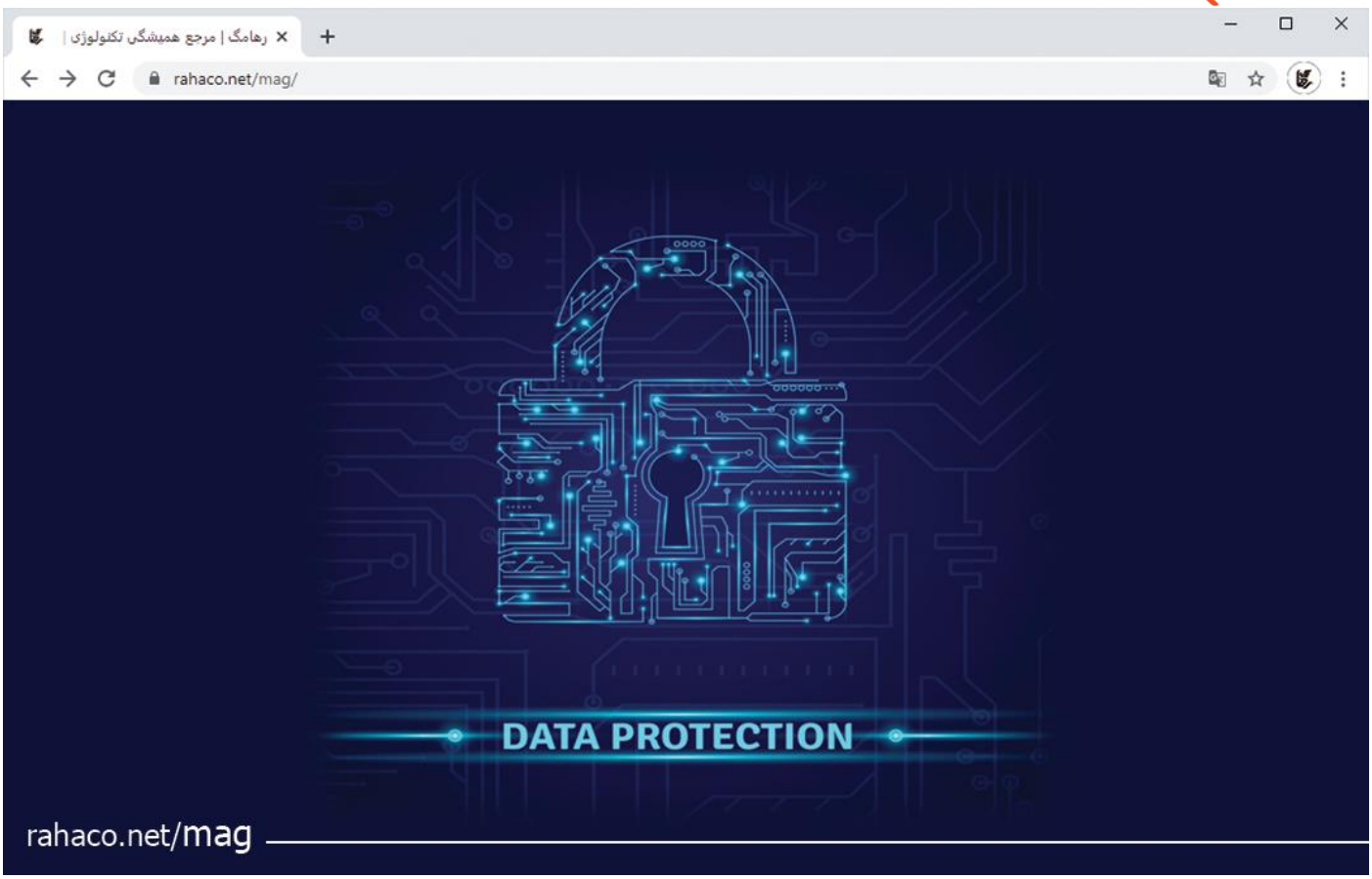
رمزنویسی و امنیت شبکه

مجموعه شرکت‌های دانش بنیان رها

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net



فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

رمزنویسی و امنیت شبکه

رمزنویسی و امنیت شبکه مانگو تمام بعدازظهر را بر روی کد اِستِرن و اساسا با کمک پیام‌های اخیری که در سقوط

Nevin Squarکپی‌برداری کرده بود کار می‌کرد.

استرن بسیار رازدار بود.

او می‌بایست به‌خوبی از مرکز لندن باخبر باشد و پیرامون آن سقوط، چیزهایی فهمید.

روشن بود که آن‌ها توجه نداشتند که ما نگو چند وقت یک‌بار پیام‌های آن‌ها را می‌خواند.

بنابراین آن‌ها از نفوذناپذیری کُد مطمئن بودند.

رمزگذاری بلوکی مدرن

اکنون به رمزگذاری‌های بلوکی مدرن توجه کنید.

که، یکی از پرکاربردترین انواع الگوریتم‌های رمزنویسی است.

که امنیت یا خدمات تعیین معرف را فراهم می‌کنند

و بر رویDES (استاندارد حفاظت داده) تمرکز می‌کنند تا اصول طراحی رمزگذاری بلوکی را نشان دهند.

رمزگذاری بلوکی در مقایسه با رمزگذاری جاری

رمزگذاری‌های بلوکی پیام‌هایی را در بلوک‌ها پردازش می‌کنند و سپس هر یک از آن‌ها رمزگشایی و یا رمزدار

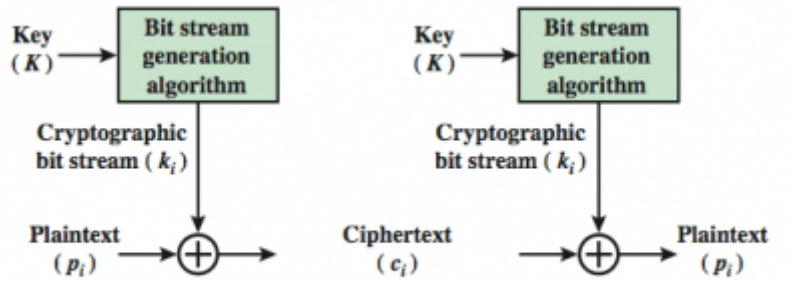
می‌شود.

مانند یک جانشین سازی بر روی کاراکترهای بسیار بزرگ ۶۴ بایتی یا بیشتر.

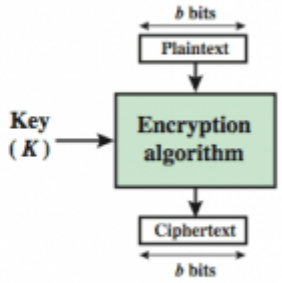
آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

رمزگذاری‌های جاری، پیام‌های یک بیتی یا بایتی را در زمان رمزگشایی یا رمزدار شدن ، پردازش می‌کنند.

بسیاری از رمزگذاری‌های رایج، رمزگذاری‌های بلوکی هستند. بهتر آنالیز می‌شوند. محدوده وسیعی از کاربردها دارند.



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

اصول رمزگذاری‌های بلوکی در رمزنویسی و امنیت شبکه

اکثریت رمزگذاری‌های بلوکی متقارن، بر مبنای ساختار رمزگذاری فیستل می‌باشند.

این امر لازم است زیرا باید قادر بود تا متن رمزگذاری شده را کشف رمز کرده تا پیام‌ها به‌طور کارآمد دریافت شوند.

رمزگذاری‌های بلوکی، مانند یکجانشین سازی بسیار بزرگ می‌باشند.

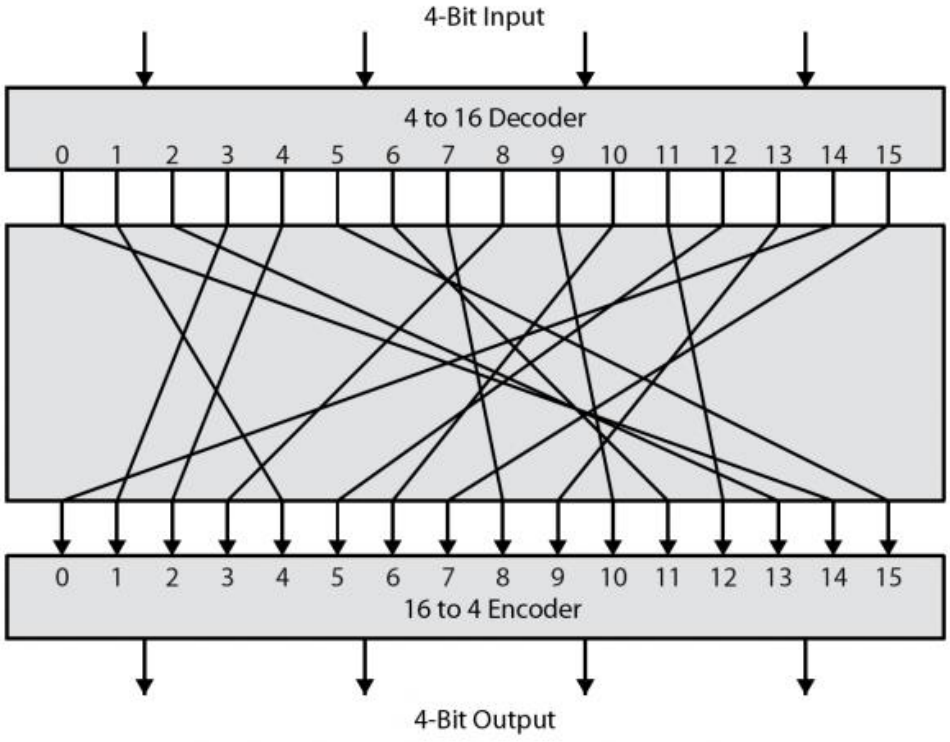
آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

و نیازمند جدول مدخل‌های ۲۶۴ برای یک بلوک ۶۴ بیتی خواهد بود.

بجای ساختن از بلوک‌های ساختمانی کوچک‌تر.

و از ایده رمزگذاری حاصل‌ضربی استفاده می‌کند.

کلاود شنون و رمزگذاری‌های تبدیلی و جانشینی



کلاود شنون، ایده شبکه‌های تبدیلی و جانشینی (S-P)را در روزنامه سال ۱۹۴۹ معرفی کرد.

مبنای رمزگذاری‌های بلوکی مدرن را تشکیل داد.

شبکه‌های S-P بر مبنای دو شبکه اولیه می‌باشند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

عملکردهای نهفته که از قبل مشاهده شدند عبارت‌اند از:

جانشینی(S-box)

تبدیلی(P-box)

اختلال و انتشار پیام‌ها و کلید را فراهم می‌کنند.

اختلال و انتشار

رمزگذاری نیازمند آن است تا مشخصه‌های آماری پیام اصلی، کاملاً پنهان شوند.

یک صفحه‌کلید رمز یک‌رویه ، این کار را انجام می‌دهد.

شنون به‌طور کارآمدتر ، ترکیب عناصر S &P را برای دستیابی به موارد ذیل پیشنهاد کرد:

اختلال – ساختار آماری پیام عادی را در سرتاسر متن رمزگذاری شده پراکنده می‌کند.

انتشار – ارتباط بین متن رمزگذاری شده و کلید را تا حد امکان پیچیده می‌سازد.

ساختار رمز فیستل

هورست فیستل، رمز فیستل را بر مبنای مفهوم رمز حاصل‌ضربی معکوس‌شدنی ابداع کرد.

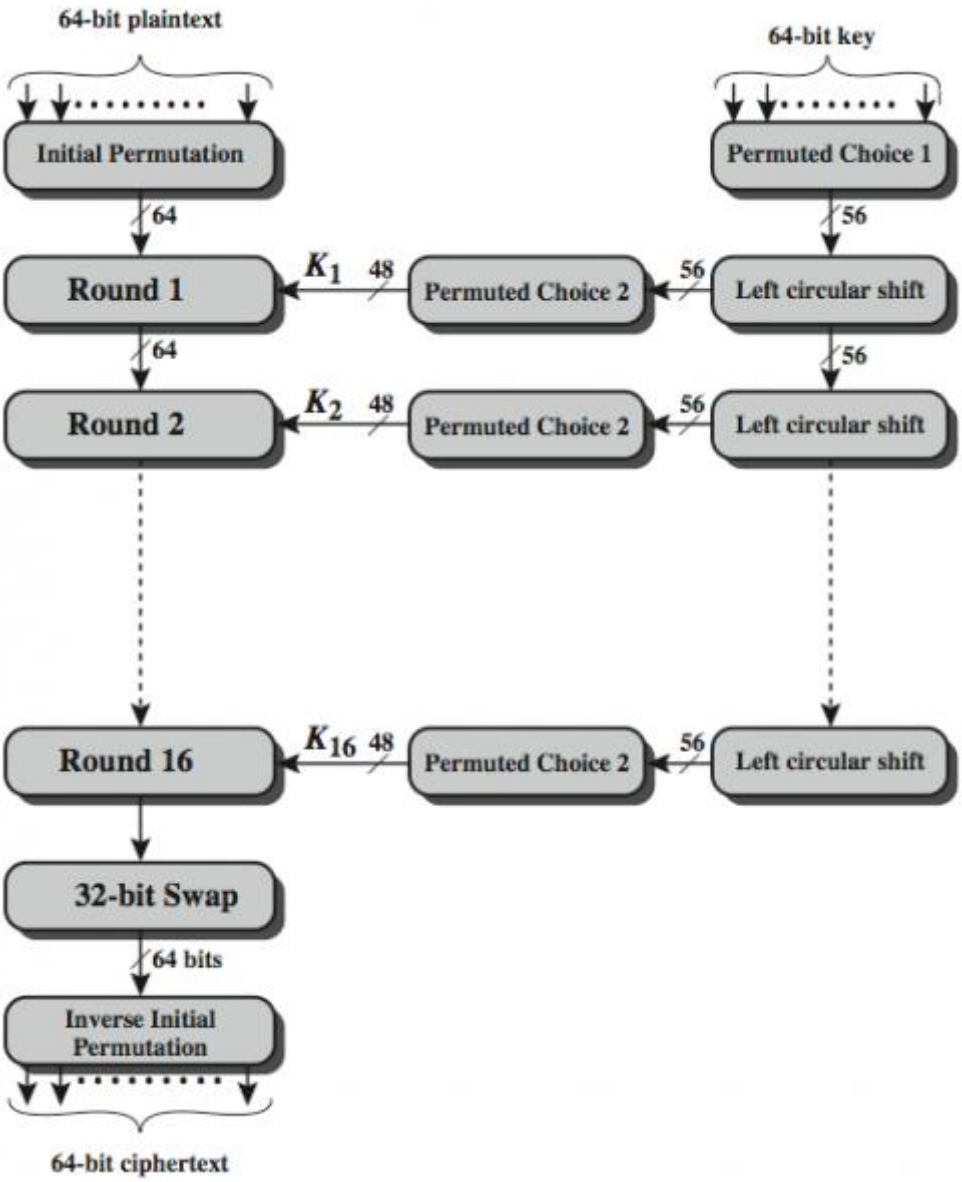
بلوک ورودی قسمت‌ها در دونیمه.

پردازش از طریق روند (round)چندگانه که یکجانشینی را در نیمه چپ داده بر مبنای عملکرد روند نیمه راست

انجام می‌دهند، سپس کلیدهای فرعی دارای نیمه‌های تعویض تبدیلی می‌شوند. مفهوم شبکه S-P شنون را اجرا

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

می‌کند.



آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

تبدیل IP اولیه

۱. اولین گام محاسبه داده
۲. ثبت‌کننده‌هایIP ، بیت‌های داده ورودی
۳. بیت‌های زوج تا نصف LH ، بایت‌های فرد تا نصفRH
۴. کاملاً منظم در ساختار) آسان در((h/w

به‌طور مثال(IP (675a6967 5e5a6b5a) = (ffb2194d 004df6fb) :

ساختار روندDES

۱. از دونیمه L و 32 R بایتی استفاده می‌کند.
۲. با توجه به هر رمز فیستل می‌تواند این‌گونه توصیف شود:

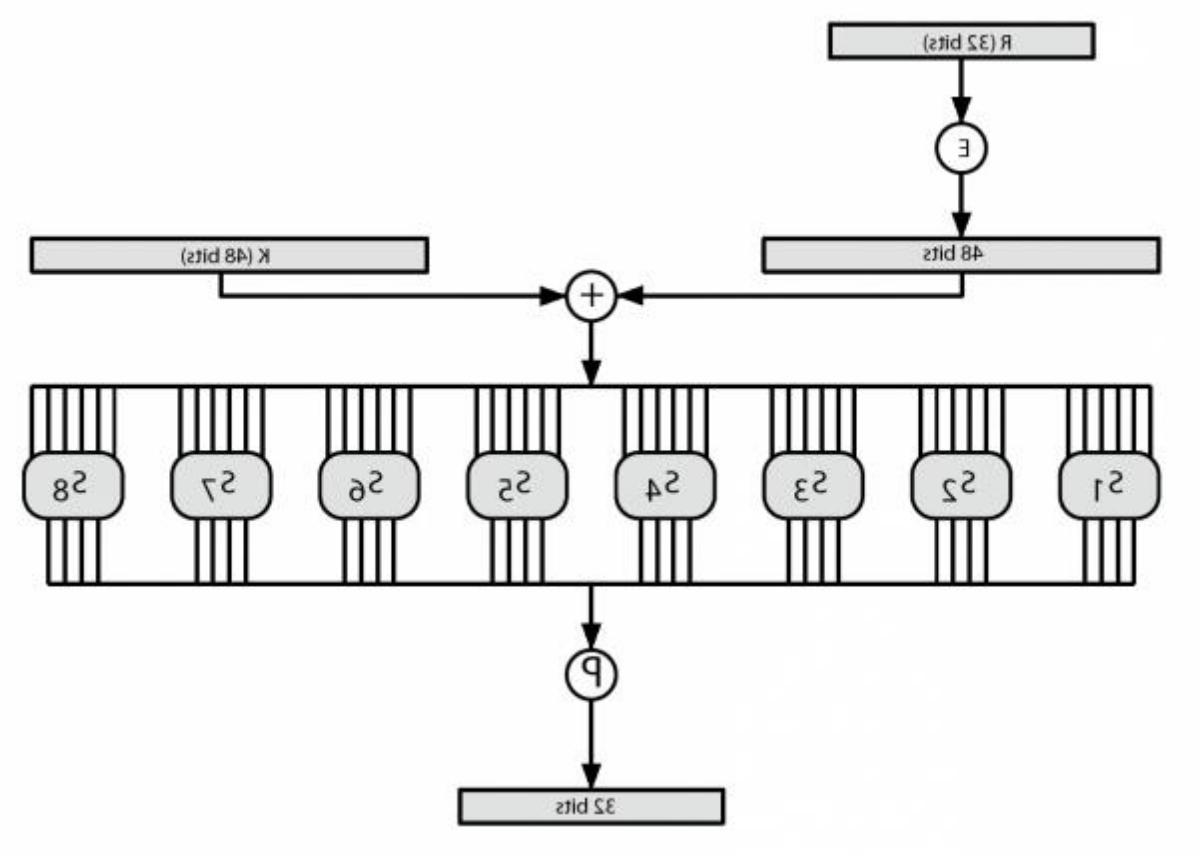
۱Li = Ri−

, Ki)۱ Å F(Ri−۱Ri = Li−

۳. F،نیمه 32 R بیتی و کلید فرعی ۴۸ بیتی را اتخاذ می‌کند.
۴. Rرا تا ۴۸ بیت با استفاده از تبدیلE ،گسترش می‌دهد.
۵. با استفاده از XOR به کلید فرعی اضافه می‌کند.
۶. از میان‌هشت – S باکس عبور می‌کند تا به نتیجه ۳۲ بیتی برسد.
۷. درنهایت با استفاده از تبدیل 32 P بایتی، تغییر می‌یابد

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

S باکس‌های COL



۱. دارای هشت S باکس می‌باشند که ۶ تا ۸ بیت را ترسیم می‌کنند.

۲. هر S باکس در حقیقت چهار باکس ۴ بیتی کوچک می‌باشد.

۳. بیت‌های خارجی ۱ و ۶ (بیت‌های سطری) یک سطر از چهار سطر را انتخاب می‌کنند.

۴. بایت‌های درونی ۵-۲ (بیت‌های به دنبال هم) جانشین می‌شوند. نتیجه، ۳۲ بیت است.

۵. انتخاب سطری به داده و کلید بستگی دارد.

۶. یک ویژگی که با عنوان اتوکلاو (اتوکی) شناخته می‌شود.

مثال5fd25e03 = S(18 09 12 3d 11 17 38 39) :

زمان‌بندی کلیدDES

۱. کلیدهای فرعی استفاده‌شده در هر روند را تشکیل می‌دهد.

۲. تغییر اولیه کلید (PC1) که ۵۶ بیت را در دونیمه ۲۸ بایتی انتخاب می‌کند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

۱۶ مرحله متشکل از:

۳. چرخاندن هر نیمه به‌طور مجزا در یک یا دو محل که به برنامه زمان‌بندی K چرخش کلید بستگی دارد.

۴. انتخاب ۲۴ بیت از هر نیمه و تغییر دادن آن‌ها.

۵. به‌وسیله PC2 برای استفاده در عملکرد روند.f

۶. به موضوعات کاربردی عملی در h/w در مقایسه با s/w توجه کنید.

کشف رمزDES

۱. در کشف رمز کردن می‌بایست گام‌های محاسبه داده با طراحی فیستل بازشوند و مراحل رمزگذاری مجدداً با استفاده از کلیدهای فرعی در ترتیب معکوس انجام گیرد.(SK16 & SK1)

۲. IP، گام نهایی FP رمزگذاری را بی‌اثر می‌کند.

۳. اولین روند به‌واسطهSK16 ، شانزدهمین روند رمزگذاری را بی‌اثر می‌کند.

۴. شانزدهمین روند به‌وسیلهSK1 ، اولین روند رمزگذاری را بی‌اثر می‌کند.

۵. سپس FP نهایی، IPرمزگذاری اولیه را بی‌اثر می‌کند.

۶. ازاین‌رو ارزش داده اصلی را ریکاوری می‌کند.

Round		δ
	02468aceeca86420 12468aceeca86420	1
1	3cf03c0fbad22845 3cf03c0fbad32845	1
2	bad2284599e9b723 bad3284539a9b7a3	5
3	99e9b7230bae3b9e 39a9b7a3171cb8b3	18
4	0bae3b9e42415649 171cb8b3ccaca55e	34
5	4241564918b3fa41 ccaca55ed16c3653	37
6	18b3fa419616fe23 d16c3653cf402c68	33
7	9616fe2367117cf2 cf402c682b2cefbc	32
8	67117cf2c11bfc09 2b2cefbc99f91153	33

Round		δ
9	c11bfc09887fbc6c 99f911532eed7d94	32
10	887fbc6c600f7e8b 2eed7d94d0f23094	34
11	600f7e8bf596506e d0f23094455da9c4	37
12	f596506e738538b8 455da9c47f6e3cf3	31
13	738538b8c6a62c4e 7f6e3cf34bc1a8d9	29
14	c6a62c4e56b0bd75 4bc1a8d91e07d409	33
15	56b0bd7575e8fd8f 1e07d4091ce2e6dc	31
16	75e8fd8f25896490 1ce2e6dc365e5f59	32
IP^{-1}	da02ce3a89ecac3b 057cde97d7683f2a	32

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

Round	K_i	L_i	R_i
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bfc09
9	04292a380c341f03	c11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP^{-1}		da02ce3a	89ecac3b

تأثیر نزول ناگهانی (بهمن)

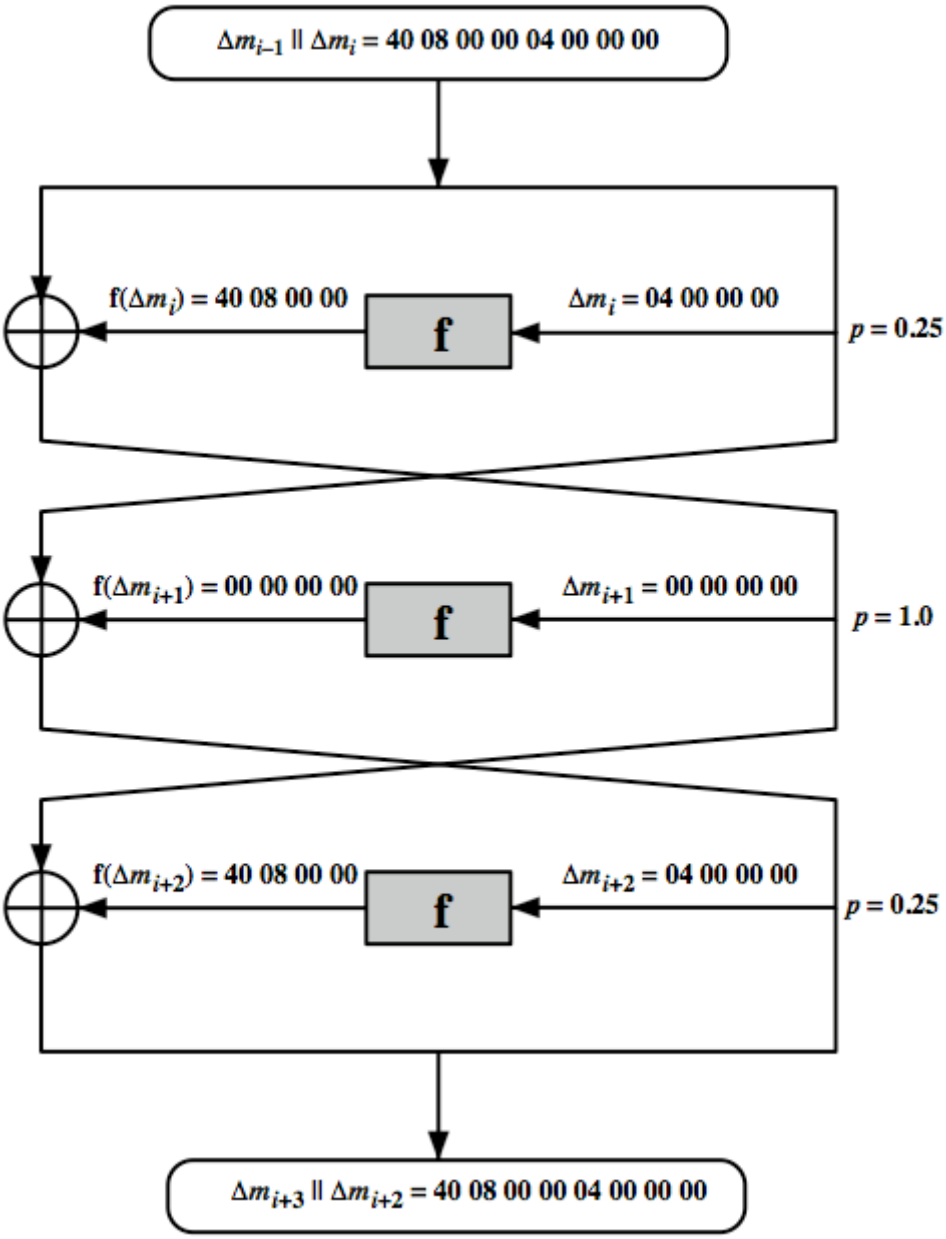
- ویژگی مطلوب کلید الگوریتم رمزگذاری.
- درجایی که تغییر یک ورودی یا زبانه کلید، منجر به تغییر تقریباً نیمی از بیت‌های برونداد می‌شود.
- و موجب می‌شود تا به‌واسطه حدس احتمالات کلیدی ، به سمت نشانه حرکت کند.
- DES، نزول ناگهانی شدیدی را نشان می‌دهد.

دوام اندازه کلیدDES

- کلیدهای ۵۶ بیتی، دارای مقادیر ۲۵۶ = ۱۰۷/۲ x ۱۶ می‌باشند.
- به نظر می‌رسد بررسی نیروی مخرب، دشوار باشد.
- پیشرفت‌های اخیر ثابت کرده‌اند که این بررسی:
- در سال ۱۹۹۷در چند ماه معدود در باب اینترنت.
- در سال ۱۹۹۸ در باب (h/w EFF) اختصاص‌یافته در چند روز معدود.
- در سال ۱۹۹۹ ترکیب مذکور در ۲۲ ساعت، ممکن است.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

- هنوز هم می‌بایست قادر باشد تا پیام عادی را تشخیص دهد.
- و باید جایگزین‌هایی را برحسب DES در نظر بگیرد.



آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

قدرت حملات تحلیلیDES

- اکنون چند حمله تحلیلی در خصوص DES داریم.
- این حملات ، برخی ساختارهای عمیق رمز را مورد دسترس قرار می‌دهد.
- با گردآوردن اطلاعات پیرامون رمزگذاری‌ها.
- که سرانجام می‌تواند همه یا برخی از بیت‌های کلید فرعی را ریکاوری کند.
- سپس در صورت لزوم به‌طور کامل به دنبال بقیه بیت‌ها باشد.
- به‌طورکلی ، این حملات، حملات آماری می‌باشند.
- کشف نوشته رمزی تفاضلی.
- کشف نوشته رمزی خطی.
- حملات کلیدی مربوطه.

شدت حملات زمان‌بندیDES

- اجرای حقیقی حملات رمز، از دانش نتایج اجرا جهت استنتاج کردن اطلاعات پیرامون کلیه بیت‌های کلید فرعی و یا برخی از آن‌ها استفاده می‌کند.
- به‌ویژه با استفاده از این واقعیت که محاسبات می‌توانند بسته به ارزش دروندادها نسبت به اطلاعات، زمان‌های متعددی را صرف کنند.
- بخصوص محاسبات گیج‌کننده در خصوص کارت‌های هوشمند.

کشف نوشته رمزی تفاضلی

- یکی از مهم‌ترین پیشرفت‌های اخیر(عمومی) در کشف نوشته رمزی.
- توسط NSA در سال ۱۹۷۰ در مقایسه با طرح DES شناخته شد.
- مورفی ، بیهام و شمیر، روش قدرتمندی را برای تحلیل رمزگذاری‌های بلوکی منتشر کردند.
- و بکار بردند تا اکثر رمزگذاری‌های بلوکی رایج را با درجات مختلف موفقیت تحلیل کنند.
- به‌طور معقول، DESدر مقایسه با لوسیفر، بر آن بافشاری داشت.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

کشف نوشته رمزی تفاضلی

- یک حمله آماری علیه رمزهای فیستل، از ساختار رمزی استفاده می‌کند که پیش‌ازاین کاربرد نداشت.
- طراحی شبکه‌هایS-P ، دارای برونداد عملکرد می‌باشد که تحت تأثیر دروندادو کلید است.
- بنابراین نمی‌تواند مقادیر قبلی را از طریق رمز بدون دانستن ارزش کلید ردیابی کند.
- کشف نوشته رمزی تفاضلی، دو جفت از رمزگذاری‌های مربوطه را مورد مقایسه قرار می‌دهد.

رمزنویسی و امنیت شبکه

- کشف نوشته رمزی تفاضلی، جفت‌های رمزدار گذاری را مورد مقایسه قرار می‌دهد
- با یک اختلاف مشخص در درونداد.
- در جستجوی یک اختلاف مشخص در برونداد است.
- و درزمانی که کلیدهای فرعی مشابه استفاده می‌شوند.
- کشف نوشته رمزی تفاضلی
- دارای برخی تفاوت‌های دروندادی است که برخی تفاوت‌های بروندادی را با احتمال P ارائه می‌کند.
- در صورت یافتن نمونه‌های برخی از احتمالات بزرگ‌تر، جفت‌های متفاوت دروندادی یا بروندادی به وقوع می‌پیوندد.
- و می‌توان به کلیدهای فرعی که درروند بکار می‌رفتند پی برد.
- سپس می‌بایست پردازش را بر روی بسیاری از روندها تکرار کرد (با کاهش احتمالات).

کشف نوشته رمزی تفاضلی

- حمله را با رمزدار کردن مکرر جفت پیام‌های عادی به‌وسیله درونداد XOR مشخص اجرا کنید تا زمانی که برونداد XOR مطلوب حاصل گردد.
- اگر روندهای واسطه با XOR موردنیاز مطابقت کند، دارای یک جفت صحیح است.
- و در غیر این صورت دارای یک جفت غلط می‌باشد و نسبت وابسته برای حمله، S/Nمی‌باشد.
- سپس می‌توان مقادیر کلیدها را برای روندها استنباط کرد.
- جفت‌های صحیح، زبانه‌ای کلید مشابهی را نشان می‌دهند.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

- جفت‌های غلط، مقادیر تصادفی را نشان می‌دهند.
- برای اعداد بزرگ روندها، احتمال آن‌قدر کم است که جفت‌های بیشتری نسبت به جفت‌های موجود با درونداد ۶۴ بیتی موردنیاز می‌باشند.
- بیهام و شمیر نشان داده‌اند که چگونه یک ویژگی تکرار شده ۱۳ روندی می‌تواند DES 16 روندی را قطع کند.

کشف نوشته رمزی خطی

- یک پیشرفت اخیر دیگر.
- همچنین یک روش آماری.
- می‌بایست بر روی روندها با کاهش احتمالات تکرار شود.
- توسط ماتسوی و همکارانش در ۱۹۹۰ ایجاد شد.
- بر مبنای یافتن تقریب‌های خطی.
- که می‌توانند به‌وسیله پیام‌های عادی مشخص ۲۴۳ به DES حمله کنند، ساده‌تر هستند اما هنوز در عمل، اجرا نشدنی‌اند.
- کشف نوشته رمزی خطی
- یافتن تقریب‌های خطی با احتمال½ =! p

,...,kc]۲,k۱,...,jb] = K[k۲,j۱,...,ia] Å C[j۲,i۱P[i

where ia ,jb ,kc are bit locations in P,C,K

- معادله خطی را برای زبانه‌های کلیدی ارائه می‌دهد.
- یک‌زبانه کلید با استفاده از الگوریتم حداکثر درست نمایی حاصل می‌کند.
- از عدد بزرگ رمزگذاری‌های نهایی استفاده می‌کند.
- کارایی آن حاصل می‌شود به‌وسیله–|p :۲/۱|.

معیار طراحیDES

- همان‌طور که توسط کوپر اسمیت [COPP94]گزارش گردید.
- ۷ معیار برای S باکس‌ها فراهم می‌شود برای:
- کشف نوشته رمزی غیرخطی.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net

- مقاوم در برابر کشف نوشته رمزی تفاضلی.
- اختلال خوب.
- سه معیار برای تغییر P که فراهم می‌شود برای:
- انتشار افزایش‌یافته.

طراحی رمزگذاری بلوکی

- هنوز هم اصول بنیادی، مانند اصول فیستل در سال ۱۹۷۰ است.
- تعداد روندها.
- هرچه بیشتر بهتر، تحقیق جامع، حمله بهتری را در بردارد.
- نقش:f
- اختلال را فراهم می‌آورد ، غیرخطی و بهمن است.
- دارای موضوعاتی است درباره اینکه چگونه s باکس‌ها انتخاب می‌شوند.
- زمان‌بندی کلیدی.
- ایجاد کلید فرعی پیچیده، بهمن کلیدی.

خلاصه رمزنویسی و امنیت شبکه

- رمزگذاری‌های بلوکی در مقایسه با رمزگذاری‌های جاری.
- طراحی و ساختار رمزگذاری فیستل.
- DES.
- جزئیات.
- دوام.
- کشف نوشته رمزی خطی و تفاضلی.
- اصول طراحی رمزگذاری بلوکی.
- پیشنهاد ما به شما برای مطالعه بیشتر تین کلاینت، زیروکلاینت و مجازی ساز

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱ www.rahaco.net