بسم الله الرحمن الرحیم

رمزنگاری و کاربرد آن در فن‌آوری اطلاعات

مؤلفان:

دکتر علی برومندنیا

(عضو هیأت علمی دانشگاه آزاد اسلامی واحد تهران جنوب)

دکتر محمدمنصور ریاحی کاسانی

(عضو هیأت علمی دانشگاه آزاد اسلامی واحد تهران شمال)

مهندس زهرا رزاق‌زاده شبستری

انتشارات «شبنما»

سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران

سرشناسه : برومندنیا، علی، ۱۳۴۶ -

عنوان و نام پدیدآور : رمزنگاری و کاربرد آن در فن‌آوری اطلاعات/ مولفان علی برومندنیا، محمدمنصور ریاحی‌کاشانی، زهرا رزاق‌زاده‌شبستری؛ ویراستاری سعید قنبری‌فشی.

مشخصات نشر : شهریار: شبنما، ۱۳۹۶.

مشخصات ظاهری : ۱۶۸ ص.مصور، جدول، نمودار.

شابک : ۱۴۰۰۰۰ریال 978-600-98582-6-2 :

وضعیت فهرست نویسی : فیپا

یادداشت : کتابنامه.

موضوع : رمزنگاری

موضوع : Cryptography

شناسه افزوده : ریاحی‌کاشانی، محمدمنصور، ۱۳۳۹ -

شناسه افزوده : رزاق‌زاده شبستری، زهرا، ۱۳۶۰ -

رده بندی کنگره : ۱۳۹۶ ۸ر۴ب/QA۲۶۸

رده بندی دیویی : ۰۰۳/۵۴

شماره کتابشناسی ملی : ۵۰۸۶۸۳۵

عنوان کتاب	:	رمزنگاری و کاربرد آن در فن‌آوری اطلاعات
نویسندگان	:	علی برومندنیا عضو هیأت علمی دانشگاه آزاد اسلامی واحد تهران جنوب محمدمنصور ریاحی کاشانی عضو هیأت علمی دانشگاه آزاد اسلامی واحد تهران شمال زهرا رزاق زاده شبستری باشگاه پژوهشگران جوان و نخبگان، واحد تهران شمال، دانشگاه آزاد اسلامی، تهران، ایران
مدیر تولید	:	احسان طاهرنژاد
صفحه آرایی	:	صدیقه رحماندوست
ویراستاری	:	سعید فتحی‌فشی
طراح جلد	:	زهرا رزاق زاده شبستری، سیده زهرا رضائی نودهی
نوبت و سال چاپ	:	اول، اسفند ماه ۱۳۹۶
قطع	:	وزیری
تعداد صفحه	:	۱۶۸ صفحه
شمارگان(تیراژ)	:	۱۰۰۰ نسخه
شابک	:	۹۷۸-۶۰۰-۹۸۵۸۲-۶-۲
قیمت	:	۱۴۰۰۰ تومان
ناشر	:	انتشارات شبنما
آدرس	:	شهریار، وائین، میلاد۳، گلشن۸، پلاک۷.
تلفن تماس	:	۰۹۱۲۸۵۵۱۱۳۵
فروش و پخش	:	۰۹۱۲۷۵۶۴۹۹۰
شماره پیام‌رسان	:	۰۹۱۰۰۷۴۰۹۹۳
رایانامه(ایمیل)	:	Shabnama96@chmail.ir
وبسایت	:	www.Shabnama96.ir

فهرست مطالب

پیشگفتار

فصل اول: تاریخچه رمزنگاری

۱-۱- تاریخچه رمزنگاری کلاسیک ۳

۱-۲- تاریخچه رمزنگاری مدرن ۱۲

فصل دوم: رمزنگاری

۲-۱- امنیت اطلاعات ۱۹

۲-۲- پنهان‌سازی اطلاعات ۲۲

۲-۲-۱- پنهان‌نگاری ۲۳

۲-۲-۲- نهان‌نگاری ۲۶

۲-۳- رمزشناسی ۲۹

۲-۴- رمزنگاری ۳۰

۲-۴-۱- مفاهیم اولیه رمزنگاری ۳۲

۲-۴-۲- اهداف رمزنگاری ۳۵

۲-۵- تحلیل رمز ۳۷

۲-۶- سیستم‌های رمزنگاری امن ۴۰

۲-۷- کاربرد رمزنگاری در زندگی خصوصی و تجاری ۴۵

فصل سوم: رمزنگاری متقارن

۳-۱- مفهوم پایه رمزنگاری متقارن ۵۱
۳-۱-۱- رمز بلوکی ۵۲
۳-۱-۲- رمز جریانی ۵۴
۳-۲- انواع الگوریتم‌های رمزنگاری متقارن ۵۷
۳-۲-۱- DES ۵۷
۳-۲-۲- DESدوگانه ۶۲
۳-۲-۳- DESسه‌گانه ۶۳
۳-۲-۴- IDEA ۶۴
۳-۲-۵- AES ۶۵
۳-۲-۶- Blowfish ۷۰
۳-۲-۷- RC4 ..... ۷۰

فصل چهارم: رمزنگاری نامتقارن

۴-۱- مفهوم پایه رمزنگاری نامتقارن ۷۵
۴-۲- کاربردهای الگوریتم‌های رمزنگاری نامتقارن ۷۶
۴-۲-۱- رمزگذاری/رمزگشایی ۷۶
۴-۲-۲- امضای دیجیتال ۷۸
۴-۲-۳- رمزگذاری و امضای دیجیتال ۷۹
۴-۳- الگوریتم RSA ۸۰
۴-۳-۱- تاریخچه مختصر ۸۱
۴-۳-۲- مفهوم پایه RSA ۸۱
۴-۳-۳- عملیات RSA ۸۴
۴-۳-۴- کاربردهای الگوریتم RSA ۸۷
۴-۴- منحنی بیضوی ۸۸
۴-۴-۱- رمزنگاری منحنی بیضوی ۸۹

فصل پنجم: تابع هش

۵-۱- مفهوم پایه تابع هش ۹۵
۵-۲- خواص تابع هش ۹۵
۵-۲-۱- ویژگی‌های کاربردی ۹۶
۵-۲-۲- ویژگی‌های امنیتی ۹۹
۵-۳- کاربردهای تابع هش ۱۰۲
۵-۳-۱- کاربردهای تابع هش در رمزنگاری ۱۰۳
۵-۴- تاریخچه مختصری از توابع هش مدرن ۱۰۷

فصل ششم: طرح‌های امضای دیجیتال

۶-۱- مفهوم پایه ای امضای دیجیتال ۱۱۳
۶-۱-۱- ایده اصلی ۱۱۵
۶-۱-۲- امضاهای الکترونیکی ۱۱۶
۶-۱-۳- مبانی طرح امضای دیجیتال ۱۱۸
۶-۲- طرح‌های امضای دیجیتال مبتنی بر RSA ۱۲۱
۶-۲-۱- مدل اساسی یک طرح امضای دیجیتال ۱۲۱
۶-۲-۲- دو رویکرد متفاوت ۱۲۳
۶-۳- طرح‌های امضای دیجیتال در عمل ۱۲۵
۶-۳-۱- امنیت طرح‌های امضای دیجیتال ۱۲۵
۶-۳-۲- استفاده طرح‌های امضای دیجیتال با رمزگذاری ۱۲۹
۶-۳-۳- ارتباط با امضای دست‌نویس ۱۳۲
۶-۳-۴- ارتباط با امضاهای الکترونیکی پیشرفته ۱۴۰

منابع و مراجع برای مطالعه بیشتر ۱۴۳

پیشگفتار

رشد سریع ارتباطات الکترونیکی باعث افزایش اهمیت مسائل مربوط به امنیت اطلاعات شده است. رمزنگاری یکی از تکنیک‌های امنیت اطلاعات می‌باشد و در قلب بسیاری از مکانیزم‌های امنیت اطلاعات تکنیکی قرار دارد. رمزنگاری یک موضوع مرتبط با زندگی روزمره می‌باشد که تحول چشمگیری داشته است. با حضور فراگیر شبکه‌های کامپیوتری و سیستم‌های توزیع شده به طور کلی و اینترنت به طور خاص، رمزنگاری تبدیل به یک فناوری توانمند برای ایمن‌سازی زیرساخت‌های اطلاعاتی شده است که مردم در حال ایجاد، استفاده و احتساب در زندگی روزمره می‌باشند.

در حال حاضر اطلاعات الکترونیکی به آسانی قابل انتقال می‌باشند و در محیط‌های نسبتا ناامن محافظت می‌شوند. این امر منجر به تغییرات اساسی، به جهت خطراتی می‌گردد که این اطلاعات در معرض آن قرار دارند. از آنجایی که تأثیرات مالی حوادث امنیت اطلاعات افزایش می‌یابد، بنابراین نیاز به کنترل و حفظ امنیت اطلاعات وجود دارد. رمزنگاری یک فناوری حیاتی است که بر پایه بسیاری از این کنترل‌ها بوده و مجموعه‌ای از مکانیزم‌های اساسی را برای اجرای خدمات امنیتی که

از اطلاعات الکترونیکی محافظت می‌نمایند، مانند محرمانگی، یکپارچگی داده‌ها و احراز هویت، فراهم می‌کند. رمزنگاری به‌خودی‌خود اطلاعات را امن نمی‌کند ولی در هسته خود بسیاری از مکانیزم‌های تکنیکی برای محافظت از اطلاعات را دارد.

با این حال، در عصر اطلاعات، بزرگترین همکاری و کمک رمزنگاری ممکن است برای تجارت باشد. بانک‌ها به مدت طولانی از رمزنگاری برای حفظ امنیت نقل و انتقالات الکترونیکی استفاده نموده‌اند. همچنین شرکت‌هایی که از لحاظ جغرافیایی توزیع شده‌اند، رمزنگاری را برای حفاظت ارتباطات خود از جاسوسی صنعتی به کار گرفته‌اند. شاید هیجان‌انگیزترین کاربردها، شامل برقراری ارتباط بین طرفینی باشد که دارای ارتباط قبلی نبوده و به همین دلیل از قبل، فرصتی برای انجام توافق بر روی کلید نداشته‌اند. همان‌طور که تجارت در اینترنت رشد می‌کند، چنین کاربردهایی روز به روز شایع‌تر می‌شود.

پیام‌های مبادله شده در سراسر شبکه‌های کامپیوتری که در دسترس عموم قرار دارند، باید محرمانه باشند و در برابر دستکاری محافظت شوند. کسب و کار الکترونیکی نیاز به امضای دیجیتالی که از لحاظ قانونی معتبر است و همچنین پروتکل‌های پرداخت امن دارد. رمزنگاری مدرن راه‌حلی را برای همه این مشکلات فراهم می‌کند.

با توجه به نقش مهم آن، دانشمندان کامپیوتر، مهندسان برق و ریاضی‌دانان، همه

باید در اصول اساسی و کاربردهای رمزنگاری دارای علم باشند. رمزنگاری یک ابزار است و بنابراین فقط در صورتی می‌تواند امنیت را تأمین کند که به درستی استفاده شود. اگر به طور صحیح مورد استفاده قرار نگیرد، ممکن است در وهله اول در تأمین امنیت با شکست مواجه شود یا اینکه امکان دارد حتی بدتر از عدم استفاده از آن باشد زیرا کاربران فکر می‌کنند که آن‌ها توسط رمزنگاری محافظت می‌شوند در حالی که در واقعیت این چنین نیست.

بنابراین، رمزنگاری برای هر فردی که علاقه‌مند به امنیت اطلاعات است، موضوع مهمی می‌باشد. با یادگیری در مورد اینکه رمزنگاری چگونه کار می‌کند، کاربردهای مختلف آن در جهان مدرن و تهدیدات برای حفاظت‌های آن، شما بهتر می‌توانید درک کنید که چگونه این روش‌ها روی شما تأثیر می‌گذارند و شاید یاد بگیرند که چگونه به طور موثرتر از اطلاعات خود حفاظت کنید.

لازم به ذکر است که فصول این کتاب با استفاده از مطالعه منابع و کتب مختلف در زمینه رمزنگاری و گردآوری و ترجمه آن‌ها، تألیف و تدوین شده است. توالی فصول این کتاب و مطالب ارائه شده در هر یک، در ادامه به ترتیب بیان می گردد.

در این کتاب، فصل اول مشتمل بر تاریخچه رمزنگاری می‌باشد که به دو بخش رمزنگاری کلاسیک و رمزنگاری مدرن تقسیم می‌شود. فصل دوم کتاب به مبحث رمزنگاری و ارتباط آن با امنیت اطلاعات می‌پردازد. در این فصل به امنیت اطلاعات

و تکنیک‌های آن به طورکلی اشاره شده است و مسائل مربوط به رمزنگاری به عنوان یکی از تکنیک‌های امنیت اطلاعات شرح داده می‌شود. در فصل سوم به بیان رمزنگاری متقارن که یک سیستم رمزنگاری مدرن است و مسائل مربوط به آن پرداخته می‌شود و مهم‌ترین الگوریتم‌های رمزنگاری موجود در این حوزه به طور مختصر بیان می‌گردد. فصل چهارم درباره دیگر سیستم رمزنگاری مدرن یعنی رمزنگاری نامتقارن می‌باشد. در این فصل نیز مسائل مربوطه مانند مفهوم و کاربردهای این سیستم و همچنین الگوریتم‌های معروف موجود در این حوزه تشریح می‌شود. فصل پنجم درباره تابع هش می‌باشد که دارای کاربردهای فراوانی در رمزنگاری است. در این فصل به مفهوم و خصوصیات و کاربردهای تابع هش اشاره شده است. فصل ششم به امضای دیجیتال می‌پردازد که یک مفهوم نسبتا جدید در دنیای مدرن است و برای ارائه عدم انکار به کار می‌رود. این فصل شامل طرح‌های امضای دیجیتال و مفاهیم مرتبط با آن است.

سپاس خداوندی را که در سایه لطف و رحمت بی‌کرانش ما را در انجام این مهم یاری نمود.

لازم به ذکر است که با سپاسگزاری‌های خود از تمامی یاری دهندگان بزرگوار و گرامی این اثر، کمال تشکر و قدردانی را نماییم.

با سپاس فراوان از همکاری و مساعدت‌های استادان بزرگوار جناب آقای دکتر میراسماعیل معصومی، جناب آقای دکتر محمدجواد شکوری، جناب آقای دکتر احسان شکوری و همکاران ایشان، سرکار خانم فاطمه حدادیان و سرکار خانم رویا باوندی.

از ناشر محترم جناب آقای امید طاهرنژاد مدیر مسئول انتشارات شبنما و همکاران ایشان که زحمت چاپ این اندوخته را برعهده داشتند، کمال تشکر را داریم.

امید آن که این اثر برای بسیاری از علاقمندان و پژوهشگران به این مباحث و حوزه پژوهشی گامی هرچند اندک، اما راه گشا و میسر واقع گردد.

دکتر علی برومندنیا دکتر محمد منصور ریاحی کاشانی مهندس زهرا رزاق زاده شبستری

تهران، بهمن ۱۳۹۲