فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

فهرست اختصارات

نوعی سیستم رمز با امنیت کامل ..... OTP = One Time Pad

کانال متقارن دودویی (باینری) ..... BSC = Binary Symmetric Channel

میدان گالویس ..... GF(.) = Galios Field

ماشین تورینگ (ماشین حالت محدود) ..... TM = Turing Machine

الفبای استاندارد مستقیم ..... DSA = Direct Standard Alphabet

معیار ناهمواری ..... M.R. = Measure of Roughness

ضریب انطباق ..... I.C. = Index of Coincidence

دنباله‌ی گالوب ..... G-sequence = Golomb sequence

دنباله‌ی اعداد شبه‌تصادفی ..... PN-sequence = Pseudo-Number sequence

ثبات انتقال با پس‌خورد ..... FSR = Feedback Shift Register

ثبات انتقال با پس‌خورد خطی ..... LFSR = Linear Feedback Shift Register

دنباله‌ی با تناوب بیشینه (ماگزیمم) ..... m-sequence = maximal sequence

ثبات انتقال با پس‌خورد غیرخطی ..... NLFSR = Non-Linear Feedback Shift Register

نوعی سیستم رمز قالبی ..... NDS = New Data Seal

استاندارد رمزگذاری داده (نوعی رمز قالبی استاندارد) ..... DES = Data Encryption Standard

جعبه‌ی جانشینی ..... S-Box = Substitution Box

نوعی سیستم رمز کلید همگانی ..... RSA = Rivest Shamir Adelman

چکیده پیام (همچنین خانواده‌ای از الگوریتم‌های چکیده‌ساز است) ..... MD = Message Digest

کدهای آشکارساز تغییر ..... MDC = Modification Detection Codes

توابع چکیده‌ساز یک‌طرفه ..... OWHF = One Way Hash Furictions

کدهای جامعیت پیام ..... MIC = Message Integrity Codes

کدهای اعتبارسنجی پیام ..... MAC = Message Authentication Codes

توابع چکیده‌ساز مقاوم در برابر تصادم ..... CRHF = Collision Resistant Hash Functions

استاندارد امضا چکیده‌ی امن ..... SHSS = Secure Hash Signature Standard

الگوریتم چکیده‌ساز امن ..... SHA = Secure Hash Algorithm

الگوریتم امضا دیجیتال ..... DSA = Digital Signature Algorithm

پیشگفتار ناشر

ورود رایانه‌ها به زندگی بشر و احاطه‌ی ایشان در عرصه‌های مختلف، آرام‌آرام زندگی انسان عصر جدید را وارد مرحله‌ای نوین کرد. پیرامون محیط زندگی هر بشر امروزی، انواع رایانه‌های شخصی، سیستم‌های ارتباطی و تبادل اطّلاعات، دستگاه‌های خودپرداز و ... انباشته شده است.

در شرایطی که زندگی بشر از شکل سنّتی خود، به شکل استحاله شده‌ی کنونی تغییر یافت، نوع زندگی انسان دگرگون شد و با این تغییر و دگرگونی، ناهنجاری‌های جامعه‌ی شهری شکل دیگری به خود گرفت. با ظهور اشکال دیگری از دارایی‌های انسان آن‌هم دارایی‌هایی از نوع رایانه‌ای، مانند انواع داده‌های صوتی، تصویری، متنی و عددی، نوع جدیدی از بزه‌کاران اجتماعی که همان سارقان و نفوذگران رایانه‌ای می‌باشند، شکل گرفت. این بزه‌کاران جدید رایانه‌ای با ساختن انواع ویروس‌ها و کرم‌های رایانه‌ای آنان را به جان رایانه‌ها انداختند تا انواع آلودگی‌ها را وارد رایانه نمایند تا با این‌کار تهدیدات خود را عملی ساخته و با هجوم بر اعصاب و روان انسان، تهدیدی جدی برای دارایی‌هایش باشند.

با توجّه به آن‌چه که ذکر شد، علم رمزشناسی که علم مطالعه‌ی محرمانه‌سازی اطّلاعات است و در دنیای مدرن به‌عنوان گرایشی از رشته‌های ریاضیات، کامپیوتر، مخابرات و فناوری اطّلاعات به‌حساب می‌آید و رابطه‌ی تنگاتنگی با نظریه‌ی اطّلاعات، امنیت کامپیوتر و مهندسی ارتباطات و فناوری اطّلاعات دارد، برای مقابله با تهدیدات جدّی سارقان رایانه‌ای، وارد عرصه‌ای جدید شد و بیش از پیش رونق گرفت و توسعه یافت.

مؤلّف محترم این کتاب که سال‌های زیادی با مسائل کاربردی، صنعتی، آموزشی و پژوهشی رمز، سروکار داشته و دارد و از طرفی هم در مراکز دانشگاهی مختلف به تدریس درس

اصول رمزنگاری در مقاطع مختلف دانشگاهی پرداخته است، اقدام به تألیف کتاب حاضر با عنوان «رمزشناسی مقدماتی» کرد و پیشنهاد چاپ و انتشار آن را هم به مؤسسه‌ی فرهنگی هنری پردازش هوشمند علائم نمود.

این مؤسسه در راستای اهداف پژوهشی و آموزشی خود به‌منظور انتشار کتابی ارزشمند در زمینه‌ی رمزشناسی، ضمن قبول پیشنهاد مؤلّف اندیشمند محترم کتاب، جناب آقای دکتر جواد شیخ‌زادگان که از اساتید جدّی درگیر با مباحث رمز می‌باشند، این کتاب را چاپ و منتشر کرد تا با ورود آن به بازار کتاب، بتواند در کنار دیگر کتاب‌های موجود در بازار، به سهم خود گامی هر چند کوچک در جهت رشد و ارتقای علمی دانشجویان این رشته و کارشناسان و دانش‌آموختگان حوزه‌ی امنیت ارتباطات و درنهایت در راستای پیشرفت و پیش‌برد اهداف فرهنگی و آموزشی کشورمان به حساب آید.

انتشارات مؤسسه‌ی فرهنگی هنری
پردازش هوشمند علائم
زمستان ۱۳۸۹

پیشگفتار مؤلف

تأمین امنیت ارتباطات از دیرباز در تبادل پیغام‌های طبقه‌بندی شده نظیر ارتباطات نظامی، امنیتی و از این قبیل، از اهمّیت خاصی برخوردار بوده است. با توسعه و گسترش ارتباطات و فناوری اطّلاعات در دو دهه‌ی اخیر و نفوذ آن در فعّالیت‌های مدنی از قبیل فعّالیت‌های اقتصادی، اجتماعی، فرهنگی‌و غیره، فضای خیلی وسیع‌تری در رابطه با موضوع امنیت ارتباطات و اطّلاعات گشوده شد و به تبع آن نیازمندی‌های متنوع زیادی در این عرصه مطرح گردید.

رمزنگاری که به‌عنوان یکی از ابزارهای تأمین امنیت ارتباطات و اطّلاعات از روزگاران قدیم شناخته شده است، مقارن توسعه و گسترش ارتباطات و فناوری اطّلاعات در دو سه دهۀ اخیر، بیش از پیش مورد توجّه قرار گرفته است؛ به‌طوری‌که از حدود دو دهه‌ی پیش، درس "اصول رمزنگاری" در تعدادی از دانشگاه‌های کشورمان ارائه گردیده و نیز در رشته‌های مخابرات، کامپیوتر و ریاضی گرایش خاصّی به نام گرایش رمز به‌وجود آمده است.

از آن‌جا که اینجانب بیش از دو دهه است که با مسائل کاربردی، صنعتی و آموزشی و پژوهشی رمز کم و بیش سروکار دارم و در این مدّت چند نیم‌سال تحصیلی به‌طور متناوب درس اصول رمزنگاری را برای مقاطع کارشناسی و کارشناسی ارشد تدریس کرده‌ام، از این‌رو علی‌رغم وجود کتاب‌های خیلی خوب خارجی و نیز تعداد خیلی محدودی کتب یا جزوات فارسی در این زمینه، نیاز به یک کتاب به زبان فارسی را که هم تاحدودی جامع مطالب رمزگاری بوده و هم به‌طور نسبی ساده و مناسب دانشجویان، به‌خصوص دانشجویان مقطع کارشناسی باشد، احساس کرده و درصدد تألیف کتاب حاضر برآمدم.

این کتاب شامل چهار فصل است که در فصل اوّل کلّیات رمزشناسی از قبیل تاریخچه، تعاریف، اصطلاحات، مفاهیم پایه‌ای و غیره آورده شده‌اند که در مجموع حدود پنجاه صفحه از

کتاب را تشکیل داده است. فصل دوم مربوط به رمزهای ابتدایی است که به‌طور عمده، روش‌های رمزنگاری، رمزگشایی و رمزشکنی سنّتی در آن بحث می‌شود و از آن‌جا که این‌گونه رمزها بر روی نویسه‌های پیغام عمل می‌کنند، از این‌رو به آن‌ها رمزهای الفبایی نیز گفته شده است. در فصل سوّم، رمزهایی بحث می‌شوند که بر روی داده‌های دودویی عمل می‌کنند، ما این‌گونه رمزها را رمزهای دیجیتال نامیده‌ایم (در مقابل رمزهای الفبایی). فصل چهارم شامل مطالبی در مورد سیستم‌های کلید عمومی (همگانی) و کاربرد آن‌هاست. علاوه بر این‌که رمزنگاری مدرن مبتنی بر سیستم‌های کلید عمومی است، این سیستم‌ها دارای کاربردهای دیگری نیز نظیر توزیع کلید و امضای دیجیتال هستند که امروزه اهمّیت هر یک از این کاربردها کمتر از رمز نگاری نیست. از این‌رو در یکی دو دهه‌ی اخیر، سیستم‌های کلید عمومی خیلی مورد توجّه قرار گرفته است. بدین ترتیب این کتاب عمده‌ی مطالب مربوط به مباحث رمز را اعم از تاریخچه، تعاریف، مفاهیم پایه، رمزهای سنتی، رمزهای دیجیتال کلاسیک، رمزهای مدرن و امضای دیجیتال را دربرگرفته است. امیدواریم که تألیف این کتاب گامی هر چند کوچک در جهت ارتقای علمی دانشجویان، دانش آموختگان و کارشناسان حوزه‌ی امنیت ارتباطات و در نهایت در راستای پیشرفت و پیشبرد اهداف عالیه آموزشی و فرهنگی کشورمان به‌حساب آید.

در خاتمه لازم می‌دانم که بدین‌وسیله مراتب تشّکر و قدردانی خود را از زحمات بی‌شایبه‌ی آقایان محّمداسماعیل قاصدی و محسن کرم‌زاده و خانم میترا پاکدل که در آماده‌سازی کتاب، حروف‌چینی و صفحه‌آرایی این اثر از هیچ کمکی مضایقه نکردند، اعلام کرده و از مسئولان پژوهشکده‌ی پردازش هوشمند علائم نیز که حمایت‌های لازم را در راستای چاپ و نشر این کتاب به‌عمل آوردند، تشکّر و سپاس‌گزاری نمایم.

والسّلام
جواد شیخ‌زادگان
زمستان۱۳۸۹

پیشگفتار مؤلف

تأمین امنیت ارتباطات از دیرباز در تبادل پیغام‌های طبقه‌بندی شده نظیر ارتباطات نظامی، امنیتی و از این قبیل، از اهمّیت خاصی برخوردار بوده است. با توسعه و گسترش ارتباطات و فناوری اطّلاعات در دو دهۀ اخیر و نفوذ آن در فعّالیت‌های مدنی از قبیل فعّالیت‌های اقتصادی، اجتماعی، فرهنگی و غیره، فضای خیلی وسیع‌تری در رابطه با موضوع امنیت ارتباطات و اطّلاعات گشوده شد و به تبع آن نیازمندی‌های متنوع زیادی در این عرصه مطرح گردید.

رمزنگاری که به‌عنوان یکی از ابزارهای تأمین امنیت ارتباطات و اطّلاعات از قدیم الآیام شناخته شده است، مقارن توسعه و گسترش ارتباطات و فناوری اطّلاعات در دو سه دهۀ اخیر، بیش از پیش مورد توجّه قرار گرفته است، به‌طوری‌که از حدود دو دهۀ پیش درس "اصول رمزنگاری" در تعدادی از دانشگاه‌های کشورمان ارائه گردیده و نیز در رشته‌های مخابرات، کامپیوتر و ریاضی گرایش خاصّی به نام گرایش رمز به‌وجود آمده است.

از آن‌جا که اینجانب بیش از دو دهه است که با مسائل کاربردی، صنعتی و آموزشی و پژوهشی رمز کم و بیش سرو کار دارم و در این مدّت چند نیم‌سال تحصیلی به‌طور متناوب درس اصول رمزنگاری را برای مقاطع کارشناسی و کارشناسی ارشد تدریس کرده‌ام، از این‌رو علی‌رغم وجود کتاب‌های خیلی خوب خارجی و نیز تعداد خیلی محدودی کتب یا جزوات فارسی در این زمینه، نیاز به یک کتاب به زبان فارسی را که هم تاحدودی جامع مطالب رمزگاری بوده و هم نسبتاً ساده و مناسب دانشجویان به‌خصوص دانشجویان مقطع کارشناسی باشد، احساس کرده و در صدد تألیف کتاب حاضر برآمدم.

این کتاب شامل چهار فصل است که در فصل اوّل کلّیات رمزشناسی از قبیل تاریخچه، تعاریف، اصطلاحات، مفاهیم پایه‌ای و غیره آورده شده‌اند که مجموعاً حدود پنجاه صفحه از

کتاب را تشکیل داده است. فصل دوم مربوط به رمزهای ابتدایی است که عمدتاً روش‌های رمزنگاری، رمزگشایی و رمزشکنی سنّتی در آن بحث می‌شود و از آن‌جا که این‌گونه رمزها بر روی نویسه‌های پیغام عمل می‌کنند، از این‌رو به آن‌ها رمزهای الفبایی نیز گفته شده است. در فصل سوّم رمزهایی بحث می‌شوند که بر روی داده‌های دودویی عمل می‌کنند، ما این‌گونه رمزها را رمزهای دیجیتال نامیده‌ایم (در مقابل رمزهای الفبایی). فصل چهارم شامل مطالبی در مورد سیستم‌های کلید عمومی (همگانی) و کاربرد آن‌هاست. علاوه بر اینکه رمز نگاری مدرن مبتنی بر سیستم‌های کلید عمومی است ، این سیستم‌ها دارای کاربردهای دیگری نیز نظیر توزیع کلید و امضای دیجیتال هستندکه امروزه اهمّیت هر یک از این کاربردها کمتر از رمز نگاری نیست . از اینرو در یکی دو دهۀ اخیر سیستم‌های کلید عمومی خیلی مورد توجّه قرار گرفته است. بدین ترتیب این کتاب عمدۀ مطالب مربوط به مباحث رمز را اعم از تاریخچه، تعاریف، مفاهیم پایه، رمزهای سنتی، رمزهای دیجیتال کلاسیک، رمزهای مدرن و امضاء دیجیتال را در بر گرفته است. امیدواریم که تألیف این کتاب گامی هر چند کوچک در جهت ارتقای علمی دانشجویان، دانش آموختگان و کارشناسان حوزۀ امنیت ارتباطات و نهایتاً در راستای پیشرفت و پیشبرد اهداف عالیه آموزشی و فرهنگی کشورمان به‌حساب آید.

در خاتمه لازم می‌دانم که بدین‌وسیله مراتب تشّکر و قدردانی خود را از زحمات بی‌شایبه‌ی آقایان محّمداسماعیل قاصدی و محسن کرم‌زاده و خانم میترا پاکدل که در آماده‌سازی کتاب، حروف‌چینی و صفحه‌آرایی این اثر از هیچ کمکی مضایقه نکردند، اعلام کرده و از مسئولان پژوهشکده پردازش هوشمند علائم نیز که حمایت‌های لازم را در راستای چاپ و نشر این کتاب به‌عمل آوردند، تشکّر و سپاس‌گزاری نمایم.

والسّلام

جواد شیخ‌زادگان

زمستان۱۳۸۹

پیشگفتار ناشر

ورود رایانه‌ها به زندگی بشر و احاطه‌ی آن در عرصه‌های مختلف، آرام‌آرام زندگی انسان عصر جدید را وارد مرحله‌ای نوین کرد. پیرامون محیط زندگی هر بشر امروزی، انواع رایانه‌های شخصی، سیستم‌های ارتباطی و تبادل اطّلاعات، دستگاه‌های خودپرداز و ... انباشته شده است.

در شرایطی که زندگی بشر از شکل سنّتی خود، به شکل استحاله شده‌ی کنونی تغییر یافت، نوع زندگی انسان دگرگون شد و با این تغییر و دگرگونی، ناهنجاری‌های جامعه‌ی شهری شکل دیگری به خود گرفت. ظهور اشکال دیگری از دارایی‌های انسان آن‌هم دارایی‌هایی از نوع رایانه‌ای، مانند انواع داده‌های صوتی، تصویری، متنی و عددی، نوع جدیدی از بزه‌کاران اجتماعی که همان سارقان و نفوذگران رایانه‌ای می‌باشند، شکل گرفت. این بزه‌کاران جدید رایانه‌ای با ساختن انواع ویروس‌ها و کرم‌های رایانه‌ای آنان را به جان رایانه‌های انداختند تا انواع آلودگی‌ها را وارد نمایند تا با این‌کار تهدیدات خود را عملی ساخته و با هجوم بر اعصاب و روان انسان، تهدیدی جدی برای دارایی‌های آن باشند.

با توجّه به آن‌چه که ذکر شد، علم رمزشناسی که علم مطالعه‌ی مخفی‌سازی اطّلاعات است و در دنیای مدرن به‌عنوان گرایشی از رشته‌های ریاضیات، کامپیوتر، مخابرات و فناوری اطلاعات به‌حساب می‌آید و رابطه‌ی تنگاتنگی با نظریه‌ی اطّلاعات، امنیت کامپیوتر و مهندسی ارتباطات و فناوری اطّلاعات دارد، برای مقابله با تهدیدات جدّی سارقان رایانه‌ای، وارد عرصه‌ای جدید شد تا با جلوگیری از اقدامات مخربانه‌ی‌شان از دغدغه‌های انسان برای حفاظت دارایی‌هایش بکاهد.

مؤلّف محترم این کتاب که سال‌های زیادی با مسائل کاربردی، صنعتی، آموزشی و پژوهشی رمز سروکار داشته و دارد و از طرفی هم در مراکز دانشگاهی مختلف به تدریس درس اصول رمزنگاری در مقاطع مختلف دانشگاهی پرداخته است، اقدام به تألیف کتاب حاضر با عنوان «رمزشناسی مقدماتی» کرد و پیشنهاد چاپ و انتشار آن را هم به مؤسسه‌ی فرهنگی هنری پردازش هوشمند علائم نمود.

این مؤسسه در راستای اهداف پژوهشی و آموزشی خود به‌منظور انتشار کتابی ارزشمند در زمینه‌ی رمزشناسی، ضمن قبول پیشنهاد مؤلّف اندیشمند محترم کتاب، جناب آقای دکتر جواد شیخ‌زادگان که از اساتید جدّی درگیر با مباحث رمز می‌باشند، این کتاب را چاپ و منتشر کرد تا با ورود آن به بازار کتاب، بتواند در کنار دیگر کتاب‌های موجود در بازار، به سهم خود گامی هر چند کوچک در جهت رشد و ارتقای علمی دانشجویان این رشته و کارشناسان و دانش‌آموختگان حوزه‌ی امنیت ارتباطات و درنهایت در راستای پیشرفت و پیش‌برد اهداف فرهنگی و آموزشی کشورمان به حساب آید.

انتشارات مؤسسه‌ی فرهنگی هنری
پردازش هوشمند علائم
زمستان ۱۳۸۹