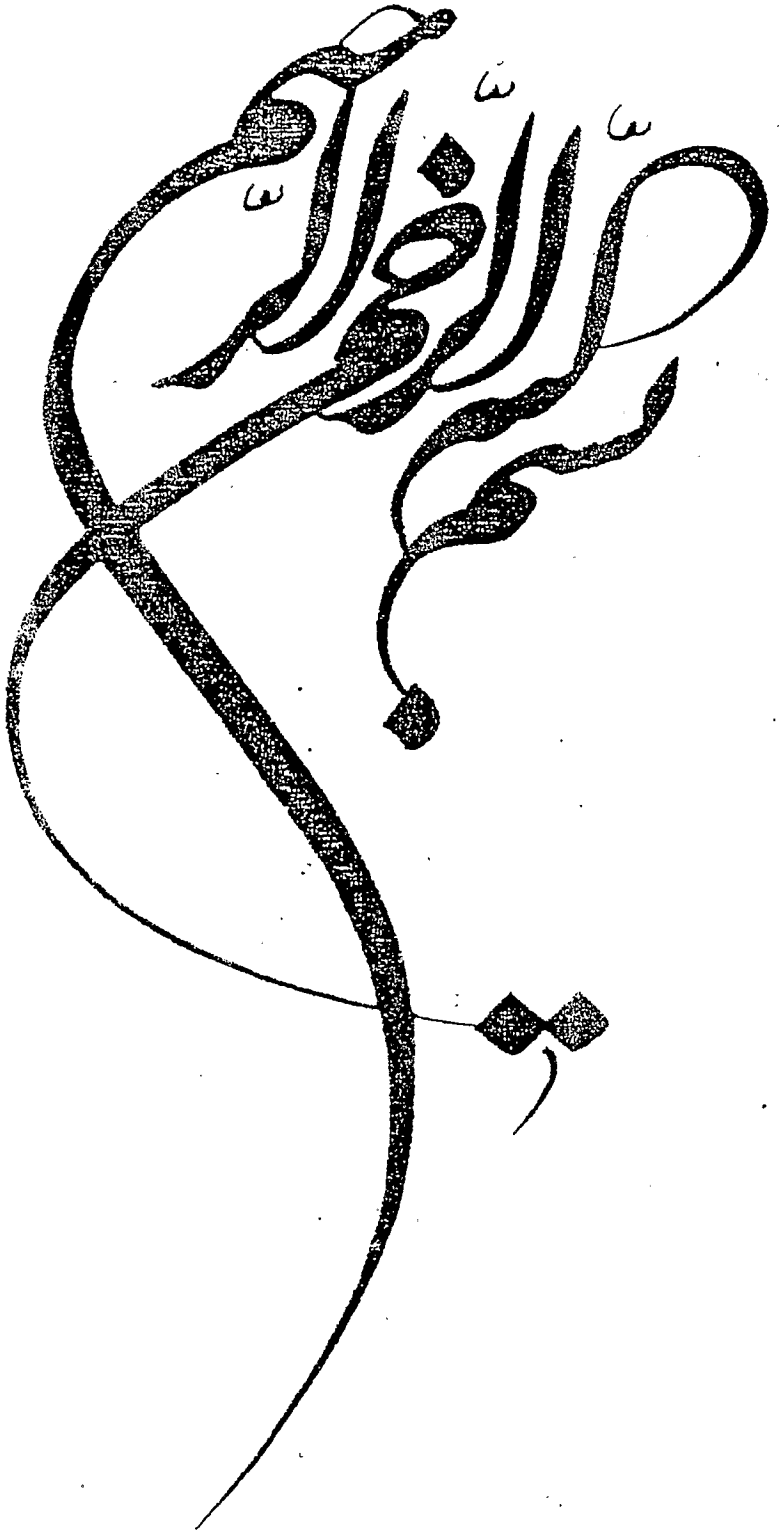
٨٧/١١/١٦٠٥
٨٧/١٠/٢١




١٠٧٧٩٩

دانشگاه گیلان
دانشکده علوم پایه
گروه ریاضی
گرایش محض

پایان نامه کارشناسی ارشد

# درجه بندی امنیت جبری تابع های بولی

از
عظمت رمضانپور مردخه

۱۳۸۷/۱۰/۱۳
۱۳۸۷/۱۰/۱۳

استاد راهنما

دکتر شهاب الدین ابراهیمی آتانی

شهریور ۸۷

۱۰۷۷۹۹

تقدیم به پدر و مادر مهربانم

که دستان پر مهرشان یاری دهنده‌ی روزهای سخت زندگیم گردید.

و

تقدیم به همسرم

که نگاه پرفروغش روشنی بخش کوچه های تاریک وجودم شد.

## تقدیر و تشکر

خدای را بی نهایت شاکرم که مرا توفیق داد تا کار پایان نامه ام را به پایان رسانم.

برخود می دانم تا از زحمات پدر و مادر عزیزم و استادان محترم خود در طول تحصیل تشکر و قدردانی نمایم.

مراتب تشکر و قدردانی خود را از استاد عزیزم آقای دکتر شهاب الدین ابراهیمی آتانی که با صبر و حوصله ی فراوان خود راهنما و پاسخگوی سوالاتم بوده و مرا در این راه یاری نمودند و از آقای دکتر حبیب ا... انصاری و آقای دکتر هاشمی که با مطالعه ی پیش نویس پایان نامه و با حسن نظر خویش یاری بخش من در تصحیح پایان نامه بوده اند ، اعلام می دارم.

# فهرست مطالب

**عنوان** **صفحه**

# فهرست جدول ها

**عنوان** **صفحه**

# فهرست شکل ها

**عنوان** **صفحه**

## چکیده


**درجه بندی امنیت جبری تابع های بولی**

**عظمت رمضانپور مردخه**

امنیت جبری تابع های بولی یکی از موضوعات بسیار مهم در رمز جاری به شمار می رود. در این پایان نامه فرمول دقیقی برای تعداد توابع بولی با امنیت جبری ۱پیدا می کنیم و سپس ساختارهایی را برای رسیدن به امنیت جبری مطلوب ارائه می دهیم و یک کران برای تعداد توابع بولی با امنیت جبری مطلوب پیدا می کنیم.



**کلید واژه**: تابع های بولی ، حمله جبری ، امنیت جبری ، خاصیت غیرخطی ، رمز جاری .

# Abstract

**Algebraic Immunity Hierachy of Boolean Functions**
**Azemat Ramzanpoor Mardakhe**

Algebraic immunity of Boolean function is a very important concept in recently introduced algebraic attack of stream cipher. In this thesis we abtain an exact formula for the number of Boolean functions with algebraic immunity one. We can also construct Boolean functions with maximum possible algebraic immunity and a lower bound of the count.

**Keywords:** Boolean functions; algebraic attack; algebraic immunity; nonlinearity; stream cipher.

## مقدمه

رمزنگاری عمر چندانی ندارد و علمی جدید محسوب می شود لذا توجه به آن از اهمیت بسیاری برخوردار بوده است و تلاش برای گسترش آن امری ضروری به شمار می‌رود. در دنیای رمزنگاری، رمز جاری جزء نیازهای اولیه برای تامین پنهان‌سازی روی کانال‌های ارتباطاتی به‌شمار می‌رود.

رمزهای جاری الگوریتم‌هایی هستند که به منظور رمزداکردن مورد استفاده قرار می‌گیرند. توابع بولی یکی از اجزای بسیار مهم در رمز جاری به‌شمار می‌روند. نقش این توابع در رمزجاری طراحی تابع ترکیب کننده و تابع فیلتر است، انتخاب صحیح یک تابع بولی به‌طور قابل ملاحظه‌ای مقاومت را در برابر انواع گوناگون حملات افزایش می‌دهد. همین امر سبب شد تا بسیاری از دانشمندان در پی مطالعه و تحقیق درباره‌ی توابع بولی برآمدند. توابع بولی دارای یک خاصیت رمزی بسیار مهم هستند که از آن تحت عنوان امنیت جبری یاد می‌کنیم. توابع بولی برای اینکه بتوانند به‌عنوان یک اولیه در سیستم رمز مورد استفاده قرار گیرند باید امنیت جبری بالایی داشته باشند زیرا اگر امنیت جبری پایین باشد مزاحم یک مجموعه‌ی بزرگ از معادلات جبری چند متغیره را روی کلیدهای راز پیدا می‌کند و با حل این معادلات درجه‌ی پایین کلید راز را کشف می‌کند. بنابراین می‌توان گفت که امنیت جبری پارامتری وابسته به محتوای حمله‌ی جبری است. در این پایان نامه امنیت جبری توابع بولی را به‌طور مفصل مورد مطالعه و بررسی قرار می‌دهیم و سپس ساختارهایی را برای رسیدن به امنیت جبری مطلوب ارائه می‌دهیم و در نهایت فرمولی دقیق برای محاسبه‌ی تعداد توابع بولی با امنیت جبری ۱ پیدا می‌کنیم.

این پایان نامه بر مبنای مرجع [۱۰] می‌باشد. در فصل اول اولیه‌های متقارن را توصیف می‌کنیم و روی اصول‌های طراحی رمزهای جاری متمرکز خواهیم شد و در ادامه‌ی فصل به‌طور مفصل توابع بولی را تعریف می‌کنیم و با نقش این توابع در سیتم رمز آشنا خواهیم شد و آن دسته از خواص رمزی این توابع را که در سیستم رمز مورد استفاده قرار می‌گیرند مطالعه می‌کنیم.

در فصل دوم امنیت جبری تابع‌های بولی را مطالعه می‌کنیم و رابطه‌ی امنیت جبری یک تابع بولی را با خاصیت

غیرخطی آن مورد بررسی قرار داده و امنیت جبری توابع بولی را بر حسب امنیت جبری زیر تابع‌های آن بیان می‌کنیم.

در فصل سوم روش ساختاری را که می‌توان به کمک آن به تابع‌های بولی با بیشترین امنیت جبری دسترسی پیدا کرد توصیف می‌کنیم.

در فصل چهارم یک روش ساختاری را که به کمک آن از یک تابع بولی داده شده به یک کلاس بزرگ از تابع‌های بولی با امنیت جبری مطلوب دسترسی پیدا، ارائه می‌دهیم. با این ساختار می‌توانیم تابع‌هایی را که در مقابل حملات جبری از خود مقاومت بیشتری نشان می‌دهند طراحی کنیم.

در فصل پنجم علاقه‌مند هستیم تا با انواع توابع بولی با امنیت جبری $k$ که $0 \leq k \leq \lceil \frac{n}{2} \rceil$ قرار دارد آشنا شویم. چون با دانستن این مطلب می‌توانیم توابع بولی را مطابق با امنیت جبری شان درجه‌بندی کنیم و همچنین در این فصل فرمول دقیقی برای محاسبه‌ی تعداد توابع بولی با امنیت جبری ۱ پیدا می‌کنیم.

# فصل ۱

# مفاهیم اولیه‌ی تابع‌های بولی

## ۱—۱ مقدمه

در این فصل اولیه‌های متقارن را توصیف خواهیم کرد و روی اصول‌های طراحی رمزهای جاری متمرکز خواهیم شد زیرا در دنیای رمز نگاری رمزهای جاری جزء نیازهای اولیه برای تامین پنهان سازی روی کانال های ارتباطاتی به شمار می‌روند. توابع بولی یکی از اجزای بسیار مهم در رمز جاری به شمار می‌روند نقش این توابع در رمز جاری طراحی تابع ترکیب کننده و تابع فیلتر می‌باشد در ادامه‌ی فصل تابع‌های بولی را تعریف می‌کنیم و نمایش‌هایی را که برای یک تابع بولی وجود دارد ارائه می‌دهیم. خواص رمزی تابع‌های بولی را معرفی کرده و سپس تعاریف و قضایایی را که در فصل های بعدی مورد نیاز خواهند بود ارائه می‌دهیم.

## ۱—۲ تاریخچه‌ی رمزنگاری [۱]

نیاز به ارتباطات هزاران سال است که در میان موجودات وجود داشته است، سخنرانی همواره یک ویژگی مهم بشر اجتماعی بوده است این ویژگی است که ما را ار حیوانات متمایز می‌سازد. حتی در زمان دایناسورها که زندگی غارنشینی بود همواره انسانها نیاز به ارتباطات پنهانی داشتند. آنها مجموعه‌ای از اطلاعات را به صورت راز از قبایل دیگری که در همسایگی غار زندگی می‌کردند مخفی نگه می‌داشتند. خلق نویسندگی پنهان کاری ارتباطاتی را با اهمیت تر ساخت براستی که طول عمر متنهای نوشته شده طولانی‌تر از نقل قول هایی است که از قبل به جا مانده است. درزمان باستان، یهودی ها سیستم رمزی را خلق کردند و آن را«اتبش»[۲] نامیدند امروزه ما این سیستم رمز را تحت عنوان رمز جانشینی می‌شناسیم. امپراتوری رم از این سیستم رمز برای پنهان ساختن متن هایشان از دید مزاحمان استفاده می‌کردند. در همان زمان که بسیاری از مردم در حال مخفی ساختن متن هایشان بودند خلاقان کنجکاو در پی کشف کردن این متنها بودند به این ترتیب بسیاری از مردم درصدد ساخت سیستمهای رمزگشایی برآمدند.

---

[۱] Cryptography

[۲] Atbash

تاریخ رمزنگاری مدرن را می توان در سال ۱۹۲۰ با ساخت سیستم *Enigma* توسط گروهی از دانشمندان آلمانی دانست. این اولین کامپیوتر اختصاصی برای رمزدار کردن به شمار می رفت. بعد از سه سال گروهی از دانشمندان انگلیسی با نحوه‌ی عملکرد این سیستم آشنا شدند و بعد از مدتی سیستم *Enigma* به طور وسیع برای رمزدارکردن مورد استفاده قرار گرفت. از این وسیله به‌طور وسیع در جنگ جهانی دوم استفاده شد. شکننده‌ی اولیه ی سیستم *Enigma* در سال ۱۹۲۳ در لهستان توسط *Poland* ساخته شد و سبب قطع جنگ به مدت یک یا دو سال گردید. این تاریخ مثال واضحی است که اهمیت رمزنگاری را برای ما نمایان می‌سازد. بنابراین نتیجه می‌گیریم که انسان ها همواره به رمزنگاری در طول دوران زندگی خود نیاز داشته‌اند.

امروزه تکنولوژی اطلاعات و ارتباطات بخش عمیقی از زندگی مارا تشکیل می دهد. مردم از تلفن های همراه، اینترنت و سیستمهای بانکداری استفاده می‌کنند. به طورکلی تر ارتباطات هر جایی که کانالهایی طراحی می‌شوند می‌توانند وجود داشته باشند. منظوراز کانال همان مهیا کننده‌ی اطلاعات است که می تواند سیم تلگراف، هوا و غیره باشد. یک کانال می‌تواند امن یا ناامن باشد، اگر اطلاعاتی که در میان یک کانال جریان دارد فقط توسط کسی که گیرنده‌ی پیام است دریافت شود می‌گوییم کانل امن است در غیر اینصورت کانال ناامن خواهد بود. رمزنگاری عمر چندانی ندارد و علمی جدید محسوب می‌شود بنابراین از اهمیت بالایی برخوردار بوده و تلاش برای گسترش آن امری ضروری به شمار می‌رود. رمزشناسی مطالعه‌ی روش‌های ارتباط ایمن است. فرض کلی این است که دو طرف که فرستنده‌ی پیام و گیرنده‌ی پیام نامیده می‌شوند قصد دارند به طور ایمن با یکدیگر ارتباط برقرار کنند مشکلی که برای فرستنده و گیرنده‌ی پیام وجود دارد، حظور یک مزاحم است که قصد دارد به اطلاعاتی که از طرف فرستنده به گیرنده ارسال می‌شود دسترسی پیدا کند. رمزنگاری کاربردهای وسیعی در زندگی روزمره‌ی ما دارد و خدمات مختلفی را برای ما فراهم می‌کند که در زیر برخی از آن ها را شرح خواهیم داد.

## ۱—۳ خدمات رمزی[۳]

رازداری داده، سندیت کاربر و یکپارچگی داده از جمله سرویسهایی هستند که در کاربردهای واقعی مورد استفاده قرار می‌گیرند، در زیر به اختصار آنها را توضیح می دهیم:

**رازداری داده:** این سرویس یکی از شناخته ترین و قدیمی ترین سرویسها می‌باشد که تعهد می‌کند اطلاعات فقط در دسترس افراد مجاز قرار داده شود. به‌عنوان مثال در بانک ها، اسناد مشتریان باید با اطمینان نگه داری شوند، چون ممکن است این اطلاعات در دسترس افراد غیر مجاز قرار گیرد، لذا راز داری داده تعهد می‌کند که اسناد مشتریان با اطمینان نگه داری شوند و همچنین در بیمارستان ها از این سرویس به طور وسیع استفاده می‌گردد.

**سندیت کاربر:** وقتی از مکانیسم (ATM) برای دریافت پول خود استفاده می‌کنیم معمولا پین کد چهار رقمی خود را وارد می‌کنیم و پول را دریافت می‌کنیم، هیچ کس جز مابدون داشتن این پین کد چهار رقمی قادر به دریافت پول نخواهد بود. در بسیاری از اوقات برای ورود به سیستم کامپیوتر خود، از اسم [۴] و اسم رمز [۵] استفاده می‌کنیم تا سیستم هیچ کس جز ما را به‌عنوان کاربر نشناسد. همه‌ی این وضعیت ها نیاز به مکانیسم ویژه‌ی سندیت دارد.

**یکپارچگی داده:** این سرویس ضمانت می‌کند که اطلاعات فرستاده در میان کانال ها تعدیل شده نیست. این سرویس در صورتی مفید خواهد بود که گیرنده‌ی پیام، فرستنده‌ی پیام را بشناسد. این سرویس با سرویس سندیت منبع داده ترکیب شده و ضمانت می‌کند شخصی که ادعا می‌کند اجازه‌ی ورود دارد واقعا فرستنده‌ی پیام است.

**توجه ۱—۳—۱:** در یک سیستم ارتباطاتی دیجیتالی همواره باید مراقب باشیم چون یک مزاحم ممکن است که به کانالها گوش کند و اطلاعات را تعدیل نماید. برای مثال در ارتباطات به صورت $e-mail$ هر کسی می تواند یک $e-mail$ بسازد و برای $A$ بفرستد بطوریکه به نظر برسد شخص $B$ آنرا فرستاده است. رمزنگاری به خوبی این مشکلات را به کمک امضاء دیجیتالی حل می‌کند. امضاهای دیجیتالی این امکان را بوجود می آورند تا نویسنده‌ی پیام بعدا نتواند

---

[۳] Cryptographic

[۴] Username

[۵] Password

نوشته‌اش را انکار نماید. امضاهای دیجیتالی قردادهایی هستند که فرستنده و گیرنده‌ی پیام قبل از شروع ارتباطات با یکدیگر می‌گذارند.

در زیر به شرح و توضیح یک مدل ارتباطاتی می‌پردازیم.

## ۱—۴ مدل ارتباطاتی

در مدل ارتباطاتی سه جزء داریم :

- فرستنده‌ی پیام : کسی که برخی پیام ها را به طرف مقابل می‌فرستد.
- گیرنده‌ی پیام : کسی که پیام ها را از فرستنده دریافت می‌کند.
- مزاحم : کسی که تمایل دارد پیامهای فرستاده شده از فرستنده به گیرنده را بخواند.

**تعریف ۱—۴—۱ :** الفبا مجموعه‌ای از نمادها است که در رمزدار کردن مورد استفاده قرار می گیرد و با نماد $\mathcal{A}$ نشان داده می‌شود.

**تعریف ۱—۴—۲ :** به اطلاعاتی که در میان کانال های امن ( کانالهایی که نفر سومی نتواند اطلاعات را تعدیل کند) از طرف فرستنده‌ی پیام به گیرنده‌ی پیام فرستاده می‌شود، متن ساده گفته می‌شود و معمولا با نماد m نشان می‌دهیم. در بیشتر موارد متن ساده بعنوان دنباله‌ای از نمادها از الفبای $\mathcal{A}$ در نظر گرفته می‌شود.

$$m^n = m_1, m_2, \ldots, m_n \qquad m_i \in \mathcal{A}, \qquad 1 \leq i \leq n$$

مجموعه‌ی همه‌ی متن‌های ساده را با نماد $\mathcal{M}$ نمایش می‌دهیم.

**تعریف ۱—۴—۳:** به اطلاعات با رمز نوشته شده‌ای که در میان یک کانال ناامن فرستاده شده متن رمزی گفته می‌شود و معمولا با نماد C نمایش می‌دهیم. در بیشتر موارد متن رمزی به عنوان دنباله‌ای از نمادها از الفبای $\mathcal{A}$ در نظر گرفته می‌شود.

$$c^n = c_1, c_2, \ldots, c_n \qquad c_i \in \mathcal{A}, \qquad 1 \leq i \leq n$$

در بیشتر موارد طول ها و الفباهای متن ساده و متن رمزی یکسان هستند. مجموعه‌ی متن های رمزی را با نماد $C$ نمایش می‌دهیم.

**تعریف ۱—۴—۴:** کلید رازی که بین فرستنده و گیرنده قبل از اینکه ارتباطات شروع شود، از طریق یک کانال امن مبادله می‌شود کلید نامیده می‌شود. کلید را به عنوان دنباله ای از l نماد از الفبای $\mathcal{A}$ در نظر می‌گیریم.

$$k = k_1, k_2, \ldots, k_l \qquad k_i \in \mathcal{A}, \qquad 1 \leq i \leq l$$

مجموعه‌ی همه‌ی کلیدها را با نماد $\mathcal{K}$ نمایش می‌دهیم.

**تعریف ۱—۴—۵:** رمزدارکردن[۶] تابع یا الگوریتمی است که متن ساده‌ی m را دریافت می‌کند و متن رمزی c را متناظر با کلید راز $k_e$ تولید می‌کند یعنی:

$$E_{k_e} : M \times K \longrightarrow C.$$

**تعریف ۱—۴—۶:** رمزگشایی[۷] تابع یا الگوریتمی است که متن رمزی c را دریافت می‌کند و متن ساده‌ی m را مطابق با کلید راز $k_d$ تولید می‌کند یعنی:

$$D_{k_d} : C \times K \longrightarrow M.$$

**تعریف ۱—۴—۷:** رمز[۸] یک دوتایی از دو تابع رمزدارکردن و رمزگشایی است. یعنی $cipher = (E, D)$ و همواره به ازای هر $m \in \mathcal{M}$ و هر $k_e \in \mathcal{K}$ و متناظر با آن برای هر $k_d \in \mathcal{K}$ باید داشته باشیم :

$$D_{k_d}(E_{k_e}(m)) = m.$$

یعنی اگر متن رمزشده‌ی m را رمزگشایی کنیم، متن m حاصل می‌شود.

در بخش بعدی جایگاه رمز نگاری را در یک سیستم ارتباطاتی نشان خواهم داد.

---

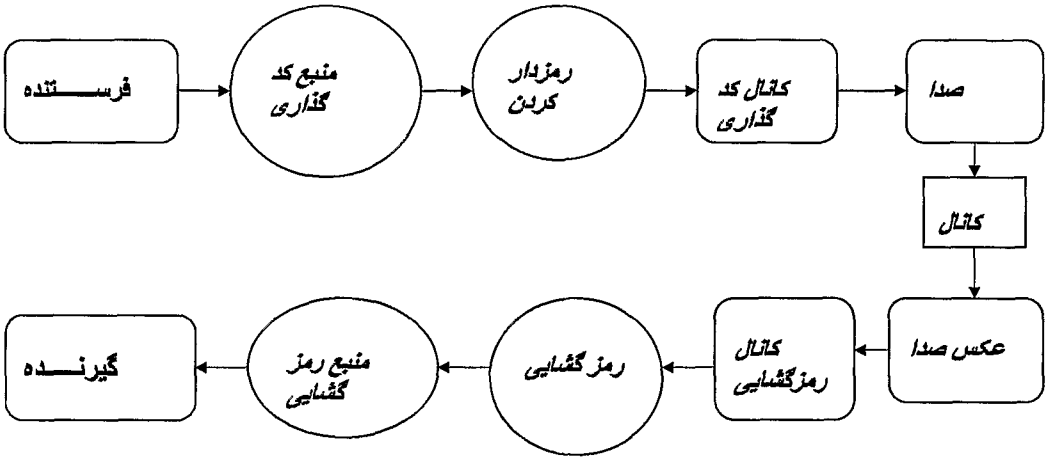
[۶] Encryption

[۷] Decryption

[۸] cipher

## ۱—۵ کانال رمزگذاری

شکل زیر یک نمونه‌ی بارز برای اطلاعاتی است که در میان یک کانال حرکت می‌کند.




شکل ۱—۱: جایگاه ارتباطات در سیستم رمزنگاری.

شکل ۱—۱ مسیر موضعی اطلاعاتی را که در میان یک کانال حرکت می‌کند، نشان می‌دهد و چهار مرحله به صورت زیر دارد:

**منبع رمزگذاری :** اطلاعات زائد را از میان فایل های گوناگون حذف می کند به طوریکه اطلاعات فشرده شوند. نمونه های بارز از منبع های کد گذار می‌توان الگوریتم های $Zip, Arj, Rar$ را نام برد. در منبع کد کشایی اطلاعات فشرده شده به حالت اول بر می‌گردند.

**رمزدار کردن :** بعد از اینکه اطلاعات زائد از میان فایلهای گوناگون پاک شدند رمزدارکردن برای امن ساختن پنهان سازی ارتباطات اجرا می شود. روش رمزدارکردن یک رمز به این صورت است که متن ساده را به عنوان ورودی می گیرد و متن رمزی را تولید می کند. روشهای رمزدارکردن و رمزگشایی از موضوعات بسیار مهم در رمزنگاری به شمار می‌روند.

**کانال رمزگذاری :** در کانال رمزگذاری برخی زوائد به داده‌های ورودی اضافه می شود تا اشتباهات دیجیتالی‌ای که در