

فهرست مطالب

صفحه	عنوان
	فصل اول: کلیات
۱	۱-۱- مقدمه
۲	۲-۱- تاریخچه رمز
۶	۳-۱- تعاریف و اصطلاحات رمزشناسی
۹	۴-۱- انواع حمله‌ها برای شکستن رمز
۹	۵- امنیت در سیستم‌های رمزنگاری
۱۰	۶-۱- معیارهای پنج‌گانه‌ی ارزیابی شانون
۱۱	۷-۱- انواع حمله‌ها از نظر هدف دشمن
۱۳	۸-۱- پارامترهای یک سیستم رمزنگاری
۱۵	۹-۱- سیستم‌های کلید همگانی
۱۷	۱۰-۱- امضای دیجیتال
۱۸	۱۱-۱- نظریه‌ی اطلاعات و رمزنگاری
۱۹	۱-۱۱-۱- آنتروپی یک منبع اطلاعات گسسته و بدون حافظه
۲۲	۲-۱۱-۱- اطلاعات متقابل
۲۳	۳-۱۱-۱- مدل رمزنگاری شانون
۲۶	۴-۱۱-۱- فاصله‌ی قابل شکست
۳۲	۱۲-۱- نظریه‌ی اعداد
۳۲	۱-۱۲-۱- همنهشت‌ها و حساب پیمانه‌ای
۳۴	۲-۱۲-۱- محاسبه‌ی عکس اعداد در فضای modn
۴۱	۳-۱۲-۱- معادلات همزمانی خطی - قضیه‌ی باقیمانده‌ی چینی
۴۳	۴-۱۲-۱- میدان گالویس
۴۸	۱۳-۱- نظریه‌ی پیچیدگی
	فصل دوم : سیستم‌های رمز ابتدایی (رمزهای الفبایی)
۵۲	۱-۲- سیستم‌های جانشینی
۵۲	۱-۱-۲- سیستم‌های جانشینی تک‌الفبایی و تک‌حرفی
۷۱	۲-۱-۲- سیستم‌های جانشینی تک‌حرفی هم‌آوایی
۷۱	۳-۱-۲- سیستم‌های جانشینی چندالفبایی

۹۳ ۴-۱-۲ سیستم‌های جانشینی چندحرفی
۱۰۲ ۲-۲ سیستم‌های رمز جابجایی
۱۰۳ ۱-۲-۲ سیستم‌های جابجایی سنتی
۱۰۶ ۲-۲-۲ سیستم جابجایی ستونی

فصل سوم : سیستم‌های رمز دیجیتال (رمزهای پی‌درپی و قالبی)

۱۱۱ ۱-۳ رمزهای پی‌درپی
۱۱۳ ۱-۱-۳ تعاریف
۱۱۳ ۲-۱-۳ معیارهای گالوب
۱۱۴ ۳-۱-۳ آزمون‌های آماری
۱۱۶ ۴-۱-۳ تولید دنباله‌ی نامحدود از دنباله‌ی محدود - ماشین حالت محدود
۱۱۸ ۵-۱-۳ شیفت رجیستر با پس‌خورد خطی (LFSR)
۱۲۵ ۶-۱-۳ فاصله‌ی قابل شکست برای LFSR n طبقه
۱۲۵ ۷-۱-۳ امنیت سیستم LFSR
۱۲۹ ۸-۱-۳ توابع پس‌خورد (فیدبک) غیرخطی
۱۳۵ ۲-۳ رمزهای قالبی
۱۳۵ ۱-۲-۳ کلیاتی در مورد رمزهای قالبی
۱۴۱ ۲-۲-۳ سیستم رمز قالبی NDS
۱۴۱ ۳-۲-۳ الگوریتم رمز قالبی DES
۱۴۹ ۴-۲-۳ طرح رمزنگاری چندگانه‌ی توکرمن
۱۴۹ ۵-۲-۳ حالت‌های مختلف بکارگیری رمز قالبی

فصل چهارم : سیستم‌های کلید عمومی

۱۵۱ ۱-۴ مقدمه
۱۵۲ ۲-۴ سیستم توزیع کلید دیفی و هلمن
۱۵۲ ۳-۴ سیستم رمزنگاری نمایی پولیگ و هلمن
۱۵۳ ۴-۴ سیستم RSA
۱۵۴ ۵-۴ ویژگی‌های سیستم رمز کلید عمومی
۱۵۵ ۶-۴ مسئله‌ی کوله‌پشتی
۱۵۶ ۷-۴ سیستم کوله‌پشتی هلمن و مرکل (کوله‌پشتی با دریچه)
۱۵۷ ۸-۴ توابع چکیده‌ساز
۱۵۸ ۹-۴ خصوصیات کلی توابع چکیده‌ساز
۱۶۰ ۱۰-۴ دسته‌بندی توابع چکیده‌ساز

۱۶۱ ۱۱-۴ کاربردهای دیگر توابع چکیده‌ساز بدون کلید
۱۶۲ ۱۲-۴ خواص اضافی توابع چکیده‌ساز یک‌طرفه
۱۶۴ ۱۳-۴ توابع چکیده‌ساز مهم
۱۶۵ ۱۴-۴ استاندارد SHS
۱۷۱ ۱۵-۴ امضای دیجیتال کلید عمومی
۱۷۲ ۱۶-۴ امضای دیجیتال و کاربرد آن
۱۷۳ ۱۷-۴ نحوه‌ی ایجاد و استفاده از امضای دیجیتال
۱۷۶ فهرست منابع و مراجع
۱۷۷ ضمائم
۱۷۷ "ضمیمه‌ی الف" واژه‌نامه‌ی انگلیسی به فارسی
۱۸۶ "ضمیمه‌ی ب" واژه‌نامه‌ی فارسی به انگلیسی
۱۹۶ "ضمیمه‌ی ج" چندجمله‌ای‌های اولیه برای LFSR nطبقه
۱۹۸ "ضمیمه‌ی د" جدول تابع توزیع مرتب‌کای

فهرست شکل‌ها

صفحه	عنوان
۱۲	شکل ۱-۱: نمودار جعبه‌ای یک سیستم رمزنگاری به‌منظور بررسی محرمانه ماندن پیام ...
۱۲	شکل ۲-۱: نمودار جعبه‌ای یک سیستم رمزنگاری به‌منظور بررسی اعتبار پیام
۱۴	شکل ۳-۱: نمودار مربوط به شرط لازم برای امنیت پیام
۱۵	شکل ۴-۱: نمودار مربوط به شرط لازم برای اعتبار پیام
۱۷	شکل ۵-۱: نمودار جعبه‌ای یک سیستم کلید همگانی امن و معتبر
۱۰۴	شکل ۱-۲: نمودار نوشتن متن اصلی در رمزنگاری جایجایی براساس اشکال هندسی
۱۰۴	شکل ۲-۲: نمودار خواندن متن رمز در رمزنگاری جایجایی براساس اشکال هندسی
۱۱۲	شکل ۱-۳: نمودار کلی یک رمزکننده پی‌درپی
	شکل ۲-۳: نمودار مربوط به تولید دنباله‌ی نامحدود کلید اجرایی از دنباله‌ی محدود کلید اصلی
۱۱۷	شکل ۳-۳: نمودار حالت برای جدول تابع (مثال)
۱۱۹	شکل ۴-۳: ساختمان کلی یک ثبات انتقال با پس‌خورد (FSR)
۱۱۹	شکل ۵-۳: ساختمان یک ثبات انتقال با پس‌خورد خطی (LFSR)
۱۳۳	شکل ۶-۳: نمودار ترکیب‌کننده‌ی ضربی (هادامارد)
۱۳۴	شکل ۷-۳: نمودار ترکیب‌کننده‌ی فلیپ فلاپ J-K
۱۳۵	شکل ۸-۳: نمودار ترکیب‌کننده‌ی Pless
۱۳۸	شکل ۹-۳: نمودار ترکیب دو سیستم ترکیب خطی قالبی
۱۳۹	شکل ۱۰-۳: نمودار ترکیب دو سیستم ترکیب خطی قالبی با عامل غیرخطی جایگشتی ..
۱۳۹	شکل ۱۱-۳: نمودار الگوریتم رمز قالبی (مثال)
۱۴۲	شکل ۱۲-۳: نمودار الگوریتم رمز قالبی DES
۱۴۴	شکل ۱۳-۳: نمودار الگوریتم تولید کلیدهای دوره‌ها برای الگوریتم رمز DES
۱۴۷	شکل ۱۴-۳: نمودار الگوریتم محاسبه تابع $f(R, K)$ در الگوریتم رمز DES
۱۴۹	شکل ۱۵-۳: نمودار الگوریتم رمز DES سه‌گانه
۱۴۹	شکل ۱۶-۳: نمودار حالت رمزنگاری پی‌درپی با استفاده از الگوریتم رمز قالبی
۱۵۰	شکل ۱۷-۳: نمودار حالت کتاب کد در بکارگیری الگوریتم رمز قالبی
۱۵۰	شکل ۱۸-۳: نمودار حالت زنجیره‌سازی قالبی با استفاده از الگوریتم رمز قالبی

- شکل ۱-۴: دسته‌بندی ساده شده‌ی توابع چکیده‌ساز و کاربرد آنها ۱۶۱
- شکل ۲-۴: استفاده از تابع فشرده‌سازی در یک تابع چکیده‌سازی تکراری ۱۷۰
- شکل ۳-۴: استفاده از SHA-1 به همراه DSA ۱۷۰
- شکل ۴-۴: ایجاد چکیده پیام از پیام اولیه ۱۷۳
- شکل ۵-۴: نحوه‌ی تولید امضا از چکیده پیام ۱۷۴
- شکل ۶-۴: اضافه شدن امضا به پیام ۱۷۴
- شکل ۷-۴: چگونگی تأیید یک امضا ۱۷۵

فهرست جداول

صفحه	عنوان
	جدول ۱-۱: زمان لازم جهت محاسبه‌ی توابع پیچیدگی مختلف زمان به ازای n های مختلف
۴۹
۵۵	جدول ۱-۲: جدول ویژنر
۵۵	جدول ۲-۲: فرکانس نسبی حروف در زبان انگلیسی
۶۴	جدول ۳-۲: فراوانی حروف اول کلمات در زبان انگلیسی
۶۴	جدول ۴-۲: فراوانی حروف آخر کلمات در زبان انگلیسی
۶۸	جدول ۵-۲: فراوانی دوحرفی‌ها در زبان انگلیسی
۶۸	جدول ۶-۲: فراوانی سه‌حرفی‌ها در زبان انگلیسی
۹۴	جدول ۷-۲: جدول سیستم رمز پلی فیئر
۱۰۰	جدول ۸-۲: توزیع فرکانسی دوحرفی‌های متن رمز (مثال صفحه‌ی ۹۸)
۱۴۳	جدول ۱-۳: جدول IP برای الگوریتم رمز DES
۱۴۳	جدول ۲-۳: جدول IP^{-1} برای الگوریتم رمز DES
۱۴۵	جدول ۳-۳: جدول PC-1 در الگوریتم تولید کید دوره‌ها
۱۴۵	جدول ۴-۳: جدول PC-2 در الگوریتم تولید کلید دوره‌ها
۱۴۶	جدول ۵-۳: جدول میزان انتقال به چپ در هر دور تولید کلید دوره‌ها
۱۴۷	جدول ۶-۳: جدول E (توسعه ۳۲ بیت به ۴۸ بیت)
۱۴۸	جدول ۷-۳: جدول P در الگوریتم محاسبه‌ی تابع $f(R, K)$
۱۴۸	جدول ۸-۳: جعبه‌ی جانشینی S_1 در الگوریتم محاسبه‌ی تابع $f(R, K)$
۱۶۴	جدول ۱-۴: خواص مقاومتی مورد نیاز برای انواع کاربردهای جامعیت داده
۱۶۶	جدول ۲-۴: خصوصیات اساسی الگوریتم‌های چکیده‌سازی امن (SHAs)

فهرست اختصارات

OTP = One Time Pad	نوعی سیستم رمز با امنیت کامل
BSC = Binary Symmetric Channel	کانال متقارن دودویی (باینری)
GF(.) = Galios Field	میدان گالیوس
TM = Turing Machine	ماشین تورینگ (ماشین حالت محدود)
DSA = Direct Standard Alphabet	الفبای استاندارد مستقیم
M.R. = Measure of Roughness	معیار ناهمواری
I.C. = Index of Coincidence	ضریب انطباق
G-sequence = Golomb sequence	دنباله‌ی گالوب
PN-sequence = Pseudo-Number sequence	دنباله‌ی اعداد شبه تصادفی
FSR = Feedback Shift Register	ثبات انتقال با پس خورد
LFSR = Linear Feedback Shift Register	ثبات انتقال با پس خورد خطی
m-sequence = maximal sequence	دنباله‌ی با تناوب بیشینه (ماکزیمم)
NLFSR = Non-Linear Feedback Shift Register	ثبات انتقال با پس خورد غیرخطی
NDS = New Data Seal	نوعی سیستم رمز قالبی
DES = Data Encryption Standard	استاندارد رمزگذاری داده (نوعی رمز قالبی استاندارد)
S-Box = Substitution Box	جعبه‌ی جانشینی
RSA = Rivest Shamir Adelman	نوعی سیستم رمز کلید همگانی
MD = Message Digest	چکیده پیام (همچنین خانواده‌ای از الگوریتم‌های چکیده‌ساز است)
MDC = Modification Detection Codes	کدهای آشکارساز تغییر
OWHF = One Way Hash Furictions	توابع چکیده‌ساز یک‌طرفه
MIC = Message Integrity Codes	کدهای جامعیت پیام
MAC = Message Authentication Codes	کدهای اعتبارسنجی پیام
CRHF = Collision Resistant Hash Functions	توابع چکیده‌ساز مقاوم در برابر تصادم
SHSS = Secure Hash Signature Standard	استاندارد امضا چکیده‌ی امن
SHA = Secure Hash Algorithm	الگوریتم چکیده‌ساز امن
DSA = Digital Signature Algorithm	الگوریتم امضا دیجیتال

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 اطلاعات، دستگاه‌های خودپرداز و ... انباشته شده است. در شرایطی که زندگی بشر از شکل سنتی خود، به شکل استحال 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 این کار تهدیدات خود را عملی ساخته و با هجوم بر اعصاب و روان انسان، تهدیدی جدی برای دارایی‌هایش باشند.

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

مؤلف 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 به منظور انتشار کتابی ارزشمند در زمینه‌ی رمزشناسی، ضمن قبول پیشنهاد مؤلف اندیشمند محترم کتاب، جناب آقای دکتر جواد شیخ‌زادگان که از اساتید جدی 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 اهمیت خاصی برخوردار بوده است. با توسعه و گسترش ارتباطات و فناوری اطلاعات در دو دهه‌ی اخیر و نفوذ آن در فعالیت‌های مدنی از قبیل فعالیت‌های اقتصادی، اجتماعی، فرهنگی و غیره، فضای خیلی وسیع‌تری در رابطه با موضوع امنیت ارتباطات و اطلاعات گشوده شد و به تبع آن نیازمندی‌های متنوع‌تری در این عرصه مطرح گردید.

رمزنگاری که به‌عنوان یکی از ابزارهای تأمین امنیت ارتباطات و اطلاعات از روزگاران قدیم شناخته شده است، مقارن توسعه و گسترش ارتباطات و فناوری اطلاعات در دو سه دهه‌ی اخیر، بیش از پیش مورد توجه 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 خاصی 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 مدت 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 تا حدودی 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 اول کلیات 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 به طور عمده، روش‌های رمزنگاری، رمزگشایی و رمزشکنی سنتی 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 سوم، 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 این که رمزنگاری مدرن مبتنی بر سیستم‌های کلید عمومی است، این سیستم‌ها دارای کاربردهای دیگری نیز نظیر توزیع کلید و امضای دیجیتال هستند که امروزه اهمیت هر یک از این کاربردها کمتر از رمزنگاری نیست. از این‌رو در یکی دو دهه‌ی اخیر، سیستم‌های کلید عمومی خیلی مورد توجه 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، دانش‌آموختگان و کارشناسان حوزه‌ی امنیت ارتباطات و در نهایت در راستای پیشرفت و پیشبرد اهداف عالی آموزش و فرهنگی کشورمان به حساب آید.

در خاتمه لازم می‌دانم که بدین وسیله مراتب تشکر و قدردانی خود را از زحمات بی‌شایبهِ آقایان محمداسماعیل 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 به عمل آوردند، تشکر و سپاس‌گزاری نمایم.

والسلام
جواد شیخ‌زادگان
زمستان ۱۳۸۹

پیشگفتار مؤلف

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

رمزنگاری که به‌عنوان یکی از ابزارهای تأمین امنیت ارتباطات و اطلاعات از قدیم الایام شناخته شده است، مقارن توسعه و گسترش ارتباطات و فناوری اطلاعات در دو دهه اخیر، بیش از پیش مورد توجه قرار گرفته است، به‌طوری‌که از حدود دو دهه پیش درس "اصول رمزنگاری" در تعدادی از دانشگاه‌های کشورمان ارائه گردیده و نیز در رشته‌های مخابرات، کامپیوتر و ریاضی گرایش خاصی 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 مدت 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 تا حدودی 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 اول کلیات 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 سنتی 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 سوم 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 اهمیت هر یک از این کاربردها کمتر از رمزنگاری نیست. از این‌رو در یکی دو دهه اخیر سیستم‌های کلید عمومی خیلی مورد توجه قرار گرفته است. بدین ترتیب این کتاب عمده 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، دانش‌آموختگان و کارشناسان حوزه امنیت ارتباطات و نهایتاً در راستای پیشرفت و پیشبرد اهداف عالی آموزشی و فرهنگی کشورمان به حساب آید.

در خاتمه لازم می‌دانم که بدین‌وسیله مراتب تشکر و قدردانی خود را از زحمات بی‌شایبیهی آقایان محمداسماعیل 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 به عمل آوردند، تشکر و سپاس‌گزاری نمایم.

والسلام

جواد شیخ‌زادگان

زمستان ۱۳۸۹

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 اطلاعات، دستگاه‌های خودپرداز و ... انباشته شده است.

در شرایطی که زندگی بشر از شکل سنتی خود، به شکل استحال 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 این کار تهدیدات خود را عملی ساخته و با هجوم بر اعصاب و روان انسان، تهدیدی جدی برای دارایی‌های آن باشند.

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

مؤلف 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 به منظور انتشار کتابی ارزشمند در زمینه‌ی رمزشناسی، ضمن قبول پیشنهاد مؤلف اندیشمند محترم کتاب، جناب آقای دکتر جواد شیخ‌زادگان که از اساتید جدی 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

