IC* مجزا ذخیره می‌شوند یا در همان *IC* اجرا کننده الگوریتم و... .

این نوع جدایی بین فرآیندهای امنیتی و نحوه پیاده‌سازی آنها، از نظر تئوری، زمینه اجرای یک سری تحلیل‌ها و حملات به الگوریتم‌های رمزنگاری را فراهم می‌کند.

بهرحال در مرحله تولید و معرفی یک عمل خاص امنیتی، شرایط مختلفی در نظر گرفته می‌شود که معمولا" برخی از آنها در دنیای واقعی عملی نیستند، مثلا" معمولا" فرض می‌شود که یک دستورالعمل رمزنگاری، در حالت ایده آل، در یک واحد بسته و ناشناخته، که ساختار داخلی آن غیرقابل مشاهده بوده و توسط هیچ موجود بدخواهی قابل دستکاری نیست، اجرا می‌شود. اگر این فرضیات برقرار باشند، آنگاه میزان امنیت یک فرآیند به قدرت الگوریتم و طول کلید آن وابسته می‌گردد. اما در عمل این فرضیات بطور کامل برقرار نیستند و مهاجمین از روشهای دیگری غیر از شکستن پیچیدگی‌های محاسباتی الگوریتم‌های رمز استفاده می‌کنند. در این زمینه، می‌توان یک الگوریتم بسیار قوی رمزنگاری را به یک قفل بسیار محکم درب یک خانه تشبیه کرد، در این مورد نیز سارقان همیشه بدنبال شکستن قفل نیستند، بلکه می‌توانند از روشهای دیگری مانند: شکستن پنجره‌ها، شکستن در از قسمت لولا، دزدیدن کلید از صاحبخانه و .... برای ورود به خانه استفاده کنند. همانند سارقان منزل، مهاجمین نیز می‌توانند از ضعفهای پیاده‌سازی فرآیندهای امنیتی، برای حمله استفاده کنند. این ضعفها به مهاجم این اجازه را می‌دهد، که بصورت کامل و یا تا حدودی، قدرت محاسباتی الگوریتم رمز را دور بزند.

برای یک سیستم رمزنگاری که بخواهد امن باقی بماند، بسیار مهم است که کلید سری تحت هیچ شرایطی قابل آشکارسازی نباشد. الگوریتم‌های رمزنگاری از نظر محاسباتی توسط بسیاری از کارشناسان مورد تحلیل قرار گرفته‌اند، اما در سالهای اخیر یک نوع جدید از حملات، توسط *Kocher* معرفی شده‌اند که بیشتر به نحوه پیاده‌سازی الگوریتم وابسته هستند تا خود الگوریتم [۱].

این حملات هنگامی قابل اجرا هستند که، بین مقدار کمیت‌های مختلف فیزیکی تولید شده در حین اجرای الگوریتم و حالت داخلی وسیله رمزنگار، همبستگی وجود داشته باشد، که این حالت داخلی، خود باید به کلید مخفی وابسته باشد.

در عمل، الگوریتم‌های رمزنگاری همیشه یا با کمک نرم‌افزارها و یا به روش سخت‌افزاری بر روی وسایل فیزیکی پیاده‌سازی می‌شوند، که این وسایل فیزیکی روی محیط پیرامون خود دارای اثرات متقابلی هستند. این اثرات متقابل می‌توانند توسط مهاجمان تحریک و یا مانیتور شوند و ممکن است منجر به لورفتن اطلاعات مفیدی برای دشمن گردند. این نوع از اطلاعات را اطلاعات مبتنی بر کانال جانبی[1] نامیده و حملاتی که از این اطلاعات استفاده می‌کنند، حملات مبتنی بر کانال جانبی[2] *(SCA)* خوانده می‌شوند. ایده اصلی حملات مبتنی برکانال جانبی بر اساس مشاهده روش اجرای الگوریتم رمز است نه خود الگوریتم.

مهاجمین سنتی با الگوریتم‌های رمز، فقط به عنوان یک موضوع کاملا" ریاضی و محاسباتی برخورد می‌کردند، اما تحلیل‌گرهای کانال جانبی، نحوه اجرای الگوریتم و پیاده‌سازی آنرا نیز در نظر می‌گیرند. به همین دلیل این حملات را حملات پیاده‌سازی[3] نیز می‌نامند.

اولین نمونه از حملات جانبی به سال ۱۹۶۵ برمی‌گردد. در آن سال سازمان جاسوسی بریتانیا[4] سعی می‌کرد که الگوریتم بکار رفته توسط سفارت مصر را بشکند، اما تلاش آنها بدلیل محدودیت‌های محاسباتی ناموفق می‌ماند. آقای، *P-Wright* ، پیشنهاد کرد که یک میکروفن را نزدیک ماشین رمزکننده دواری که توسط مصریها استفاده می‌شد، قرار داده و از طریق آن صدای کلیک کردن‌های ماشین را بشنوند. با گوش کردن به کلیکهای روتور که منشی هرروز صبح آنها را ریست می‌کرد، *MI5* توانست با موفقیت، موقعیت تعدادی از هسته‌های روتورهای ماشین رمزنگار را پیدا کند. این اطلاعات اضافی توان محاسباتی لازم برای شکستن رمزها را کاهش داد و *MI5* توانست سالها از سفارت مصر جاسوسی کند.[۲]

[1] *Side Channel Information*
[2] *Side Channel Attack*
[3] *Implementation Attack*
[4] *MI5*

اساس حملات کانال جانبی بسیار ساده است، این حملات بدین دلیل عمل می‌کنند که یک همبستگی بین اندازه بعضی از کمیت‌های فیزیکی در حین محاسبه (مانند توان مصرفی، زمان اجرا، امواج الکترومغناطیسی منتشرشده، صدای تولیدی و...) و حالت داخلی وسیله پردازنده، وجود دارد. این حالت داخلی نیز به نوبه خود با کلید مخفی مرتبط است. پس یک همبستگی بین اطلاعات کانال جانبی و اعمال محاسباتی وابسته به کلید وجود دارد که هدف از حملات کانال جانبی یافتن این رابطه و استفاده از آن است. ثابت شده‌است که حملات مبتنی بر کانال جانبی چندین برابر حملات ریاضی‌وار موثربوده و نسبت به آنها عملی‌تر هستند.

بهرحال وقتی ما بخواهیم از حالت نوشته و تئوری به مرحله اجرا در دنیای واقعی برویم همه چیز سخت‌تر می‌شود و همه مسایل جزئی که از نظر تئوری به چشم نمی‌آمدند، به مشکلات بسیار بزرگی تبدیل می‌شوند.

محدودیت‌های یک وسیله رمزنگار در دنیای واقعی چیست؟ دشمن برای انجام یک عمل ویژه روی یک وسیله خاص چه خروجی‌ها و ورودی‌هایی را می‌تواند ملاحظه و یا دستکاری کند؟ و... .

جواب دادن به این سوالات بسیار سخت است، اما طراحی یک ساختار مقاوم در مقابل این حملات، احتیاج به توجه ویژه به این سوالات دارد.

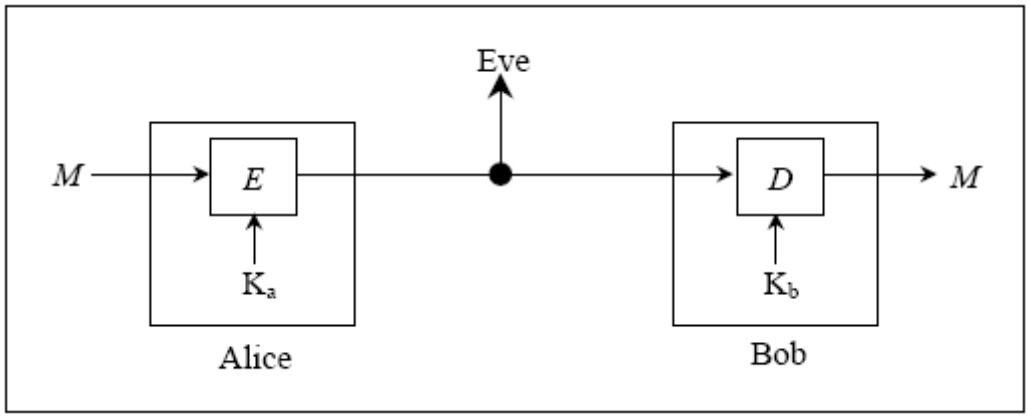
نتایج محاسبات فیزیکی معمولا" یک کمیت فیزیکی است و دشمن می‌تواند این نتایج را ببیند، در بعضی از موارد این مشاهدات می‌تواند منجر به لو رفتن اطلاعات شوند.

دشمن توسط این حملات فیزیکی امیدوار است که بتواند امنیت سیستم را خراب کند و این کار معمولا" با استخراج بعضی از اسرار از برخی از وسایل که خیلی امن نیستند، انجام می‌شود.

یک سیستم رمزنگاری را حداقل از دو دیدگاه می‌توان ملاحظه کرد، از یک طرف، می‌توان آنرا یک موضوع کاملا"ریاضی‌وار فرض کرد، یعنی آنرا بعنوان یک نگاشت که یک ورودی را به یک خروجی تبدیل می‌کند و ممکن است یک کلید را بعنوان پارامترورودی داشته‌باشد، در نظر گرفت. از منظری دیگر، این الگوریتم، در صورت مفید بودن، باید توسط یک برنامه روی یک پردازنده، در یک محیط ویژه اجرا شود و بنابراین خواص ویژه‌ای را تولید می‌کند. اولین دیدگاه در حملات و تحلیل‌های سنتی رمز کاربرد دارد، ولی دیدگاه دوم در حملات کانال جانبی.

حملات *SCA* از خواص ویژه پیاده‌سازی الگوریتم استفاده می‌کنند و بنابراین حالت عمومی ندارند (زیرا به نحوه اجرا بستگی دارند)، اما معمولا" بسیار قویتر و ساده‌تر از حملات کلاسیک بوده و باید در طراحی‌ها به‌دقت مورد توجه قرار گیرند.

در تحلیل‌های کلاسیک، هنگام ارزیابی یک پروتکل رمزنگاری، معمولا" فرض می‌کنند که دشمن یک توصیف کامل از پروتکل را دانسته وفقط کلید را نمی‌داند. علاوه بر این دشمن ممکن است بتواند از تبادل اطلاعات بین دو طرف ممانعت به عمل آورد و یا ممکن است روی طبیعت داده‌ها کنترل داشته باشد. (مثلا" با انتخاب پیامها در *Chosen Message Attack* روی امضای دیجیتال، یا با انتخاب متنهای رمزشده در *Chosen Ciphertext Attack* در یک طرح رمز کلید عمومی). دشمن سپس تصمیم می‌گیرد که بین اهداف پروتکل و حل مساله مورد نظر خود رابطه‌ای برقرار کند و در این راه از بعضی از ضعفهای پروتکل استفاده می‌کند. در این فرآیند، مسایل مجرد ریاضی نیز می‌توانند در یادگیری خواص رمزنگاری مفید باشند. رمزنگارها معمولا" میزان امنیت یک الگوریتم را با توابع ریاضی بکاررفته در آن، ارزیابی می‌کنند. شکل(۱-۱) مدل کلاسیک یک سیستم رمزنگاری و رمزگشائی را نشان می‌دهد. در این مدل، الگوریتم‌های امن رمزنگاری فقط در مقابل مهاجمانی که به یک جعبه بسته و ناشناخته دسترسی داشتند، امنیت را برقرار می‌کردند، اما بهرحال این شرایط، کافی و بسنده نبودند. حملات در مدل امنیتی کلاسیک، فقط از خواص ریاضی الگوریتم رمز استفاده می‌کنند.



شکل(۱-۱): مدل کلاسیک یک سیستم رمزنگاری و رمزگشائی