دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)
دانشکده علوم کامپیوتر

پروژه درس جبرخطی عددی – الگوریتم های رمزنگاری

نگارش
علیرضا مختاری

استاد راهنما
خانم آمیتیس فرجی

استاد
دکتر دهقان

ماه و سال
۲۲ آذر ۱۴۰۴

چکیده

این پروژه با هدف بررسی و پیاده‌سازی عملی الگوریتم‌های کلیدی رمزنگاری، نقش بنیادین **جبر خطی** و **ماتریس‌ها** را در امنیت اطلاعات مدرن تبیین می‌کند. با تمرکز بر پیاده‌سازی دستی سه رمزنگاری مهم **رمز Hill** به عنوان نمونه‌ای کلاسیک و مبتنی بر حساب پیمانه‌ای، **رمز DES** به عنوان استاندارد قدیمی و با ساختار فیستل، و **رمز AES-128** (به عنوان استاندارد پیشرفته و مبتنی بر محاسبات در میدان محدود با ۲۵۶ عنصر) توانایی ریاضی این الگوریتم‌ها در تضمین محرمانگی مورد تحلیل قرار گرفته است.

در این پیاده‌سازی‌ها، توابعی برای تبدیل داده‌ها به ساختار ماتریسی، انجام عملیات اصلی رمزنگاری شامل ضرب ماتریس پیمانه‌ای، تبدیل‌های جابه‌جایی، و عملیات پیچیده میدان محدود (مانند ترکیب ستون‌ها یا MixColumns)ارائه شده است. نتایج آزمون‌های جامع نشان‌دهنده عملکرد موفقیت‌آمیز هر سه الگوریتم در فرآیندهای رمزنگاری و رمزگشایی با دقت کامل است. این مستندات به طور مفصل، ساختار ریاضی هر الگوریتم، نحوه استفاده از ماتریس‌ها در مراحل انتشار (Diffusion) و سردرگمی (Confusion)را تشریح کرده و درکی عمیق از کاربرد جبر خطی در امنیت سایبری فراهم می‌آورد.

واژه‌های کلیدی:

رمزنگاری ، جبرخطی ، رمز AES ، ماتریس ، میدان محدود

فهرست مطالب

صفحه

فصل اول

مقدمه

مقدمه

با گسترش ارتباطات دیجیتال و انتقال حجم بالای داده‌ها در بسترهای ناامن، مسئله‌ی حفظ محرمانگی اطلاعات به یکی از چالش‌های اساسی دنیای فناوری تبدیل شد. از همان سال‌های ابتدایی استفاده از رایانه‌ها و شبکه‌ها، نیاز به روشی برای جلوگیری از دسترسی افراد غیرمجاز به داده‌ها احساس می‌شد. رمزنگاری به عنوان راهکاری برای پاسخ به این نیاز شکل گرفت؛ هدف اصلی آن تبدیل اطلاعات قابل‌فهم به شکلی غیرقابل‌خواندن برای افراد غیرمجاز و بازگرداندن آن توسط گیرنده‌ی مجاز است.

در ابتدا، الگوریتم‌های رمزنگاری بسیار ساده بودند و عمدتاً بر پایه‌ی جایگزینی یا جابه‌جایی حروف عمل می‌کردند. این روش‌ها در زمان خود تا حدی کارآمد بودند، اما با پیشرفت توان محاسباتی و توسعه‌ی روش‌های تحلیل رمز، به‌تدریج ضعف‌های آن‌ها آشکار شد. الگوریتم‌های کلاسیک معمولاً الگوهای قابل تشخیص داشتند و در برابر حملات آماری یا آزمون و خطا مقاومت کافی از خود نشان نمی‌دادند. همین مسئله باعث شد که روش‌های سنتی دیگر پاسخگوی نیازهای امنیتی سیستم‌های مدرن نباشند.

با پیچیده‌تر شدن تهدیدات امنیتی، رمزنگاری نیز به سمت استفاده از ساختارهای ریاضی قوی‌تر حرکت کرد. در این میان، جبر خطی به‌عنوان یکی از شاخه‌های مهم ریاضیات، نقش پررنگی در طراحی و تحلیل الگوریتم‌های رمزنگاری پیدا کرد. دلیل این موضوع آن است که بسیاری از داده‌ها را می‌توان به‌صورت بردارها و ماتریس‌ها نمایش داد و عملیات رمزنگاری را به شکل مجموعه‌ای از تبدیل‌های ریاضی روی این ساختارها در نظر گرفت.

یکی از مزیت‌های اصلی استفاده از جبر خطی در رمزنگاری، امکان انجام تبدیل‌های خطی روی داده‌ها به شکلی منظم و ساختارمند است. نمایش داده‌ها به‌صورت بردار این امکان را فراهم می‌کند که چندین بیت یا نماد به‌طور هم‌زمان پردازش شوند، در حالی که در روش‌های ساده‌تر معمولاً هر واحد داده به‌صورت جداگانه بررسی می‌شد. این ویژگی نه‌تنها باعث افزایش سرعت عملیات رمزنگاری می‌شود، بلکه تحلیل و پیاده‌سازی الگوریتم‌ها را نیز ساده‌تر و منسجم‌تر می‌کند.

علاوه بر این، ماتریس‌ها ابزار قدرتمندی برای انجام تبدیل‌های پیچیده هستند. بسیاری از الگوریتم‌های رمزنگاری از ضرب ماتریسی برای ترکیب داده‌ها استفاده می‌کنند؛ عملیاتی که به‌راحتی قابل پیاده‌سازی

روی رایانه‌هاست و با معماری سخت‌افزاری سیستم‌های امروزی سازگاری بالایی دارد. همین موضوع باعث شده است که الگوریتم‌های مبتنی بر جبر خطی از نظر کارایی محاسباتی گزینه‌ی مناسبی برای کاربردهای عملی باشند.

از سوی دیگر، استفاده از مفاهیم جبر خطی امکان طراحی الگوریتم‌هایی با ساختار ریاضی مشخص را فراهم می‌کند؛ ساختاری که هم قابل تحلیل است و هم می‌توان نقاط ضعف و قوت آن را به‌صورت دقیق بررسی کرد. این ویژگی برای ارزیابی امنیت الگوریتم‌ها اهمیت بالایی دارد، زیرا طراحان رمزنگاری می‌توانند میزان مقاومت روش‌های خود را در برابر انواع حملات بررسی کنند.

در این پروژه، تمرکز اصلی بر بررسی نقش جبر خطی در رمزنگاری و تحلیل الگوریتم‌هایی است که به‌طور مستقیم از مفاهیم این شاخه‌ی ریاضی استفاده می‌کنند. ابتدا پیش‌نیازهای لازم به‌صورت ساده و قابل‌فهم معرفی می‌شوند و سپس نحوه‌ی عملکرد الگوریتم‌ها، کاربردهای آن‌ها و نقاط ضعفشان مورد بررسی قرار می‌گیرد. هدف نهایی این است که نشان داده شود چرا جبر خطی به یکی از ابزارهای کلیدی در رمزنگاری مدرن تبدیل شده و چه نقشی در امنیت داده‌های امروزی ایفا می‌کند.

فصل دوم

پیش نیاز

۲- پیش‌نیازهای ریاضی

برای درک نحوه‌ی عملکرد الگوریتم‌های رمزنگاری مبتنی بر جبر خطی، لازم است ابتدا با برخی مفاهیم پایه‌ی ریاضی و ساختاری آشنا شویم. هدف این فصل ارائه‌ی توضیحاتی شهودی و قابل‌فهم از این مفاهیم است، به‌گونه‌ای که حتی خواننده‌ای که پیش‌زمینه‌ی عمیقی در جبر خطی یا رمزنگاری ندارد، بتواند روند کلی الگوریتم‌ها را در فصل‌های بعدی دنبال کند.

۲-۱- بردار و نمایش داده‌ها

در ساده‌ترین حالت، داده‌هایی که قرار است رمزنگاری شوند، مانند متن یا فایل، به‌صورت دنباله‌ای از اعداد در نظر گرفته می‌شوند. یکی از روش‌های رایج برای این کار، نمایش داده‌ها به‌صورت **بردار** است. بردار را می‌توان مجموعه‌ای مرتب از اعداد دانست که به‌صورت یک واحد در نظر گرفته می‌شود. این نوع نمایش این امکان را فراهم می‌کند که چندین بخش از داده به‌طور هم‌زمان پردازش شوند، نه اینکه هر عنصر به‌صورت جداگانه بررسی شود.

در الگوریتم‌هایی مانندHill Cipher ، متن ورودی به بلوک‌هایی تقسیم می‌شود که هر بلوک به‌صورت یک بردار عددی نمایش داده می‌شود. این رویکرد باعث می‌شود عملیات رمزنگاری ساختارمندتر شده و تغییر در یک بخش از ورودی، روی کل خروجی تأثیر بگذارد.

۲-۲- ماتریس و نقش آن در رمزنگاری

ماتریس را می‌توان تعمیمی از بردار دانست که شامل چندین سطر و ستون است. ماتریس‌ها ابزار اصلی انجام تبدیل‌های خطی هستند و در بسیاری از الگوریتم‌های رمزنگاری نقش کلیدی دارند. استفاده از ماتریس این امکان را می‌دهد که داده‌های ورودی به‌صورت هم‌زمان و منسجم تغییر داده شوند.

یکی از مزیت‌های مهم ماتریس نسبت به ساختارهای ساده‌تر مانند آرایه‌ی یک‌بعدی این است که ماتریس‌ها می‌توانند روابط پیچیده‌تری بین اجزای داده ایجاد کنند. در رمزنگاری، این ویژگی باعث

افزایش پخش‌شدگی اطلاعات می‌شود؛ به این معنا که هر بخش از خروجی بـه چنـدین بخـش از ورودی وابسته خواهد بود. این خاصیت، تحلیل رمز را برای مهاجم دشوارتر می‌کند.

در الگوریتمHill ، رمزنگاری عملاً بر پایه‌ی ضرب یک ماتریس کلیـد در بـردار پیـام انجـام می‌شـود. در الگوریتم‌های مدرن‌تر مانند AES نیز اگرچـه سـاختار کلـی پیچیـده‌تر اسـت، امـا همچنـان از عملیـات ماتریسی برای ترکیب داده‌ها استفاده می‌شود.

۳-۲- عملیات پیمانه‌ای(Modular Arithmetic)

از آنجا که داده‌های دیجیتال محدود هستند و معمـولاً در بازه‌هـای مشخصـی از اعـداد قـرار می‌گیرنـد، بسیاری از الگوریتم‌های رمزنگاری از عملیات پیمانه‌ای استفاده می‌کنند. در این نوع محاسبات، نتیجـه‌ی عملیات همیشه در یک بازه‌ی مشخص باقی می‌ماند.

این مفهوم در الگوریتم Hill بسیار حیاتی است، زیرا عملیات ماتریسی در یک فضای محدود عددی انجام می‌شود. در AES و DES نیز عملیات پیمانه‌ای باعث می‌شـود خروجی‌هـا در قالـب قابـل‌پردازش بـرای سیستم‌های دیجیتال باقی بمانند. استفاده از این نوع محاسبات، علاوه بر کنترل دامنـه‌ی مقـادیر، باعـث سازگاری الگوریتم با سخت‌افزار و نرم‌افزارهای موجود می‌شود.

۴-۲- تبدیل‌های خطی و غیرخطی

یکی از مفاهیم مهم در رمزنگاری، تفاوت بین تبدیل‌های خطی و غیرخطی است. تبدیل خطی را می‌توان عملیاتی دانست که ساختار کلی داده را حفظ می‌کند و قابل توصیف با ابزارهای جبر خطی است. این نوع تبدیل‌ها معمولاً سریع و ساده هستند و به‌راحتی پیاده‌سازی می‌شوند.

با این حال، تبدیل‌های کاملاً خطی به‌تنهایی بـرای ایجـاد امنیـت کـافی نیسـتند. بـه همـین دلیـل، در الگوریتم‌هـای مـدرن ماننـد AES وDES ، در کنـار تبـدیل‌های خطـی (ماننـد عملیـات ماتریسـی)، از بخش‌های غیرخطی نیز استفاده می‌شود. این ترکیب باعث افزایش پیچیدگی الگـوریتم و مقاومـت آن در برابر حملات تحلیلی می‌شود.

۲-۵- ساختار بلوکی در الگوریتم‌ها

هر سه الگوریتمHill ، DESو AES از مفهوم **پردازش بلوکی** استفاده می‌کنند. در این روش، داده‌ی ورودی به بلوک‌هایی با اندازه‌ی مشخص تقسیم شده و هر بلوک به‌صورت جداگانه رمزنگاری می‌شود. این ساختار باعث می‌شود الگوریتم‌ها مقیاس‌پذیر باشند و بتوانند حجم‌های بزرگ داده را مدیریت کنند.

درHill Cipher ، اندازه‌ی بلوک به ابعاد ماتریس کلید وابسته است. در DES و AES نیز اندازه‌ی بلوک ثابت بوده و عملیات رمزنگاری روی هر بلوک تکرار می‌شود. این شباهت ساختاری باعث می‌شود بتوان این الگوریتم‌ها را از دیدگاه مفهومی با یکدیگر مقایسه کرد.

۲-۶- جمع‌بندی پیش‌نیازها

مفاهیمی مانند بردار، ماتریس، عملیات پیمانه‌ای و تبدیل‌های خطی، پایه‌ی اصلی الگوریتم‌هایی هستند که در ادامه بررسی می‌شوند. هدف از این فصل ارائه‌ی درکی شهودی از این مفاهیم بود، نه ورود به جزئیات ریاضی پیچیده. با درک این پیش‌نیازها، خواننده می‌تواند در فصل بعدی، نحوه‌ی عملکرد الگوریتم‌هایHill ، DESو AES را بهتر دنبال کرده و نقش جبر خطی را در هر یک از آن‌ها تشخیص دهد.

فصل سوم

توضیحات الگوریتم

۳- مدل‌های رمزنگاری

در این فصل، سه الگوریتمHill ، DESو AES بررسی می‌شوند. این الگوریتم‌ها از نظر تاریخی و ساختاری تفاوت‌های قابل‌توجهی با یکدیگر دارند، اما هر سه به‌نوعی از مفاهیم جبر خطی برای پردازش داده‌ها استفاده می‌کنند. هدف این فصل، توضیح نحوه‌ی عملکرد این الگوریتم‌ها، دلیل طراحی آن‌ها، نقش جبر خطی در هر کدام، و بررسی نقاط قوت و ضعفشان است.

۳-۱- الگوریتمHill Cipher

الگوریتم Hill یکی از نخستین الگوریتم‌های رمزنگاری است که به‌صورت مستقیم از مفاهیم جبر خطی استفاده می‌کند. این الگوریتم در زمانی معرفی شد که روش‌های ساده‌ی جایگزینی حروف دیگر پاسخگوی نیازهای امنیتی نبودند. هدف اصلی Hill این بود که به‌جای رمز کردن هر حرف به‌صورت مستقل، چندین حرف به‌طور هم‌زمان و وابسته به یکدیگر رمز شوند تا الگوهای آماری متن اصلی از بین برود.

در این الگوریتم، متن ورودی ابتدا به مقادیر عددی تبدیل می‌شود و سپس به بلوک‌هایی با اندازه‌ی ثابت تقسیم می‌گردد. هر بلوک را می‌توان به‌صورت یک بردار عددی در نظر گرفت. کلید رمزنگاری در Hill Cipherیک ماتریس مربعی است که ابعاد آن با اندازه‌ی بلوک‌ها متناسب است. عملیات اصلی الگوریتم، ضرب این ماتریس کلید در بردار پیام است.

نقش جبر خطی در این الگوریتم کاملاً اساسی است. استفاده از ماتریس به‌جای آرایه‌ی یک‌بعدی باعث می‌شود که هر عنصر خروجی به ترکیبی از چندین عنصر ورودی وابسته باشد. این ویژگی، پخش‌شدگی اطلاعات را افزایش می‌دهد و باعث می‌شود تغییر کوچک در ورودی، تغییرات گسترده‌ای در خروجی ایجاد کند. اگر به‌جای ماتریس از ساختارهای ساده‌تر استفاده می‌شد، این سطح از وابستگی بین داده‌ها به‌دست نمی‌آمد.

ورودی الگوریتم Hill شامل متن اصلی و ماتریس کلید است و خروجی آن متن رمزشده می‌باشد. در فرآیند رمزگشایی، از معکوس ماتریس کلید استفاده می‌شود؛ موضوعی که نشان می‌دهد انتخاب ماتریس باید به‌گونه‌ای باشد که معکوس‌پذیر باشد. این نکته یکی از محدودیت‌های مهم الگوریتم است.

با وجود نوآوری‌های مفهومی، Hill Cipherنقاط ضعف جدی دارد. این الگوریتم در برابر حملات متن معلوم آسیب‌پذیر است و با داشتن تعداد کافی از زوج‌های متن ساده و متن رمز، می‌توان کلید را به‌دست آورد. به همین دلیل، Hill Cipherامروزه کاربرد عملی در سیستم‌های امنیتی ندارد و بیشتر به‌عنوان یک الگوریتم آموزشی برای نشان دادن نقش جبر خطی در رمزنگاری استفاده می‌شود.

۲-۳- الگوریتمDES

الگوریتم DES در دوره‌ای طراحی شد که نیاز به یک استاندارد رسمی برای رمزنگاری داده‌ها در سیستم‌های کامپیوتری وجود داشت. هدف اصلی DES ایجاد الگوریتمی بود که هم از نظر امنیتی قابل‌قبول باشد و هم بتوان آن را به‌صورت عملی و سریع روی سخت‌افزار پیاده‌سازی کرد.

DESیک الگوریتم رمزنگاری بلوکی است که داده‌ها را در بلوک‌های با اندازه‌ی ثابت پردازش می‌کند. ورودی الگوریتم شامل یک بلوک داده و یک کلید رمزنگاری است و خروجی آن بلوک رمزشده می‌باشد. ساختار کلی DES بر پایه‌ی تکرار چندین مرحله‌ی مشابه طراحی شده است تا پیچیدگی رمزنگاری افزایش یابد.

درDES ، جبر خطی به‌صورت مستقیم و ساده مانند Hill Cipher دیده نمی‌شود، اما در لایه‌های داخلی الگوریتم حضور دارد. بسیاری از عملیات ترکیب و جابه‌جایی داده‌ها را می‌توان به‌صورت تبدیل‌های خطی روی بردارهای بیتی در نظر گرفت. استفاده از این تبدیل‌ها باعث می‌شود داده‌ها به شکلی منظم و قابل‌تحلیل پردازش شوند و در عین حال پیاده‌سازی الگوریتم ساده باقی بماند.

یکی از دلایل استفاده از این ساختارها، سازگاری بالا با سخت‌افزارهای زمان طراحی DES بود. عملیات خطی و جابه‌جایی بیت‌ها به‌سرعت قابل اجرا بودند و برای سیستم‌های عملی گزینه‌ی مناسبی محسوب

می‌شدند. اگرچه DES از بخش‌های غیرخطی نیز استفاده می‌کند، اما بخش قابل‌توجهی از ساختار آن مبتنی بر ترکیب‌های خطی داده‌هاست.

با گذشت زمان و افزایش توان محاسباتی، نقطه‌ضعف اصلی DES آشکار شد. اندازه‌ی کلید این الگوریتم نسبتاً کوچک است و در برابر حملات brute-force مقاومت کافی ندارد. به همین دلیل، DESبه‌تدریج از چرخه‌ی استفاده خارج شد و امروزه بیشتر به‌عنوان یک الگوریتم تاریخی و آموزشی مورد بررسی قرار می‌گیرد.

۳-۳- الگوریتمAES

الگوریتم AES به‌عنوان جایگزین DES طراحی شد تا ضعف‌های امنیتی آن را برطرف کند. هدف اصلی AESارائه‌ی الگوریتمی بود که هم از نظر امنیتی مقاوم باشد و هم از نظر کارایی، برای کاربردهای گسترده‌ی امروزی مناسب باشد.

AESنیز یک الگوریتم رمزنگاری بلوکی است، اما ساختار داخلی آن به‌شکل واضح‌تری از مفاهیم جبر خطی استفاده می‌کند. داده‌ها در AES به‌صورت ماتریس‌هایی از مقادیر در نظر گرفته می‌شوند و عملیات رمزنگاری شامل مجموعه‌ای از تبدیل‌های خطی و غیرخطی روی این ماتریس‌هاست.

یکی از دلایل اصلی استفاده از ماتریس در AES این است که این ساختار امکان انجام تبدیل‌های هم‌زمان و منظم روی داده‌ها را فراهم می‌کند. عملیات ترکیب سطرها و ستون‌ها را می‌توان به‌صورت تبدیل‌های خطی مدل‌سازی کرد که هم سریع هستند و هم باعث افزایش پخش‌شدگی اطلاعات می‌شوند. اگر داده‌ها به‌صورت آرایه‌های ساده پردازش می‌شدند، دستیابی به این سطح از امنیت و ساختارپذیری دشوارتر بود.

ورودی AES شامل یک بلوک داده و یک کلید رمزنگاری است و خروجی آن بلوک رمزشده می‌باشد. در هر مرحله، داده‌ها تحت چندین عملیات مشخص قرار می‌گیرند که هر کدام نقش خاصی در افزایش امنیت دارند. این مراحل به‌گونه‌ای طراحی شده‌اند که تغییر کوچک در ورودی یا کلید، تغییرات گسترده‌ای در خروجی ایجاد کند.

در حال حاضر، AESیکی از پرکاربردترین الگوریتم‌های رمزنگاری در جهان است و در زمینه‌هایی مانند ارتباطات امن، ذخیره‌سازی داده و سیستم‌های بانکی مورد استفاده قرار می‌گیرد. ترکیب مناسب تبدیل‌های خطی و غیرخطی، همراه با طراحی دقیق ساختار الگوریتم، باعث شده است که AES در برابر بسیاری از حملات شناخته‌شده مقاوم باشد.

۴-۳- جمع‌بندی فصل

الگوریتم‌هایHill ، DESو AES هر کدام در پاسخ به نیازهای امنیتی دوره‌ی خود طراحی شده‌اند و میزان استفاده‌ی آن‌ها از جبر خطی با گذشت زمان تکامل یافته است Hill Cipher .نمونه‌ای ساده و آموزشی از کاربرد مستقیم جبر خطی است، DESمرحله‌ای میانی در گذار به الگوریتم‌های مدرن محسوب می‌شود، و AES نمونه‌ای کامل از استفاده‌ی هدفمند و پیشرفته‌ی مفاهیم جبر خطی در رمزنگاری امروزی است. بررسی این الگوریتم‌ها نشان می‌دهد که چگونه ابزارهای ریاضی، به‌ویژه جبر خطی، نقش مهمی در افزایش امنیت داده‌ها ایفا کرده‌اند.

فصل چهارم

کاربردهای دیگر جبر خطی در رمزنگاری

٤- کاربردهای دیگر جبر خطی در رمزنگاری

جبر خطی تنها در الگوریتم‌های کلاسیک یا مدرن رمزنگاری مانندHill ، DESو AES کاربرد ندارد، بلکه ابزار قدرتمندی است که در حوزه‌های گسترده‌ای از امنیت داده مورد استفاده قرار می‌گیرد. در این فصل، برخی از مهم‌ترین کاربردهای دیگر جبر خطی در امنیت داده معرفی می‌شوند و به صورت مختصر توضیح داده می‌شود که چرا این مفاهیم ریاضی برای هر کاربرد مناسب هستند.

۴-۱- رمزنگاری مبتنی بر شبکه‌ها(Lattice-based Cryptography)

یکی از زمینه‌های پیشرفته و رو به رشد در امنیت داده، رمزنگاری مبتنی بر شبکه‌هاست. این الگوریتم‌ها بر پایه‌ی ساختارهای برداری چندبعدی طراحی می‌شوند که به شدت با جبر خطی مرتبط هستند. در این روش‌ها، داده‌ها به صورت بردارهای چندبعدی در فضای شبکه قرار می‌گیرند و عملیات رمزنگاری شامل ترکیب‌های خطی پیچیده روی این بردارها است.

مزیت اصلی این روش، مقاومت بالای آن در برابر حملات کوانتومی است. شبکه‌ها امکان ایجاد معادلات خطی و ماتریسی پیچیده را فراهم می‌کنند که حل آن‌ها حتی با توان محاسباتی بسیار بالا دشوار است. به همین دلیل، جبر خطی ابزار اصلی طراحی و تحلیل این الگوریتم‌ها محسوب می‌شود. پیش‌نیاز لازم برای فهم این روش، درک مفاهیم بردار و ماتریس است که در فصل دوم توضیح داده شد.

۴-۲- کاهش ابعاد و تحلیل داده‌ها برای امنیت(PCA)

در زمینه‌های تشخیص نفوذ و تحلیل داده‌های امنیتی، حجم اطلاعات می‌تواند بسیار زیاد باشد. یکی از روش‌های مدیریت این حجم، استفاده از **کاهش ابعاد داده‌ها** با کمک تکنیک‌هایی مانند تحلیل مؤلفه‌های اصلی (PCA) است PCA .بر پایه جبر خطی عمل می‌کند و داده‌ها را به صورت بردارها و ماتریس‌ها پردازش می‌کند تا ابعاد آن‌ها کاهش یابد و الگوهای مهم داده حفظ شوند.

استفاده از PCA در امنیت داده باعث می‌شود الگوهای حمله یا رفتار غیرعادی سریع‌تر شناسایی شوند. تبدیل داده‌ها به فضای برداری و محاسبه مؤلفه‌های اصلی، بدون دانش جبر خطی امکان‌پذیر نیست. این مثال نشان می‌دهد که جبر خطی نه‌تنها در رمزنگاری بلکه در تحلیل و مانیتورینگ امنیت داده نیز حیاتی است.

۴-۳- امضای دیجیتال و کدهای تصحیح خطا

جبر خطی در امضای دیجیتال و کدهای تصحیح خطا نیز کاربرد دارد. برای مثال، برخی الگوریتم‌های امضای دیجیتال از ماتریس‌ها برای تولید کلید عمومی و خصوصی استفاده می‌کنند. عملیات ضرب ماتریسی و ترکیب بردارها در این الگوریتم‌ها باعث می‌شود هر امضا به کلید منحصر به فرد وابسته باشد و قابل جعل نباشد.

در کدهای تصحیح خطا، داده‌ها به صورت بلوک‌های برداری منتقل می‌شوند و ماتریس‌های مشخص برای اضافه کردن بیت‌های بررسی استفاده می‌شوند. این ساختار باعث می‌شود خطاها قابل شناسایی و اصلاح باشند. جبر خطی در اینجا نقش اصلی در طراحی الگوریتم‌ها و تضمین صحت داده‌ها دارد.

۴-۴- رمزنگاری چندطرفه و اشتراک‌گذاری امن داده‌ها

در محیط‌های مدرن که داده‌ها بین چندین طرف به اشتراک گذاشته می‌شوند، حفظ امنیت و محرمانگی اهمیت ویژه‌ای پیدا می‌کند. جبر خطی در این زمینه برای ایجاد **طرح‌های اشتراک‌گذاری امن** به کار می‌رود. به این صورت که داده‌ها به بردارها یا ماتریس‌هایی تقسیم می‌شوند و هر بخش به شکل رمزنگاری‌شده بین طرف‌ها توزیع می‌شود. ترکیب بخش‌های داده با استفاده از تبدیل‌های خطی امکان بازیابی داده اصلی را تنها به کاربران مجاز می‌دهد.

این روش‌ها در سیستم‌های بانکی، پردازش ابری و مدیریت داده‌های حساس کاربرد دارند و نشان می‌دهند که جبر خطی فراتر از الگوریتم‌های رمزنگاری سنتی، در معماری امنیت داده نیز نقش دارد.

۵-۴- جمع‌بندی

جبر خطی ابزار قدرتمندی است که نه تنها در رمزنگاری کلاسیک و مدرن کاربرد دارد، بلکه در زمینه‌های پیشرفته‌ای مانند رمزنگاری مقاوم در برابر کوانتوم، تحلیل داده‌های امنیتی، امضای دیجیتال، کدهای تصحیح خطا و اشتراک‌گذاری امن داده‌ها نیز نقش حیاتی ایفا می‌کند. مزیت اصلی استفاده از مفاهیم بردار و ماتریس این است که داده‌ها را می‌توان به‌صورت منظم و ساختارمند پردازش کرد و پیچیدگی لازم برای امنیت را ایجاد نمود.

با آشنایی با کاربردهای دیگر جبر خطی در امنیت داده، می‌توان درک بهتری از نقش این شاخه‌ی ریاضی در طراحی الگوریتم‌های امن و تحلیل داده‌ها پیدا کرد و فهمید چرا این ابزار هنوز یکی از کلیدی‌ترین عناصر در حوزه امنیت اطلاعات محسوب می‌شود.

فصل پنجم

مثال واقعی و نتیجه‌گیری

۵- فصل پنجم: مثال واقعی و نتیجه‌گیری

توی این فصل یک مثال واقعی میزنیم از الگوریتم Hill برای دیدن بقیه مثال ها و نتایج کدی که در کنار پروژه قرار گرفته است به صورت کامل چند مثال عملی داره

۵-۱- مثال واقعی

برای روشن‌تر شدن نقش جبر خطی در رمزنگاری و نحوه‌ی عملکرد الگوریتم‌ها، یک سناریوی ساده اما واقعی از رمزنگاری پیام متنی با الگوریتم Hill ارائه می‌شود. فرض کنید یک شرکت کوچک می‌خواهد پیام «HELLO» را به شکل امن بین دفتر مرکزی و یکی از شعب خود منتقل کند. هدف این است که اگر کسی به پیام دسترسی پیدا کند، بدون کلید رمز نتواند محتوای آن را بخواند.

۱- داده ورودی

پیام اصلی:

HELLO

کلید رمز (ماتریس ۲×۲):

| 3 3 |

| 2 5 |

در این سناریو، پیام ابتدا به مقادیر عددی تبدیل می‌شود (A=0, B=1, …, Z=25) و سپس به بلوک‌های دو حرفی تقسیم می‌شود. این تبدیل داده‌ها به بردارهای عددی، نمونه‌ای از استفاده‌ی جبر خطی برای نمایش داده‌هاست.

۲- خروجی رمزنگاری‌شده

پس از ضرب هر بردار پیام در ماتریس کلید و اعمال عملیات پیمانه‌ای(mod 26) ، پیام رمزنگاری‌شده به شکل زیر به دست می‌آید:

RMQBT

این متن برای فردی که کلید را ندارد، به هیچ وجه قابل فهم نیست. تنها گیرنده‌ی مجاز که ماتریس کلید و روش رمزگشایی را می‌داند، می‌تواند با استفاده از معکوس ماتریس، پیام اصلی را بازگرداند.

۳- تحلیل امنیتی

تحلیل این مثال نشان می‌دهد که استفاده از ماتریس باعث وابستگی هر حرف رمز به چندین حرف پیام اصلی می‌شود. این وابستگی پخش‌شدگی اطلاعات را افزایش می‌دهد و تحلیل رمز را برای مهاجم سخت‌تر می‌کند. با این حال، همان‌طور که در فصل سوم توضیح داده شد، Hill Cipherدر برابر حملات متن معلوم آسیب‌پذیر است و برای استفاده عملی در سیستم‌های امروزی کافی نیست. با این وجود، این مثال نشان می‌دهد که جبر خطی چگونه پایه‌ی منطقی و ساختارمند برای رمزنگاری فراهم می‌کند.

۲-۵- نتیجه‌گیری

بررسی الگوریتم‌هایHill ، DESو AES و کاربردهای دیگر جبر خطی در امنیت داده نشان می‌دهد که این شاخه‌ی ریاضی هنوز نقش کلیدی در طراحی سیستم‌های امن ایفا می‌کند. جبر خطی به طراحان رمزنگاری اجازه می‌دهد داده‌ها را به شکل ساختارمند پردازش کنند، پیچیدگی کافی برای امنیت ایجاد کنند و عملیات را به شکل قابل پیاده‌سازی روی سیستم‌های کامپیوتری درآورند.

با گذر زمان، برخی الگوریتم‌ها مانند Hill و DES منسوخ شده‌اند .Hill به دلیل ضعف در برابر تحلیل آماری و DES به دلیل اندازه‌ی کوچک کلید و آسیب‌پذیری در برابر حملات brute-force دیگر در سیستم‌های عملی کاربرد ندارند. جایگزین آن‌ها، الگوریتم‌هایی مانند AES و رمزنگاری مبتنی بر شبکه‌ها است که ترکیبی از عملیات خطی و غیرخطی را به کار می‌برند و امنیت بسیار بالاتری فراهم می‌کنند.

آینده این حوزه با توسعه‌ی الگوریتم‌های مقاوم در برابر حملات کوانتومی و استفاده‌ی گسترده از روش‌های تحلیل داده، بیش از پیش به جبر خطی وابسته است. مفاهیم بردار، ماتریس و تبدیل‌های خطی به پایه‌ای برای رمزنگاری امن، تحلیل داده‌ها و اشتراک‌گذاری ایمن تبدیل شده‌اند و انتظار می‌رود که در سال‌های آینده نیز نقش حیاتی خود را حفظ کنند.

منابع

منابع انگلیسی

- [۲] Daemen, J., & Rijmen, V. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer, 2002.
- [۳] Hill, L. S.; "Cryptography in an Algebraic Alphabet," *The American Mathematical Monthly*, ۳۶(۶), ۳۰۶-۳۱۲, ۱۹۲۹.
- [۴] Katz, J., & Lindell, Y. *Introduction to Modern Cryptography*, CRC Press, 2014.
- [۵] Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. *Handbook of Applied Cryptography*, CRC Press, 1996.
- [۶] National Institute of Standards and Technology; *Advanced Encryption Standard (AES)*, FIPS PUB 197, 2001.
- [۷] National Institute of Standards and Technology; *Data Encryption Standard (DES)*, FIPS PUB 46-3, 1999.
- [۸] Paar, C., & Pelzl, J. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer, 2009.
- [۹] Stinson, D. R. *Cryptography: Theory and Practice*, CRC Press, 2005.

پیوست کدها (Primary Sources / Appendix)

- [۱۰] پیاده‌سازی کد: فایل aes_cipher.py، پروژه رمزنگاری با استفاده از ماتریس و جبر خطی.
- [۱۱] پیاده‌سازی کد: فایل des_cipher.py، پروژه رمزنگاری با استفاده از ماتریس و جبر خطی.

- **[۱۲]** پیاده‌سازی کد: فایل hill_cipher.py، پروژه رمزنگاری با استفاده از ماتریس و جبر خطی.
- **[۱۳]** پیاده‌سازی کد: فایل test.py، پروژه رمزنگاری با استفاده از ماتریس و جبر خطی.