به نام خداوند بخشنده مهربان

مبانی امنیت شبکه

Fundamentals of Network Security



یاشار ابری

دانشکده مهندسی، دانشگاه تهران

Yasharabri.ut.ac.ir@gmail.com

yasharabri@ut.ac.ir

۳

رمزهای بلوکی و استاندارد رمزنگاری داده (DES)

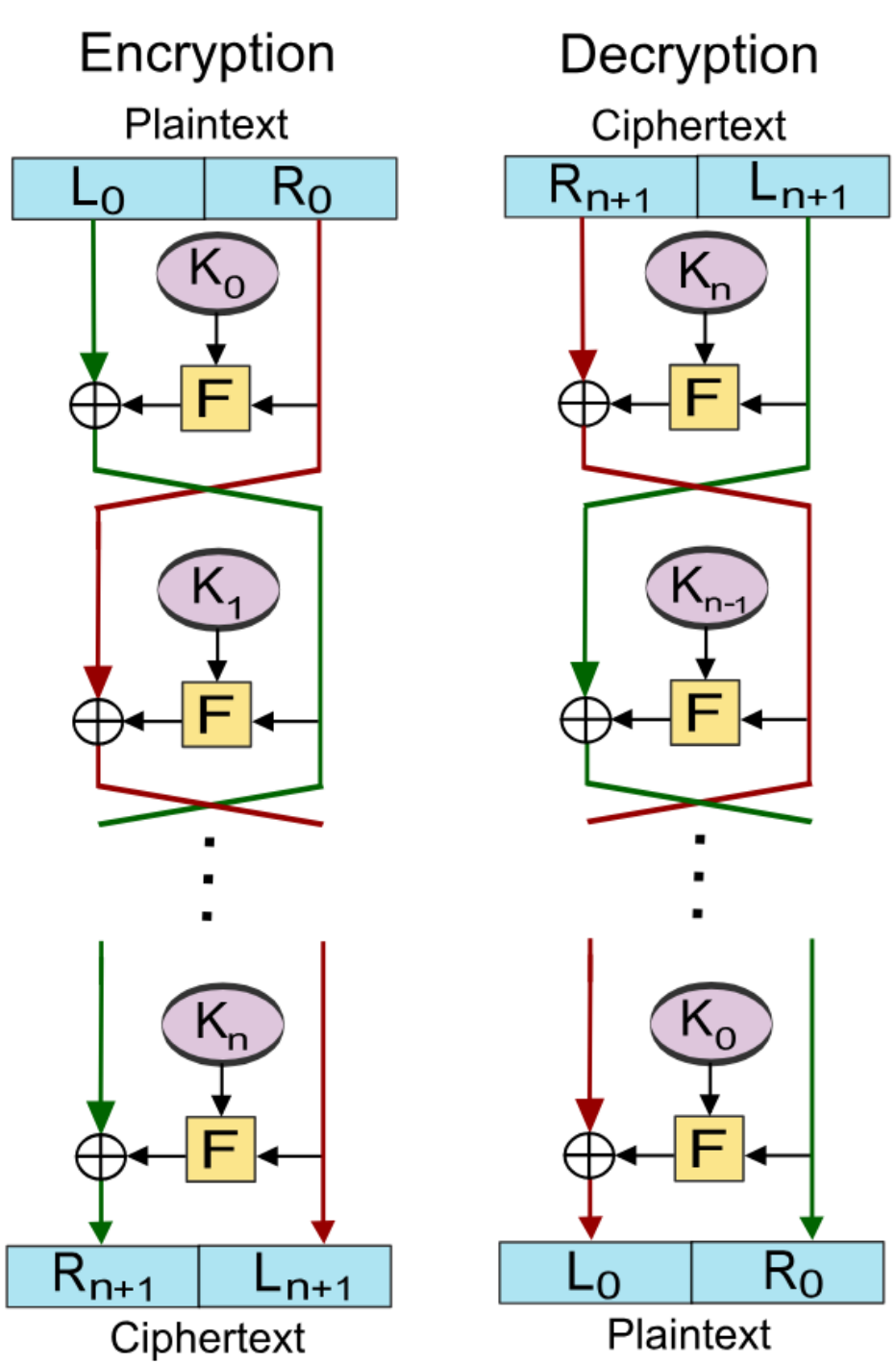
- سرفصل‌های این بخش:
  - اصول رمزهای بلوکی و شبکه فایستل
  - ساختار و تاریخچه DES
  - قدرت DESو روش‌های تحلیل رمز نوین
  - اصول طراحی رمزهای بلوکی

اصول رمزهای بلوکی و شبکه فایستل

- **ایده کلود شانون:** شانون در ۱۹۴۹ دو اصل بنیادی برای رمز قوی معرفی کرد: درهم‌سازی (Confusion، پیچیده‌کردن رابطه کلید و متن رمز) و انتشار (Diffusion، پخش‌کردن تأثیر هر بیت متن ساده روی کل متن رمز).
- **مشکل اجرای مستقیم رمز جانشینی ایده‌آل:** یک جانشینی کاملاً دلخواه روی بلوک‌های بزرگ به جدول‌هایی نجومی بزرگ نیاز دارد که در عمل غیرقابل ذخیره است.
- **راه‌حل هورست فایستل:** فایستل در IBM پیشنهاد داد به‌جای یک جانشینی کامل، بلوک را به دو نیمه تقسیم کرده و طی چند دور، با یک تابع ساده Fو کلید دور، نیمه‌ها را به‌نوبت تغییر دهیم تا هم درهم‌سازی و هم انتشار به‌تدریج ایجاد شود.
- **مزیت کلیدی ساختار فایستل:** رمزگشایی دقیقاً با همان ساختار رمزگذاری اما با ترتیب معکوس کلیدهای دور انجام می‌شود، بدون نیاز به این‌که تابع Fبرگشت‌پذیر باشد.

حضرت امام علی بن محمد هادی علیه السلام: حسد خوبی‌ها را از بین می‌برد و خودخواهی دشمنی و بیزاری می‌آورد. بحار جلد ۷۲ صفحه ۱۹۹

نمودار دور از شبکه فایستل با دو نیمه L و R، تابع F



حضرت امام علی بن موسی الرضا علیه السلام: مسلمان کسی است که مردم از دست و زبان او آسوده باشند و از ما نیست آنکه همسایه‌اش از شر او در امان نباشد.

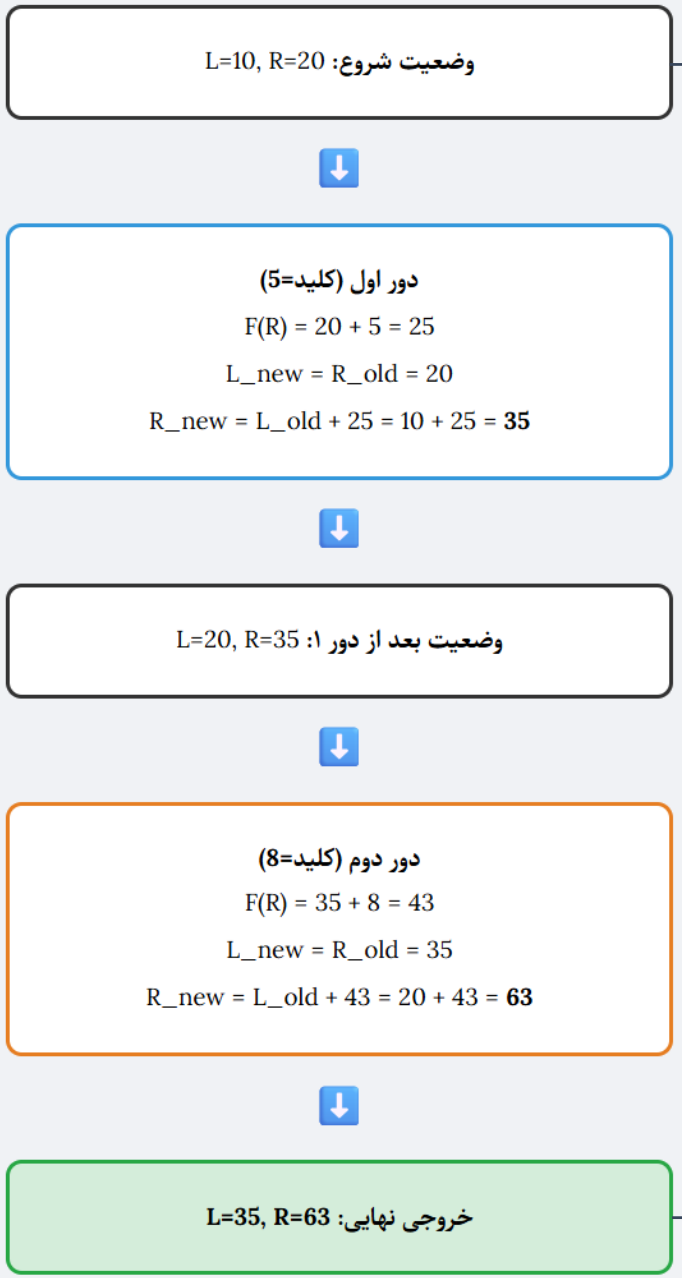
عیون الاخبار جلد ۱ صفحه ۲۴

مثال رمزگذاری شبکه فایستل

- **در هر دور:** سمت راست (R) وارد تابع F می‌شود (جمع با کلید)، سپس با سمت چپ (L) جمع می‌شود تا R جدید ساخته شود.
- **جابه‌جایی (Swap):** نکته کلیدی اینجاست که در پایان هر دور، R قدیمی به جای L جدید می‌نشیند.

حضرت امام موسی بن جعفر علیه السلام:
سه چیز تباهی می‌آورد: پیمان شکنی، رها کردن سنت، جدا شدن از جماعت.
میزان الحکمه حدیث ۲۱۲۵۰

نمودار کامل شبکه فیستل (۲ دور)



پیام اصلی

پیام رمزگذاری شده

حضرت امام حسن بن علی مجتبی علیه السلام: هر که احسان‌های خود را برشمارد، بخشندگی خویش را از بین برده است.

بحارالانوار جلد ۷۸ صفحه ۱۱۳

ctrl + / ctrl -

مثال رمزگشایی شبکه فایستل

- **ترتیب کلیدها:** در رمزنگاری از کلید ۵ و سپس ۸ استفاده کردیم. در رمزگشایی، ترتیب دقیقاً برعکس شد (ابتدا ۸، سپس ۵).
- **عملیات معکوس:** به جای اینکه حاصل تابع F را با سمت دیگر جمع کنیم، آن را از سمت دیگر کم کردیم تا اثر رمزنگاری خنثی شود.

حضرت امیرالمومنین علی بن ابیطالب علیه السلام:
هر کس عیب خود را ببیند از پرداختن به عیوب دیگران باز می‌ماند.
تحف العقول صفحه ۸۸

نمودار رمزگشایی شبکه فیستل (۲ دور)

پیام رمزگذاری شده →

وضعیت شروع رمزگشایی: L=35, R=63

⬇

دور اول (کلید=8)

F(L) = 35 + 8 = 43

L_new = R_old - F = 63 - 43 = **20**

R_new = L_old = 35

⬇

وضعیت بعد از دور ۱: L=20, R=35

⬇

دور دوم (کلید=5)

F(L) = 20 + 5 = 25

L_new = R_old - F = 35 - 25 = **10**

R_new = L_old = 20

⬇

خروجی نهایی (پیام اصلی): L=10, R=20 ← پیام رمزگشایی شده (اصلی)

حضرت اباعبدالله الحسین علیه السلام:

چیزی را به زبان نیاورید که از ارزش شما بکاهد.

جلال العیون جلد ۲

صفحه ۲۰۵

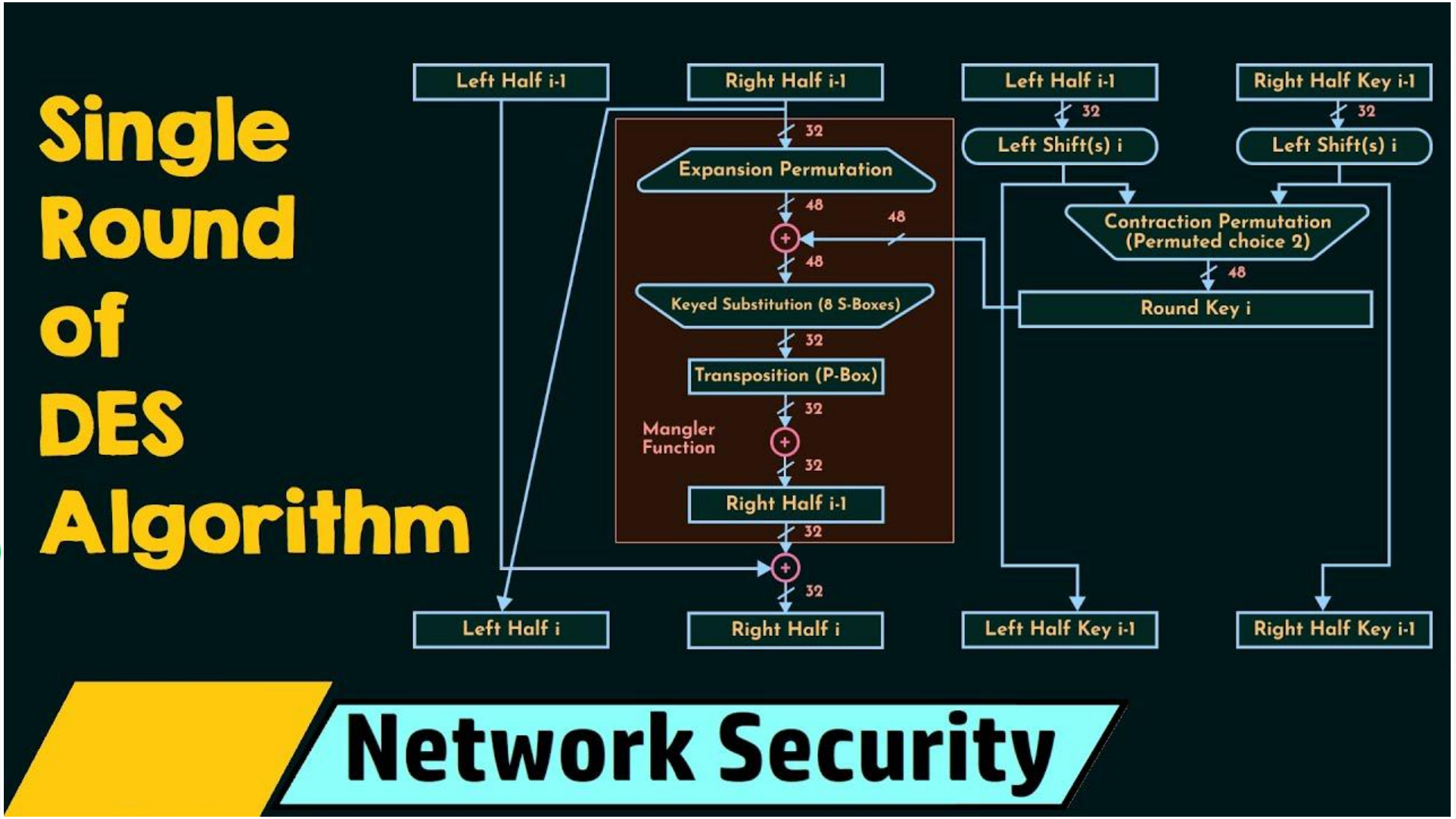
ctrl + / ctrl -

استاندارد رمزنگاری داده (DES)

- **خاستگاه:** DES بر پایه رمز Lucifr که در IBM توسط تیم هورست فایستل توسعه یافته بود ساخته شد؛ NBS (بعدها NIST) در سال ۱۹۷۷ آن را به‌عنوان استاندارد فدرال آمریکا اعلام کرد.
- **ساختار:** یک شبکه فایستل با بلوک ۶۴ بیتی، کلید مؤثر ۵۶ بیتی و ۱۶ دور رمزگذاری؛ در هر دور از جعبه‌های جانشینی (S-Box) غیرخطی برای ایجاد درهم‌سازی استفاده می‌شود.
- **نقش NSA و بحث‌ها:** NSA در طراحی S-Boxها مشارکت داشت و طول کلید را از ۱۲۸ بیت پیشنهادی IBM به ۵۶ بیت کاهش داد؛ این موضوع سال‌ها شبهه ایجاد کرد، هرچند بعدها مشخص شد S-Boxها در برابر تحلیل دیفرانسیلی (که آن زمان هنوز عمومی نشده بود) مقاوم‌سازی شده بودند.

حضرت امام علی بن محمد هادی علیه السلام: از حد خود تجاوز نکن و روزگار را در کار خدا دخیل مدان.
تحف العقول صفحه ۴۸۳

نمودار کلی یک دور DES



حضرت رسول الله صلی الله علیه و آله و سلم: خدیجه دختر خولید و فاطمه دختر محمد و مریم دختر عمران و عاصیه دختر مزاحم بهترین زنان اهل بهشت هستند.

اسد الغابه جلد ۵ صفحه ۴۳۷

ctrl + / ctrl -

قدرت DES و تحلیل رمز مدرن

- **آسیب‌پذیری طول کلید:** با ۵۶ بیت، فضای کلید حدود ۷۲ کوادریلیون حالت دارد؛ در سال ۱۹۹۸ ماشین Deep Crack ساخته EFF توانست یک کلید DES را در کمتر از سه روز با جستجوی فراگیر پیدا کند و ضعف عملی آن را اثبات کرد.
- **تحلیل دیفرانسیلی:** با مقایسه چگونگی تفاوت‌های ورودی روی خروجی‌های زوج‌های متن ساده، می‌توان اطلاعاتی درباره کلید فرعی هر دور استخراج کرد؛ DES در برابر این حمله نسبتاً مقاوم طراحی شده بود.
- **تحلیل خطی:** با یافتن یک تقریب خطی احتمالاتی بین بیت‌های ورودی، کلید و خروجی، می‌توان با تعداد زیادی جفت متن ساده-رمز، کلید را با احتمال بالا حدس زد.
- **راه‌حل موقت و جایگزین نهایی:** برای افزایش طول کلید مؤثر، Triple DES (اجرای سه‌باره DES با دو یا سه کلید) به‌کار گرفته شد، اما به دلیل کندی و اندازه بلوک کوچک، NIST مسابقه‌ای برای جایگزینی کامل آن برگزار کرد که به AES ختم شد.

حضرت امیرالمومنین علی بن ابیطالب صلوات الله علیه و آله:
فقه کامل کسی است که نه مردم را از رحمت خدا دلسرد کند و نه از مهر و لطفش ناامید سازد و نه از مکر خداوندی ایمن‌شان سازد.
نهج البلاغه صفحه ۴۸۳

اصول طراحی رمزهای بلوکی

معیار طراحی	توضیح
تعداد دورها	افزایش تعداد دورها امنیت را بالا می‌برد اما سرعت را کاهش می‌دهد؛ باید نقطه تعادل پیدا شود.
طراحی تابع دور (F)	تابع Fباید غیرخطی، حساس به تغییر کوچک ورودی و مقاوم در برابر تحلیل دیفرانسیلی/خطی باشد.
الگوریتم زمان‌بندی کلید	کلیدهای فرعی هر دور باید طوری از کلید اصلی مشتق شوند که یافتن کلید اصلی از روی یک کلید فرعی دشوار باشد.
سرعت رمزگذاری نرم‌افزاری	سرعت رمزگذاری/رمزگشایی در نرم‌افزار و سخت‌افزار باید برای کاربردهای عملی)مثل شبکه پرسرعت (مناسب باشد.

حضرت امام حسن بن علی مجتبی علیه السلام: به مردم بیاموز و دانش دیگران را فراگیر تا دانش خود را استوار کرده و آنچه را که ندانسته‌ای بدانی.

کشف الغمه جلد ۲ صفحه ۱۹۷