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

۵ توابع دور AES و حالت‌های عملکرد رمز بلوکی

- سرفصل‌های این بخش:
  - چهار تبدیل اصلی هر دور AES
  - چرا ECB ناامن است
  - حالت‌های CBC، CFB، OFB، CTR و GCM

توابع دور AES

تبدیل	توضیح	نقش اصلی (درهم‌سازی/انتشار)
SubBytes	هر بایت با استفاده از یک جدول جایگشتی ثابت جایگزین می‌شود تا رابطه خطی بین ورودی و خروجی از بین برود.	درهم‌سازی غیرخطی
ShiftRows	بایت‌های هر سطر از ماتریس حالت به‌صورت دوره‌ای جابه‌جا می‌شوند تا بایت‌ها بین ستون‌ها پخش شوند.	انتشار در سطح سطر
MixColumns	هر ستون با یک ضرب ماتریسی در میدان متناهی ترکیب می‌شود تا تأثیر هر بایت به کل ستون منتشر شود (در دور آخر حذف می‌شود).	انتشار در سطح ستون
AddRoundKey	کلید فرعی همان دور با عملیات XOR به ماتریس حالت اضافه می‌شود؛ کلیدهای دور از کلید اصلی توسط الگوریتم گسترش کلید تولید می‌شوند.	ترکیب با کلید دور

حضرت امام علی بن الحسین زین العابدین علیه السلام:
من پسر کسی هستم که فرشتگان آسمان بر او گریستند، من پسر کسی هستم که جنیان در زمین و پرندگان آسمان بر او نوحه سرایی کردند.
بحارالانوار جلد ۴۵ صفحه ۱۷۴

چرا رمز بلوکی به «حالت عملکرد» نیاز دارد؟

- **مشکل رمزگذاری بلوک به بلوک:** اگر پیام طولانی‌تر از یک بلوک باشد، باید آن را به چند بلوک تقسیم کرد؛ ساده‌ترین راه، رمزگذاری هر بلوک به‌طور مستقل با همان کلید است.
- **حالت کتاب کد الکترونیکی (ECB):** در این حالت بلوک‌های یکسان از متن ساده همیشه به بلوک‌های رمز یکسان تبدیل می‌شوند؛ این یعنی الگوهای تکراری در داده اصلی (مثل نواحی یکنواخت یک تصویر) در متن رمزشده هم قابل مشاهده می‌ماند.
- **راه‌حل: زنجیره بلوک رمز (CBC):** هر بلوک متن ساده پیش از رمزگذاری با بلوک رمزشده قبلی XOR می‌شود و بلوک اول با یک بردار مقداردهی اولیه (IV) تصادفی ترکیب می‌شود؛ این وابستگی زنجیره‌ای باعث می‌شود بلوک‌های یکسان، خروجی متفاوت تولید کنند.

حضرت امام علی بن الحسین زین العابدین علیه السلام:

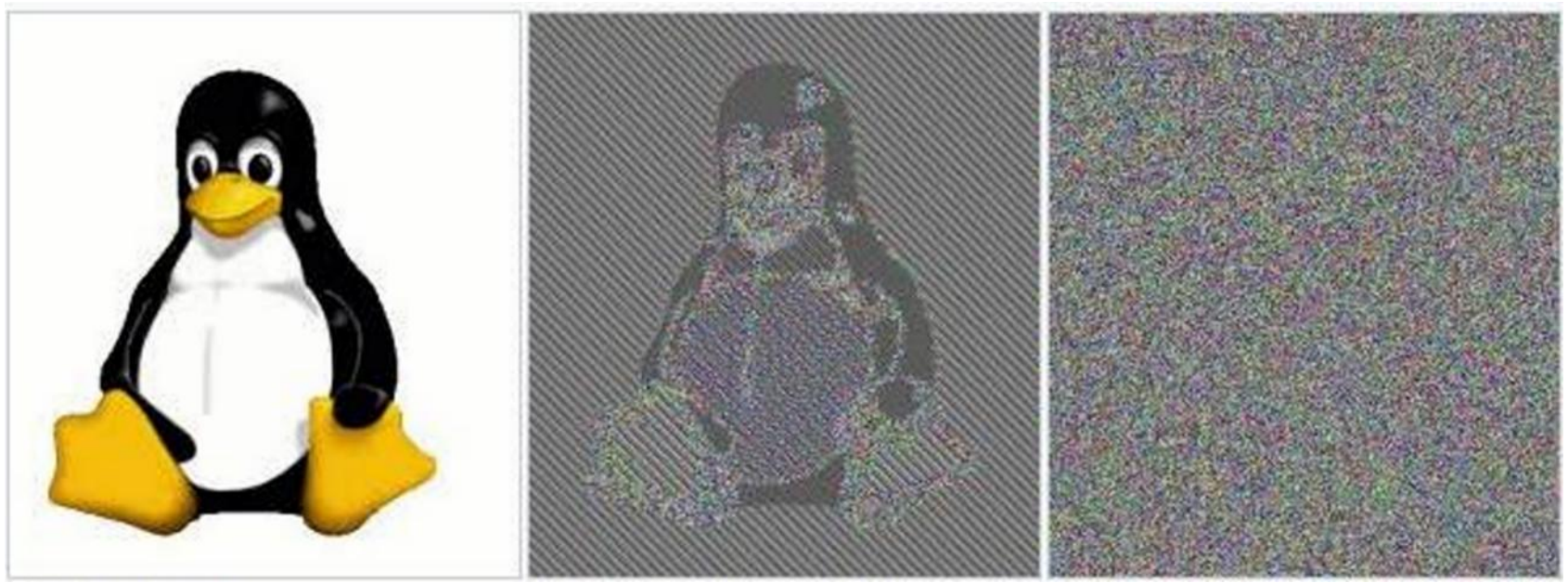
از دروغ کوچک و بزرگ، جدی و شوخی بپرهیز، زیرا آن کس که در چیز کوچک دروغ گفت، به دروغ بزرگتر نیز جرأت پیدا می‌کند.

اصول کافی جلد ۴ صفحه ۳۵

تصویر معروف پنگوئن لینوکس

- تصویر معروف پنگوئن لینوکس که با رمزگذاری ECB الگوی اصلی همچنان قابل تشخیص است در مقابل نسخه رمزشده با CBC که کاملاً نویز به‌نظر می‌رسد.

- CBC و سایری از حالت‌ها
- ECB
- اصلی



حضرت صدیقه کبری فاطمه زهرا سلام الله علیها:

اگر آنچه را که ما اهل بیت دستور داده‌ایم عمل کنی و از آنچه نهی کرده‌ایم خودداری نمایی، تو از شیعیان ما هستی وگرنه نیستی.

تفسیر امام عسکری علیه السلام صفحه ۳۲۰

مقایسه بصری ECB و CBC (تأثیر حالت عملکرد بر امنیت داده‌ها):

- تصویر پنگوئن لینوکس و دو مدل رمزگذاری آن نشان می‌دهد که:

- **خروجی حالت ECB:** حفظ الگوها و خطوط اصلی تصویر؛ نشان‌دهنده این ضعف که رمزگذاری مستقل بلوک‌ها، اطلاعات ساختاری و الگوهای تکراری داده (مانند نواحی یکنواخت) را لو می‌دهد و تصویر همچنان قابل تشخیص است.
- **خروجی حالت CBC:** تبدیل کامل داده‌ها به یک نویز تصادفی و غیرقابل تشخیص؛ نشان‌دهنده قدرت وابستگی زنجیره‌ای در از بین بردن الگوها و پنهان‌سازی کامل محتوای اصلی.

حضرت امام حسن ابن علی عسکری علیه السلام:
محبت نیکان برای نیکان، ثوابی است برای نیکان و محبت بدان به نیکان، فضیلتی است برای نیکان.
تحف العقول صفحه ۴۸۹

سایر حالت‌های عملکرد

حالت	کاربرد نوعی	ویژگی کلیدی
CFB	انتقال داده بایت به بایت (مثل ترمینال‌های قدیمی)	رمز بلوکی را به رمز دنباله‌ای تبدیل می‌کند؛ نیاز به پرکردن (Padding) ندارد.
OFB	کانال‌های پرنویز	دنباله شبه‌تصادفی از قبل و مستقل از داده تولید می‌شود؛ خطای انتقال گسترش پیدا نمی‌کند.
CTR	ذخیره‌سازی و شبکه‌های پرسرعت	با شمارنده افزایشی، امکان رمزگذاری و رمزگشایی کاملاً موازی و تصادفی‌دسترس را فراهم می‌کند.
GCM	TLS۱.۳، پروتکل‌های مدرن	ترکیب حالت CTR با تولید همزمان کد احراز اصالت؛ هم محرمانگی و هم جامعیت را تضمین می‌کند.
XTS	رمزگذاری کامل دیسک (BitLocker)	طراحی‌شده مخصوص بلوک‌های ذخیره‌سازی با اندازه ثابت مانند سکتورهای دیسک.

حضرت امام جعفر بن محمد صادق علیه‌السلام: به‌راستی که خداوند کربلا را حرم امن و با برکت قرار داد، پیش از آنکه مکه را حرم قرار دهد.

کامل الزیارات، صفحه ۲۶۹