اصول رمزنگاری و کشف رمز

سعید طلعتی، [illegible]شت وری، جلیل مظلوم

طلعتی، سعید، ۱۳۶۷
اصول رمزنگاری و کشف رمز/سعید طلعتی، حشمت نوری، جلیل مظلوم.
تهران: نشر لوزی، ۱۳۹۴.
مصور(بخشی رنگی)،جدول ،نمودار
۹۷۸-۶۰۰-۹۵۱۳۷-۶-۹
فیپا
نوری، حشمت، ۱۳۵۵ - مظلوم، جلیل، ۱۳۵۳
۱۳۹۴ ۶الف۸ط/Z۱۰۳
۶۵۲/۸
۴۱۱۲۳۱۴

- ناشر: موسسه انتشاراتی لوزی
- عنوان کتاب: اصول رمزنگاری و کشف رمز
- مؤلفین: سعید طلعتی، حشمت نوری، جلیل مظلوم
- نوبت چاپ: اول ۱۳۹۴
- تیراژ: ۱۰۰۰ نسخه
- قیمت: ۲۲۰۰۰۰ ریال

فهرست مطالب

فهرست عناوین

صفحه

پیشگفتار ۱

رمزنگاری ابزاری عمومی ۲

به خط مقدم خوش آمدید ۲

قسمت اول ۴

کلید امنیت ۴

بخش اول ۵

قفل ها وکلیدها ۵

قفل ها وترکیب ها ۵

شرح اصطلاحات رمزشناسی ۷

پنهان کردن نوشته ها ۷

بخش دوم ۸

جایگزینی ۸

تحلیل رمز سزار ۱۱

قدرت یافتن مردم عادی ۱۱

اهمیت جداسازی روش وکلید ۱۲

اضافه کردن کلیدها ۱۳

ضعف رمزهای سزار: شکست برای پنهان کردن الگوهای زبان شناسی ۱۴

تکرارکلمات وحروف ۱۵

جایگزینی پیچیده : رمز Vigenere ۱۵

بخش سوم ۸

جابه جایی رمزها : حرکت به اطراف ۸

الگوها وتحلیل رمز ۱۱

اضافه کردن پیچیدگی بیشتر ۱۱

جا به جایی کامپیوتری ۱۲

اترکیب جا به جایی وجایگزینی ۱۳

بخش چهارم ۸

پراکندن وبه هم ریختن : چگونه رمزنگاران درپایان بازی برنده می شوند ۲۵

فهرست عناوین

صفحه

پراکندگی (ترکیب پراکندگی وجابه جایی) ۲۶
رمزبولی با یوس ۲۶
اصول به هم ریختن ۲۸
قفل ها و کلیدهای رمزشناسی ۲۹
بخش پنجم ۳۱
روش DES ۳۱
نیازتاریخی به یک استاندارد رمزنگاری ۳۱
چرخه کلیدهای کامپیوتر ۳۳
DES دوبل و سوبل ۳۳
مدهای DES ۳۴
روش آوالانچ ۳۴
اعداد باینری وحروف کامپیوتری ۳۴
بخش ششم ۳۶
تحول رمزنگاری به سمت جهانی شدن ۳۶
رمزنگاری جدید ۳۶
واردشدن نسل کامپیوتر ۳۷
بخش هفتم ۳۹
اطمینان ازکلیدرمز ۳۹
حمله به تأییدیه ۴۲
درستی پیام ۴۳
استفاده ازMAC برای اطمینان ازدرستی پیام ۴۴
چراهردوازکدهای تأییدپیام استفاده می کنند ۴۶
فشرده سازی فایل وMAC ۴۶
بخش هشتم ۴۷
مشکلات تبادل کلیدرمز ۴۷
استفاده ازطرف سوم ۴۹
مرکزتقسیم کلیدوبازسازی کلید ۵۱
مشکلات استفاده ازنفرسوم ۵۲
قسمت دوم ۵۳
رمزنگاری کلید عمومی ۵۳

صفحه

فهرست عناوین

بخش نهم ۵۴

کلید عمومی پیشرو، تبادل عمومی کلیدهای رمز ۵۴

جستجوی راه حلی برای تحویل کلید ۵۴

توسعه یک نوآوری درحل مشکل تحویل کلید رمز ۵۴

راه حل اول : پایگاه داده ای ازجفت های کلیدوسریال نامبر ۵۴

راه حل دوم : پایگاه داده ای رمزمی شود ۵۶

دیدگاه مرکل : جفت های رمزشده کلیدوسریال نامبر جداگانه ۵۶

سیاه کلاه به مشکل می خورد ۵۸

راه حل جدید: تمامی کار مرکل ۵۹

مشکلات روش دیفی - هلمن ۶۱

بخش دهم ۶۲

استفاده ازکلیدعمومی به طرز محرمانه ۶۲

گرایش های جدید به مقوله های منیع قدیمی ۶۲

ضمانت های محرمانه بودن ۶۴

توزیع کلیدعمومی ۶۴

دوراه برای محرمانه بودن ۶۶

بخش یازدهم ۶۷

ایجادکلیدهای عمومی : حقه های ریاضی ۶۷

آسان بودن کارآلیس ۶۸

حقه های ریاضی ۷۰

ریاضی مدرسه ای ۷۱

تقسیم وباقی مانده ۷۲

وارونگی مدورلاتور ۷۵

استفاده ازمدولاتور وارونه برای ایجاد کلیدعمومی ۷۷

جمع بندی همه ۷۸

به دردسرانداختن کلاه سیاه ۷۸

بخش دوازدهم ۸۱

ایجاد امضاهای دیجیتالی وکلیدخصوصی ۸۱

ضمانت امضای نوشته شده ودیجیتالی ۸۲

بررسی ومقایسه مجوز ۸۳

مجوز کلید خصوصی ۸۳

صفحه

فهرست عناوین

بخش شانزدهم ۱۱۲

گواهی های دیجیتالی ۱۱۲

رمز کردن گواهی دیجیتالی ۱۱۳

حمله به گواهی های دیجیتالی ۱۱۳

حمله به ایجادکننده گواهی امضا ۱۱۳

مفهوم گواهی های دیجیتالی ۱۱۴

نیازکاربران گواهی دیجیتالی ۱۱۴

دریافت کلیدعمومی اول ۱۱۵

گواهی های مرورگرها ۱۱۵

بخش هفدهم ۱۱۸

کلیدعمومی X.509 ..... ۱۱۸

کلیدعمومی تایید شده ۱۱۹

تقاضانامه، تایید وتضمین ۱۱۹

ایجاد شبکه مطمئن X.509 ..... ۱۲۰

نام های منتشرشده ۱۲۴

X.509 داده ها را تایید می کند ۱۲۵

جدول(۲-۱۷) : فیلد های نسخه سوم X.509 ..... ۱۲۵

بخش هجدهم ۱۲۷

خصوصی سازی وایمنی ۱۲۷

تاریخ PGP ۱۲۷

مقایسه گواهی های X.509 و PGP ۱۲۷

ایجاد شبکه های مطمئن ۱۲۹

باب کلیدآلیس را تایید می کند ۱۲۹

قسمت چهارم ۱۳۴

سیستم های جهان واقعی ۱۳۴

پارامترهای رمزنگاری e-mail ۱۳۴

پارامترهای رمزنگاری مباحث SSL و Ipsec ۱۳۵

بخش نوزدهم ۱۳۶

e-mail ایمن ۱۳۶

پیام های رمزنگاری شده e-mail ۱۳۶

فهرست عناوین

صفحه

فراخوان سیستم های رمزنگاری ۱۳۷
اطمینان ومجوزدرانتخاب سرویس ۱۳۹
رمزکردن وسپس کلیدخصوصی گذاشتن ۱۳۹
اختصاص کلیدخصوصی وسپس رمزکردن ۱۴۰
تشخیص ویروس های e-mail ۱۴۰

بخش بیستم ۱۴۱

SSL و TLS ۱۴۱
تاریخ SSL ۱۴۱
تبادل گواهی های دیجیتال ۱۴۴
توافق کلیدی (تبادل) ۱۴۵
مجوز ۱۴۶
اطمینان ودرستی ۱۴۷
متغیرهای TLS ۱۴۸
Diffie – Hellmen تابع ۱۴۸
مقایسه TLS ، SSLV3 و SSLV2 ..... ۱۴۹
مشکل بزرگ SSLV2 ..... ۱۴۹
مشکلی با TLS و SSL ۱۴۹
ایجادرمزهای مشترک ۱۵۰

بخش بیست ویکم ۱۵۲

بررسی Ipsec ۱۵۲
افزایش امنیت ۱۵۲
مدیریت کلید ۱۵۳
توزیع دستی ۱۵۳
توزیع خودکار ۱۵۳
قسمت اول Ipsec : مجوزکاربرد وتبادل کلیداستفاده از IKE ۱۵۴
ترتیب کلید Ipsec و SSL/TLS ۱۵۴
فازها ۱۵۴
فاز اول : مجوزوتوافق کلیدی ۱۵۵
پیام های رمزنگاری شده e-mail ۱۳۶
فاز دوم : تنظیم پارامترهای رمزنگاری ۱۵۶
مزایای تبادل کلید دردوفاز ۱۵۶
تبادل کلیدهای رمزنگجاری داده ها ۱۵۷

صفحه

فهرست عناوین

جدول(۲-۲۱) ۱۵۷
ایجادکلیدهای رمزنگاری برای برنامه های جداگانه ۱۵۷
قسمت دوم Ipsec : محرمانه بودن داده هاودرستی پیام یا انتقال فایل ۱۵۸
قرارداد مد ۱۵۹
جدول(۲-۲۱) بسته های داده ای Ipsec بایکی ازچهارگزینه حفاظت می شوند ۱۶۰
قراردادها ۱۶۰
مدها ۱۶۱
مثال های AH ۱۶۳
کنترل مدیریت ۱۶۴
بخش بیستم ودو ۱۶۶
حمله های رمزشده ۱۶۶
حمله بازپخش ۱۶۶
مردی درمیان حمله ۱۶۶
یافتن کلیدها درحافظه ۱۶۸
جابه جایی یک کلیدجعل شده ۱۶۹
حمله Cut و Paste ۱۶۹
کلیدعمومی به عنوان ابزار رمزنگاری ۱۷۰
حمله به متن ساده انتخاب شده ۱۷۰
استانداردهای رمزنگاری کلیدعمومی ۱۷۲
کلاه سیاه ازکلیدخصوصی RSA باب استفاده می کند ۱۷۲
بخش بیستم وسوم ۱۷۶
حفاظت ازکلیدها ۱۷۶
کارت های هوشمند(Smart Cards) ۱۷۶
انواع کارت های هوشمند ۱۷۷
درکارت هوشمندچیست؟ ۱۷۸
حفاظت ها ومحدودیت ها ۱۷۸
حمله به کارت های هوشمند ۱۷۸
سخن آخر ۱۸۰
چه کسانی و ازکجا این الگوریتم را پیشنهاد کرده اند؟ ۱۸۰
چرا NIST ، Rijndael را به AES پیشنهاد کرد؟ ۱۸۰
چرا چهارالگوریتم دیگرانتخاب نشده اند؟ ۱۸۱

فهرست عناوین

صفحه

آیا AES جایگزین DES سه گانه و DES می شود؟ ۱۸۱
آیا NIST روی خواستگاه خارجی این الگوریتم تاکیددارد؟ ۱۸۱
کلیدهای AES تقریبا چقدربزرگ است؟ ۱۸۱
کلیدهای عمومی H.X.Mel و Doris Baker ۱۸۱
کلید H.X.Mel PGP ۱۸۲
کلید Doris Baker PGP ۱۸۳

ضمیمه الف ۱۸۴

ریاضیات کلیدعمومی و متن درارتباط با اعداد تصادفی ۱۸۴

حروف به منزله اعداد ۱۸۴
چرا ریاضی؟ ۱۸۵
یک مطلب دیگر ۱۸۶
بعضی مسائل پایه ای ۱۸۸
معکوس کردن ۱۸۸
یا ۱۹۰
سایرمعکوس ها ۱۹۱
معکوس های رمزگذاری ۱۹۳
اعداد اول ۱۹۳
ریاضیات مدولی(Modular) ۱۹۴
عبارات توانی ۱۹۹
RSA ۲۰۰
$7^{10} \ mod \ 11 = 1$ ۲۰۱
دونکته ۲۰۵
امنیت ۲۱۳
سئوال آخر ۲۱۵
یا فتن اعداد اول ۲۱۵
امتحان فری ۲۱۹
یافتن مقدارمعکوس : توسط الگوریتم اقلیدوسی ۲۲۳
برای یافتن جواب می توان به روش زیر عمل کرد ۲۲۳

سایرالگوریتم های کلیدعمومی ۲۲۷

قدم اول : ساختن زوج کلید ۲۲۷
قدم دوم : تطابق مقادیرمحاسبه شده ۲۲۸

صفحه

فهرست عناوین

قدم سوم : تطابق محاسبات مقداررمزی ۲۲۸
قدم چهارم : محاسبات کلیدرمزی مقصد ۲۲۸
ایمنی ۲۳۰
مدول های اولیه ۲۳۳
درهرزوج عدد بالا X عدد اول وy عدد دوم است. تمام این نقاط به نتایج یکسانی منتج می شوندبه جزعدد آخرکه بینهایت جواب داده است . به این نقاط ، متقلب یاCHEATER گفته می شود. دراین حالت درمعادلات بحث تقسیم بر صفر بوجود می آیدکه بینهایت است ۲۳۴
اضافه کردن نقاط ۲۳۵
و ۲۳۶
ایمنی ۲۳۸
کاربردهای دیگرمنحنی بیضوی ۲۳۹
انواع دیگرمنحنی های بیضوی ۲۴۰
بخش های دیگرایمنی ۲۴۰
ساخت اعداد تصادفی - ساختگی ۲۴۰
چرا تصادفی؟ ۲۴۱
بذرها ۲۴۳
آنتروپی ۲۴۳
بقیه بذرها ۲۴۴
بذربه عنوان کلید ۲۴۴
خلاصه ۲۴۴
ضمیمه ب ۲۴۵
جزئیاتی درموردIKE ومدیریت کلید ۲۴۵
قسمت اول : تاییداعتبارIKE ومدیریت کلید ۲۴۵
IKE و حفاظت شبکه ۲۴۵
مرحله ۱ IKE ۲۴۵
مرحله ۲ IKE ۲۴۶
اختفای کامل پیشرو ۲۴۸
حالت های مرحله اول IKE : مهاجم واصلی ۲۴۹
حمله قطع خدمات ۲۵۱
حمله دست وپاگیر ۲۵۳
کوکی های هوشیار ۲۵۴
امکانات تایید اعتبار ۲۵۴

فهرست عناوین

صفحه

مشخصات ۲۵۵
جدول B-L چگونگی ارسال مشخصات درمهاجم واصلی ۲۵۶
قسمت دوم : محرمانه بودن انبوه پیام ها ودرستی پیغام ها ۲۵۶
رشته اعداد ومقابله با پاسخ ۲۵۷
ساختار ۲۵۷
ESP ۲۵۸
AH ۲۵۹
ترکیب کردن SA ها ۲۵۹
مدیریت کنترل وپردازش Ipsec ۲۵۹