رمزشناسی در ایران و جهان

چالش‌های پژوهشی، آموزش و ساختارهای اجرایی

جـــواد مهاجـــری

حمود سلماسی‌زاده

شید دلاور

همکاران:

زهرا احمدیان، نصور باقری، وحید جهاندیده، [illegible] مرتضوی، علی ورداسبی

مؤسسهٔ انتشارات علمی دانشگاه صنعتی شریف

مؤسسهٔ انتشارات علمی
دانشگاه صنعتی شریف

رمزشناسی در ایران و جهان: چالش‌های پژوهشی، آموزش و ساختارهای اجرایی

تألیف جواد مهاجری، محمود سلماسی‌زاده، مهشید دلاور، زهرا احمدیان، نصور باقری، وحید جهاندیده، سیدامیر مرتضوی، علی وردا...

طراحی جلد: الهه احمدی میرقائد

مؤسسهٔ انتشارات علمی دانشگاه صنعتی شریف

چاپ اول: ۱۳۹۵

شمارگان: ۱۰۰۰

بها: ۲۷۰۰۰ تومان

شابک: ۹۷۸-۹۶۴-۲۰۸-۱۷۹-۰ ISBN 978-9[illegible]-208-179-0

تلفن: ۶۶۰۱۳۱۲۹-۶۶۱[illegible]۶۱۶۴۰۷۰

دفتر مرکزی: خیابان آزادی ـ دانشگاه صنعتی شریف

دفتر فروش: میدان انقلاب ـ خیابان شهید منیری جاوید (اردیبهشت) ـ ساختمان بهمن ـ پلاک ۸۷ ـ [illegible] بهارم ـ واحد ۴۰۲

تلفن: ۶۶۴۰۵۱۳۲-۶۶۹۶۷۸۹۶

وبگاه: http://sina.sharif.ir/~publishing **پست الکترونیکی:** publishing@sharif.edu

فروش اینترنتی: www.saneibook.com , www.ketabiran.ir

سرشناسه: مهاجری، جواد، ۱۳۴۰، سلماسی‌زاده، محمود، ۱۳۲۹.
عنوان و نام‌پدیدآور: رمزشناسی در ایران و جهان: چالش‌های پژوهشی، آموزش و ساختارهای اجرایی/ تألیف جواد مهاجری، محمود سلماسی‌زاده، مهشید دلاور و همکاران.
مشخصات نشر: تهران، دانشگاه صنعتی شریف، مؤسسهٔ انتشارات علمی، ۱۳۹۵.
مشخصات ظاهری: ۳۱۲ ص.
شابک: 978-964-208-179-0
وضعیت فهرست‌نویسی: فیپا.
یادداشت: جواد مهاجری، محمود سلماسی‌زاده، مهشید دلاور، زهرا احمدیان، نصور باقری، وحید جهاندیده، سیدامیر مرتضوی، علی ورداسبی.
یادداشت: کتابنامه.
موضوع: رمزنگاری
موضوع: Cryptography
شناسهٔ افزوده: دلاور، مهشید، ۱۳۶۲.
شناسهٔ افزوده: دانشگاه صنعتی شریف. مؤسسهٔ انتشارات علمی.
شناسهٔ افزوده: Sharif University of Technology. Institute of Scientific Publications
رده‌بندی کنگره: ۱۳۹۵ ۸ر۹م/Z۱۰۳
رده‌بندی دیویی: ۶۵۲/۸
شمارهٔ کتابشناسی ملی: ۴۵۰۴۱۱۸

بسم الله الرحمن الرحیم

فهرست مطالب

پیشگفتار

در عصر حاضر شاهد شکل‌گیری فضایی به نام «فضای تولید و تبادل اطلاعات» هستیم که عمده فعالیت‌های کلان و استراتژیک ازجمله روابط و تعاملات حاکمیتی، مدیریت زیرساخت‌های حیاتی و منابع مالی اطلاعاتی کشورها، همچنین، تعاملات تجاری، مالی، کسب‌وکار، فعالیت‌های آموزشی و حتی روابط و تعاملات روزمرهٔ آحاد جامعه را شامل می‌شود. گسترش روزافزون این فضا، در حال ایجاد فرصت‌های بی‌شمار، تهدیدات و مخاطرات جدید فراوانی به همراه داشته است به‌گونه‌ای که این فضا در معرض انواع حملات، آسیب‌ها و چالش‌ها از شنود اطلاعات مهم و ارزشمند، نقض حریم خصوصی افراد و نهادها تا تخریب بانک‌های اطلاعاتی حساس و ایجاد اختلال در زیرساخت‌های حیاتی قرار دارد. کم‌توجهی به مقولهٔ تأمین امنیت آن می‌تواند حوزه‌های وسیعی مانند حاکمیت، شبکه‌های ارتباطی و شبکه‌های مدیریت و توزیع انرژی را تحت‌تأثیر قرار دهد. یکی از مؤلفه‌های اساسی و پایه در تأمین امنیت فضای تولید و تبادل اطلاعات (افتا)، مباحث مربوط به رمزنگاری و پروتکل‌های رمزنگاشتی است، به‌طوری‌که تأمین امنیت این فضا بدون توجه و استفادهٔ صحیح از ابزارهای رمزنگاشتی عملاً ناممکن است.

مباحث رمزشناسی و امنیت داده ویژگی‌های خاصی دارند که کسب دانش مطلوب با توجه به این ویژگی‌ها امکان‌پذیر خواهد بود. از جملهٔ این ویژگی‌ها می‌توان به موارد زیر اشاره کرد.

- رمزشناسی، علمی میان‌رشته‌ای است که حوزه‌های وسیعی از دانش، مانند الکترونیک، مخابرات، علوم کامپیوتر، ریاضی و فیزیک را شامل می‌شود.
- حاکمیت، متولی تأمین امنیت در فضای تولید و تبادل اطلاعات است. لذا هدایت، راهبری و سیاست‌گذاری فعالیت‌های کلان آموزشی، پژوهشی و فناورانهٔ مرتبط با رمزشناسی نیز بر عهدهٔ حاکمیت است.

- افتا به‌شدت متأثر از تغییرات سریع و چشمگیر در فناوری‌های مرتبط و مورداستفاده است. برای مثال، تحولات جاری در حوزهٔ رایانش کوانتومی می‌تواند منجر به بروز تهدیدات بسیار جدی علیه بسیاری از استانداردهای رمزنگاری در حوزهٔ الگوریتم‌ها و پروتکل‌های رمزنگاشتی شود و تغییرات وسیعی را در این حوزه به دنبال داشته باشد. همچنین، نحوهٔ پیاده‌سازی الگوریتم‌ها مباحث جدیدی را در حوزهٔ حملات کانال جانبی به دنبال داشته است.

مباحث موجود در زمینهٔ رمزشناسی را می‌توان در شش حوزهٔ الگوریتم‌های رمز متقارن، توابع چکیده‌ساز، سامانه‌های رمز نامتقارن، پروتکل‌های رمزنگاشتی، پیاده‌سازی و حملات کانال جانبی و امنیت تئوری اطلاعاتی دسته‌بندی کرد که چهار محور اول در این کتاب موردتوجه و بررسی قرار گرفته است.

به‌طورکلی، الگوریتم‌های رمزنگاشتی به دو دستهٔ الگوریتم‌های رمز کلید متقارن و الگوریتم‌های رمز کلید نامتقارن (کلید عمومی) تقسیم می‌شوند. الگوریتم‌های رمز قالبی و جریانی دو خانوادهٔ مهم الگوریتم‌های موجود در رمزنگاری متقارن هستند. الگوریتم‌های رمز قالبی نوعاً کندتر از رمزهای جریانی هستند (۲۰ تا ۴۰ سیکل بر بایت) و در پیاده‌سازی سخت‌افزاری، تعداد گیت بیشتری لازم دارند (حدود ۵۰۰۰ تا ۱۰۰۰۰۰ گیت). این الگوریتم‌ها، ساختار بسیار انعطاف‌پذیری دارند که استفاده از آن‌ها را در سبک‌های مختلف عملکردی مثل محرمانگی، احراز اصالت، و رمزگذاری احراز اصالت‌شده و همچنین توابع یک‌طرفه و توابع چکیده‌ساز ممکن می‌سازد.

یک تابع چکیده‌ساز، یک پیام با طول دلخواه را به‌عنوان ورودی دریافت می‌کند و چکیده‌ای با طول ثابت از آن را به‌عنوان خروجی تولید می‌نماید. طول خروجی معمولاً بین ۱۲۸ بیت تا ۵۱۲ بیت متغیر است. توابع چکیده‌ساز کاربردهای متفاوتی دارند. از زیرگروه‌های توابع چکیده‌ساز می‌توان به یک‌طرفه[1] بودن تابع و دشواری یافتن زوج ورودی‌هایی با خروجی یکسان اشاره کرد. می‌توان توابع چکیده‌ساز را در دو گروه اصلی تحت‌عنوان توابع چکیده‌ساز بدون کلید که بیشتر تحت‌عنوان «توابع چکیده‌ساز» از آن‌ها یاد می‌شود و توابع چکیده‌ساز کلیددار که بیشتر تحت‌عنوان «کدهای احراز اصالت پیام» از آن‌ها یاد می‌شود، تقسیم‌بندی کرد.

امنیت اکثر سامانه‌های رمز نامتقارن بر دشوار بودن حل یک مسئلهٔ ریاضی شناخته‌شده

1. one way

استوار است. انواع روش‌های رمزنگاری کلید عمومی را می‌توان به روش‌های مبتنی بر سخت بودن حل مسئلهٔ تجزیهٔ اعداد بزرگ، لگاریتم گسسته، کدینگ و مشبکه‌ها دسته‌بندی کرد. از انواع امضاهای دیجیتال می‌توان به امضاهای کور، وکالتی، تراگذر و غیرقابل‌انکار اشاره کرد. کاربردها و ملزومات امنیتی جدید منجر به‌ظهور دسته‌ای از روش‌های رمزنگاری با قابلیت خاص مانند طرح‌های رمز هم‌ریخت، جستجوپذیر، تابعی، ویژگی‌بنیاد و انکارپذیر شده است. همچنین، توجه به روش‌های مقاوم در برابر حملات مبتنی بر رایانش کوانتومی از سایر مباحث مهم این حوزه به‌شمار می‌رود.

پروتکل‌های رمزنگاشتی شامل مجموعه‌ای از دستورات و الگوریتم‌هایی هستند که برای نیل به اهداف امنیتی مشخص و در ترتیب معینی انجام می‌یابند. پروتکل‌های رمزنگاشتی از مجموعه‌ای از اولیه‌های[1] رمزنگاشتی مانند رمزنگاری کلید عمومی و رمزنگاری کلید خصوصی تشکیل می‌شوند. امنیت پروتکل‌های رمزنگاشتی بر برخی فرضیات عام و متداول مانند فرض وجود رشته بیت تصادفی مشترک[2]، پیشگوی تصادفی[3]، کانال پخش[4] و مرکز محاسبات معتمد[5] استوار است. با توجه به نقش کارکرد و اولیه‌های مورداستفاده در پروتکل، می‌توان تعاریف مختلفی برای امنیت پروتکل‌های رمزنگاشتی ارائه کرد. پروتکل‌های احراز اصالت، برقراری کلید، اثبات‌های دانش‌صفر، طرح‌های تعهد، محاسبات امن چندنهادی، انتقال کورکورانه، مجموعه‌های دانش‌صفر و تبادل منصفانه ازجمله پروتکل‌های مهم بررسی در این کتاب به‌شمار می‌روند.

با توجه به اهمیت مقولهٔ رمزشناسی، فعالیت‌های متمرکز، هدفمند، دقیق و سازمان‌یافته در این زمینه همراه با سرمایه‌گذاری‌های وسیع، در دنیا به انجام رسیده یا در حال انجام است. ازجملهٔ این فعالیت‌ها می‌توان به اقدامات نهاد امنیت ملی امریکا (NSA)[6]، مؤسسهٔ فناوری و استاندارد ملی امریکا (NIST)[7]، اجرای پروژه‌های ECRYPT در اتحادیهٔ اروپا و فعالیت‌های متمرکز و سازمان‌یافته در کانادا اشاره کرد.

نهاد امنیت ملی امریکا همراه با مؤسسهٔ فناوری و استاندارد ملی این کشور، نقش بسیار مهمی در توسعهٔ تحقیقات علمی در زمینهٔ رمزنگاری داشته‌اند. ازجمله فعالیت‌های این دو نهاد،

---

1. primitive
2. common random string
3. random oracle
4. broadcast channel
5. trusted computing base
6. National Security Agency
7. National Institute of Standards and Technology

می‌توان به همکاری در طراحی و تدوین استانداردهای رمزنگاری DES و AES و توابع چکیده‌ساز SHA-1 و SHA-2 و SHA-3 اشاره کرد. نهاد امنیت ملی امریکا میلیون‌ها دلار برای تحقیقات دانشگاهی سرمایه‌گذاری کرده است که نتیجهٔ آن تولید بیش از ۳۰۰۰ مقاله از سال ۲۰۰۷ تا ۲۰۱۱ بوده است. از فعالیت‌های بارز مؤسسهٔ فناوری و استاندارد ملی امریکا می‌توان به انتشار بیش از ۳۰۰ سند در چهار دستهٔ استانداردهای پردازش اطلاعات فدرال[1] (FIPS)، سری ۸۰۰ انتشارات ویژه (SP)[2]، آگاهی‌نامهٔ آزمایشگاه فناوری اطلاعات[3] (ITL) و گزارش‌های بین نهادی NIST[4] (NIST IR) اشاره کرد. در حال حاضر، تعداد افراد شاغل در مؤسسهٔ فناوری و استاندارد ملی امریکا، بیش از ۳۰۰۰ نفر مشتمل بر دانشمند، مهندس، تکنیسین و ... است. بودجهٔ NIST در سال‌های مالی ۲۰۱۳ و ۲۰۱۴ به‌ترتیب ۷۶۹ و ۸۵۰ میلیون دلار بوده و بودجهٔ درخواستی برای سال ۲۰۱۵ مبلغ ۹۰۰ میلیون دلار است.

پروژهٔ شبکه کتاب‌های علمی اروپا در رمزشناسی (ECRYPT)، طی دو فاز بین سال‌های ۲۰۰۴ تا ۲۰۰۸ و ۲۰۰۸ تا ۲۰۱۲ به انجام رسید. فاز اول این پروژه، با مشارکت ۳۲ مؤسسهٔ متشکل از ۲۳ دانشگاه و ۹ مؤسسهٔ صنعتی، با هدایت و راهبری دانشگاه لوون بلژیک در ۱۴ کشور بلژیک، فرانسه، آلمان، انگلستان، دانمارک، ایتالیا، سوئیس، هلند، نروژ، سوئد، اتریش، لهستان، یونان و اسپانیا و بودجه‌ای در حدود ۸ ۴۱۸ ۴۳۲ یورو انجام شد. در فاز دوم پروژه، ۱۱ مؤسسه متشکل از ۹ دانشگاه و ۲ مؤسسهٔ صنعتی از ۸ کشور بلژیک، فرانسه، آلمان، انگلستان، ایتالیا، سوئیس، هلند و اتریش به‌عنوان هستهٔ اصلی همراه با ۱۷ دانشگاه و ۵ مؤسسهٔ صنعتی دیگر به‌عنوان اعضای معین تحت هدایت و راهبری دانشگاه لوون بلژیک مشارکت داشتند. اعتبار در نظرگرفته‌شده برای این فاز در حدود ۳ میلیون یورو بود. از اهداف این پروژه، می‌توان به هماهنگ‌سازی تحقیقات دانشگاهی و صنعتی، به‌کارگیری امکانات پژوهشی و صنعتی موجود، یکپارچه‌سازی پژوهش‌ها و اجتناب از فعالیت‌های پراکنده، تقویت جنبه‌های علمی و کاربردی درزمینهٔ رمزنگاری و بهبود الگوریتم‌ها و پروتکل‌های رمزنگاشتی با هدف افزایش کارایی و امنیت و کاهش هزینه‌ها اشاره کرد. تمرکز فعالیت‌های پژوهشی پروژه در فاز اول، در قالب آزمایشگاه‌های مجازی و در حول پنج محور الگوریتم‌های رمزنگاری متقارن، رمزنگاری کلید عمومی، پروتکل‌های رمزنگاشتی، پیاده‌سازی و نهان‌نگاری بود که این فعالیت‌ها در فاز دوم به

1. Federal Information Processing Standards
2. Special Publication (SP) 800 series
3. Information Technology Laboratory
4. NIST Interagency Reports

الگوریتم‌های رمزنگاری متقارن و نامتقارن، پروتکل‌های رمزنگاشتی، و پیاده‌سازی در قالب آزمایشگاه‌های مجازی مربوطه کاهش یافت.

نهاد تأمین امنیت ارتباطات کانادا (CSEC)، به‌عنوان نهاد امنیتی پیشرو برای دولت کانادا، مسئولیت ارائهٔ برنامه‌های آموزشی و افزایش سطح آگاهی برای کارمندان و متخصصان فعال درزمینهٔ IT در دولت کانادا را عهده‌دار است. برنامه‌های آموزشی در CSEC، حوزهٔ وسیعی از اقدامات از جمله معرفی کلی اصول امنیت ارتباطات و اطلاعات، برنامه‌های کامل مطالعاتی برای توسعه، انجام کار و مدیریت سامانه‌های اطلاعاتی را شامل می‌شود. این نهاد، برای انجام پژوهش‌های رمزنگارانهٔ خود، مؤسسهٔ ریاضیات و محاسبات تات[1] (با نام اختصاری TIMC) را تأسیس کرده است که در زمینه‌های پژوهشی با دانشگاه‌های برجستهٔ کانادا همکاری دارد. CSEC، برای انجام وظایف و دست‌یابی به اهداف موردنظر خود، به یک مجموعه از ۱۳۵۰ کارمند مستعد در زمینه‌های کاری و تجربه‌های گسترده، از مهندسان و متخصصان علوم کامپیوتر و برنامه‌نویسان گرفته تا فیزیک‌دانان، ریاضیدانان و متخصصان زبان و تحلیل‌گران اطلاعات تکیه دارد. پژوهش‌های رمزنگاری در دانشگاه کلگری[2] توسط مؤسسهٔ «امنیت، حریم خصوصی و تضمین اطلاعات (ISPIA)» هدایت و سازمان‌دهی می‌شود. ISPIA یک نهاد پژوهشی چندرشته‌ای در دانشگاه کلگری است که پژوهش‌های آن طیف وسیعی از حوزه‌ها، از رمزنگاری نظری و علم کوانتوم تا امنیت نرم‌افزار، کدهای مخرب، امنیت سامانه‌های عامل و شبکه، و مسائل فنی و قانونی در مورد حریم خصوصی و حقوق دیجیتال را در بر می‌گیرد. افزایش مشارکت و پایه‌ریزی همکاری‌های مؤثر با مؤسسات دانشگاهی دیگر، جوامع تخصصی، صنعت و دولت؛ حفظ یک برنامهٔ فعال برای جذب پژوهشگران برجسته و حمایت مالی و پشتیبانی از فعالیت‌های آموزشی و توسعه‌ای از فعالیت‌های ISPIA به‌شمار می‌روند. مرکز تحقیقاتی رمزنگاشتی کاربردی (CACR) در دانشگاه واترلو[3]، نهادی حاصل از همکاری دانشگاه، دولت مرکزی و چند شرکت بزرگ در کاناداست. مجموعه اعضای هیئت علمی این مرکز از دانشکده‌های برق و کامپیوتر، علوم کامپیوتر، ترکیبیات و بهینه‌سازی، فیزیک و ریاضیات محض تشکیل می‌شود.

شاید بتوان فراگیرترین شیوهٔ استفاده از الگوریتم‌ها و پروتکل‌های رمزنگاری را در تأمین امنیت اطلاعات مبادله‌شده در شبکه‌های تلفن همراه مشاهده کرد. فرایند طراحی و انتخاب

---

1. Tutte
2. Calgary
3. Waterloo

الگوریتم‌های رمز مورداستفاده در این شبکه‌ها طی نسل‌های دوم تا چهارم تلفن همراه با تغییرات، رویکردها و نوسانات قابل‌توجهی روبه‌رو بوده است. به‌طورکلی، رویکردهای موجود برای طراحی و انتخاب الگوریتم‌های رمز استاندارد و یا مورداستفاده در شبکه‌های بزرگ و هدایت و اجرای فعالیت‌های رمزنگاری را می‌توان در سه مدل به شکل زیر طبقه‌بندی کرد.

۱. انتخاب الگوریتم از طریق فراخوان و اعمال تغییرات توسط تیم خبرهٔ داخلی برای رسیدن به اهداف امنیتی موردنظر. مانند روند انتخاب استاندارد رمزهای قالبی DES
۲. طراحی الگوریتم موردنظر توسط تیم خبرهٔ داخلی. مانند روند تولید توابع چکیده‌ساز SHA1 و SHA2 توسط NIST و الگوریتم‌های A5/1 و A5/2 در GSM
۳. انتخاب الگوریتم استاندارد از طریق یک فراخوان عمومی و انتخاب یکی از الگوریتم‌های برنده‌شده در رقابت بدون اعمال تغییرات در طراحی آن براساس نتایج حاصل از ارزیابی عمومی مانند نحوهٔ انتخاب استاندارد رمز قالبی AES یا تابع چکیده‌ساز SHA3

نکتهٔ قابل‌توجه در روند انتخاب DES که در مدل ۱ طبقه‌بندی می‌شود، بالا بودن سطح دانش افراد فعال در NIST نسبت به عموم جامعهٔ رمزنگاری است؛ به‌طوری‌که تغییرات اعمال‌شده توسط NIST بر روی الگوریتم انتخابی موجب بهبود الگوریتم و افزایش مقاومت آن در برابر تحلیل‌های تفاضلی شد. فرایند انتخاب DES و ابهامات موجود در چرایی تغییرات ایجادشده در آن توسط NIST، نقش قابل‌توجهی در گسترش رمزنگاری مدرن و ورود آن به محیط‌های دانشگاهی داشت.

از بین الگوریتم‌هایی که با استفاده از مدل ۲ انتخاب شدند، الگوریتم‌های A5/1 و A5/2 به‌دلیل محدودیت در تعداد و دانش فنی طراحان دارای ضعف‌های عمده‌ای بودند و پس از انتشار به‌سرعت شکسته شدند. ولی با وجود ارائهٔ حملات موفق علیه توابع چکیده‌ساز SHA1 و SHA2 این توابع همچنان از نظر عملی امن محسوب می‌شوند.

نکتهٔ قابل‌توجه در فرایند انتخاب الگوریتم‌ها در مدل سوم، مشارکت جامعهٔ علمی جهانی در طراحی، تحلیل و انتخاب الگوریتم‌هاست که موجب مقبولیت عمومی آن‌ها شده است. همچنین

دردسترس بودن اطلاعات مربوط به طراحی و تحلیل این الگوریتم‌ها و وجود انگیزهٔ لازم برای تحلیل آن‌ها در نزد جامعهٔ علمی رصد امنیتی آن‌ها را موجب شده است.

در ایران تهیه، تدوین و ابلاغ دو سند «سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات (افتا)» و «سند راهبردی امنیت فضای تولید و تبادل اطلاعات (افتا)» که به‌طور اختصاصی به این موضوع پرداخته‌اند، همچنین توجه به جایگاه این موضوع در سایر اسناد بالادستی مانند نقشهٔ جامع علمی کشور و برنامهٔ پنجم توسعه حاکی از توجه ویژهٔ سیاست‌گذاران و برنامه‌ریزان کلان کشور به این مقولهٔ مهم و حیاتی است.

با توجه به ظرفیت‌های بالقوه و بالفعل موجود در کشور و با توجه به نتایج حاصل از انجام فعالیت‌های سازمان‌یافته در ساختارهای موجود در دنیا و رویکردهای اتخاذشده در طراحی و تدوین استانداردها و الگوریتم‌های رمزنگاشتی، به‌نظر می‌رسد تنها راه رسیدن به اهداف درنظر گرفته‌شده در اسناد بالادستی و سرآمدی علمی در حوزهٔ رمزشناسی، توسعهٔ علم رمز و تربیت نیروهای کارآمد و متخصص طی یک برنامهٔ مدون و منسجم باشد.

فصول اول تا چهارم این کتاب به دسته‌بندی موضوعی و بررسی زمینه‌های پژوهشی، معرفی چالش‌ها و مسائل باز در حوزهٔ الگوریتم‌های رمز متقارن، توابع چکیده‌ساز، سامانه‌های رمز نامتقارن و پروتکل‌های رمزنگاشتی اختصاص یافته است. در فصل پنجم کتاب، مباحث مربوط به طول کلید الگوریتم‌های رمز موردتوجه قرار گرفته است. فصل ششم به معرفی و بررسی برخی از ساختارهای تأثیرگذار بین‌المللی در حوزهٔ رمزشناسی و امنیت پرداخته است. درنهایت، در فصل هفتم، وضعیت آموزش و پژوهش در ایران در حوزهٔ رمزشناسی و امنیت داده موردبررسی قرار گرفته است.

فرهاد مهاجری

محمود سلماسی‌زاده

مهشید دلاور

زمستان ۹۵