امنیت شبکه و داده

تهیه و تنظیم: سهراب پورخلیلی

منابع:

- امنیت داده ها . دکتر علی ذاکرالحسینی . انتشارات نص
- معماری امنیت شبکه . شون کانوری . انتشارات نص
- انجمن رمز ایران www.isc.org.ir
- Cryptography and Network security: Principles and practice . William Stallings . Prentice Hall

مقدمه

- **رمزنگاری** دانشی است که به بررسی و شناختِ اصول و روش‌های انتقال یا ذخیرهٔ اطلاعات به صورت امن (حتی اگر مسیر انتقال اطلاعات و کانال‌های ارتباطی یا محل ذخیره اطلاعات ناامن باشند) می‌پردازد.

مقدمه

- رمزنگاری دانش تغییر دادن متن پیام یا اطلاعات به کمک کلید رمز و با استفاده از یک الگوریتم رمز است، به صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج اطلاعات اصلی از اطلاعات رمز شده باشد و شخصی که از یکی یا هر دوی آن‌ها اطلاع ندارد، نتواند به اطلاعات دسترسی پیدا کند. دانش رمزنگاری بر پایه مقدمات بسیاری از قبیل تئوری اطلاعات، نظریه اعداد و آمار بنا شده‌است و امروزه به طور خاص در علم مخابرات مورد بررسی و استفاده قرار می‌گیرد. معادل رمزنگاری در زبان انگلیسی کلمه Cryptography است، که برگرفته از لغات یونانی kryptos به مفهوم «محرمانه» و graphien به معنای «نوشتن» است.

رمزنگاری، پنهان‌نگاری، کدگذاری

- در رمزنگاری، وجود اطلاعات یا ارسال شدن پیام به هیچ وجه مخفی نمی‌باشد، بلکه ذخیره اطلاعات یا ارسال پیام مشخص است، اما تنها افراد مورد نظر می‌توانند اطلاعات اصلی را بازیابی کنند. بالعکس در پنهان‌نگاری، اصل وجود اطلاعات یا ارسال پیام محرمانه، مخفی نگاه داشته می‌شود و غیر از طرف ارسال‌کننده و طرف دریافت‌کننده کسی از ارسال پیام آگاه نمی‌شود.

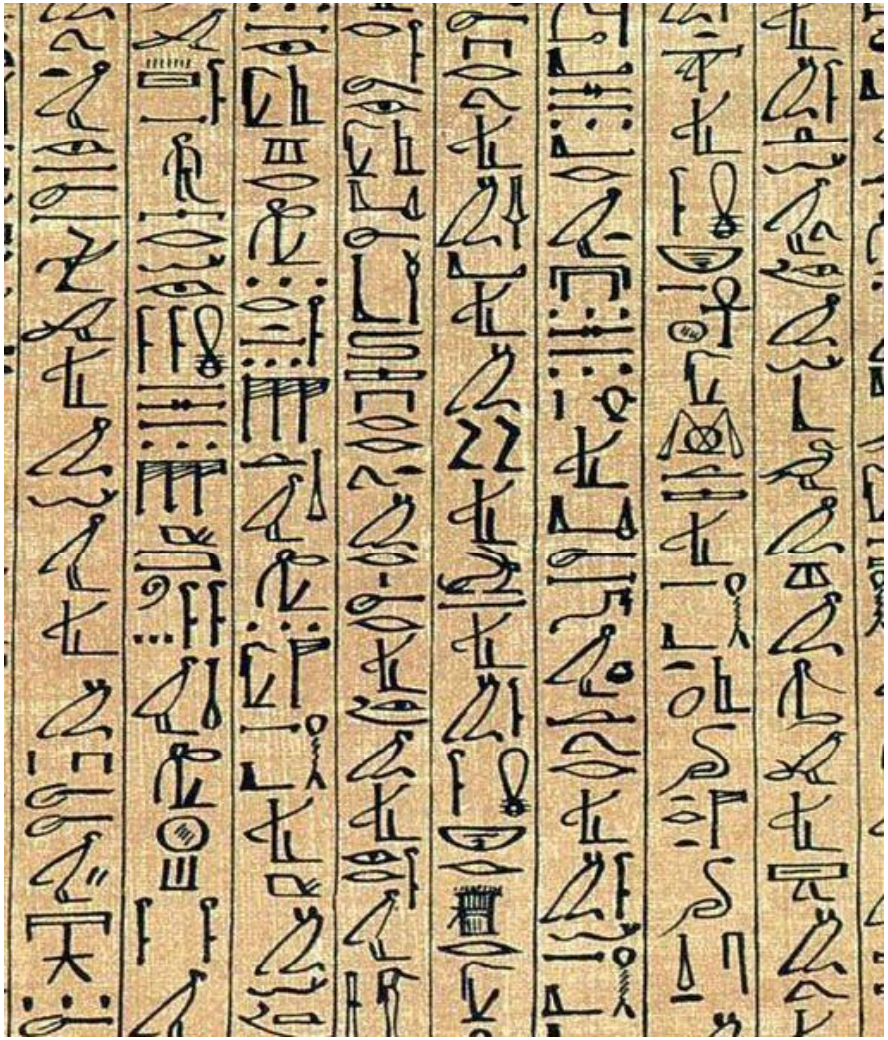
رمزنگاری، پنهان‌نگاری، کدگذاری

- در رمزنگاری محتویات یک متن به صورت حرف به حرف و در بعضی موارد بیت به بیت تغییر داده می‌شود و هدف تغییر محتوای متن است نه تغییر ساختار زبان‌شناختی آن. در مقابل کدگذاری تبدیلی است که کلمه‌ای را با یک کلمه یا نماد دیگر جایگزین می‌کند و ساختار زبان‌شناختی متن را تغییر می‌دهد.

تاریخچه رمزنگاری

- ریشهٔ واژهٔCryptography برگرفته از یونانی به معنای «محرمانه نوشتن متون» است. رمزنگاری پیشینهٔ طولانی ودرخشان دارد که به ۵۵۰۰ سال قبل برمی گردد .
- رمز نگاری و رسم الخط قدمت یکسانی دارند با این تفاوت که رسم الخط از نمادها نه برای مخفی کردن بلکه برای انتشار افکار استفاده می شود.

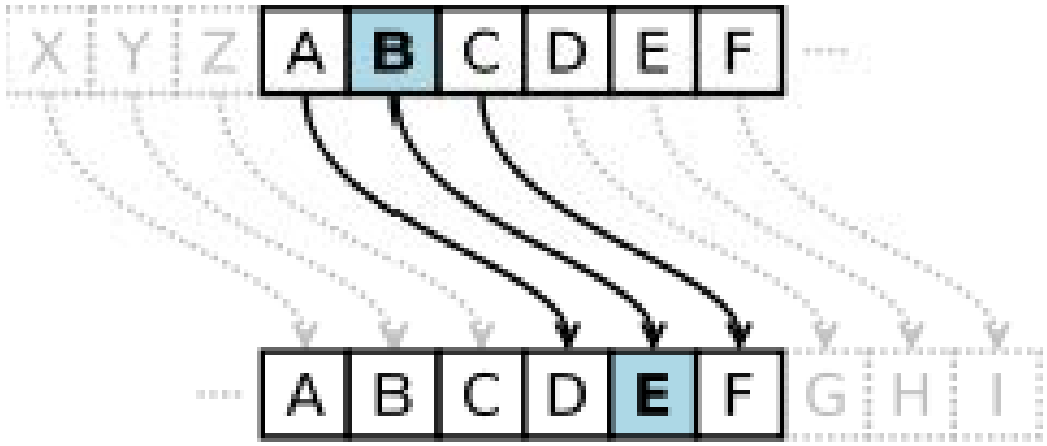
تاریخچه رمزنگاری



- خط میخی و هیرو گلیف اولین رسم الخطها بودند که ساختار رمزگونه و پیچیده ای داشتند.

تکنیک رمزنگاری سزار

- در بررسی نخستین استفاده‌کنندگان از تکنیک‌های رمزنگاری به سزار (امپراتور روم) و نیز الکندی که یک دانشمند مسلمان است برمی‌خوریم، که البته روش‌های خیلی ابتدایی رمزنگاری را ابداع و استفاده کرده‌اند. به عنوان مثال، با جابجا کردن حروف الفبا در تمام متن به اندازه مشخص آن را رمز می‌کردند و تنها کسی که از تعداد جابجا شدن حروف مطلع بود می‌توانست متن اصلی را استخراج کند .

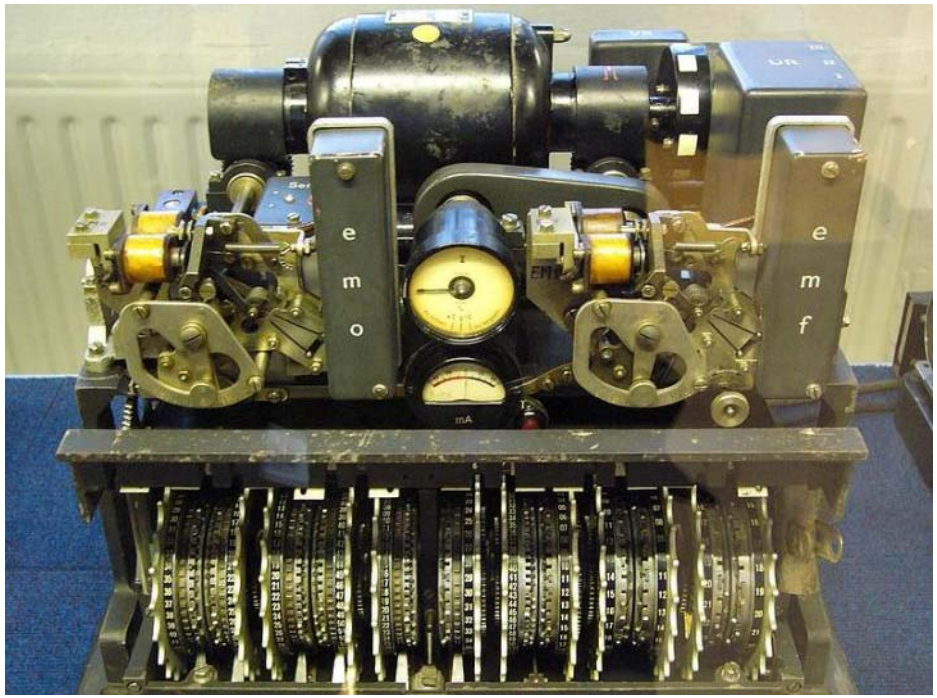


استفاده از استوانه و نوار کاغذی برای رمز کردن پیام

- یکی دیگر از شیوه‌های رمزنگاری ابتدایی، پیچیدن یک نوار کاغذی بر روی استوانه‌ای با قطر مشخص و سپس نوشتن پیام روی کاغذ پیچیده شده بوده‌است. بدیهی است بدون اطلاع از مقدار قطر استوانه، خواندن پیام کار بسیار دشواری خواهد بود و تنها کسانی که نسخه‌های یکسانی از استوانه را داشته باشند می‌توانند پیام را بخوانند.

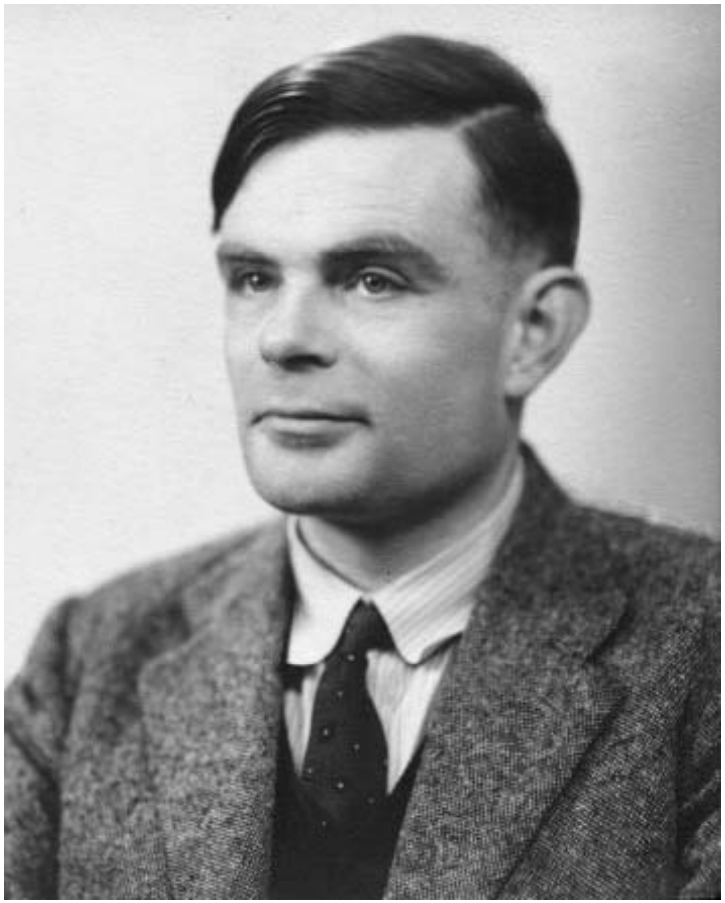
ماشین رمزکنندهٔ لورنتز

- ماشین رمزکنندهٔ لورنتز که در جنگ جهانی دوم توسط آلمان برای رمز کردن پیام‌های نظامی مورد استفاده قرار گرفته‌است.



ماشین انیگما

انیگما نام دسته‌ای از ماشین‌های الکترومکانیکی مبتنی بر روتور است که برای رمزنگاری و رمزگشایی پیام‌های محرمانه بکار می‌رفته. ماشین انیگما در سالهای ۱۹۲۰ میلادی به عنوان یک محصول تجاری عرضه شد.



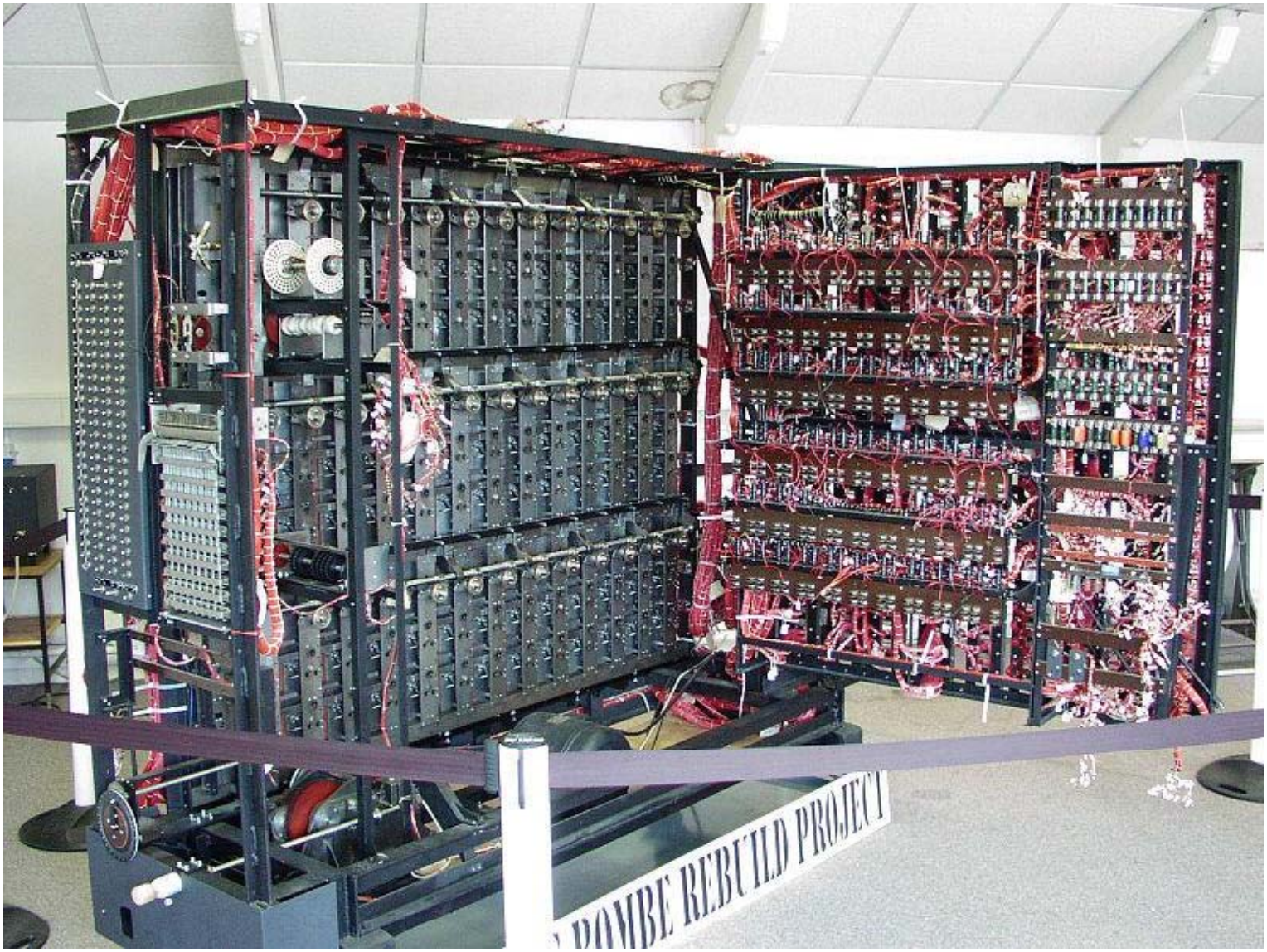
ارتش آلمان نازی مدل خاصی از این ماشین به نام انیگمای ورماخت را تولید نمود و به منظور رمزنگاری و رمزگشایی پیام‌های نظامی در طول جنگ جهانی دوم بکار برد. متفقین با بکارگیری اطلاعات بدست آمدن از جاسوسان، بررسی تجهیزات به غنیمت گرفته شده و تلاش دانشمندان و ریاضی‌دانان، از جمله آلن تورینگ، موفق به گشودن رمز پیامهای ارتش آلمان شدند.

ماشین بامب

در هفته‌های ورود به بلچلی پارک، تورینگ ماشینی الکترو مکانیکی طراحی کرده بود که می‌توانست انیگما را سریع تر از بامبای سال ۱۹۳۲ کد شکنی کند . بدلیل ساخت لهستانی الاصل آن بامبا، بامب نامگذاری شده.

بامب با بهسازی که توسط گوردونِ ولچمن صورت گرفت، تبدیل به یکی از وسایل اصلی وبطور عمده مکانیزه هجوم به پیام‌های توسط انیگمامحافظت شده آلمان‌ها گردید.

بامب تورینگ برای اولین با در ۱۸ مارس ۱۹۴۰ نصب شد . بیشتر از دویست بامب تا پایان جنگ جهانی مورد استفاده قرار گرفتند.


BOMBE REBUILD PROJECT

اصول ششگانه کرکهف

- آگوست کرکهف شهرت خود را از پژوهشهای زبانشناسی و کتابهایی که در این خصوص و زبان ولاپوک نوشته بود بدست آورد.
- او در سال ۱۸۸۳ دو مقاله با عنوان «رمز نگاری نظامی» منتشر کرد. در این دو مقاله شش اصل اساسی وجود داشت که اصل دوم آن به عنوان یکی از قوانین رمز نگاری هنوز هم مورد استفاده دانشمندان در رمز نگاری پیشرفته‌است :

اصول ششگانه کرکهف

- سیستم رمزنگاری اگر نه به لحاظ تئوری که در عمل غیر قابل شکست باشد.
- سیستم رمز نگاری نباید هیچ نکته پنهان و محرمانه‌ای داشته باشد. بلکه تنها چیزی که سری است کلید رمز است.
- کلید رمز باید به گونه‌ای قابل انتخاب باشد که اولاً بتوان براحتی آن را عوض کرد و ثانیاً بتوان آنرا به خاطر سپرد و نیازی به یاداشت کردن کلید رمز نباشد.

اصول ششگانه کرکهف

- متون رمز نگاری باید از طریق خطوط تلگراف قابل مخابره باشند.
- دستگاه رمز نگاری یا اسناد رمز شده باید توسط یکنفر قابل حمل و نقل باشد.
- سیستم رمزنگاری باید به سهولت قابل راه اندازی باشد.

رمزنگاری پیشرفته

- با پدید آمدن کامپیوترها و افزایش قدرت محاسباتی آنها، دانش رمزنگاری وارد حوزهٔ علوم کامپیوتری گردید و این پدیده، موجب بروز سه تغییر مهم در مسائل رمزنگاری شد:

رمزنگاری پیشرفته

- وجود قدرت محاسباتی بالا این امکان را پدید آورد که روش‌های پیچیده‌تر و مؤثرتری برای رمزنگاری به وجود آید.
- روش‌های رمزنگاری که تا قبل از آن اصولاً برای رمز کردن پیام به کار می‌رفتند، کاربردهای جدید و متعددی پیدا کردند.
- تا قبل از آن، رمزنگاری عمدتاً روی اطلاعات متنی و با استفاده از حروف الفبا انجام می‌گرفت؛ اما ورود کامپیوتر باعث شد که رمزنگاری روی انواع اطلاعات و بر مبنای بیت انجام شود.

تعاریف و اصطلاحات

عناصر مهمی که در رمزنگاری مورد استفاده قرار می‌گیرند به شرح زیر می‌باشد:

- متن آشکار (Plaintext / Clear text)
- پیام و اطلاعات را در حالت اصلی و قبل از تبدیل شدن به حالت رمز، متن آشکار یا اختصاراً پیام می‌نامند. در این حالت اطلاعات قابل فهم توسط انسان است.
- متن رمز (Cipher text)
- به پیام و اطلاعات بعد از درآمدن به حالت رمز، گفته می‌شود. اطلاعات رمز شده توسط انسان قابل فهم نیست.

تعاریف و اصطلاحات

- رمزگذاری (رمز کردن Encryption)
- عملیاتی است که با استفاده از کلید رمز، پیام را به رمز تبدیل می‌کند.
- رمزگشایی (باز کردن رمز Decryption)
- عملیاتی است که با استفاده از کلید رمز، پیام رمز شده را به پیام اصلی باز می‌گرداند. از نظر ریاضی، این الگوریتم عکس الگوریتم رمز کردن است.

تعاریف و اصطلاحات

- کلید رمز (Key)
- اطلاعاتی معمولاً عددی است که به عنوان پارامتر ورودی به الگوریتم رمز داده می‌شود و عملیات رمزگذاری و رمزگشایی با استفاده از آن انجام می‌گیرد. انواع مختلفی از کلیدهای رمز در رمزنگاری تعریف و استفاده می‌شود.

تعاریف و اصطلاحات

- می توان فرآیند رمزنگاری را، در سمت فرستنده، تابعی به شکل زیر تصور کرد:

C متن رمز
P متن آشکار
K کلید رمز

$$c = f(p, k)$$

تعاریف و اصطلاحات

- می توان فرآیند رمزنگاری را، در سمت گیرنده، تابعی به شکل زیر تصور کرد:

$$p = f^{-1}(c, k)$$

- رمزنگاری، مسئله نگاه داشتن یک پیام با طول بزرگ و دلخواه را به مسئله سری نگاه داشتن یک کلید کوتاه کاهش می دهد.

$$c = f(p,k)$$

$$p = f^{-1}(c,k)$$

سرویس رمزنگاری

- به طور کلی، سرویس رمزنگاری، به قابلیت و امکانی اطلاق می‌شود که بر اساس فنون رمزنگاری حاصل می‌گردد. قبل از ورود کامپیوترها به حوزه رمزنگاری، تقریباً کاربرد رمزنگاری محدود به رمز کردن پیام و پنهان کردن مفاد آن می‌شده است. اما در رمزنگاری پیشرفته سرویس‌های مختلفی از جمله موارد زیر ارائه گردیده‌است:

سرویس رمزنگاری

- محرمانگی یا امنیت محتوا
- ارسال یا ذخیره اطلاعات به نحوی که تنها افراد مجاز بتوانند از محتوای آن مطلع شوند، که همان سرویس اصلی و اولیهٔ پنهان کردن مفاد پیام است.
- سلامت محتوا
- به معنای ایجاد اطمینان از صحت اطلاعات و عدم تغییر محتوای اولیهٔ آن در حین ارسال است. تغییر محتوای اولیهٔ اطلاعات ممکن است به صورت اتفاقی (در اثر مشکلات مسیر ارسال) و یا به صورت عمدی باشد.

سرویس رمزنگاری

- احراز هویت یا اصالت محتوا
- به معنای تشخیص و ایجاد اطمینان از هویت ارسال‌کننده اطلاعات و عدم امکان جعل هویت افراد می‌باشد.
- عدم انکار
- به این معنی است که ارسال‌کنندهٔ اطلاعات نتواند در آینده ارسال آن را انکار یا مفاد آن را تکذیب نماید.

انواع سیستمهای رمزنگاری

به طور کلی سیستمهای رمزنگاری به دو دسته کلی تقسیم می شوند:

- رمزنگاری متقارن یا کلید خصوصی

Symmetric key cryptosystem

- رمزنگاری نامتقارن یا کلید عمومی

Public key cryptosystem

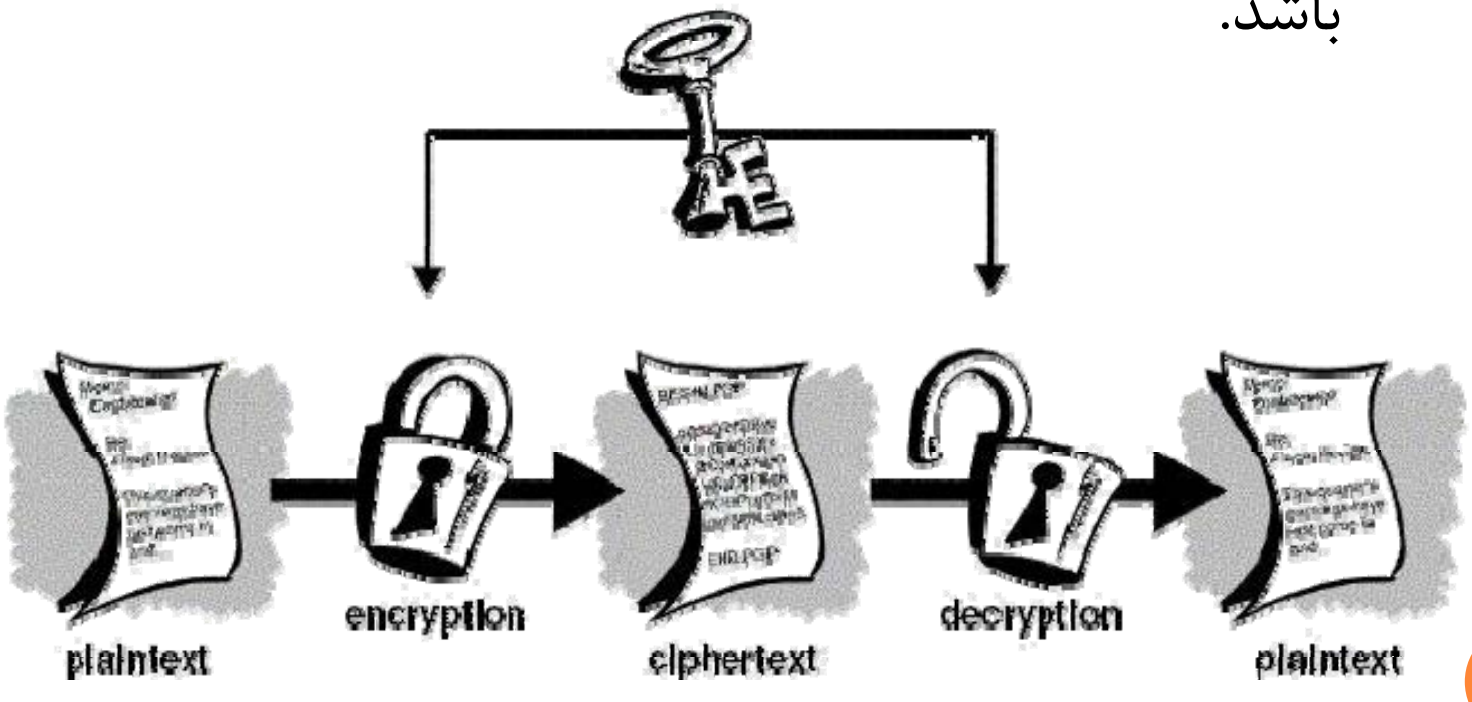
رمزنگاری متقارن

سایر اصطلاحات :

- Symmetric key cryptosystem
- Single key
- Private key
- Secret Key
- One key

رمزنگاری متقارن

در این روش، رمزنگاری و رمزگشایی اطلاعات با کلیدی مشابه صورت می گیرد. این کلید باید بین طرفین ارتباط توافق شده باشد.



ویژگی های کلی سیستمهای رمزنگاری متقارن

- سرعت بالا و امکان پیاده سازی نرم افزاری و سخت افزاری، به صورت بلادرنگ با سرعت مناسب
- رمزنگاری داده ها در قالب بلوکهایی با طول ثابت و عموماً کوتاه
- نیاز به توافق و رد و بدل کردن کلید رمز به روشی مطمئن
- نیاز به تعداد کلید بالا در ارتباطات چند طرفه و مشکل به خاطر سپاری یا نگهداری کلیدها در هر طرف
- در این روشها، معمولاً رمزنگاری چند دور (Round) تکرار می شود تا امنیت بالاتری ایجاد شود.
- تشابه عمل رمزنگاری و رمزگشایی (با تعویض متغیرها و ثابتها)

معرفی چند روش رمزنگاری متقارن و مدرن

- RC6
- Serpent
- IDEA
- AES
- 3-DES
- DES

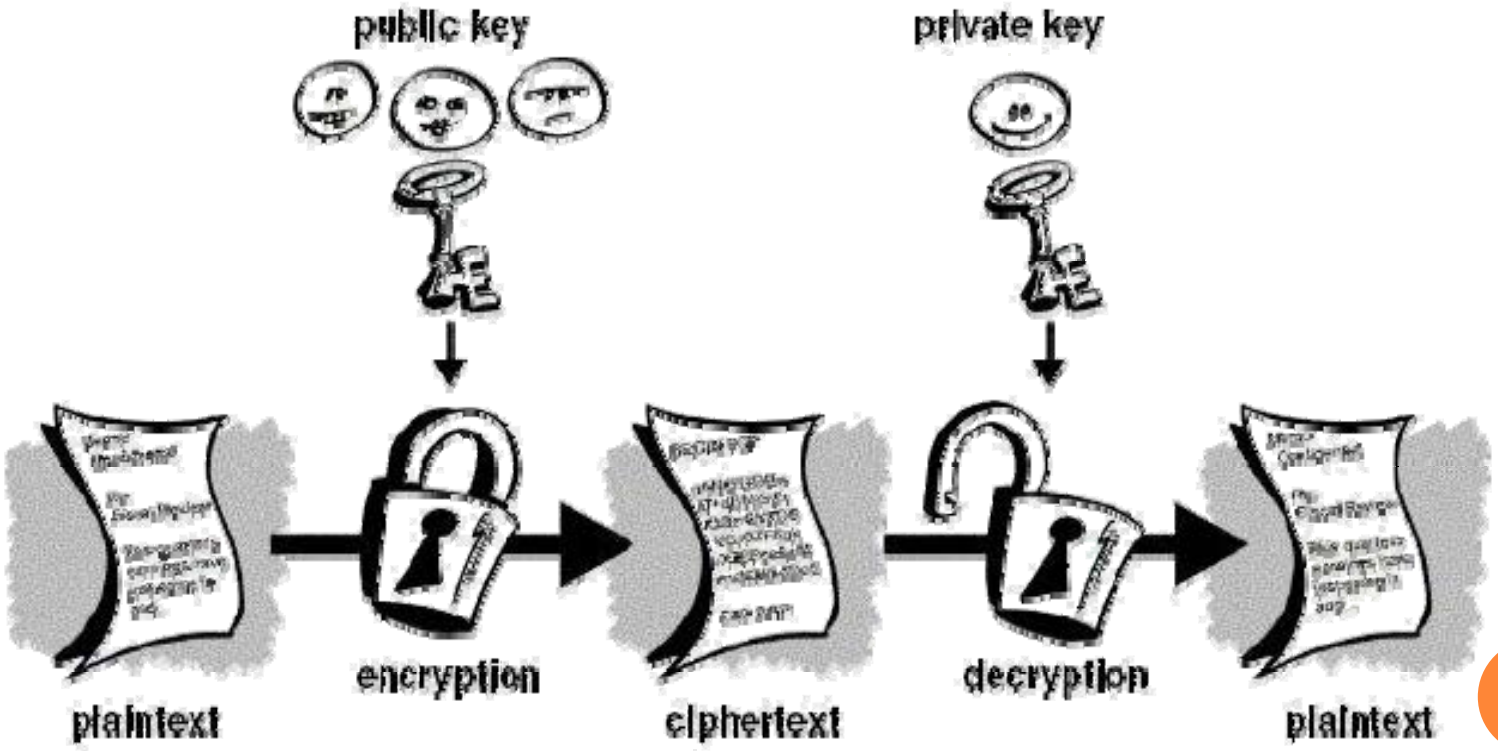
رمزنگاری کلید عمومی

سایر اصطلاحات :

- Asymmetric key cryptosystem
- Public key
- Double key

رمزنگاری کلید عمومی

در این روش از دو کلید عمومی (Public key) و کلید خصوصی (Private key) برای رمزنگاری و رمزگشایی استفاده می شود.



رمزنگاری کلید عمومی

قفلی را مجسم کنید که دارای دو کلید سبز و قرمز است، کلید سبز فقط در جهت ساعتگرد می چرخد و صرفاً می تواند آن را قفل کند ولی وقتی قفل بسته شد نمی توان با کلید سبز آن را باز کرد. این کلید می تواند در اختیار دوست و دشمن قرار گیرد.

در سمت مقابل کلید قرمز فقط در جهت عکس و برای باز کردن قفل می چرخد، این کلید نزد صاحب قفل می ماند و از آن مراقبت می شود. تجسم چنین قفلی در دنیای مجازی با الگوریتم رمزنگاری کلید عمومی تحقق یافته است.

رمزنگاری کلید عمومی

در این روش دو پارامتر به عنوان "کلید عمومی" و "کلید خصوصی" تعریف شده است. از "کلید عمومی" برای رمزنگاری استفاده می شود و به راحتی می توان آن را در اختیار دیگران قرار داد.

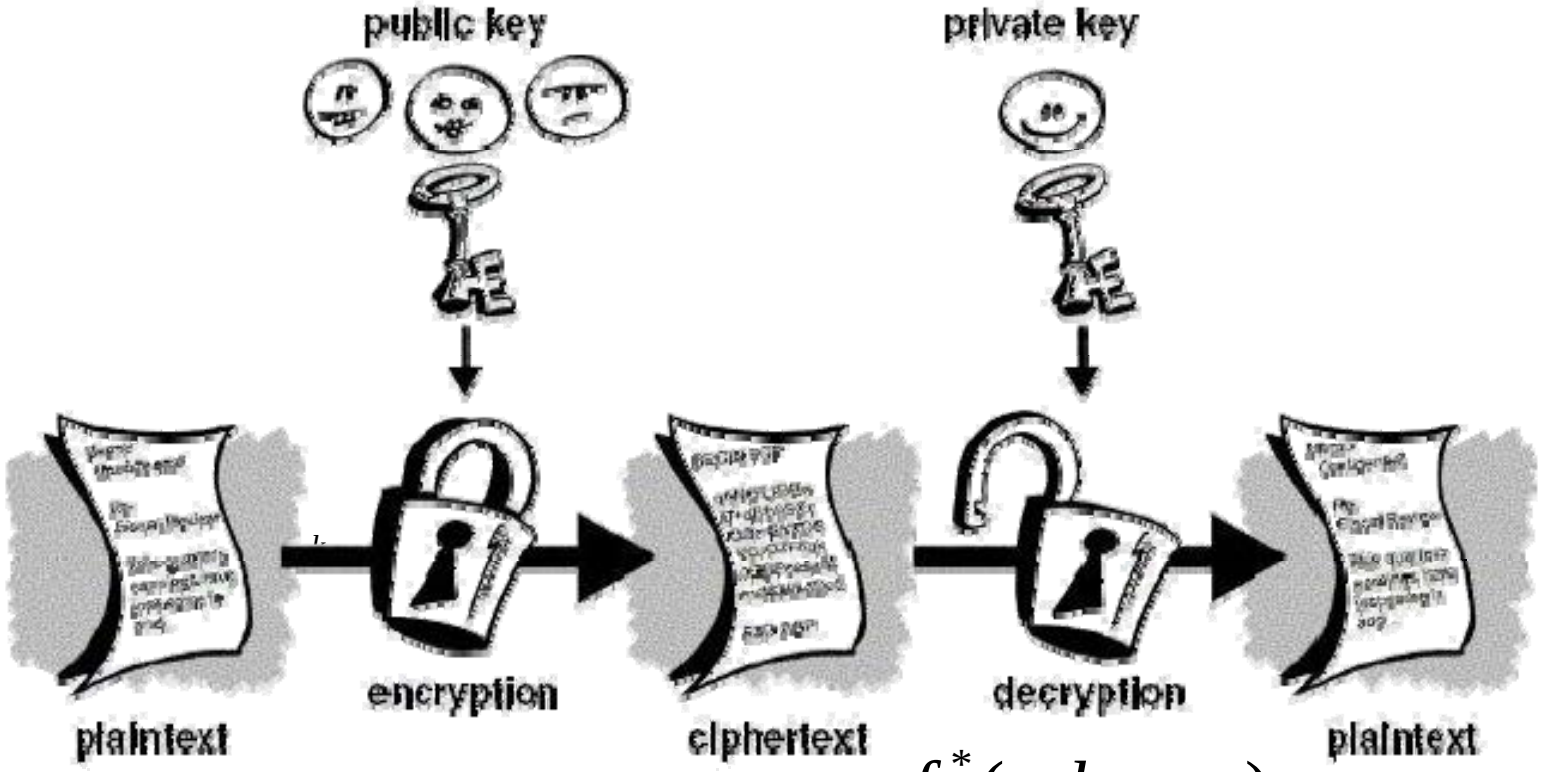
پارامتر "کلید خصوصی" در نزد صاحب آن، به صورت سری، می ماند و از آن برای رمزگشایی پیام رمز شده استفاده می شود.

در چنین روشی، برای یک ارتباط چند گانه، صرفاً به تعداد طرفین ارتباط به کلید نیاز می باشد.

اشکال بزرگ این روش در سرعت پایین آن است که استفاده از آن را برای کل پیام با اشکال مواجه می کند.

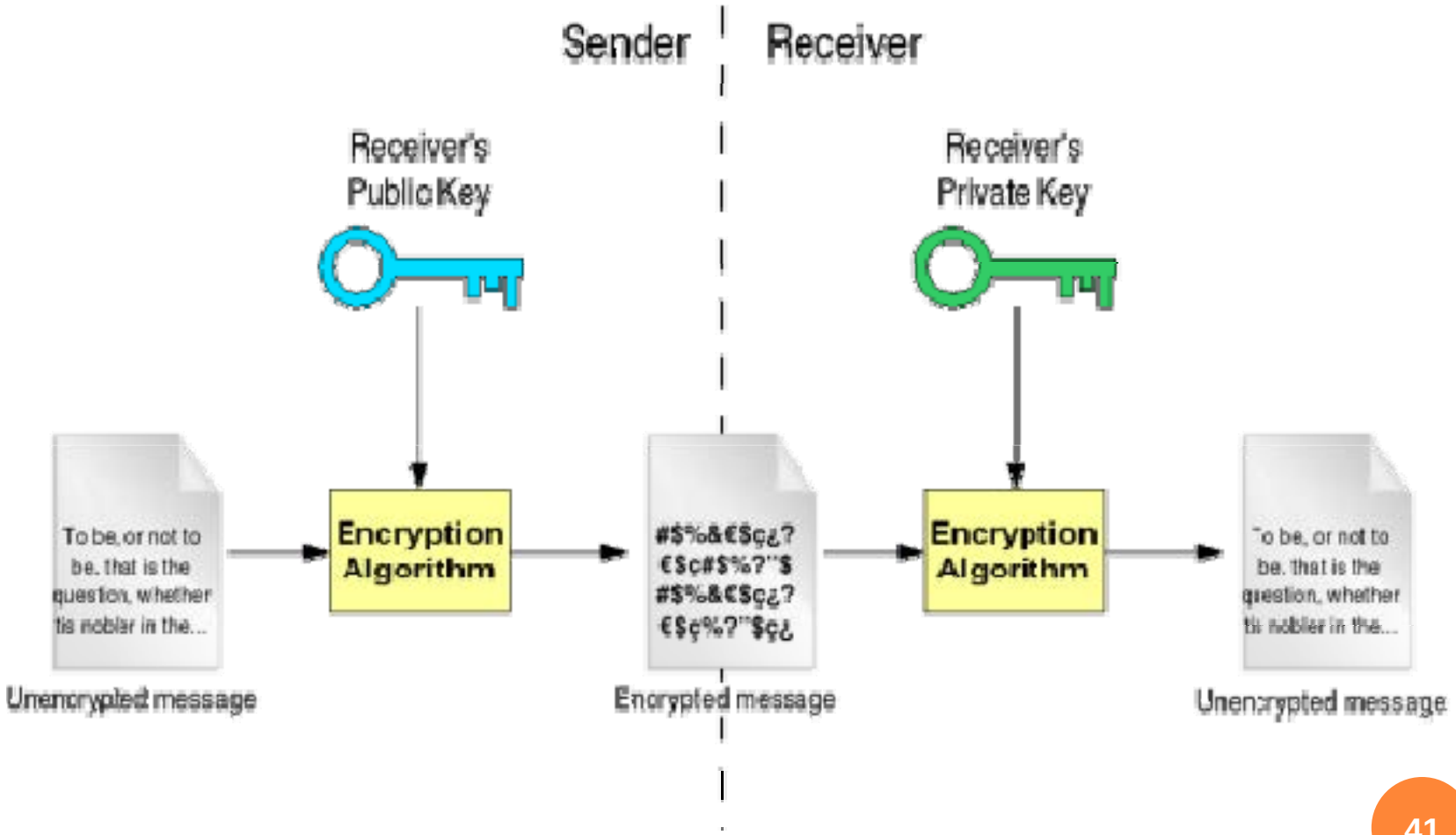
معرفی چند روش رمزنگاری نامتقارن و مدرن

- RSA
- ELGamal
- Diffie Hellman

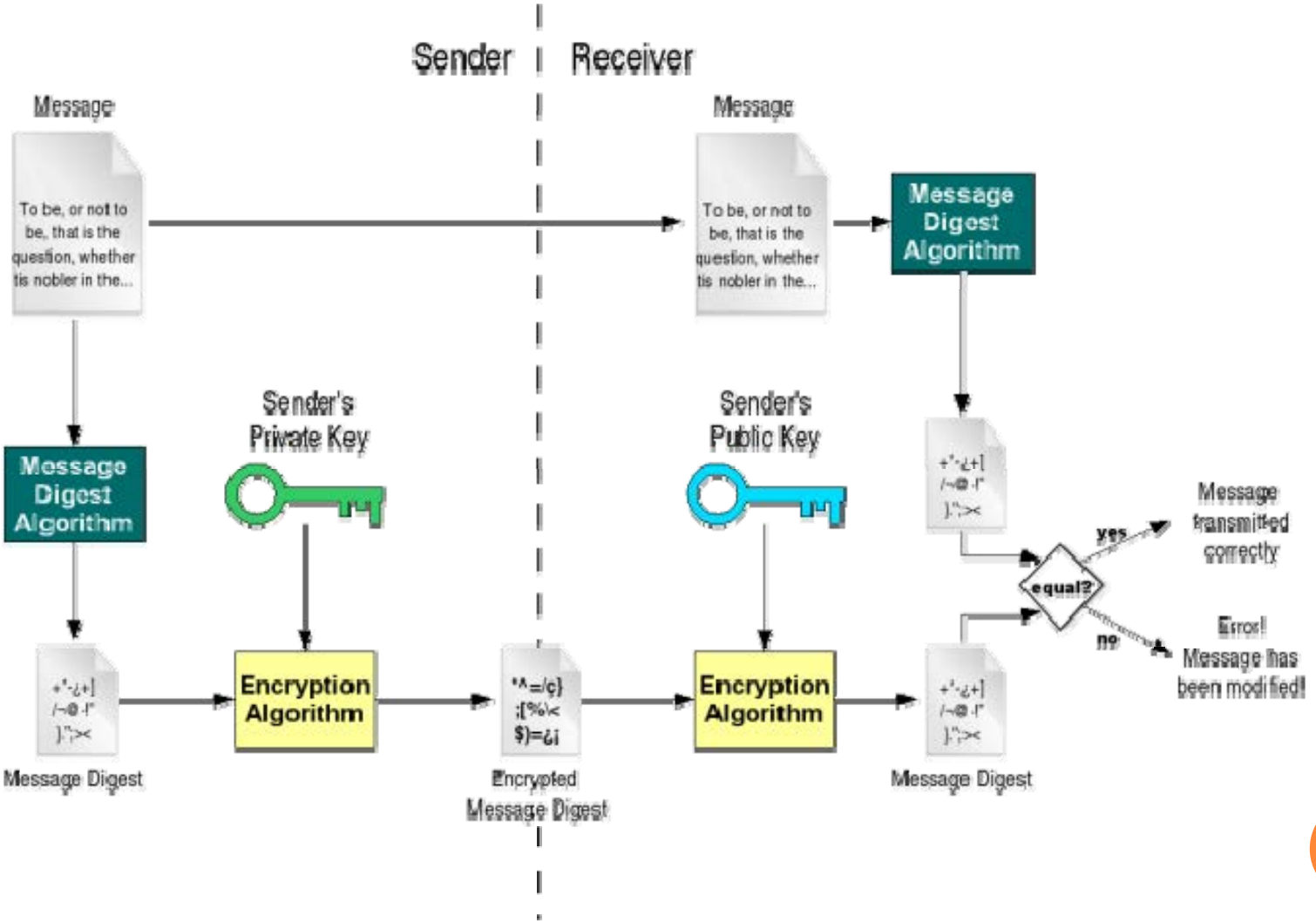

public key
private key
plaintext
encryption
ciphertext
decryption
plaintext

$$f^*(c, k_{private})$$

رمزنگاری نامتقارن



امضای دیجیتال



حساسیت کلید در روشهای متقارن و نامتقارن

- اولین اصل بنیادی در رمزنگاری اطلاعات، کافی بودن طول کلید است.
- "فضای کلید" (Key space) : کل تعداد حالاتی که باید بررسی شود تا یک کلید پیدا شود.
- Work Factor : به متوسط تعداد حالاتی گفته می شود که برای پیدا کردن یک کلید باید بررسی شود.
- به عنوان مثال درب یک کیف سامسونت، با رمز سه رقمی، می تواند به ۱۰۰۰ وضعیت مختلف تنظیم شود (فضای کلید) ولی سارق به طور متوسط با بررسی ۵۰۰ رمز (Work Factor) می تواند کلید یا رمز سامسونت را پیدا کند.

حساسیت کلید در روشهای متقارن و نامتقارن

- برای روشهای متقارن یک کلید ۱۲۸ بیتی کاملاً کفایت می کند. فضای کلیدی که چنین کلیدی ایجاد می کند معادل تعداد مولکولهای پانصد میلیارد تن آب است. اگر کسی بخواهد با سرعت یک میلیون کلید در ثانیه چنین فضایی را جستجو کند، زمانی به نتیجه می رسد که عمر خورشید به پایان رسیده باشد.

حساسیت کلید در روشهای متقارن و نامتقارن

- بحث کلید در روشهای رمزنگاری کلید عمومی کاملاً متفاوت است. در این روشها با توجه به اینکه انتخاب کلیدها تابع ضوابط خاصی است (اعداد اول) هرگاه رمزشکن بخواهد با جستجو و آزمون کلیدها رمزی را بشکند لازم نیست کل این فضا را جستجو کند (اعداد زوج، ضرایب ۳،۵ ۷و ... اعداد مربع، مکعب و ... از فضای جستجو حذف می شود)

پس ناحیه جستجو بسیار کوچک می شود، بنابراین در روشهای کلید عمومی حتی گاهی کلیدهای ۱۰۲۴ بیتی نیز کفایت نمی کند.

رمزشکنی و تحلیل رمز

- هرگاه کسی تلاش کند بدون جستجو و آزمون کل فضای کلید، و بر اساس ویژگیهای آماری متن رمز شده و ساختار "منطقی/ ریاضی" الگوریتم، کلید رمز را حدس بزند یا متنی را از رمز خارج کند، به این تلاش "رمزشکنی " (Cipher Breaking) یا "تحلیل رمز" (Cryptanalysis) گفته می شود.
- این روشها پایه علمی دارند و یک شاخه از علوم به حساب می آیند.

انواع رمزشکنی و تحلیل رمز

- Cipher text only (صرفاً متن رمز شده)
- در این حالت رمزشکن فقط اطلاعات رمز شده را در اختیار دارد و بدون هیچ اطلاع دیگری تلاش می کند آنرا از رمز خارج کند. در چنین وضعیتی حتی اگر بخشی از متن به دست بیاید تلاش رمز شکن موفق خواهد بود.

انواع رمزشکنی و تحلیل رمز

- Known plaintext (متن شناخته شده و آشکار)
- گاهی رمزشکن با وضعیتی مواجه است که متن رمز نشده و متن رمزنگاری شده را در اختیار دارد و هدف به دست آوردن کلید رمز می باشد.

انواع رمزشکنی و تحلیل رمز

- Chosen plaintext (متن انتخابی و شناخته شده)
- گاهی رمز شکن اطلاعات رمز شده و فقط بخش کوچکی از متن اصلی را در اختیار دارد و تلاش می کند کل متن اصلی یا بخشهایی از کلید رمز را به دست بیاورد.

حمله به رمز

- به هر گونه تلاش برای یافتن کلید، یا رمزگشایی غیر مجاز داده های رمز شده (در هر یک از وضعیتهای سه گانه گفته شده) اصطلاحاً حمله به رمز گفته می شود.

اصول اساسی رمز نگاری

- استحکام (Firmness)
- هر الگوریتم رمزنگاری، بایستی علیه حملات سه گانه گفته شده مستحکم بوده و نتیجه تلاش رمزشکن ناموفق و مأیوس کننده باشد. بعضی از الگوریتمهای رمزنگاری علیه بعضی از حملات فوق مقاوم نیستند. چنین روشهایی به طور عام بی ارزشند ولی در ترکیب با سایر روشها یا برای موارد خاص می توانند مورد استفاده قرار گیرند.

اصول اساسی رمز نگاری

- تازگی (Freshness)
- فرض کنید آلیس (مشتری) برای باب (اپراتور بانک) پیامی مهم و رمزنگاری شده، مبنی بر انتقال پول از حسابش به یک حساب دیگر ارسال می کند. فرض کنید شخص ثالثی پیام را دریافت می کند اما با توجه به استحکام آن موفق به شکست رمز آن نمی شود ولی یک هفته بعد همان پیام را از طرف آلیس، به دروغ، برای باب می فرستد و باب با رمزگشایی آن، عمل خواسته شده را انجام می دهد غافل از اینکه این پیام تکراری و دروغ است. بنابراین رمزنگاری اطلاعات اگر چه لازم است ولی هرگز کافی نیست. باید مکانیزمهایی در کنار فرآیند رمزنگاری اتخاذ شود تا از "حمله تکرار" (Reply Attack) پیشگیری شده و "تازگی پیامها" به اثبات برسد.

  مثلاً می توان از تاریخ و زمان و مهلت اعتبار یا یک شناسه ترتیبی یکتا استفاده کرد.

اصول اساسی رمز نگاری

- افزونگی (Redundancy)
- فرض کنید پیامی حاوی، شماره دانشجویی، شماره درس و نمره درس، برای بانک اطلاعاتی یک دانشگاه جهت ثبت نمره یک درس دانشجوی مورد نظر استفاده شود. در اینصورت اگر شخص ثالث حتی قادر به رمزگشایی این بسته نباشد می تواند با ایجاد تغییرات تصادفی مکرر در آن منجر به ثبت اطلاعات نادرست زیادی در بانک اطلاعاتی شود. بنابراین پیامها باید دارای افزونگی (اطلاعات اضافه) ، به نحو هوشمندی، باشند تا ایجاد هر تغییر تصادفی، با احتمال بالایی، پیام را نامعتبر نماید.

پروتکلهای رمزنگاری

- به طور کلی، یک پروتکل رمزنگاری، مجموعه‌ای از قواعد و روابط ریاضی است که چگونگیِ ترکیب کردن الگوریتم‌های رمزنگاری و استفاده از آن‌ها به منظور ارائه یک سرویس رمزنگاری خاص در یک کاربرد خاص را فراهم می‌سازد.

معمولاً یک پروتکل رمزنگاری مشخص می‌کند که:

- اطلاعات موجود در چه قالبی باید قرار گیرند.
- چه روشی برای تبدیل اطلاعات به عناصر ریاضی باید اجرا شود .
- کدامیک از الگوریتم‌های رمزنگاری و با کدام پارامترها باید مورد استفاده قرار گیرند .
- روابط ریاضی چگونه به اطلاعات عددی اعمال شوند .
- چه اطلاعاتی باید بین طرف ارسال‌کننده و دریافت‌کننده رد و بدل شود .
- چه مکانیسم ارتباطی برای انتقال اطلاعات مورد نیاز است.

انواع پروتکلهای امنیتی

عموماً پروتکلهای امنیتی در سه رده زیر دسته بندی می شوند:

- پروتکلهای مبتنی بر حکمیت عنصر ثالث

Arbitrated Protocol

- پروتکلهای مبتنی بر قضاوت ثانوی

Adjudicated Protocol

- پروتکلهای خوداتکا

Self Enforced Protocol

پروتکلهای مبتنی بر حکمیت عنصر ثالث

- کلیه تراکنشهای بین طرفین یک نشست از طریق یک عنصر ثالث که مورد وثوق همگان است نظارت و هماهنگی می شود.
- عنصر ثالث (حکم) در این پروتکل، کلید رمز همگان را می داند و تمام تعاملات رمزنگاری شده افراد از طریق او صورت می گیرد.
- در چنین پروتکلهایی، درستی عملکرد "عنصر حکمیت" و عدم نفوذپذیری آن نقش حیاتی دارد و می تواند منجر به بروز گلوگاه و نقطه حساس به خرابی در سیستم امنیتی شود.

پروتکلهای مبتنی بر قضاوت ثانوی

- یک عنصر ثالث در شبکه به عنوان ناظر بیرونی نقش بسیار کوتاه ولی کلیدی در تعاملات افراد ایفا می کند و بقیه تراکنشها را مستقیماً بر عهده طرفین یک نشست می گذارد.
- تا زمانیکه طرفین یک روال سالم و بی اشکال را دنبال می کنند عنصر ثالث حضور موثری ندارد ولی به محض ایجاد مشکل، وارد عمل می شود.
- با توجه به نقش کوتاه این پروتکلها در یک نشست، نقش مشکل "نقطه حساس به خرابی" و "تأخیر" کمتر خواهد شد.

پروتکلهای خوداتکا

- پروتکلهایی هستند که در آنها هیچ عنصر ثالثی وجود ندارد و بنابراین ماهیت پیچیده تری دارند، زیرا پشتوانه حقوقی ناظر را ندارند.

روش رمزنگاری سزار

- این روش قدیمی ترین روش رمزنگاری "جانشینی تک حرفی" (Mono Alphabetic Substitution) می باشد، که مبنای آن بر جانشینی هر حرف از جدول الفبا با حرف یا نماد دیگری می باشد.
- در روش سزار هر حرف الفباء با سه حرف بعدی جانشین می شود.

A	B	C	D	E	.	.	.
D	E	F	G	H	.	.	.

روش رمزنگاری سزار

- یا به عبارت ریاضی:

$$C=f(p)=(p+3) \bmod 26$$

- یا به صورت کلی تر با کلید k :

$$C=f(p,k)=(p+k) \bmod 26$$

در اینجا کلید، تعداد انتقال هر حرف را نشان می دهد.

جانشینی تک حرفی

- در این روش، حتی بدون شیفت و با یک ترتیب تصادفی حروف باز هم رمزنگاری محکم نیست اگرچه $26! = 10^{88}$ حالت مختلف، به اندازه کافی بزرگ است اما هر زبان دارای شاخص های مشخص و شناخته شده ای است که حتی با جاگذاری تصادفی حرف یا نماد دیگری نیز، با استفاده از آن، امکان شناسایی حرف اصلی وجود خواهد داشت.
- ضمناً هر زبان دارای یک دیکشنری می باشد، که با استفاده از آن، می توان ، حتی با داشتن چند حرف از یک کلمه، سازگارترین کلمه را شناسایی کرد.
- هرگاه یک سیستم رمزنگاری به صورت جانشینی تک حرفی عمل کند، رمزشکن به راحتی می تواند با تحلیل آماری کاراکترهای متن رمز و تطابق آن با نمودارهای مربوطه کاراکترهای جایگزین را شناسایی کند.

تناظر حروف الفبا و اعداد

کتابت یکی از مهمترین ابزارهای ارتباطی انسان می باشد . بوسیله نوشتن انسان می تواند بسیاری از تجربیات خود را در صفحات محفوظ نگاه داشته و برای نسل بعدی برجای بگذارد.
در دنیا زبانهای متفاوتی وجود دارند . براساس مناطق متفاوت زبان رایج هرملیت با لهجه ها و گویشهای متفاوت صحبت می شود .
با توجه به نکته بالا می توان دریافت که هر زبان دارای لهجه متفاوتی بوده و این تفاوت لهجه بر نوشتار زبان تاثیر گذاشته و املاء آن زبان نیز متفاوت خواهد بود . بعنوان مثال تعداد حروف در زبان فارسی ۳۲ حرف است که نحوه قرار گرفتن حروف در کنار هم ممکن است اصوات متفاوتی را بوجود بیاورد .

تناظر حروف الفبا و اعداد

اگر حروف زبان فارسی را با زبانهای دیگر مقایسه کنیم متوجه می شویم که حروف موجود، در زبانهای دیگر هم وجود دارند و حتی ممکن است برخی از حروف نیز وجود نداشته باشند بعنوان مثال در زبان عربی ۲۸ حرف وجود دارد و برای حروف گ ، ژ ، پ ، چ حروف متناظری وجود ندارد و یا ۲۶ زبان انگلیسی که برخی از حروف مانند خ ، ق و امثالهم با ترکیبی از حروف دیگر ساخته می شوند این تفاوت حتی در نحوه تلفظ حروف نیز ممکن است وجود داشته باشد بعنوان مثال حرف R در زبان انگلیسی که در زبان فرانسه ق تلفظ می شود .

اگر نمونه ای از یک متن را انتخاب کرده و حروف موجود در آن را مورد بررسی آماری قرار دهیم به نکات جالبی برخورد خواهیم کرد .

در بررسی انجام شده کلیه حروف موجود در متن یک داستان از "چالز دیکنز" به حروف کوچک تبدیل شده و فراوانی مربوط به هر حرف نیز محاسبه شده است نتیجه به دست امده به شرح زیر است:

درصد فراوانی	تعداد	حرف
7.69	9454	a
1.61	1979	b
2.54	3122	c
4.69	5764	d
12.26	15073	e
2.01	2468	f
2.46	3021	g
6.87	8454	h
6.88	8463	i
0.09	116	j
0.84	1038	k
3.77	4635	l
2.35	2885	m
6.56	8066	n
7.99	9821	o
1.75	2156	p
0.08	97	q
5.85	7192	r
6.51	8007	s
8.98	11049	t
2.74	3375	u
0.87	1070	v
2.53	3106	w
0.12	147	x
1.90	2332	y
0.07	88	z

تناظر حروف الفبا و اعداد

اگر زبانهای دیگر بجز زبان انگلیسی را نیز مانند بالا مورد بررسی قراردهیم مشاهده می کنیم که درصد فراوانی حروف متفاوت خواهد بود برای روشن تر شدن مطلب، یک متن آلمانی را بررسی می کنیم. طول کلمات و فراوانی تعداد حروف نسبت به متن اول متفاوت است حال اگر به صورت آماری متن دوم را بررسی کنیم نتایج زیر به دست خواهد آمد :

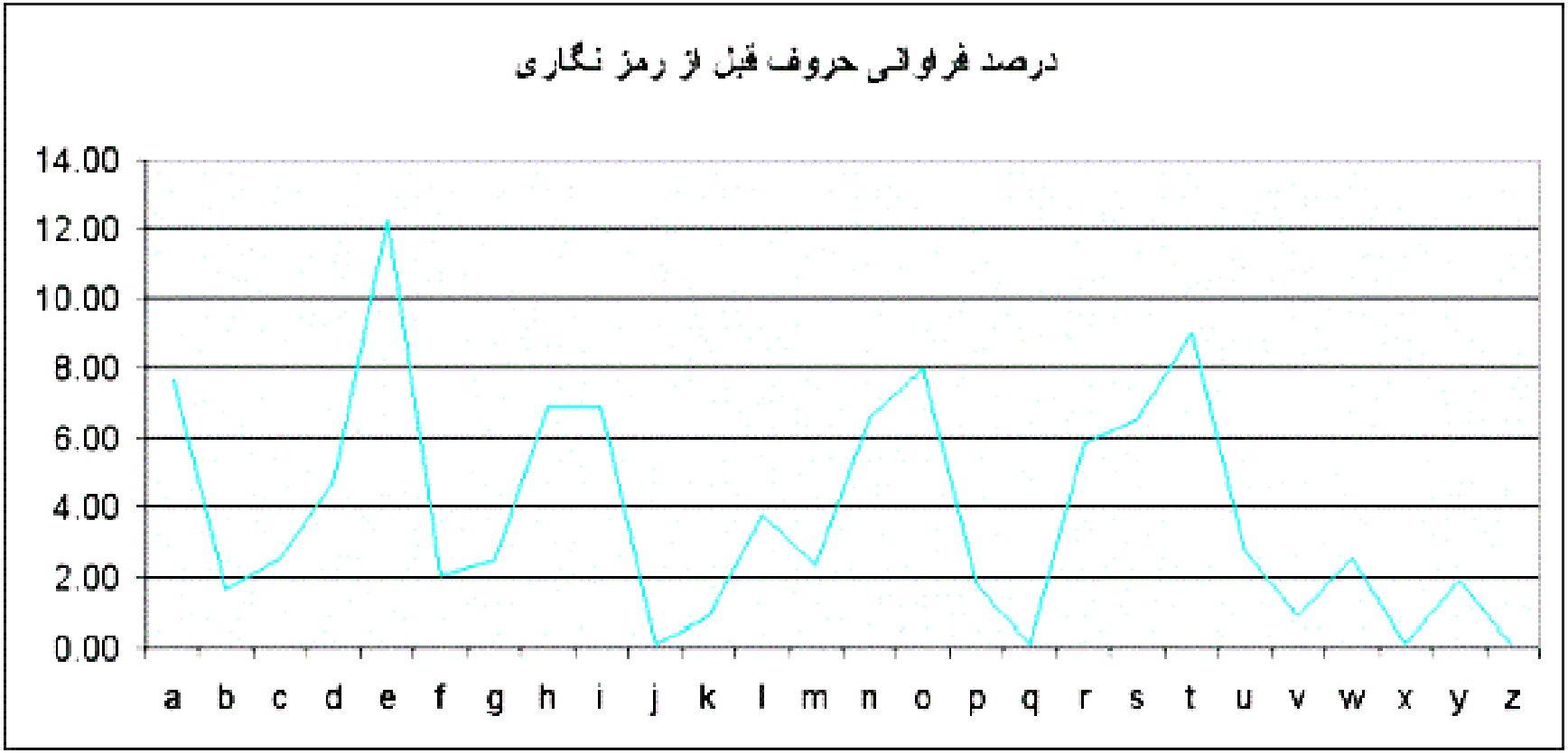
درصد فراوانی	تعداد	حرف
6.26	118	a
1.80	34	b
3.23	61	c
5.25	99	d
16.54	312	e
1.75	33	f
2.39	45	g
4.14	78	h
7.69	145	i
0.27	5	j
1.70	32	k
2.86	54	l
3.66	69	m
10.18	192	n
3.29	62	o
1.70	32	p
0.00	0	q
8.17	154	r
5.99	113	s
5.57	105	t
3.34	63	u
1.43	27	v
1.54	29	w
0.11	2	x
0.32	6	y
0.85	16	z

تناظر حروف الفبا و اعداد

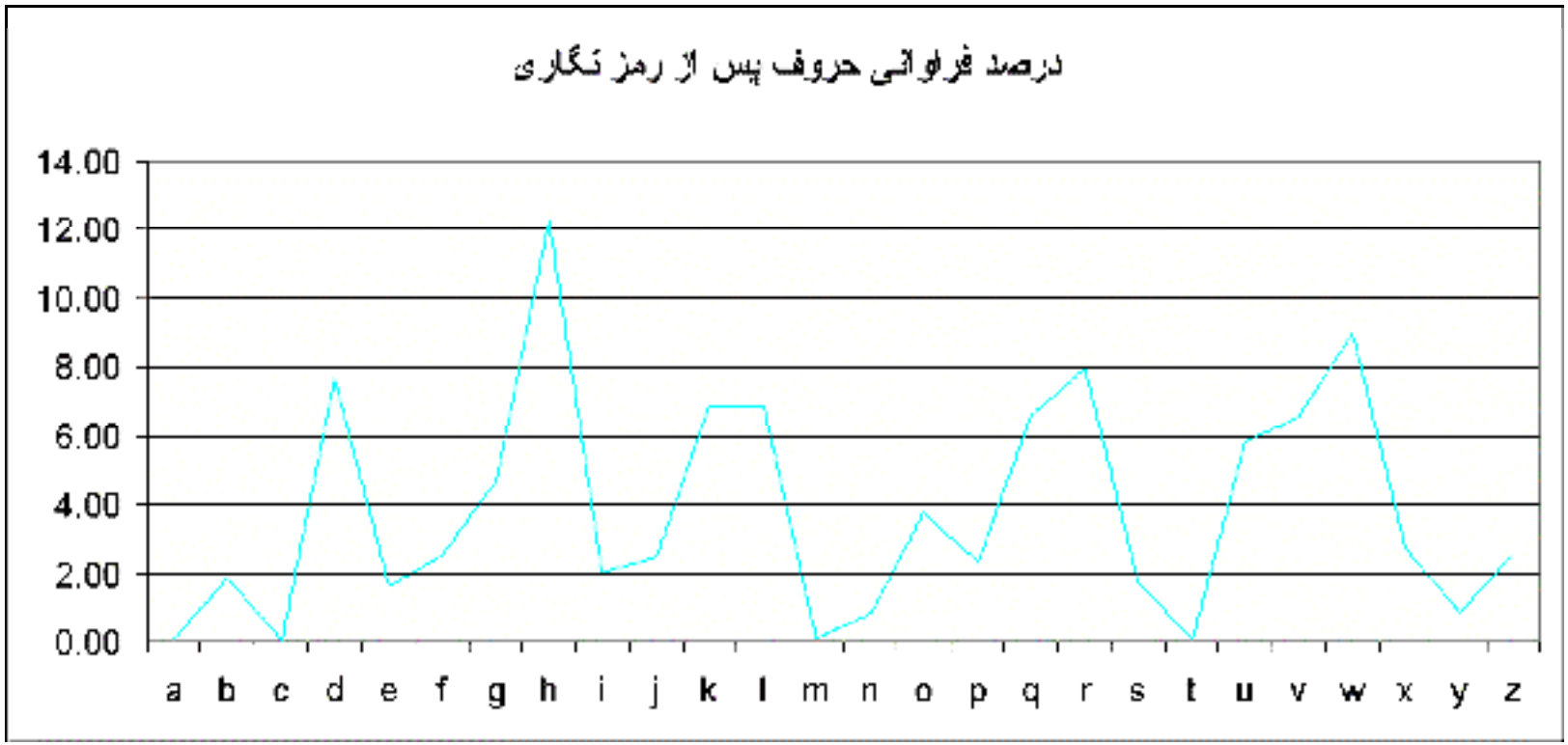
- با بررسی آماری دو متن ملاحظه میکنیم که حروف موجود در دو جدول دارای فراوانی متعددی هستند بعنوان مثال حرف n در متن انگلیسی دارای ۶.۵۶٪ و در متن آلمانی دارای فراوانی ۱۰.۱۸٪ می باشد همچنین حرفq در متن انگلیسی دارای فراوانی ۰.۰۸ ٪ و در متن آلمانی برابر صفر است.

حال اگر متون بالا را که مورد بررسی قرار دادیم با الگوریتمی نظیر سزار رمزنگاری کنیم با حروف موجود جای خود را به حروف دیگری در همان مجموعه حروف الفبا خواهند داد ولی فراوانی حروف در متن رمز شده تغیری نخواهد کرد.
شخصی که متصدی گشایش رمز است ابتدا به فراوانی حروف توجه کرده و پس از آن هر کدام از حروف را معادل حرفی قرار می دهد که فراوانی آن نزدیک به فراوانی اصلی حرف در نمونه مرجع باشد بنابراین متن رمز شده به سهولت استخراج می شود برای درک بهتر به نمودار هائی که در زیر آمده است توجه کنید .

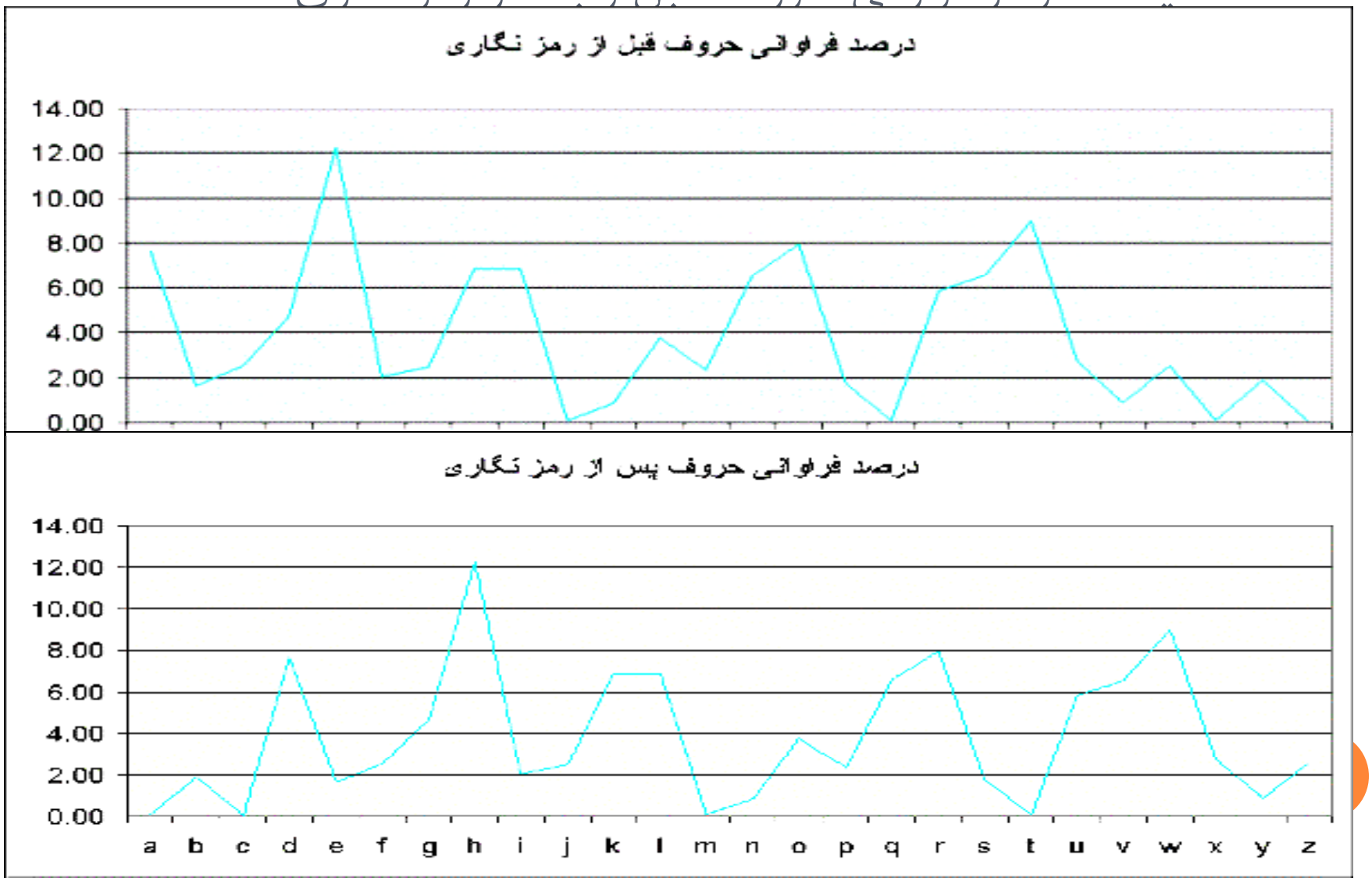
تناظر حروف الفبا و اعداد



- در نمودار به سهولت می توان فراوانی هر حرف را تشخیص داد حال اگر متن بالا را به روش سزار رمز کنید مشاهده میکنید که نمودار به مقدار سه واحد به سمت راست حرکت کرده , فراوانی حرف e به حرف h منتقل شده است



مقایسه نمودار فراوانی حروف، قبل و بعد از رمز نگاری



رمزنگاری دو حرفی PLAYFAIR

روش "پلی فر" در ۱۸۵۴ به دربار بریتانیا پیشنهاد شد.

در این روش برای رمزنگاری :

1. فواصل خالی حذف می شود.
2. متن دو حرف دو حرف تفکیک می شود.
3. در صورت وجود دوحرفی های مشدد، بین آنها x یا z قرار داده می شود.

رمزنگاری دو حرفی PLAYFAIR

4. جدولی ۵*۵ در نظر گرفته می شود.(معادل ۲۵ خانه، زیرا حروف انگلیسی ۲۶ حرف است و J و I معادل در نظر گرفته می شوند.)
5. کلید رمز از بالا و چپ، با حذف حروف تکراری، در جدول نوشته می شود.
6. سایر خانه های جدول، به ترتیب ، با حروف غایب جدول الفبا پر می شود.

اکنون جدول رمز آماده است. برای رمزنگاری، متن اصلی، دو حرف دو حرف، طبق روال زیر جایگزین می شود:

رمزنگاری دو حرفی PLAYFAIR

الف) هرگاه دو حرف اصلی در یک سطر جدول باشند، هر حرف با حرف سمت راست آن جایگذاری می شود.

ب) هرگاه دو حرف اصلی در یک ستون باشند، هر حرف با حرف زیرین آن جایگذاری می شود.

ج) هرگاه دو حرف اصلی در یک سطر و یک ستون نباشند، سطر محل حرف اول را ادامه می دهیم تا حرف محل تلاقی آن را با ستون حاوی حرف دوم را به دست آوریم.(حرف اول) آنگاه سطر حاوی حرف دوم را ادامه می دهیم تا حرف محل تلاقی آن را با ستون حاوی حرف اول به دست آوریم.(حرف دوم)

رمزنگاری دو حرفی PLAYFAIR

- طبق روال فوق، کل متن، به صورت دو حرف دو حرف رمز خواهد شد.
- برای رمزگشایی این روش کافی است، عکس همین روش را انجام داد.
- برای شکستن چنین رمزی، به راحتی می توان از شاخصهای آماری دو یا چند حرفی ها استفاده کرد. و نهایتاً نتایج را با دیکشنری تطابق داد، به همین دلیل این روش در قرن بیستم جایی ندارد.

مثال: رمزنگاری دو حرفی PLAYFAIR

- فرض کنید می خواهیم متن زیر را به روش Playfair با استفاده از کلید spaghetti رمزنگاری کنیم.

Plaintext: My daddy go back home

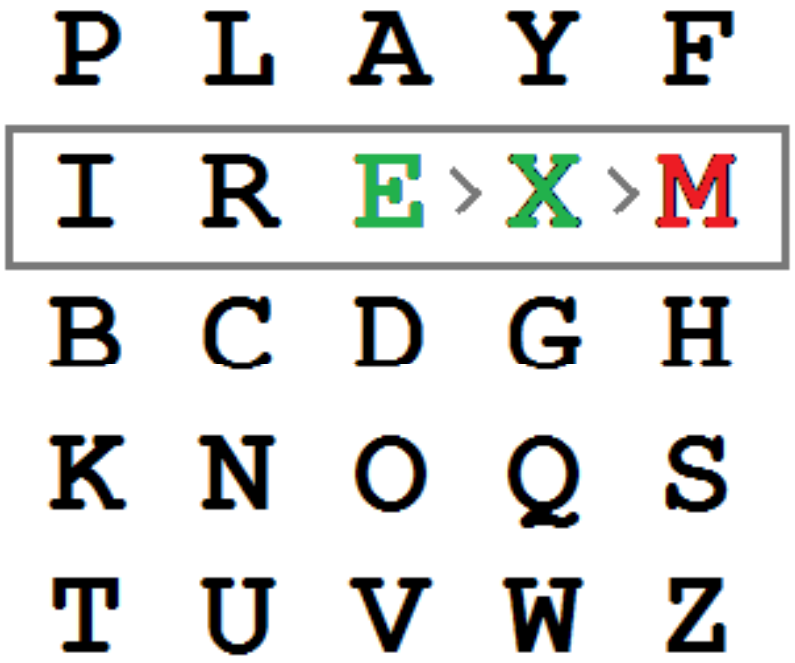
عملیات رمزنگاری و رمزگشایی مربوطه را مرحله به مرحله بنویسید.

مثال: رمزنگاری دو حرفی PLAYFAIR

- My daddy go back home
- Mydaddygobackhome
- My da dd yg ob ac kh om e
- My da dx dy go ba ck ho me

S	P	A	G	H
E	T	I	B	C
D	F	K	L	M
N	O	Q	R	U
V	W	X	Y	Z

مثال: رمزنگاری دو حرفی Playfair



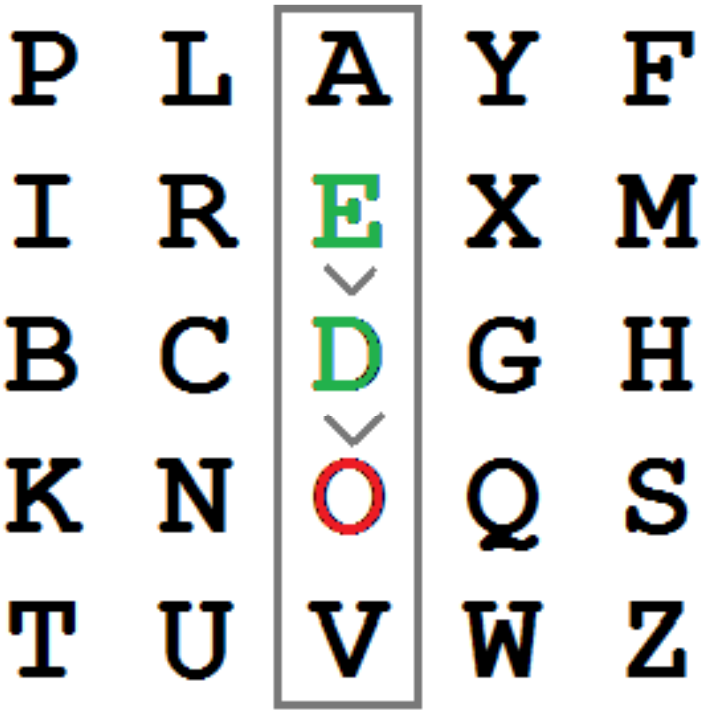
EX

Shape: Row

Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

مثال: رمزنگاری دو حرفی Playfair

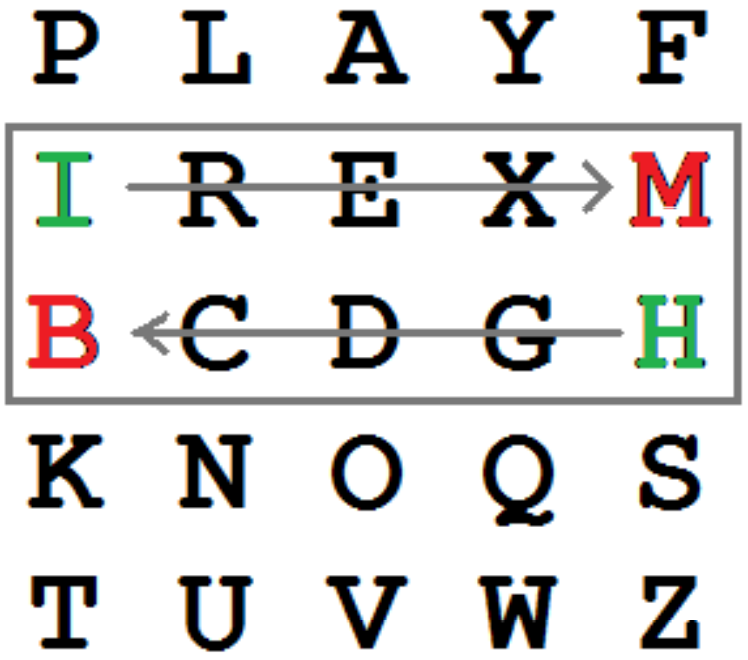


DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

مثال: رمزنگاری دو حرفی Playfair



HI

Shape: Rectangle
Rule: Pick Same Rows,
Opposite Corners

BM

رمزنگاری چند حرفی هیل

- Hill's Polyalphabetic cipher
- با توجه به وجود شاخص های آماری برای دو یا سه حرفی ها، در روش هیل از گروههای بیش از سه حرفی استفاده می شود.
- در این روش از جبر ماتریسی استفاده می شود.
- مراحل رمزنگاری به روش هیل عبارت است از:

1. هر حرف از الفبای انگلیسی با یک عدد صحیح، بین 0 تا 25 جایگزین می شود.
2. برای یک روش n حرفی، یک ماتریس ستونی n*1، برای هر گروه n حرفی ایجاد می شود.

رمزنگاری چند حرفی هیل

3. در این روش از یک ماتریس مربعی n*n به عنوان کلید استفاده می شود. (باید توجه داشت که دترمینان این ماتریس صفر نبوده و وارون پذیر باشد)
4. روش رمزنگاری هیل به صورت زیر نمایش داده می شود:

$$C=(k.p) \bmod 26$$

نهایتاً در این روش برای هر گروه n حرفی، یک ماتریس خطی n*1 رمزنگاری شده به دست می آید.

رمزنگاری چند حرفی هیل

- در رمزنگاری هیل هرچه طول گروههای n حرفی افزایش یابد، امنیت روش بهبود خواهد یافت ولی در عوض کلید رمز که همان ماتریس k است به شدت بزرگ شده و راهی جز یادداشت کردن آن باقی نمی ماند.
- در مجموع روش هیل به حمله مبتنی بر "متن شناخته شده" (Known plaintext) حساس است، چرا که خطی است و با داشتن تعداد کافی متن اصلی و معادل رمز شده آن می توان به کلید دست یافت.
- در فرآیند رمزگشایی از ماتریس وارون k استفاده می شود:

$$P=(k^{-1}.c) \bmod 26$$

مفهوم ماتریس معکوس یا وارون

- اگر A یک ماتریس مربعی باشد، A^{-1} ماتریس معکوس آن گفته می شود اگر:

$AA^{-1}=A^{-1}A=I$

- I ماتریس واحد یا یکه گفته می شود که عناصر روی قطر اصلی آن یک و سایر عناصر صفر است.
- برای به دست آوردن ماتریس معکوس:

$$A^{-1}=\frac{1}{|A|}A^{*}=\frac{1}{|A|}N^{T}$$

مفهوم ماتریس معکوس یا وارون

- در این رابطه $|A|$ دترمینان ماتریس A ، N ماتریس الحاقی و T ترانهاده آن را نشان می دهد.
- روابط مربوطه در زیر نشان داده شده است.

$$A=\begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix} \quad N=\begin{bmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{bmatrix}$$

مفهوم ماتریس معکوس یا وارون

$$N^T = \begin{bmatrix} M_{11} & M_{21} & M_{31} \\ M_{12} & M_{22} & M_{32} \\ M_{13} & M_{23} & M_{33} \end{bmatrix}$$

$$M_{23} = (-1)^{2+3} \begin{bmatrix} A_{11} & A_{12} \\ A_{31} & A_{32} \end{bmatrix}$$

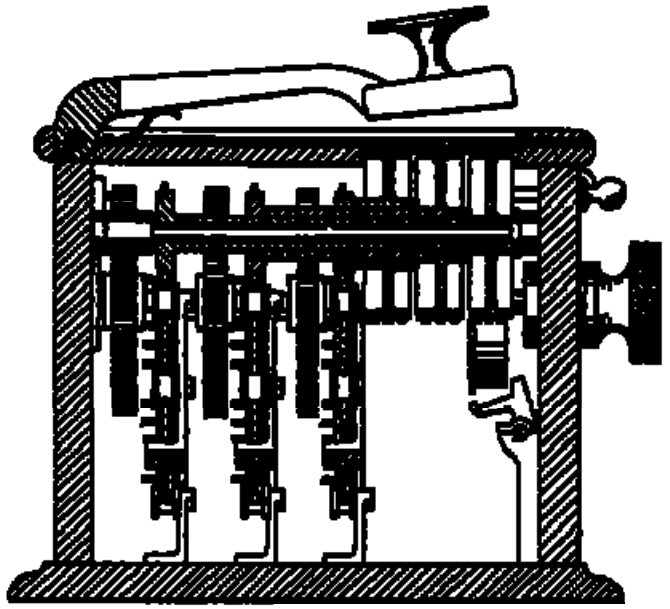
$$N = \begin{bmatrix} M_{11} & M_{12} & M_{13} \\ M_{21} & M_{22} & M_{23} \\ M_{31} & M_{32} & M_{33} \end{bmatrix}$$

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}$$

مثال : رمزنگاری چند حرفی هیل

- فرض کنید به روش رمزنگاری چند حرفی هیل می خواهیم سه حرف SOH را رمزنگاری و رمزگشایی کنیم. با استفاده از کلید K اینکار را انجام دهید.

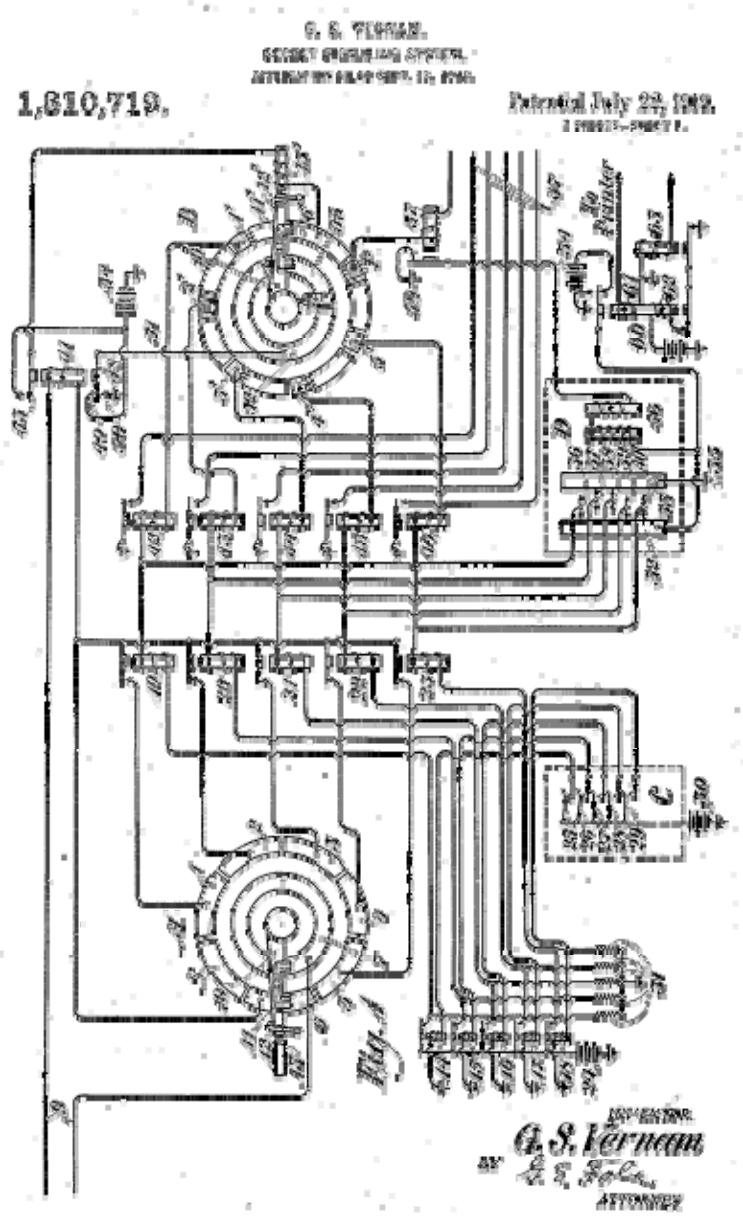
$$K = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 1 & 0 \\ 2 & 0 & 3 \end{bmatrix}$$



ماشین رمز نگاری "هیل"

رمزنگاری ONE TIME PAD

- این روش در سال ۱۹۱۸ توسط "Vernam" طراحی شد و به همین نام نیز خوانده می شود.
- در این روش از مفهوم عملگر XOR در ماشینهای تحریر برای رمزنگاری استفاده کرد.
- در این روش برای هر پیام یک کلید منحصر به فرد، به طول پیام اصلی لازم است که آنرا Pad می نامند.
- در این روش برای رمزنگاری پیامی به طول n از کلیدی تصادفی، مانند k، به طول n استفاده می شود که با پیام اصلی XOR شده و پیام رمزنگاری شده را تولید می کند.
- در سمت دیگر نیز کلید با پیام رمز XOR می شود تا پیام اصلی را تولید نماید.



- مدار پیشنهادی گیلبرت ورنام برای رمزنگاری متون

مثال: رمزنگاری One Time Pad

- رمزنگاری

$$11010011 \oplus 10101001 = 01111010$$

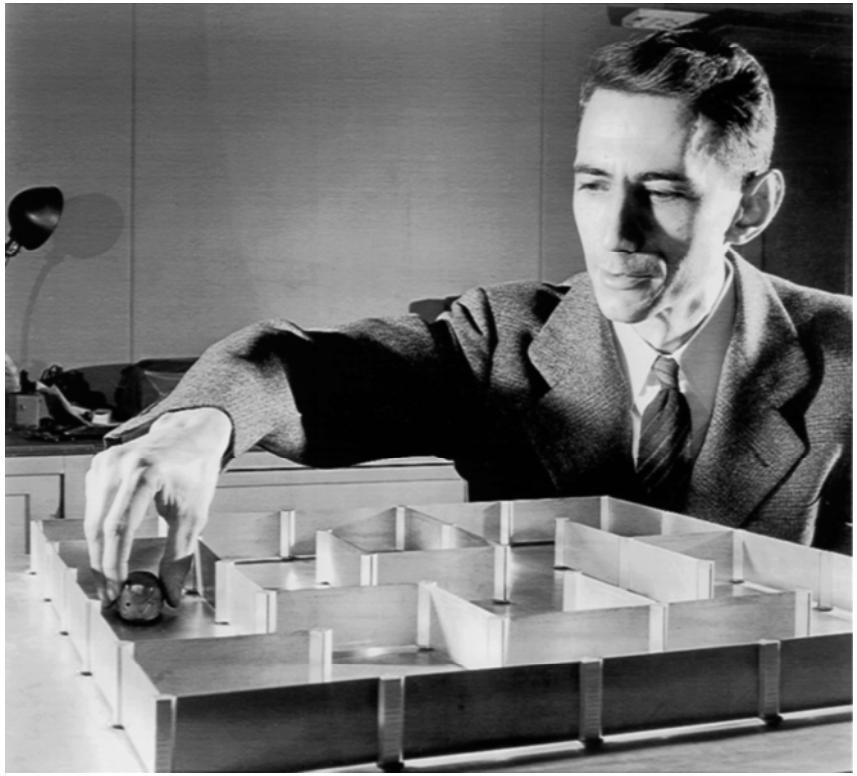
- رمزگشایی

$$01111010 \oplus 10101001 = 11010011$$

مزیت روش One Time Pad

- این روش "الگوی متعالی امنیت" نامیده شد، زیرا رمزشکن با هر توان محاسباتی و هر سطح از هوشمندی نمی تواند رمز را کشف کند.

شرایط روش رمزنگاری "بی قید و شرط امن"



- در ۱۹۴۹ "کلود شانون" اثبات کرد که هرگاه کلید رمز شرایط زیر را داشته باشد، رمزنگاری اطلاعات از طریق XOR کردن متن و کلید، "بی قید و شرط امن" خواهد بود و میزان توان محاسباتی و هوش رمزشکن هیچ تأثیری در شکستن رمز ندارد:

شرایط روش رمزنگاری "بی قید و شرط امن"

- شرط اول- دنباله بیتهای کلید به صورت کاملاً تصادفی انتخاب شود و احتمال صفر و یک بودن بیتهای کلید دقیقاً ۰.۵ و مستقل از یکدیگر باشد.
- شرط دوم- طول کلید و متن اصلی برابر باشد (در صورتیکه طول کلید کوتاهتر از متن اصلی باشد مجبور به تکرار کلید خواهیم شد که این موضوع شرط استقلال بیتهای کلید را مخدوش می کند)
- شرط سوم- برای رمزنگاری متون مختلف، هیچگاه از یک کلید دو بار استفاده نشود.

معایب روش One Time Pad

1. از آنجا که کلید باید از لحاظ طول، با اصل پیام هم اندازه باشد بنابراین هرگز در عمل نمی توان کلید را به خاطر سپرد. (بر خلاف اصول کرکهف)
2. چون برای پیامهای مختلف بایستی از Pad های متفاوت استفاده کرد و از هیچ Pad بیش از یکبار استفاده نمی شود لذا فرستنده و گیرنده مجبورند پیشاپیش تعداد زیادی Pad را از قبل توافق و ذخیره کنند.
3. حجم کل داده هایی که می تواند ارسال شود به حداکثر طول Pad بستگی دارد.

معایب روش One Time Pad

4. اگر گیرنده، به هر دلیل، فقط یک بیت از پیام رمز را از دست بدهد و آنرا تشخیص ندهد، مابقی بیتهای دریافتی از لحاظ ترتیب با Pad هماهنگ نیستند و مابقی متن از رمز خارج نخواهد شد.
5. تولید دنباله تصادفی Pad به "مولدهای شبه تصادفی" نیاز دارد.
6. روش One Time Pad به حملات Known Plaintext هرگز مقاوم نیست. زیرا

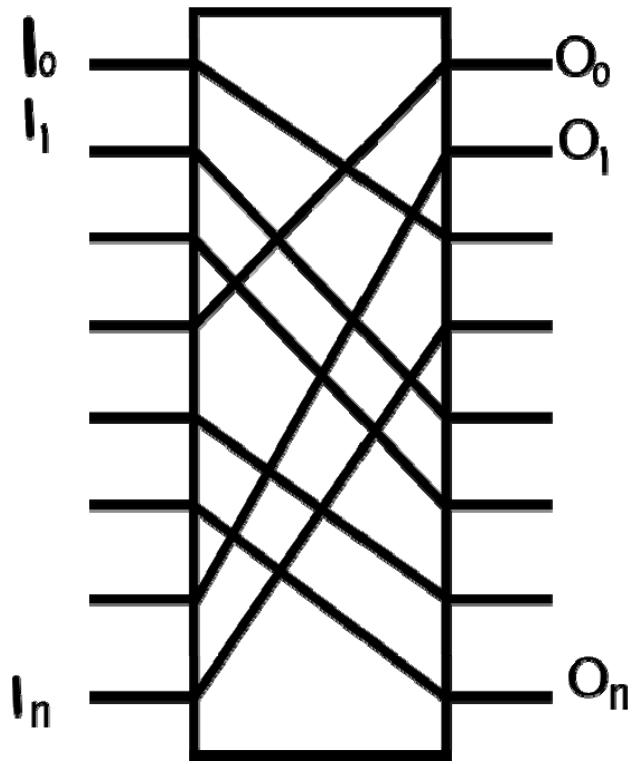
$$K = P \oplus C$$

اجزای سیستمهای رمزنگاری مدرن

- در سیستمهای رمزنگاری مدرن، داده ها در چندین مرحله (Round) درهم سازی می شوند و ضمن استفاده از عملگر پرقدرت XOR از اجزای درهم ساز دیگری نیز بهره می گیرند.
- یکی از ساده ترین مؤلفه های رمزنگاری که در ترکیب با دیگر اجزاء در بسیاری از روشهای مدرن و متقارن کاربرد دارد P-BOX و S-BOX است.

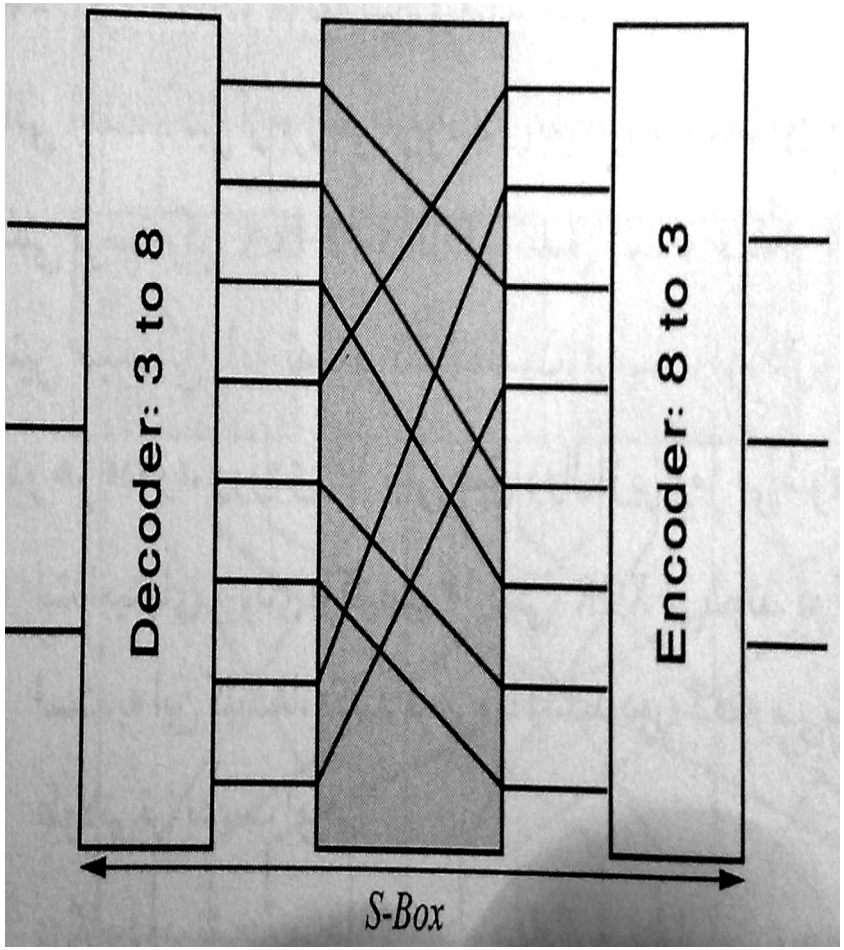
P-BOX

- جعبه جایگشت Permutation Box
- ابزاری است برای در هم ریختن بیتهای ورودی، به شکل دلخواه
- این ابزار بدون تغییر مقدار بیتها، صرفاً جای آنها را به هم می ریزد.



P-BOX

S-BOX



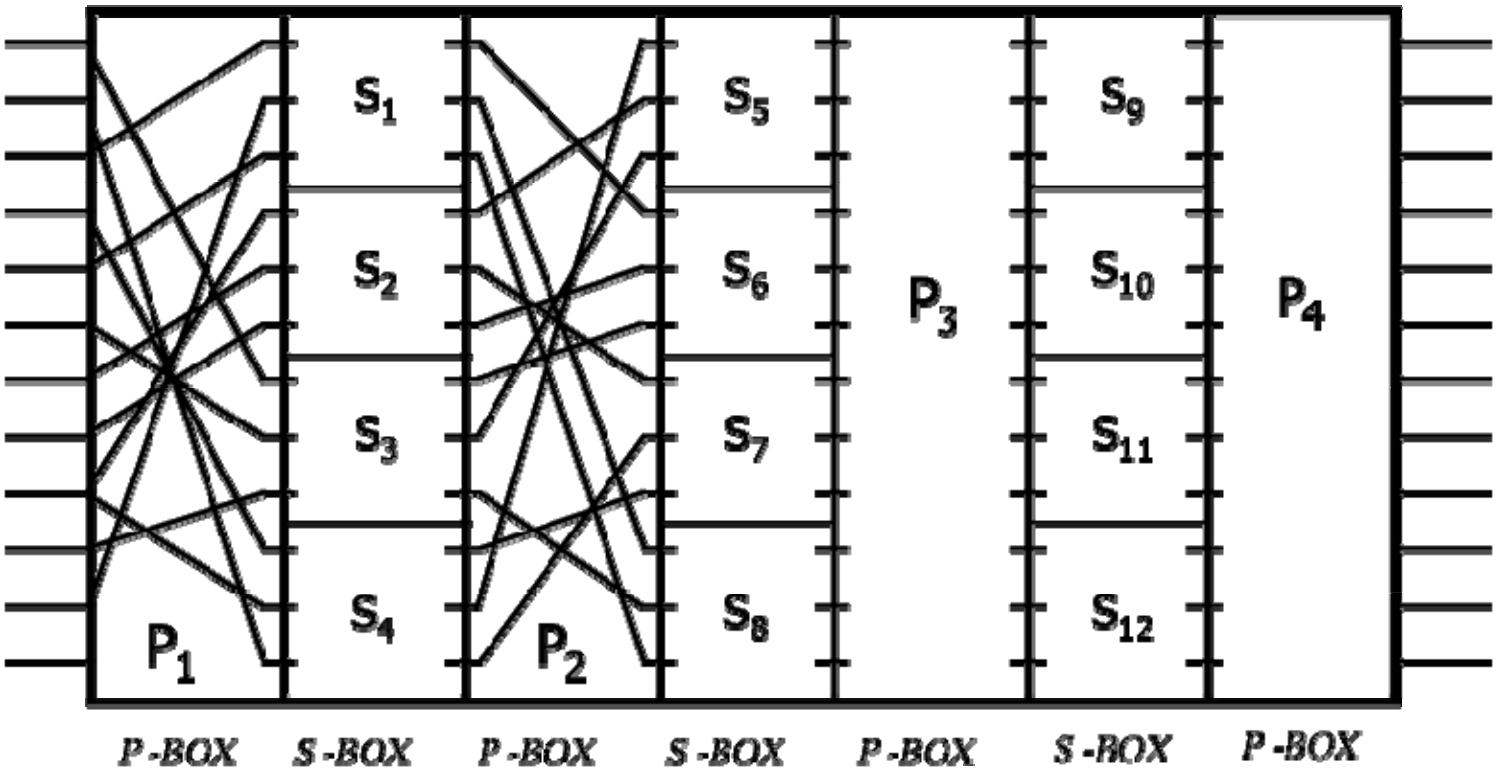
جعبه جانشینی

Substitution Box

برای ایجاد یک نگاشت دلخواه n به n استفاده می شود.

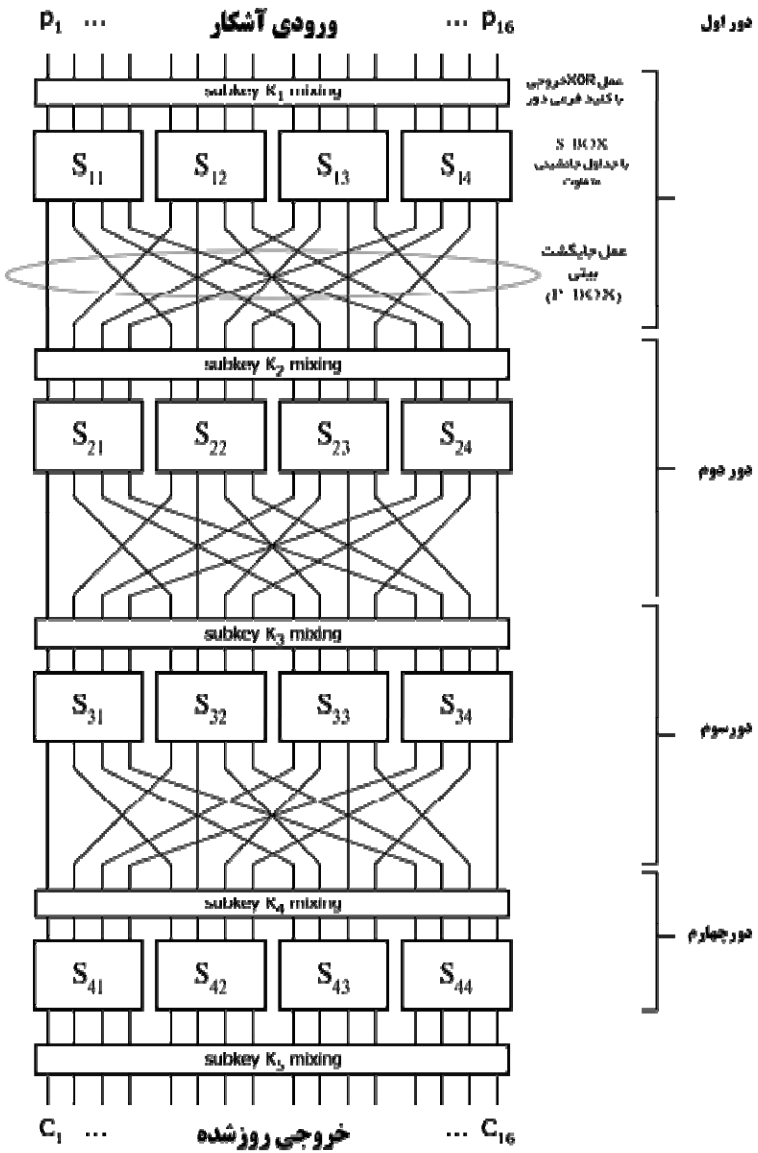
اشکال آن در مواردی است که تعداد ورودی ها بالاست. لذا در چنین مواردی از ترکیب مختلط آن استفاده می شود.

طراحی یک S-BOX مختلط ۱۲ در ۱۲



رمزنگاری SPN

- شبکه جانشینی و جایگشت کلید دار
- Substitution and Permiutation Network
- P-BOX و S-BOX دو مؤلفه بنیادی برای سیستمهای رمزنگاری مدرن می باشند ولی به تنهایی کافی نیستند.
- در SPN از سه رکن S-BOX ، P-BOX و تلفیق کلید با عملگر XOR در چند Round باکلیدهای متفاوت، در هر Round استفاده می شود.


P_1 ... ورودی آشکار ... P_{16}
دور اول
عمل XORخروجی با کلید فرعی دور
S BOX با جداول جانشینی متفاوت
عمل جایگشت بیتی (P BOX)
subkey K_1 mixing
S_{11} S_{12} S_{13} S_{14}
subkey K_2 mixing
S_{21} S_{22} S_{23} S_{24}
دور دوم
subkey K_3 mixing
S_{31} S_{32} S_{33} S_{34}
دورسوم
subkey K_4 mixing
S_{41} S_{42} S_{43} S_{44}
دورچهارم
subkey K_5 mixing
C_1 ... خروجی روزشده ... C_{16}

ویژگیهای بنیادین سیستمهای مدرن رمزنگاری متقارن

هر سیستم رمزنگاری مدرن باید در بالاترین سطح ممکن دارای دو ویژگی "پخش و پراکنده سازی" (Diffusion) و "گمراه کنندگی" (Confusion) باشد. این دو اصطلاح در ۱۹۴۹ توسط "کلود شانون" (پدر تئوری اطلاعات) معرفی و از آن پس مورد استناد قرار گرفت.

DIFFUSION

پخش و پراکنده سازی

- سیستم رمزنگار باید ساختار و کل شاخصهای آماری متن را بر روی کل متن رمزشده، توزیع و پراکنده کند.
- به بیان دیگر یک سیستم رمزنگار هرگز نباید ویژگی های آماری متن را، به هر نحو، در خروجی رمز شده منتقل کند.
- بدین ترتیب هرگاه خروجی یک سیستم رمزنگار را تحلیل آماری می کنید، نباید هیچگونه "همبستگی" (Correlation) بین خروجی، کلید و بیتهای متن رویت شود.

CONFUSION

گمراه کنندگی

- گمراه کنندگی بدین معناست که، در عمل، هرگز نباید بتوان بین ورودی، خروجی و کلید هیچ رابطه سرراست و مشخصی پیدا کرد.
- به بیان دیگر، پیچیدگی یک سیستم رمزنگاری متقارن باید آنقدر زیاد و ژرف باشد که استنتاج رابطه ای که بر اساس آن، خروجی سیستم بر حسب کلید و ورودی به دست می آید، در عمل ممکن نباشد.

- در ادامه هفت ویژگی مهم دیگر سیستمهای رمزنگار متقارن خوب را ملاحظه می کنید:

AVALANCHE EFFECT اثر فروپاشی بهمنی

- اثر فروپاشی بهمنی، در سیستمهای رمزنگاری متقارن، بدین معناست که یک تغییر بسیار جزئی در ورودی یا کلید (حتی به اندازه یک بیت) به طرز بسیار گسترده، غیرقابل پیش بینی و غیر متمرکز، خروجی را تغییر داده و متحول کند و در عین حال هیچ شاخص آماری از این تغییر بر جای نگذارد.

PSEUDO-NOISE PRODUCTION تولید شبه نویز

- هرگاه خروجی رمزنگار را به ازای هزاران ورودی یا کلید مختلف مشاهده می کنید، باید آن را شبیه به یک دنباله کاملاً تصادفی، مستقل از ورودی، مستقل از کلید و بدون هیچ شاخص آماری مرتبط با متن، ارزیابی کنید. چنین سیستمی به اصطلاح "دنباله شبه نویز" تولید می کند.

رعایت اصل دوم کرکهف

- آگاهی از جزئیات الگوریتم رمزنگاری، هرگز نباید سبب تضعیف آن شود و امنیت الگوریتم صرفاً باید در گرو مخفی نگه داشتن کلید سری باشد.
- مخفی نگه داشتن کلیات روش (شامل الگوریتم و مراحل رمزنگاری) و جزئیات روش (شامل جداول جانشینی، ترتیب جایگشت، ماهیت ثابت ها و متغیرها و استدلال هر عمل) هرگز، در بلند مدت، کمکی به امنیت و استحکام روش نمی کند.

وجود مؤلفه های غیرخطی

- در الگوریتمهای رمزنگاری متقارن باید از مؤلفه های غیر خطی استفاده شود.
- به عنوان مثال S-BOX با جدول جانشینی مناسب می تواند به شدت غیرخطی عمل کند، در حالیکه جایگشت بیتی یا جمع معمولی فرآیندی خطی است.
- عدم وجود عناصر غیرخطی در یک سیستم رمزنگار متقارن در تضاد با ویژگی گمراه کنندگی آن است، زیرا بیتهای ورودی و کلید، با رابطه خطی، خروجی را توصیف کرده و در نتیجه امکان تشخیص خروجی بر حسب ورودی وجود خواهد داشت.

مفهوم تابع غیرخطی

- تابعی مانند f را غیرخطی گوییم اگر:

$$f(a+b) \neq f(a) + f(b)$$

- تابعی مانند f را به شدت غیرخطی گوییم هرگاه نه تنها خطی نباشد بلکه حتی تخمین آن نیز به صورت زیر غیر ممکن باشد:

$$f(a+b) = g_0(f(a)) + g_1(f(b))$$

برابری طول خروجی با ورودی

- سیستم رمزنگار متقارن حق ندارد طول داده ها را افزایش دهد یا از آن بکاهد.
- طول ورودی و خروجی، معمولاً ضمن یکسان بودن ثابت است.

عدم امکان مدلسازی رمزنگار با روابط جبری

- الگوریتم باید چنان پیچیده و گمراه کننده باشد که هرگز نتوان آن را با رابطه جبری (حتی به صورت تقریبی) مدل کرد.

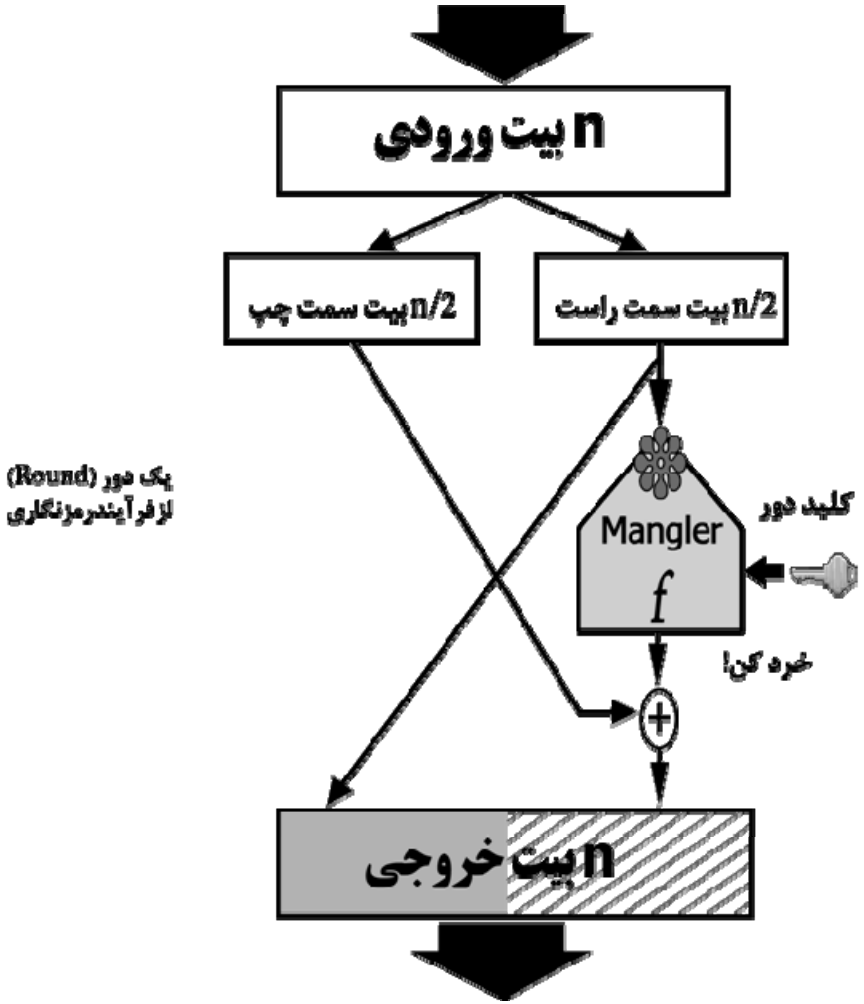
قدرت تمام کلیدها

- نباید بین کلیدها، در فضای حالت، تفاوتی وجود داشته باشد.
- چیزی به عنوان کلید ضعیف یا قوی نباید برای الگوریتم وجود داشته باشد. به عنوان مثال اگر کلید تماماً 0 یا 1 نیز در نظر گرفته شود نباید خروجی ویژگی قابل تشخیصی از خود نشان دهد.

FEISTEL

معماری رمز فیستل

- "هارست فیستل" از پژوهشگران شرکت IBM الگویی عام برای رمزنگاری متقارن پیشنهاد کرد که برای حدود ۳۰ سال مورد توجه بود و بسیاری از روشهای مدرن رمزنگاری بر اساس معماری رو طراحی شدند.


n بیت ورودی
n/2 بیت سمت چپ
n/2 بیت سمت راست
یک دور (Round)
از فرآیند رمزنگاری
Mangler
f
کلید دور
خرد کن!
n بیت خروجی

ویژگیهای معماری رمز فیستل

1. رمزنگاری مشتمل بر تعدادی مرحله تکراری و مشابه است که دور (Round) نامیده می شوند. در هر دور فقط کلید رمز (Round key-Subkey) و احتمالاً ثابتها تغییر می کنند و ماهیت عمل در تمام دورها یکسان است.
2. ورودی هر دور به دو نیمه چپ و راست تقسیم شده و در هر دور یک نیمه از ورودی دست نخورده باقی می ماند در حالیکه نیمه دوم بر اساس ترکیبی بسیار پیچیده و به شدت غیرخطی از نیمه اول و دوم و کلید، رمزنگاری می شود.
3. برای رمزنگاری هر دور، در اختیار داشتن نیمه دست نخورده و کلید دور، کافی است.
4. پس از هر دور باید جای دو نیمه، تعویض شود تا نیمه دست نخورده در دور بعدی مشمول عمل رمزنگاری شود.

ویژگیهای معماری رمز فیستل

5. فرایند رمزنگاری یک نیمه از ورودی، در هر دور، باید توسط تابعی به نام "تابع خردکن" (Mangler) انجام شود که به شدت غیرخطی وغیرجبری است. استحکام و سرعت سیستم رمزنگاری در گرو ماهیت درونی این تابع است.
6. برای انجام رمزگشایی به معکوس تابع خردکن نیازی نیست. بلکه با اعمال مجدد این تابع بر روی پارامترهای ورودی هر دور (شامل کلید و نیمه چپ و راست) رمزگشایی صورت می گیرد. این ویژگی موجب شباهت عملیات رمزنگاری و رمزگشایی و در نتیجه استفاده از سخت افزار یکسان می شود.
7. تعداد دورها باید به قدری زیاد باشد که دنبال کردن رابطه ورودی، خروجی و کلید، در عمل غیر ممکن باشد (بین ۱۰ تا ۳۲ دور مرسوم است) افزایش دورها ویژگی گمراه کنندگی را افزایش خواهد داد.

ویژگیهای معماری رمز فیستل

8. هر دور باید کلید منحصر به فردی داشته باشد. در عین حال کلیدهای فرعی باید به روش نامتعارف و پیچیده ای از یک کلید اصلی (شاه کلید) تولید شوند. این روش تعیین کننده استحکام رمزنگاری است.
9. روش تولید کلیدهای فرعی، از شاه کلید، حتماً باید یکطرفه (One Way) باشد تا حتی با لو رفتن کلیدهای فرعی امکان کشف شاه کلید وجود نداشته باشد.

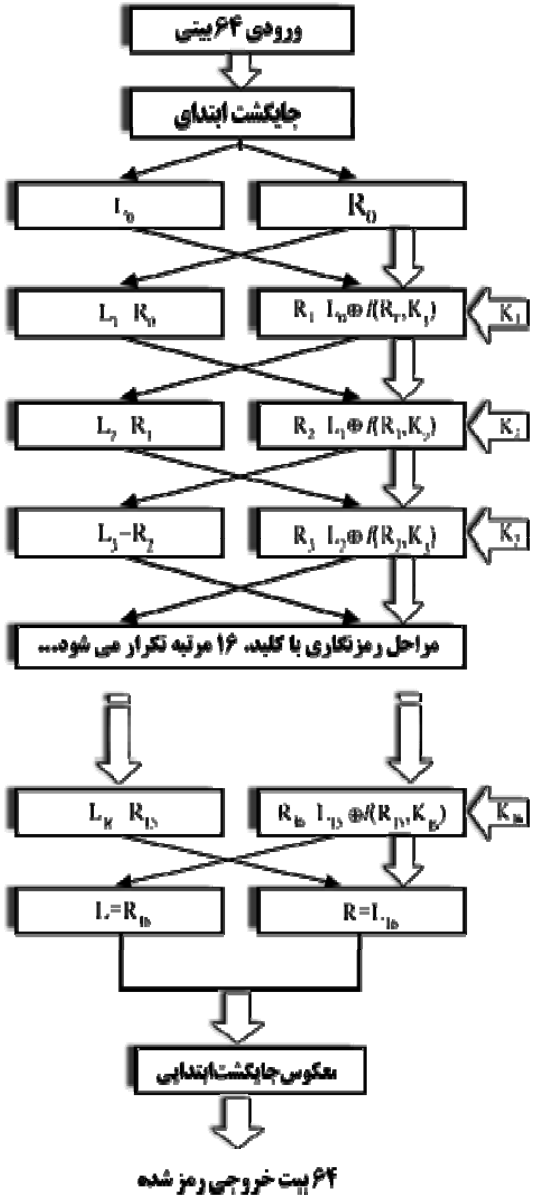
ویژگیهای معماری رمز فیستل

10. پیاده سازی سخت افزاری و نرم افزاری باید بتوان ترجیحاً به صورت بلادرنگ داده ها را رمزنگاری و رمزگشایی کند.
11. طول شاه کلید و کلیدهای فرعی باید به قدری بزرگ باشد که امکان کشف انها با سعی و خطا وجود نداشته باشد.
12. حداقل طول مجاز داده، ۶۴ بیت است. اما در روشهای جدید هر بلوک داده ۱۲۸ بیت در نظر گرفته می شود.

استاندارد رمزنگاری DES

در ابتدای دهه هفتاد، دولت امریکا (CIA و NSA) و شرکت IBM مشترکاً روشی را برای رمزنگاری داده ها ایجاد کردند تا به عنوان استانداردی برای محرمانه نگه داشتن اسناد دولتی مورد استفاده قرار گیرد، این روش (Data Encryption Standard) DES نام گرفت.

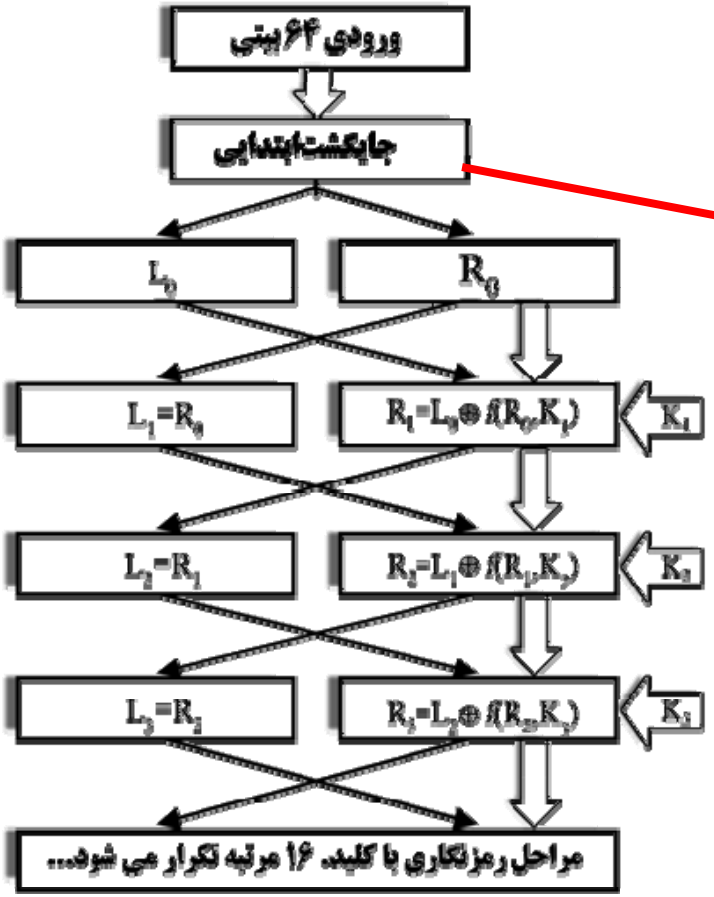
این روش نقطه عطفی در تاریخ چند هزار ساله رمزنگاری قلمداد می شود. روش DES سرآغاز علم رمزنگاری، به صورت آکادمیک، مدرن و هدفمند است.


ورودی ۶۴ بیتی
جایگشت ابتدای
L_0
R_0
L_1 R_0
R_1 $L_0 \oplus f(R_0, K_1)$
K_1
L_2 R_1
R_2 $L_1 \oplus f(R_1, K_2)$
K_2
L_3 R_2
R_3 $L_2 \oplus f(R_2, K_3)$
K_3
مراحل رمزنگاری با کلید، ۱۶ مرتبه تکرار می شود...
L_{16} R_{15}
R_{16} $L_{15} \oplus f(R_{15}, K_{16})$
K_{16}
$L=R_{16}$
$R=L_{16}$
معکوس جایگشت ابتدایی
۶۴ بیت خروجی رمز شده

کلیات الگوریتم DES

- ورودی، یک رشته ۶۴ بیتی است. بنابراین ابتدا باید متن به گروههای هشت کاراکتری دسته بندی شود.
- در اولین گام (جایگشت ابتدایی) از جایگشت زیر برای به هم ریختن ترکیب بیتها استفاده می شود، که آنرا "جایگشت مقدماتی" (Initial Permutation) می نامند. هدف از اینکار به هم ریختن وابستگی آماری بیتهای مجاور است.

کلیات الگوریتم DES



جدول جایگشت مقدماتی (IP)

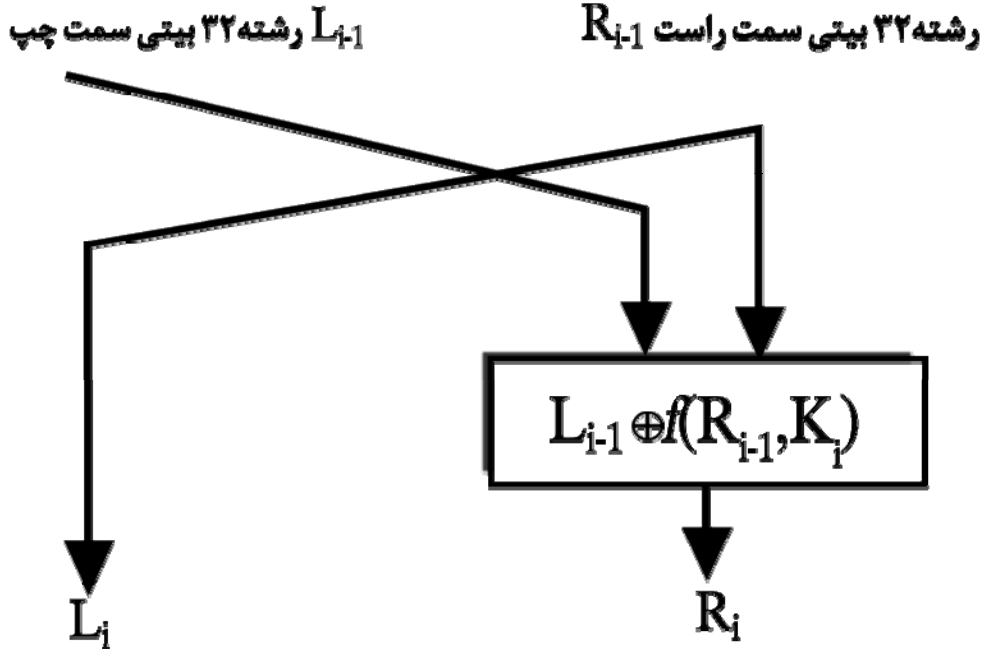
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

کلیات الگوریتم DES

- در گام دوم، رشته ۶۴ بیتی ورودی به دو نیمه ۳۲ بیتی چپ و راست تقسیم می شود.
- در گام سوم، فرآیند رمزنگاری مبتنی بر کلید آغاز می شود و تا ۱۶ دور ادامه می یابد.
- هر دور به یک کلید ۴۸ بیتی متفاوت نیاز دارد که همگی به روشی پیچیده و غیرخطی از کلید ۵۶ بیتی اصلی، استخراج می شوند.

الگوی رمزنگاری در هر دور

$$\begin{cases} R_i = L_{i-1} \oplus f(R_{i-1}, K_i) \\ L_i = R_{i-1} \end{cases}$$



کلیات الگوریتم DES

- پس از دور شانزدهم، جای دو نیمه ۳۲ بیتی عوض شده و عکس عمل جایگشت ابتدایی، بر اساس جدول زیر صورت می گیرد تا بیتها سر جای اصلی شان برگردند.

جدول جایگشت معکوس (IP^{-1})							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

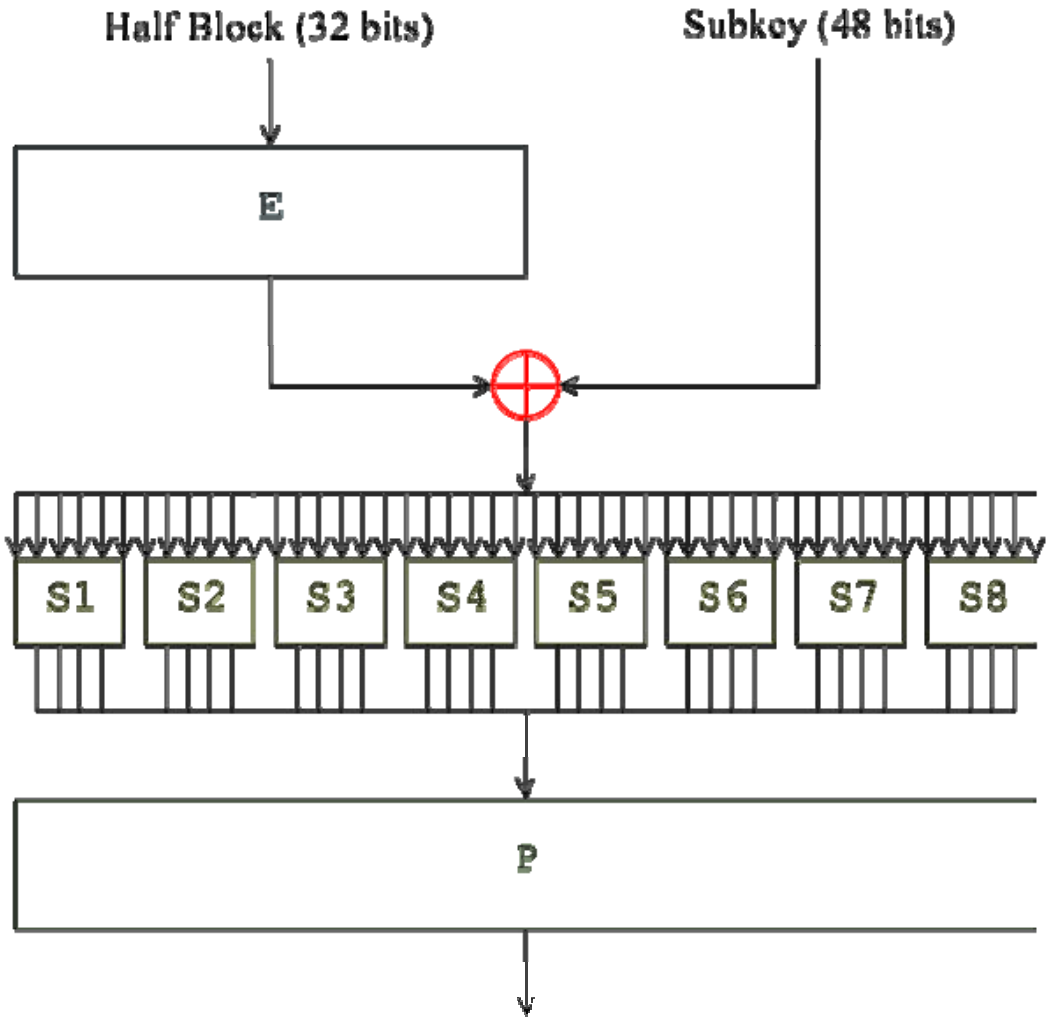
مقایسه جداول بازگشت مقدماتی و معکوس

جدول جایگشت مقدماتی (IP)							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

جدول جایگشت معکوس (IP^{-1})							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

- هدف از استفاده از جایگشت های ابتدایی و انتهایی، بدین شکل، این است که الگوریتم را از بالا به پایین و بالعکس متقارن می کنند، در نتیجه عمل رمزگشایی به مدار مستقلی نیاز ندارد.

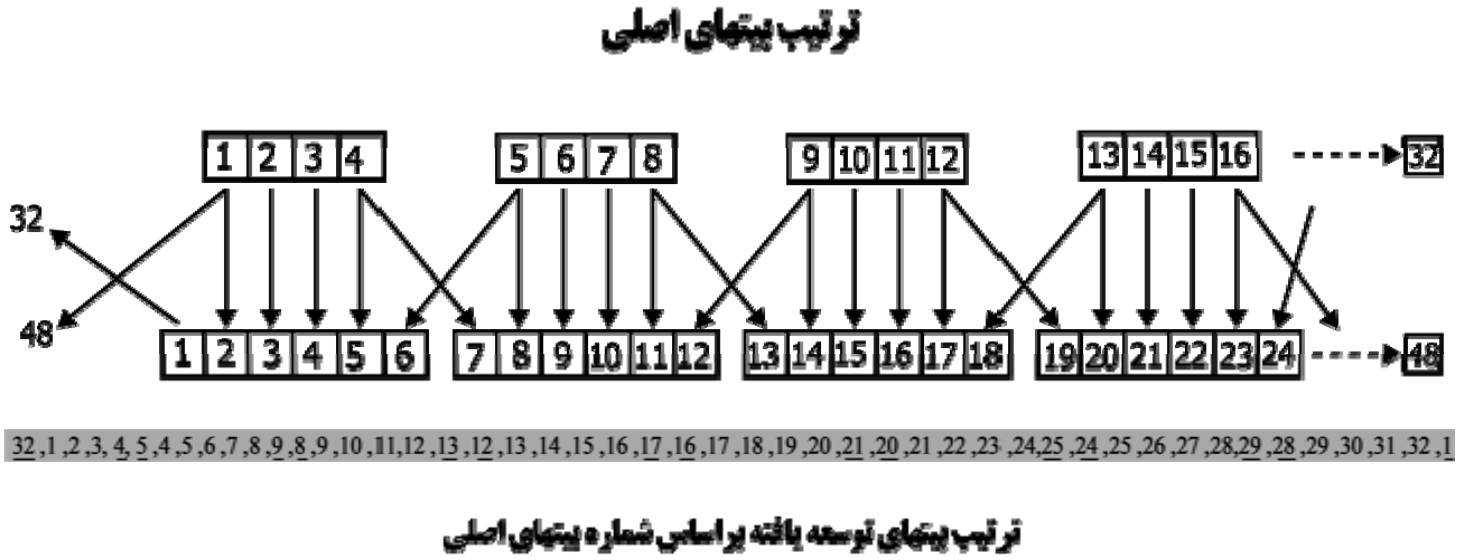
جزئیات تابع $F(R_{I-1},K_I)$



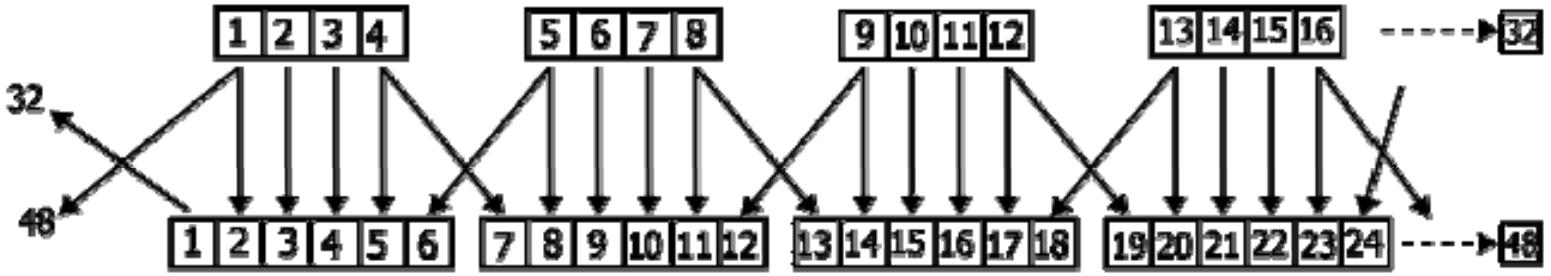
این تابع، غیرخطی و مشتمل بر عملیات های توسیع (Expansion)، جانشینی، XOR و جایگشت است و پیچیدگی و استحکام DES از همین تابع ناشی می شود.

مراحل عملیات تابع $F(R_{I-1},K_I)$

- در گام اول، رشته ۳۲ بیتی ورودی R_{i-1} به یک رشته ۴۸ بیتی توسعه داده می شود.
- در این مرحله، هر گروه ۴ بیتی ورودی به ۶ بیت توسعه داده می شود.



ترتیب بیتهای اصلی



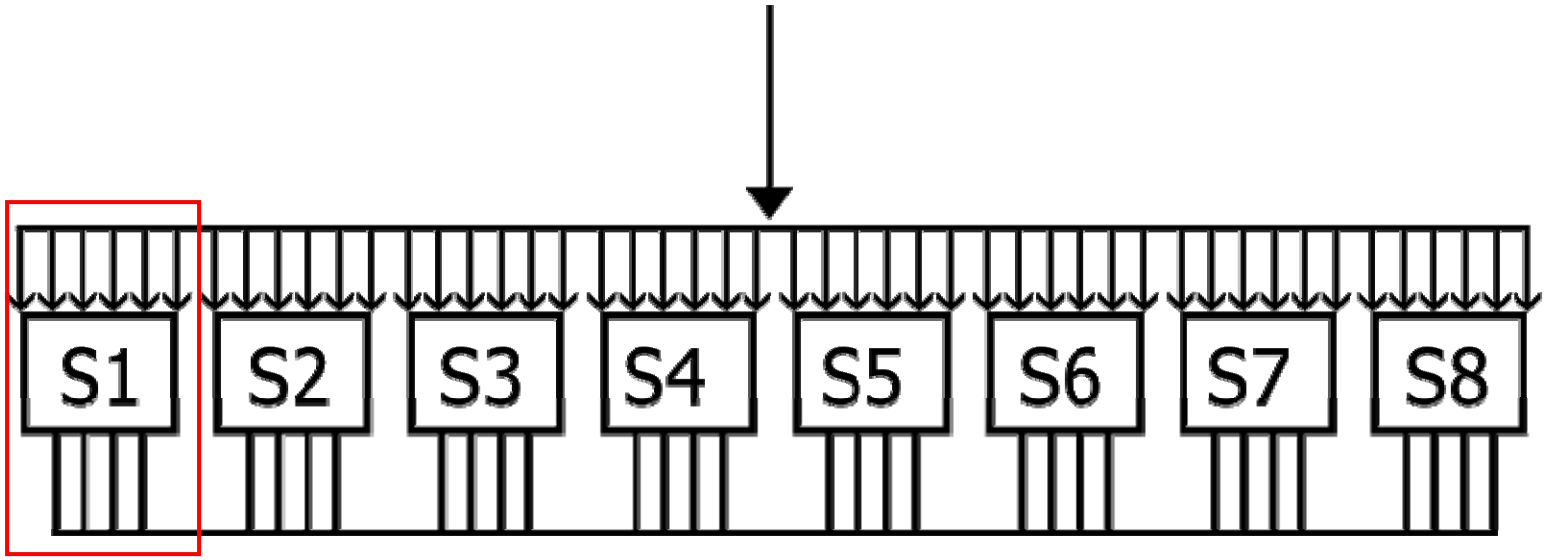
32 ,1 ,2 ,3, 4, 5 ,4 ,5 ,6 ,7 ,8 ,9 ,8 ,9 ,10 ,11,12 ,13 ,12 ,13 ,14 ,15 ,16 ,17 ,16 ,17 ,18 ,19 ,20 ,21 ,20 ,21 ,22 ,23 ,24,25 ,24 ,25 ,26 ,27 ,28,29 ,28 ,29 ,30 ,31 ,32 ,1

ترتیب بیتهای توسعه یافته براساس شماره بیتهای اصلی

بیتهای تکرای	ترتیب بیتهای اصلی				بیتهای تکرای
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

مراحل عملیات تابع $F(R_{I-1},K_I)$

- در گام دوم، کلید ۴۸ بیتی با ورودی توسعه داده شده، XOR می شود.
- در گام سوم، رشته ۴۸ بیتی باید با استفاده از هشت S-Box به ۳۲ بیت کاهش یابد. این کار با جداول زیر انجام می شود.



مراحل عملیات تابع $F(R_{I-1},K_I)$

S-box 1:

b_5b_0 \ $b_4b_3b_2b_1$	0000	0001	0010	0011	0100	1011	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

- هر S-Box شش بیت ورودی دارد: $b_5b_4b_3b_2b_1b_0$
- ضمناً هر جدول جانشینی ۴ سطر و ۱۶ ستون دارد و با اعداد ۴ بیتی 0 تا 15 پر شده است.
- اگر b5b0 شماره سطر و b4b3b2b1 شماره ستون باشد، عدد چهار بیتی مربوط به آن به خروجی خواهد رفت.

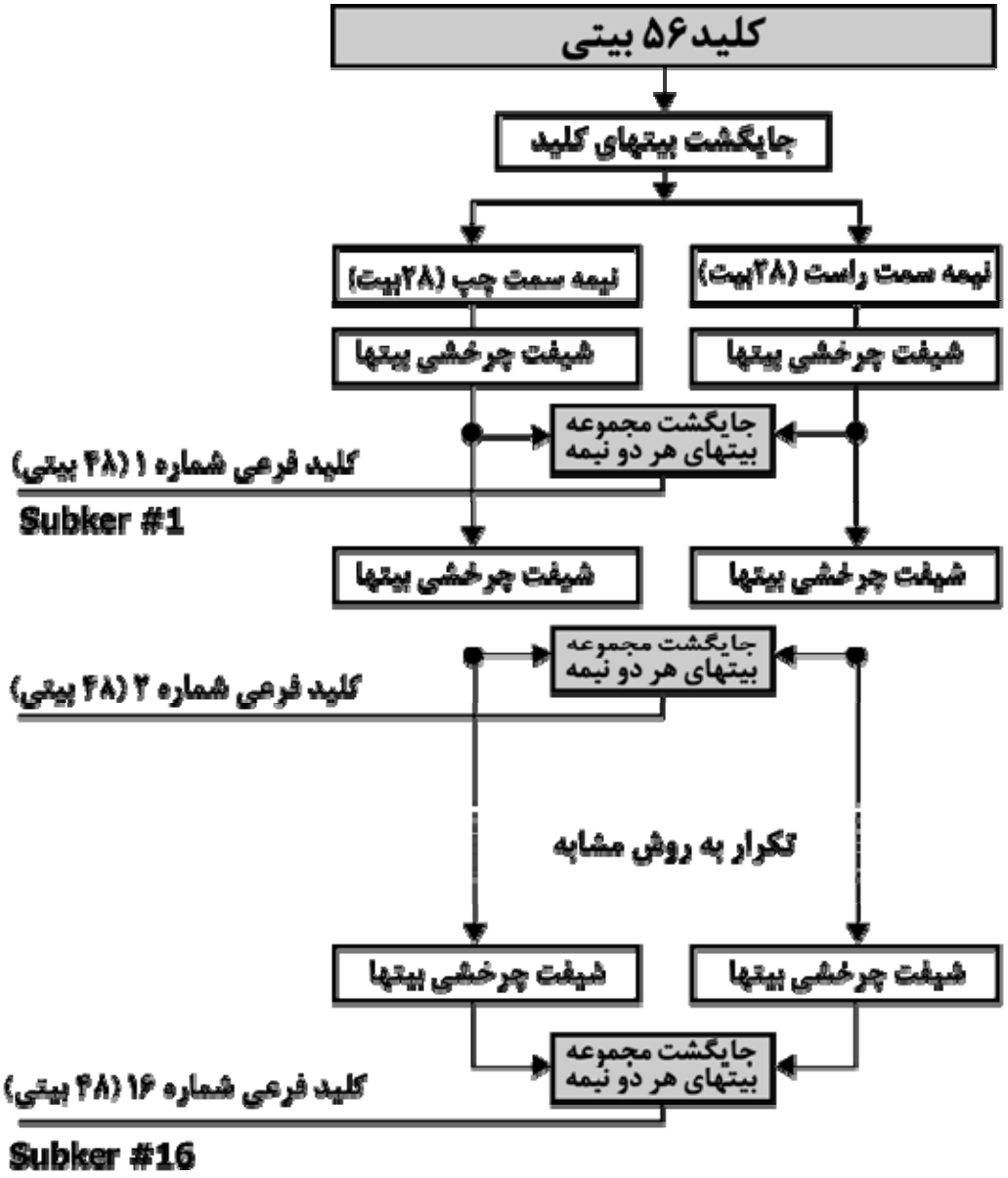
مراحل عملیات تابع $F(R_{I-1},K_I)$

- در گام چهارم، با استفاده از یک P-Box، از جایگشت ۳۲ بیتی استفاده می شود.

جدول جایگشت نهایی در تابع f							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

روش استخراج کلیدهای فرعی از کلید اصلی

- در بعضی از مراجع، کلید DES، ۶۴ بیتی عنوان می شود ولی (8*8=64) از هر بایت، یک بیت، Parity bit است پس نهایتاً 7*8=56 بیت برای کلید اصلی می ماند و هشت بیت توازن در جایگشت ابتدایی حذف می شود.
- روال تولید کلیدهای فرعی از کلید اصلی، برگشت پذیر نیست. بدین معنی که با داشتن چند کلید فرعی نمی توان به کلید اصلی رسید.
- استخراج ۱۶ کلید فرعی ۴۸ بیتی از کلید اصلی ۵۶ بیتی بر اساس شکل زیر انجام می شود:


کلید ۵۶ بیتی
جایگشت بیتهای کلید
نیمه سمت چپ (۲۸بیت)
نیمه سمت راست (۲۸بیت)
شیفت چرخشی بیتها
شیفت چرخشی بیتها
جایگشت مجموعه بیتهای هر دو نیمه
کلید فرعی شماره ۱ (۴۸ بیتی)
Subker #1
شیفت چرخشی بیتها
شیفت چرخشی بیتها
جایگشت مجموعه بیتهای هر دو نیمه
کلید فرعی شماره ۲ (۴۸ بیتی)
تکرار به روش مشابه
شیفت چرخشی بیتها
شیفت چرخشی بیتها
جایگشت مجموعه بیتهای هر دو نیمه
کلید فرعی شماره ۱۶ (۴۸ بیتی)
Subker #16

روش استخراج کلیدهای فرعی از کلید اصلی

- برای استخراج ۱۶ کلید فرعی، روال زیر ۱۶ بار تکرار می شود:
- در گام اول، بر اساس جدول جایگشت 7*8=56 سلولی زیر، کلید ۶۴ بیتی اولیه به ۵۶ بیت کاهش می یابد.
- در این جدول مضارب ۸ که بیتهای توازن هستند حذف شده است.

جدول جایگشت اولیه کلید (pc-1)						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	30	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	3	5	28	20	12	4

روش استخراج کلیدهای فرعی از کلید اصلی

- در گام دوم، خروجی ۵۶ بیتی مرحله قبل به دو نیمه ۲۸ بیتی تقسیم شده و طبق یک جدول به دو رجیستر با قابلیت "شیفت چرخشی به چپ" (Circular left shift) وارد می شوند و در هر دور ۱ یک تا دو بیت شیفت داده می شوند.
- در گام سوم، طبق جدول جایگشت 6*8=48 سلولی زیر، ضمن جایگشت، ۵۶ بیت ورودی به ۴۸ بیت کاهش می یابد. خروجی ۴۸ بیتی این مرحله کلید دور (یا فرعی) می باشد.

روش استخراج کلیدهای فرعی از کلید اصلی

- در جدول PC-2 بعضی بیتها وجود ندارند.
- برای تولید مابقی کلیدها، همین روال از گام دوم به بعد، با جداول جانشینی متفاوت، تکرار می شود.

جدول جایگشت ثانویه (pc-2)							
14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

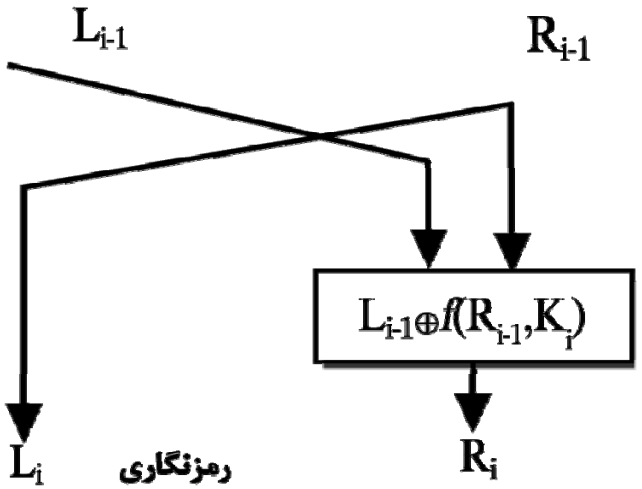
رمزگشایی DES

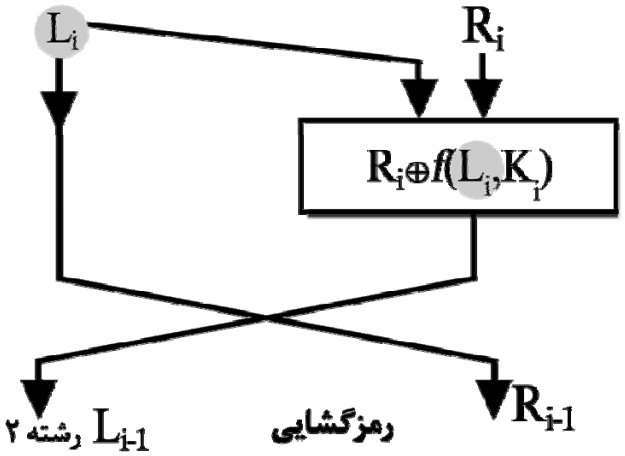
- یکی از زیباییهای DES آن است که عمل رمزگشایی داده ها به الگوریتم مجزایی نیاز ندارد.
- هرگاه در الگوریتم رمزنگاری، ترتیب کلیدها را واژگون کنید، رمزگشایی صورت خواهد گرفت.
- به عبارت دیگر، هر گاه کلیدهای فرعی K_1 تا K_{16} را بطور برعکس از K_{16} تا K_1 و بلوک رمزشده را به عنوان داده ورودی به الگوریتم اعمال کنید، داده ها رمزگشایی خواهد شد.

رمزگشایی DES

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

$$R_i \oplus f(R_{i-1}, K_i) = L_{i-1} \oplus f(R_{i-1}, K_i) \oplus f(R_{i-1}, K_i) = L_{i-1}$$





بررسی استحکام DES

- یکی از اشکالات DES ، کلید کوتاه ۵۶ بیتی آن است که عملاً از پس حملات مختلف بر نیامده است. هر چند رمزگشایی DES بدون داشتن، بخشی از متن اصلی، یا زبان نگارش کار بسیار مشکلی است.
- یکی از نقاط ضعف DES ، پشتیبانی آژانس امنیت ملی امریکا (NSA) است که همیشه شبهه استحکام و امنیت آن را به دنبال داشته است.