



اصول و مفاهیم

رمزنگاری

مطابق با سرفصل وزارت علوم، تحقیقات و فناوری برای رشته‌های کامپیوتر و

فناوری اطلاعات

مؤلف:

دکتر محمد علی ترکمانی

شناسه : ترکمانی، محمدعلی، ۱۳۵۴ -

عنوان و نام پدیدآور: اصول و مفاهیم رمزنگاری / مولف محمدعلی ترکمانی .

مشخصات نشر : مشهد: ارسطو، ۱۳۹۴.

مشخصات ظاهری : ۲۸۴ ص.: مصور، جدول ، نمودار .: ۱۷×۲۴ س م .

شابک : ۹۷۸ - ۶۰۰ - ۷۵۵۸ - ۵۱ - ۵

وضعیت فهرست نویسی : فیپای مختصر

یادداشت: این مدرک در آدرس <http://opac.nlai.ir> قابل دسترسی است.

شماره کتابشناسی ملی : ۳۷۶۶۴۲۸

نام کتاب : اصول و مفاهیم رمزنگاری

مولف : دکتر محمد علی ترکمانی

ناشر : ارسطو (با همکاری سامانه اطلاع رسانی چاپ و نشر ایران)

صفحه آرای، تنظیم و طرح جلد : علی بیات

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : پنجم - ۱۳۹۸

تعداد صفحات: ۲۹۰ ص

چاپ : مدیران

قیمت : ۵۸۰۰۰ تومان

تلفن های مرکز پخش : ۳۵۰۹۶۱۴۵ - ۳۵۰۹۶۱۴۶ - ۰۵۱ - ۰۹۱۷۷۱۶۴۹۴۰

وب سایت: www.chaponashr.ir/Torkamani

این اثر مشمول قانون حمایت از مولفان و مصنفان و هنرمندان است. هر کس تمام یا قسمتی از این اثر را بدون اجازه مولف نشر یا پخش یا عرضه کند، مورد پیگرد قانونی قرار خواهد گرفت.

فهرست مطالب

فصل اول: مفاهیم امنیت اطلاعات و رمزنگاری ۱۴

۱-۱- امنیت اطلاعات چیست؟ ۱۴

۱-۲- اصول امنیت اطلاعات ۱۴

۱-۳- اصطلاحات امنیتی ۱۵

۱-۳-۱- آسیب پذیری ۱۵

۱-۳-۲- حمله ۱۶

۱-۳-۳- تهدید ۱۶

۱-۳-۴- مفهوم AAA در امنیت اطلاعات ۱۷

۱-۳-۵- عدم انکار (سندیت) ۱۸

۱-۴- نفوذگر یا هکر ۱۸

۱-۶- برخی از حملات متداول ۱۸

۱-۶-۱- افشای پیام یا سرقت اطلاعات ۱۸

۱-۶-۱-۱- استراق سمع یا شنود اطلاعات ۱۸

۱-۶-۲- تحلیل ترافیک ۱۹

۱-۶-۳- نقاب زنی یا بدل ۱۹

۱-۶-۴- حمله مرد میانی ۱۹

۱-۶-۵- حمله روز تولد ۲۰

۱-۶-۶- حملات جهت یافتن کلمات عبور ۲۰

۱-۶-۸- حمله تکرار ۲۱

۱-۷- رمزنگاری چیست؟ ۲۲

- ۱-۷-۱- سیستم‌های رمزنگاری ۲۳
- ۱-۷-۱-۱- رمزنگاری متقارن ۲۳
- ۱-۷-۱-۲- رمزنگاری نامتقارن ۲۴
- ۱-۷-۳- علم تحلیل رمز یا شکستن رمز ۲۵
- ۱-۷-۴- عملیات مورد استفاده در یک سیستم رمزگذاری ۲۵
- ۱-۷-۶- اصول اساسی رمزنگاری ۲۶
- ۱-۸- سئوالات تشریحی ۲۷
- ۱-۹- سئوالات چهارگزینه‌ای ۲۸
- پاسخنامه ۲۹

فصل دوم: مروری بر مفاهیم ریاضی مورد نیاز ۳۲

- ۲-۱- بخش پذیری ۳۲
- ۲-۱-۱- قضیه تقسیم ۳۲
- ۲-۱-۲- بزرگترین مقسوم علیه مشترک ۳۳
- ۲-۱-۲-۱- الگوریتم اقلیدسی ۳۳
- ۲-۱-۲-۱-۱- قضیه ۳۳
- ۲-۱-۲-۲- نکات مهم ۳۴
- ۲-۱-۲-۲- الگوریتم اقلیدسی توسعه یافته ۳۴
- ۲-۲- اعداد اول ۳۵
- ۲-۲-۱- مسئله تجزیه اعداد ۳۵
- ۲-۲-۲- هم نهشتی ۳۵
- ۲-۳- الگوریتم توان رسانی سریع ۳۷
- ۲-۴- قضیه باقیمانده چینی برای حل دستگاه هم نهشتی ۴۰
- ۲-۵- ماتریس‌ها ۴۷

- ۴۸..... ۱-۵-۲- جمع دو ماتریس
- ۴۸..... ۲-۵-۲- ضرب یک عدد در یک ماتریس
- ۴۸..... ۳-۵-۲- ضرب ماتریسها
- ۴۹..... ۴-۵-۲- محاسبات دترمینان ماتریس 2×2
- ۴۹..... ۵-۵-۲- محاسبه دترمینان ماتریس 3×3
- ۵۰..... ۵-۵-۲- ۱-روش ساروس برای محاسبه دترمینان
- ۵۰..... ۶-۵-۲- ماتریس وارون
- ۵۲..... ۶-۲- تعریف
- ۵۳..... ۷-۲- پیش زمینه های ریاضی در رمزنگاری AES
- ۵۳..... ۱-۷-۲- نظریه گروه، حلقه و میدان
- ۵۳..... ۱-۷-۲- گروه
- ۵۴..... ۲-۷-۱-۲- حلقه
- ۵۷..... ۳-۷-۲- میدان
- ۵۸..... ۴-۷-۲- حلقه های چند جمله ای
- ۶۱..... ۵-۷-۲- میدان گالوا $GF(p)$
- ۶۱..... ۸-۲- الگوریتم گسسته
- ۶۳..... ۹-۲- سئوالات تشریحی
- ۶۵..... ۱۰-۲- سئوالات چهارگزینه ای
- ۷۰..... پاسخنامه

فصل سوم: رمزنگاری کلاسیک، مدرن و اصول رمزنگاری متقارن..... ۷۱

- ۷۱..... ۱-۳- رمزگذاری کلاسیک و مدرن
- ۷۱..... ۱-۳-۱- اصول کرشهف برای سیستمهای رمزنگاری مدرن
- ۷۲..... ۲-۳- ویژگیهای سیستمهای مدرن رمزنگاری متقارن

- ۳-۳-۳- مرور برخی از الگوریتم‌های رمزنگاری کلاسیک ۷۵
- ۳-۳-۱- رمزنگاری سزار ۷۶
- ۳-۳-۲- رمزنگاری ورنام ۷۸
- ۳-۳-۳- رمزنگاری جابجایی ستونی ۷۸
- ۳-۳-۴- ترکیب جایگشتی و جایگزینی ۷۹
- ۳-۳-۵- رمزنگاری Hill ۸۰
- ۳-۴- تکنیک‌های رمزنگاری متقارن ۸۷
- ۳-۴-۱- رمز رشته‌ای یا دنباله‌ای ۸۷
- ۳-۴-۲- رمز بلاکی ۸۸
- ۳-۴-۲-۱- جایگزینی و جایگشتی بلاکی ۸۹
- ۳-۴-۲-۱-۱- جایگزینی بلاکی (S-BOX) ۸۹
- ۳-۴-۲-۱-۲- جابجایی بلاکی (جایگشتی) یا P-BOX ۸۹
- ۳-۴-۲-۱-۲-۱- طریقه حمله به P-BOX ۸۹
- ۳-۴-۳- ویژگی ساختار فیستل برای رمزنگاری متقارن ۹۱
- ۳-۵- سئوالات تشریحی ۹۳
- ۳-۶- سئوالات تشریحی ۹۷
- ۳-۷- سئوالات چهارگزینه‌ای ۹۸
- پاسخنامه ۱۰۰

فصل چهارم: الگوریتم‌های رمزنگاری متقارن ۱۰۱

- ۴-۱- رمزنگاری DES ۱۰۱
- ۴-۱-۱- جزئیات تابع $F_{Ri} - 1, Ki$ ۱۰۳
- ۴-۱-۲- روش استخراج کلیدهای فرعی از کلید اصلی یا شاه کلید ۱۰۹
- ۴-۱-۳- رمزگشایی DES ۱۱۰

۱۱۰	۴-۱-۴- خاصیت بهمنی DES
۱۱۲	۴-۱-۵- نکات مهم الگوریتم DES
۱۱۲	۴-۱-۶- الگوریتم 2DES
۱۱۳	۴-۱-۷- الگوریتم 3DES
۱۱۳	۴-۱-۷-۱- نکات مهم الگوریتم 3DES
۱۱۴	۴-۱-۸- امنیت DES
۱۱۴	۴-۲- الگوریتم AES
۱۲۶	۴-۲-۱- گسترش کلید در AES
۱۳۰	۴-۲-۲- توصیف ریاضی روش AES
۱۳۳	۴-۲-۳- چندجمله‌ای با ضرایبی در $GF(2^8)$
۱۳۴	۴-۲-۳-۱- ضرب چندجمله‌ای با ضرایبی در $GF(2^8)$
۱۳۵	۴-۲-۳-۲- تبدیل MixColumns () در رمزنگاری AES
۱۳۷	۴-۳- سئوالات تشریحی
۱۳۸	۴-۳- سئوالات چهارگزینه‌ای
۱۴۴	پاسخنامه

فصل پنجم: رمزنگاری با کلید عمومی ۱۴۵

۱۴۵	۵-۱- رمزنگاری با کلید عمومی
۱۴۶	۵-۲- الگوریتم RSA
۱۴۸	۵-۲-۱- انتخاب کلید
۱۴۸	۵-۲-۲- روش رمزگذاری و رمزگشایی
۱۵۲	۵-۲-۳- کارایی الگوریتم RSA
۱۵۳	۵-۲-۴- الگوریتم RSA به عنوان یک رمز قالبی (بلاکی)
۱۵۵	۵-۳- تبادل کلید با استفاده از رمزنگاری RSA

۱-۳-۵- پروتکل توزیع کلید متقارن با استفاده از کلید عمومی	۱۵۶
۴-۵- رمزنگاری کلید عمومی الجمال	۱۵۸
۵-۵- روش مبادله کلید دیفی- هلمن	۱۶۲
۱-۵-۵- الگوریتم مبادله کلید دیفی - هلمن	۱۶۲
۲-۵-۵- حمله مرد میانی علیه الگوریتم «دیفی - هلمن»	۱۶۶
۶-۵- مقایسه الجمال، دیفی- هلمن، RSA و AES	۱۶۷
۷-۵- الگوریتم نامتقارن منحنی بیضوی	۱۶۸
۱-۷-۵- تعریف منحنی بیضوی	۱۶۸
۲-۷-۵- منحنی‌های بیضوی در میدان‌های متناهی	۱۶۹
۳-۷-۵- رمزگذاری توسط منحنی‌های بیضوی (ECC)	۱۷۱
۴-۷-۵- توزیع کلید توسط ECC	۱۷۲
۵-۷-۵- رمزگذاری و رمزگشایی توسط ECC	۱۷۲
۶-۷-۵- امنیت ECC	۱۷۳
۸-۵- مقایسه رمزنگاری متقارن و نامتقارن	۱۷۳
۶-۵- سئوالات تشریحی	۱۷۴
۷-۵- سئوالات چهارگزینه‌ای	۱۷۷
پاسخنامه	۱۸۱

فصل ششم: رمزشکنی و تحلیل رمز ۱۸۲

۱-۶- رمزشکنی و تحلیل رمز	۱۸۲
۲-۶- انواع حملات تحلیل رمز	۱۸۳
۳-۶- اختفاء کامل	۱۸۴
۴-۶- الگوریتم رمزگذاری و رمزگشایی امن	۱۸۵

۱۸۶	۵-۶- رمزشکنی DES
۱۸۶	۱-۵-۶- رمزشکنی تفاضلی
۱۸۶	۲-۵-۶- رمزشکنی خطی
۱۸۶	۶-۶- حمله به RSA
۱۸۸	۷-۶- سئوالات تشریحی
۱۹۰	۸-۶- سئوالات چهارگزینه ای
۱۹۳	پاسخنامه

فصل هفتم: مدهای رمزنگاری بلوکی ۱۹۴

۱۹۴	۱-۷- مقدمه
۱۹۴	۲-۷- حالت کد الکترونیک (ECB) در رمزهای بلوکی
۱۹۶	۳-۷- حالت زنجیره کردن بلوک رمز (CBC)
۱۹۸	۴-۷- حالت پسخورد رمز (CFB)
۱۹۹	۵-۷- حالت پسخورد خروجی (OFB)
۲۰۱	۶-۷- سئوالات تشریحی
۲۰۲	۷-۷- سئوالات چهارگزینه ای
۲۰۴	پاسخنامه:

فصل هشتم: صحت پیام، MAC، امضای دیجیتال و گواهینامه ۲۰۶

۲۰۶	۱-۸- صحت پیام با استفاده از MAC
۲۰۸	۲-۸- تصادم یا تلاقی یا برخورد
۲۰۸	۱-۲-۸- توابع درهم‌ساز مقاوم در مقابل برخورد
۲۰۸	۲-۲-۸- شبه برخورد
۲۰۹	۳-۸- الگوریتم‌های MAC

۲۰۹	MD4 و MD2 الگوریتم‌های
۲۱۰	MD5 الگوریتم
۲۱۴	SHA الگوریتم
۲۱۶	 SHA-2
۲۱۸	 SHA-256 شبه کد الگوریتم
۲۲۱	 SHA-512 الگوریتم
۲۲۳	MD و SHA مقایسه توابع درهم ساز خانواده
۲۲۵	 HMAC کد احراز اصالت
۲۲۶	 HMAC امنیت
۲۲۷	امضای دیجیتال
۲۲۸	گواهینامه
۲۲۹	استاندارد x.509 برای گواهینامه‌های دیجیتالی
۲۳۴	 X.500 نحوه نام گذاری
۲۳۶	ابطال گواهینامه‌های دیجیتالی
۲۳۷	CRL روش
۲۳۹	 DCRL روش
۲۴۰	 OCSP پروتکل
۲۴۳	سئوالات تشریحی
۲۴۳	سئوالات چهارگزینه‌ای
۲۵۱	 پاسخنامه

فصل نهم: امنیت پست الکترونیکی ۲۵۲

۲۵۲	ایمیل امن
۲۵۲	۹-۱-۱ سیستم اول

۲۵۳.....	۹-۱-۲-سیستم دوم
۲۵۴.....	۹-۱-۳-سیستم سوم
۲۵۵.....	۹-۲-استاندارد PGP
۲۵۷.....	۹-۳-پست الکترونیکی چند منظوره امن S/MIME
۲۵۸.....	۹-۴-سئوالات تشریحی
۲۵۹.....	۹-۵-سئوالات چهارگزینه‌ای
۲۶۰.....	پاسخنامه

فصل دهم: زیر ساخت کلید عمومی ۲۶۰

۲۶۰.....	۱۰-۱-زیر ساخت کلید عمومی
۲۶۲.....	۱۰-۲-اهداف امنیتی زیر ساخت کلید عمومی
۲۶۲.....	۱۰-۳-وظایف زیر ساخت کلید عمومی
۲۶۲.....	۱۰-۴-اجزای زیر ساخت کلید عمومی
۲۶۳.....	۱۰-۴-۱-مرجع ثبت نام (CA)
۲۶۳.....	۱۰-۴-۲-فهرست کلید عمومی
۲۶۴.....	۱۰-۴-۳-سرویس دهنده بازیابی کلید
۲۶۵.....	۱۰-۴-۴-پروتکل های مدیریتی
۲۶۶.....	۱۰-۴-۵-پروتکل های عملیاتی
۲۶۶.....	۱۰-۵-معماری های زیرساخت کلید عمومی
۲۶۷.....	۱۰-۵-۱-معماری متمرکز
۲۶۷.....	۱۰-۵-۲-معماری سلسله مراتبی
۲۷۰.....	۱۰-۵-۳-معماری شبکه‌ای
۲۷۳.....	۱۰-۵-۴-معماری پل

۶-۱۰-سوالات تشریحی ۲۷۴

۷-۱۰-سوالات چهارگزینه ای ۲۷۴

پاسخنامه: ۲۷۷

فصل یازدهم: تسهیم راز ۲۸۰

۱-۱۱-مفهوم تسهیم راز ۲۸۰

۲-۱۱-انواع طرح های تسهیم راز ۲۸۱

۱-۲-۱۱-طرح تسهیم راز آستانه ای (n,m) ۲۸۱

۲-۲-۱۱-طرح تسهیم راز کامل ۲۸۲

۳-۲-۱۱-طرح تسهیم راز همه یا هیچ ۲۸۲

۴-۲-۱۱-طرح های تسهیم راز با امنیت محاسباتی ۲۸۲

۵-۲-۱۱-طرح های تسهیم راز ایده آل ۲۸۳

۶-۲-۱۱-طرح های تسهیم راز آستانه ای وزن دار ۲۸۳

۳-۱۱-بررسی دو طرح تسهیم راز اولیه ۲۸۳

۱-۳-۱۱-طرح تسهیم راز بلکلی ۲۸۳

۲-۳-۱۱-طرح تسهیم راز شمیر ۲۸۵

۴-۱۱-سوالات تشریحی ۲۸۶

۵-۱۱-سوالات چهارگزینه ای ۲۸۷

پاسخنامه: ۲۸۹

پیوست: جدول کدهای اسکی ۲۹۰

مراجع: ۲۹۱

مقدمه:

رمزنگاری علمی است که به بررسی و مطالعه روش‌ها و الگوریتم‌های رمزنگاری می‌پردازد. رمزگذاری عبارت است از یک نظام یا الگوی ریاضی / منطقی که بر اساس آن اطلاعات و مفاهیم قابل فهم برای همگان، طبق روالی برگشت‌پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می‌شود. این اطلاعات نامفهوم و گنگ توسط کسی که روال معکوس و پارامترهای لازم را می‌داند قابل برگشت و بهره‌برداری است. به این روال معکوس، رمزگشایی می‌گویند. بسیاری از نیازمندیهای امنیتی به وسیله رمزگذاری تامین می‌گردد. رمزنگاری موجب جلوگیری از بسیاری از مشکلات امنیتی در سیستمها و شبکه‌های رایانه‌ای می‌شود.

علیرغم اینکه درس رمزنگاری یکی از دروس تخصصی در رشته‌های مهندسی کامپیوتر و فناوری اطلاعات محسوب می‌شود، اما مرجع مناسبی برای آن وجود ندارد. حجم مراجع معرفی شده برای این درس بسیار زیاد است و تدریس این مطالب در یک نیم سال تحصیلی دشوار است. ضمناً هیچکدام از مراجع موجود به تنهایی سرفصل‌های مورد نیاز برای این درس را پوشش نمی‌دهند.

این کتاب به منظور سهولت کار اساتید و دانشجویان گرامی و همچنین افزایش کیفیت آموزشی درس رمزنگاری تدوین گردیده است. در این کتاب سعی شده است که مطالب با زبانی ساده و به همراه مثال‌های متنوعی ارائه گردد. در انتهای هر فصل مجموعه سئوالات تستی به همراه حل آنها آورده شده است. همچنین تعدادی تشریحی و مسئله به همراه پاسخ برخی از مسائل ارائه شده است تا دانشجویان گرامی بهتر بتوانند خود را برای آزمون‌هایی که در پیش رو دارند آماده نمایند. امید است این اثر مورد توجه همکاران و دانشجویان گرامی قرار گیرد. از اساتید و دانشجویان گرامی تقاضا دارم نقطه نظرات خود را از طریق ایمیل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا ان شاء الله در ویرایش‌های بعدی کتاب اشکالات یا کاستی‌های احتمالی آن، مورد تجدید نظر قرار گیرد.

در پایان وظیفه خود می‌دانم از زحمات آقای مهندس علی بیات به خاطر طراحی جلد و همچنین از مدیریت انتشارات ارسطو و سامانه اطلاع رسانی چاپ و نشر ایران جناب آقای حسین قنبری به خاطر مساعدت در کار چاپ تشکر و قدردانی نمایم.

محمد علی ترکمانی

بهار ۱۳۹۴

فصل اول

مفاهیم امنیت اطلاعات و رمزنگاری

۱-۱- امنیت اطلاعات چیست؟

امنیت اطلاعات عبارت است از حفاظت اطلاعات در مقابل دسترسی های غیر مجاز، استفاده، افشاء، اختلال، اصلاح، مطالعه، بازرسی، ضبط یا تخریب، همچنین علم مطالعه روش های حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر تغییرات غیرمجاز از محرمانگی، تمامیت و دسترس پذیری اطلاعات. سایر ویژگی های دیگر امنیت اطلاعات از قبیل اصالت، اعتبار، انکارناپذیری، قابلیت جوابگویی و قابلیت اطمینان اطلاعات نیز می تواند مشمول این حفاظت باشند.

یک سیستم درست سیستمی است که اگر ورودی خوب و درست به آن داده شود خروجی درست به ما می دهد. اما سیستم امن سیستمی است که اگر حمله کننده به آن ورودی بد بدهد، سیستم خراب نشود. به طور کلی طراحی امکانات بیشتر در یک سیستم از نظر امنیت اطلاعات در دسر ساز است. زیرا باید کنترل روی ورودی ها بیشتر باشد. در امنیت اطلاعات به دنبال ساده بودن و مینیمم بودن سیستم هستیم. در صورتی که در یک سیستم خوب همیشه به دنبال امکانات بیشتر هستیم. در کل هدف ما این است که یک سیستمی داشته باشیم که هم درست و هم امن باشد.

۱-۲- اصول امنیت اطلاعات

یک سیستم امن باید دارای ویژگی های زیر باشد:

- **محرمانگی:**^۱ اطلاعات باید تنها توسط افرادی که تأیید صلاحیت شده‌اند، قابل دیدن باشد. به عنوان مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت را دارند. محرمانگی به وسیله رمزنگاری تأمین می‌شود.
 - **صحت:**^۲ داده‌ها نباید به صورت تصادفی یا عمدی تغییر داده شوند، نابود شده و یا گم شوند. به عنوان مثال جعل اطلاعات^۳ صحت را به چالش می‌کشد.
 - **دسترسی پذیری:**^۴ هرگاه کاربر به سیستم نیاز داشت سیستم وجود داشته باشد. به عبارت دیگر سیستم باید قادر باشد هنگام درخواست کاربر، سرویس یا سرویس‌های مورد نظر را ارائه دهد. به عنوان مثال قطع کردن ارتباط^۵ و یا از کار انداختن یک کامپیوتر سرویس دهنده عدم دسترسی‌پذیری را فراهم می‌کند. نمونه ای از این حملات، حمله انکار سرویس یا DOS است.^۶
- در کنار این سه اصل اساسی، نیازمندیهای امنیتی دیگری نظیر عدم انکار،^۷ تایید هویت^۸ نیز مطرح است. منظور از عدم انکار این است که فرستنده نتواند ادعا کند پیام از طرف وی ارسال نشده است.

۳-۱- اصطلاحات امنیتی

۱-۳-۱- آسیب‌پذیری^۹

Confidentiality

Integrity

Fabrication

Availability

Interruption

Denial of Service

Non-Repudiation

Authentication

Vulnerability

آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است. آسیب‌پذیری می‌تواند در یکی از موارد زیر باشد:

- طراحی سیستم: در این حالت پروتکل یا الگوریتم ایراد دارد. به عنوان مثال طراحی پروتکل TCP/IP درست انجام نشده و بسته‌های TCP/IP به صورت متن ساده (رمز نشده) هستند. این یک ایراد طراحی است که یک آسیب‌پذیری را برای این پروتکل به وجود آورده است و باعث شده است که اگر یک نفر گوش کند، بتواند محتوای بسته‌های IP را ببیند.
- پیاده‌سازی: به عنوان مثال فرض کنید در برنامه نویسی یک پروتکل، مواردی (نظیر اصول یا استانداردهای کدنویسی امن) را رعایت نکرده‌ایم، یا اشتباهاتی داریم. علاوه بر این، در پیاده‌سازی TCP/IP با توابع C یک سری آسیب‌پذیری‌هایی دیده می‌شود که علت آن اشکالات موجود در زبان C است. برای رفع این مورد باید از نسخه‌های جدیدتر این زبان و یا زبان جاوا استفاده کرد.
- عملیات سیستم ایراد دارد: فرآیندها درست انجام نمی‌شود. به عنوان مثال یک فرم پر شده و باید به دست یک نفر برسد ولی به فرد دیگری می‌رسد که نباید آنرا ببیند.

۲-۳-۱- حمله^۲

در علم امنیت شبکه، حمله عبارتست از بهره برداری از آسیب‌پذیری‌های یک سیستم. متخصصان رمزنگاری حمله را به این صورت تعریف می‌کنند: به هرگونه تلاش غیر مجاز برای یافتن کلید رمزنگاری یا رمزگشایی داده‌های رمز شده، حمله می‌گویند.

۳-۳-۱- تهدید^۳

مجموعه‌ای از شرایط و پیشامدها که پتانسیل صدمه زدن به سیستم را دارد. فردی بدخواه که انگیزه و توانایی حمله را داشته باشد و یا یک سیستم که امکان یک حمله را فراهم می‌کند یک تهدید است.

^۱Clear Text

^۲Attack

^۳Threat

۴-۳-۱- مفهوم AAA در امنیت اطلاعات

در دنیای امنیت اطلاعات به واژه مخفف AAA برخورد می‌کنیم که مخفف سه کلمه ذیل است:

- **Authentication:** تأیید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر موجودیت (مانند یک شخص یا یک سرویس دهنده بانکی) بررسی می‌کند که آیا شریک او در یک ارتباط، همان فردی است که ادعا می‌کند یا یک شخص اخلاص‌گر ثالث است که خود را به جای طرف واقعی جا زده است.
- **Authorization:** اجازه^۱ مکانیزمی است که بر اساس آن مشخص می‌شود فرد یا موجودیتی که هویت آن احراز شده، مجوز انجام چه کارها و عملیاتی را در سیستم دارد.
- **Accounting:** حسابداری مکانیزمی است که مشخص می‌کند فرد مورد نظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به عنوان مثال اعتبار کافی دارد یا خیر.

در میان این سه واژه، مهمترین مرحله Authentication است که تامین دو مورد دیگر را نیز بسیار ساده می‌سازد.

به عنوان مثال وقتی فردی می‌خواهد به سیستم دسترسی پیدا کند، ما می‌خواهیم بدانیم آیا همان فرد مورد نظر است یا خیر، تایید هویت انجام می‌دهیم. اما اجازه، بیشتر مفهوم کنترل سطح دسترسی را می‌دهد. به عنوان مثال، در سیستم اینترنتی یک دانشگاه، کاربر هنگام ورود ابتدا تایید هویت می‌شود که مشخص شود کاربری مجاز است یا خیر. در این سیستم اساتید و دانشجویان و سایر پرسنل دانشگاه مجاز به ورود هستند. اما در خصوص اجازه دسترسی، واضح است که یک دانشجو تایید هویت شده و وارد سیستم می‌شود ولی اجازه ویرایش نمرات را ندارد.

در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تایید هویت می‌شود و وارد یک فروشگاه الکترونیکی می‌شود. وی اجازه خرید کردن را دارد. بنابراین Authorization

^۱Authorization

نیز با موفقیت انجام می‌شود. اما ممکن است موجودی این فرد در سایت برای خرید کردن کافی نباشد. بنابراین فرایند Accounting به وی اجازه خرید را نخواهد داد.

۵-۳-۱-عدم انکار (سندیت)^۱

عدم انکار یعنی عمل ارسال و دریافت پیام و نیز محتوای داده و پیام توسط فرستنده و گیرنده قابل انکار نباشد (سرویزی که از انکار فرستنده و گیرنده جلوگیری می‌کند). از این رو، وقتی پیامی ارسال گردید، فرستنده می‌تواند ثابت کند که گیرنده پیام را دریافت کرده است.

۴-۱-نفوذگر یا هکر^۲

به کسی که به تلاش میکند به یک سیستم کامپیوتری دسترسی غیرمجاز داشته باشد، هکر گفته می‌شود.

۶-۱-برخی از حملات متداول

در این قسمت برخی از حملات متداول معرفی می‌شوند.

۱-۶-۱-افشای پیام^۳ یا سرقت اطلاعات^۴

خواندن یک ایمیل محرمانه یا شنود یک ارتباط تلفنی نمونه‌ای از این نوع حمله است. واضح است که این حمله عدم محرمانگی را فراهم می‌کند. (محرمانگی را به چالش می‌کشد).

۱-۶-۱-۱-استراق سمع یا شنود اطلاعات^۵

در این حمله اطلاعات مبادله شده، به روش‌های گوناگون سرقت و یا شنود می‌شوند. به برنامه‌های استراق سمع، Sniffer گویند. اینگونه نرم‌افزارها این امکان را در اختیار مهاجم قرار می‌دهند که

^۱ Non-repudiation

^۲ hacker

^۳ Release of Message

^۴ Interception

^۵ Eavesdropping

بتواند بسته‌های شبکه را دریافت، مشاهده و سپس ارسال نماید. گونه دیگری از استراق سمع، استراق کارت‌های اعتباری و یافتن رمز کارت‌های اعتباری است.

۲-۶-۱- تحلیل ترافیک

در کانال‌های ارتباطی ناامن اطلاعات به صورت رمز شده ارسال می‌گردد تا چنانچه مهاجم پیام‌ها را شنود کند، نتواند پیام اصلی را از داخل آن استخراج نماید. اما حمله کننده می‌تواند اطلاعاتی از قبیل مبداء، مقصد و اندازه پیام‌ها را تحلیل نموده و از آنها برای یافتن برخی از پیام‌ها یا تعیین کلید رمزنگاری استفاده نماید. به عنوان مثال در یک سیستم نظامی ممکن است دشمن حجم داده‌های ارسالی را تحلیل کرده و چنانچه در یک روز خاص حجم اطلاعات بیش از اندازه معمول باشد، حدس بزند که احتمالاً قرار است عملیاتی انجام گردد.

۳-۶-۱- نقاب‌زنی یا بدل^۱

حمله‌ای است که در آن حمله کننده خودش را جای فرد دیگری جا می‌زند. در واقع حمله کننده هویت فرد دیگری را سرقت می‌نماید. این حمله نوعی جعل اطلاعات است و عدم صحت را به دنبال دارد. اما چون مهاجم موفق شده خودش را به جای قربانی جا بزند، در ادامه می‌تواند اطلاعات محرمانه قربانی را خوانده (عدم محرمانگی) و یا با ارسال بسته‌های زیاد قابلیت دسترسی را به چالش بکشد. در ادبیات امنیت شبکه به این نوع حمله، Spoofing (حقه بازی) نیز می‌گویند. به عنوان مثال در IP Spoofing حمله کننده IP خودش را به عنوان IP شخص دیگری جا می‌زند و همه بسته‌های قربانی را دریافت کند. بدترین حالت آن هم این است که IP خودش را به عنوان gateway IP قرار دهد.

۴-۶-۱- حمله مرد میانی^۲

در این حمله نفوذگر بین دو کامپیوتری که در حال تبادل اطلاعات هستند قرار می‌گیرد. در این روش مهاجم می‌تواند به نوعی اطلاعات رد و بدل شده بین دو کامپیوتر را دریافت کرده و آنرا ویرایش کند، بدون آنکه کلاینت متوجه این موضوع شود. هدف اصلی این نوع حملات

^۱Masquerade

^۲Man in the Middel

دسترسی به اعتبارات کلاینت‌ها و یا کاربران شبکه است. توسط این روش می‌توان اطلاعات نرم‌افزارهای مبتنی بر وب و یا مبتنی بر سیستم عامل کاربران را به دست آورد. فرض کنید دو نفر با یکدیگر در ارتباط هستند. در ادبیات امنیت شبکه به این دو نفر معمولاً باب و آلیس گفته می‌شود. تصور کنید فردی بتواند به عنوان حمله‌کننده ارتباط میان این دو نفر را قطع نماید. این فرد باید بتواند ارسال پیغام‌ها را طوری انجام دهد که باب و آلیس متوجه نشوند. در واقع باید بتواند نوع ارسال پیغام‌ها را تقلید نماید. در این حالت باب و آلیس تحت حمله مرد میانی قرار گرفته‌اند.

۵-۶-۱- حمله روز تولد^۱

حمله روز تولد نامی است که به گروهی از حملات قوی اطلاق می‌شود. اگر یک عملیات زمانی که با یک داده تصادفی تغذیه می‌شود، یکی از ارزش‌های k را باز گرداند، آنگاه با ارزش‌گذاری مکرر آن عملیات برای داده‌های مختلف، انتظار می‌رود که پس از $1.2k^{1/2}$ آزمایش به خروجی یکسانی دست یابیم. در واقع اگر به دنبال یافتن یک برخورد هستیم، با استفاده از تناقض (پارادوکس) روز تولد می‌توان انتظار داشت که پس از $1.2k^{1/2}$ آزمایش مقادیر احتمالی داده، به یک تلاقی برسیم. وان اورشات^۲ و وینر^۳ نشان دادند که چنین حمله‌ای می‌تواند به کار گرفته شود. پارادوکس روز تولد به شرح زیر است. فرض کنید گروهی از افراد در یک اتاق هستند. احتمال اینکه دو نفر از آنها روز تولد یکسانی داشته باشند چقدر است؟ به طور شگفت‌انگیزی این احتمال زیاد است. به عنوان مثال اگر ۲۳ نفر در یک اتاق باشند، آنگاه با احتمال حداقل $1/2$ ، دو نفر از آنها روز تولد مشترک دارند. در کتب کلاسیک رمزنگاری اثبات این موضوع نشان داده شده است.

۶-۶-۱- حملات جهت یافتن کلمات عبور

^۱Birthday

^۲Van Oorschot

^۳Wiener

متداول ترین روش هایی که برای یافتن کلمات عبور به کار می روند عبارتند از:

- **جستجوی جامع:**^۱ جستجوی جامع یک روش برای شکستن کلمات رمز و به دست آوردن آنها است. حمله جستجوی جامع حروف را به صورت ترکیبی استفاده می کند و با تست کردن آنها رمز عبور را پیدا می کند. برای مقابله با این روش باید کلمات رمزی با طول زیاد انتخاب کرد و یا کلمات رمز را هر دفعه تغییر داد. در این روش حمله کننده باید تمام رمزهای عبور (یا کلیدهای رمزنگاری) ممکن که برای رمزگذاری استفاده می شوند را امتحان کند تا کلمه عبور یا متن رمز نشده را به دست آورد.
- **واژه نامه:**^۲ یک روش برای به دست آوردن کلمات عبور با استفاده از لغات دیکشنری است. واژه نامه در اصل لغتنامه ای از کلمات معروف می باشد که در یک فایل ذخیره شده اند و به وسیله یک ابزار برای شکستن کلمات رمز، مورد استفاده قرار می گیرد. برای مقابله با این حمله باید از کلماتی استفاده کرد که در لغتنامه وجود ندارد.
- **روش ترکیبی برای شکستن کلمات عبور :** در این روش از ترکیب دو روش قبل استفاده می شود.

۸-۶-۱- حمله تکرار^۳

به عمل دریافت داده در بین راه و ارسال مجدد آن با هدف دستیابی غیر مجاز، تکرار گویند. به عنوان مثال وقتی یک هکر به وسیله ابزارهای sniffer بسته های اطلاعاتی را از روی سیم بر می دارد، یک حمله تکرار رخ داده است. وقتی بسته ها دزدیده شدند، هکر اطلاعات مهم و نام های کاربری و کلمات عبور را از درون آن استخراج کرده و دوباره بسته ها را روی خط قرار می دهد و یا به آنها به صورت دروغین پاسخ می دهد.

^۱Brute force , or Exhaustive key search

^۲Dictionary

^۳Reply

۷-۱- رمزنگاری چیست؟

رمزنگاری علمی است که به بررسی و مطالعه روش‌ها و الگوریتم‌های رمزنگاری می‌پردازد. رمزگذاری عبارت است از یک نظام یا الگوی ریاضی/منطقی که بر اساس آن اطلاعات و مفاهیم قابل فهم برای همگان، طبق روالی برگشت‌پذیر به اطلاعاتی نامفهوم و گنگ تبدیل می‌شود. این اطلاعات نامفهوم و گنگ توسط کسی که روال معکوس و پارامترهای لازم را می‌داند قابل برگشت و بهره برداری است. به این روال معکوس، رمزگشایی می‌گویند. در برخی از کتاب‌ها واژه رمزنگاری را به جای رمزگذاری نیز به کار می‌برند. می‌توان فرایند رمزگذاری را به تابعی به شکل زیر تصور کرد:

$$C = f_E(P, K)$$

در این تابع P پیامی است که باید رمز شود که به آن متن ساده می‌گویند. K پارامتری است که متن ساده بر اساس آن به صورت غیر قابل پیش بینی و مبهم، درهم و بی معنی می‌شود. به پارامتر K ، کلید رمز یا کلید رمزگذاری می‌گویند. C حاصل فرایند رمزنگاری متن ساده P با کلید K و تابع رمزگذاری f_E است که به آن متن رمز می‌گویند. همچنین می‌توان فرایند رمزگشایی را نیز که طی آن متن رمز به متن ساده تبدیل می‌شود، به صورت زیر نمایش داد:

$$P = f_D(C, K)$$

در این رابطه f_D تابع رمزگشایی و K کلید رمزگشایی می‌باشد.

در اینجا به ذکر یک مثال از کاربرد رمزنگاری می‌پردازیم. فرض کنید در یک کانال مخابراتی ناامن، فرستنده می‌خواهد یک پیام محرمانه را برای گیرنده ارسال نماید و هدف وی حفظ محرمانگی پیام است. روش انجام کار به این ترتیب است که متن ساده یا رمز نشده توسط یک الگوریتم رمزنگاری رمز می‌شود و خروجی آن که متن رمز است، برای گیرنده ارسال می‌شود. در مقصد نیز رمزگشایی متن رمز شده، توسط یک الگوریتم رمزگشایی انجام می‌شود و متن ساده اولیه به دست می‌آید.

ⓈCryptography

ⓈEncryption

ⓈDecryption

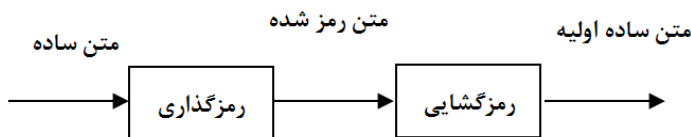
ⓈPlaintext/Clear Text

ⓈKey

نکته: برای نوشتن متن نیاز به حروف یا سمبل‌هایی از یک الفبا داریم که یک مجموعه غیر تهی است و آنرا با Σ نمایش می‌دهیم و به آن الفبای رمزنگاری می‌گوییم. به عنوان مثال الفبای رمزنگاری سزار برابر است با مجموعه حروف انگلیسی.

۱-۷-۱- سیستم‌های رمزنگاری

یک سیستم رمزنگاری، سیستمی است که عملیات رمزگذاری و رمزگشایی را انجام می‌دهد (شکل ۱-۱). عملیات رمزگذاری یا رمزنگاری می‌تواند توسط سخت‌افزار یا نرم‌افزار انجام شود.



شکل ۱-۱: یک سیستم رمزنگاری

تمرین: فرم ریاضی یک سیستم رمزنگاری یا دستگاه رمزنگاری به صورت یک پنج تایی نشان داده می‌شود. در این خصوص تحقیق کنید.

سیستم‌های رمزنگاری از نظر تعداد کلید به دو دسته متقارن و نامتقارن تقسیم می‌شوند که در ادامه شرح داده می‌شوند.

۱-۷-۱-۱- رمزنگاری متقارن^۲

در رمزنگاری متقارن (شکل ۱-۳) کلیدهای رمزنگاری و رمزگشایی یکسان هستند. اگر P متن ساده، C متن رمز شده، K کلید مشترک یا کلید سری، E تابع رمزگذاری و D تابع رمزگشایی باشد، فرم ریاضی عملیات رمزنگاری و رمزگشایی به صورت زیر است:

$$C=E(K,P)$$

$$P=D(K,C)$$

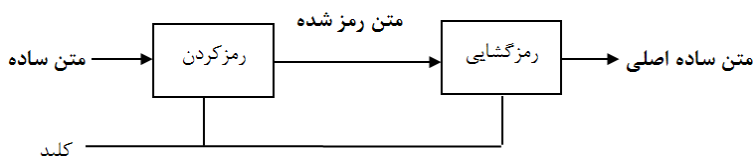
^۱Cryptosystem

^۲Symmetric

^۳Shared Key

^۴Secret Key

همانطور که از نام کلید مشترک (کلید سری) هم پیدا است، این کلید بین فرستنده و گیرنده پیام مشترک است و باید سری بماند.



شکل ۱-۲: رمزنگاری متقارن

۲-۱-۷-۱-۲ رمزنگاری نامتقارن^۱

در این روش (شکل ۱-۳) کلیدهای رمزنگاری و رمزگشایی متفاوت هستند. فرم ریاضی این روش به صورت زیر است:

$$C = E(K_E, P), P = D(K_D, C)$$

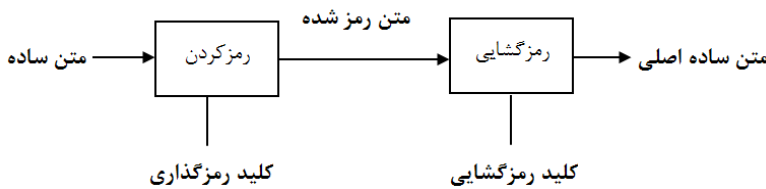
K_E و K_D به ترتیب کلید رمزگذاری و کلید رمزگشایی هستند. C ، E ، P و D نیز مشابه با روش متقارن هستند. یکی از مهم‌ترین روش‌های رمزنگاری نامتقارن، رمزنگاری با کلید عمومی^۲ است. در این روش هر فرد دارای یک کلید خصوصی^۳ و یک کلید عمومی^۴ است. کلید خصوصی را فقط مالک آن می‌داند، اما کلید عمومی را همه می‌دانند و در واقع مانند کلید مشترک در رمزنگاری متقارن، سری نیست. از کلید عمومی برای رمزگذاری و از کلید خصوصی برای رمزگشایی استفاده می‌شود.

در رمزنگاری متقارن، مشکل اصلی توزیع کلید است. یعنی فردی که رمزگذاری را انجام می‌دهد، چگونه کلید را به فردی که می‌خواهد رمزگشایی انجام دهد، برساند. آیا در هنگام انتقال کلید، کلید ربوده می‌شود؟ اما در روش رمزنگاری با کلید عمومی، این مشکل وجود ندارد.

^۱Asymmetric

^۲Public Key

^۳Private Key



شکل ۱-۳: رمزنگاری نامتقارن

۳-۷-۱- علم تحلیل رمز یا شکستن رمز

علم تحلیل رمز یا شکستن رمز، علمی است که به مطالعه روش‌ها و اصولی می‌پردازد که بر اساس آنها می‌توان بدون در اختیار داشتن کلید رمز (یا اطلاعات لازم برای رمزگشایی)، داده‌های رمزنگاری شده را از رمز خارج کرد یا کلید رمز را به دست آورد. علم شکستن رمز شامل مباحث زیر است:

- شکستن پیام: یعنی از متن رمز شده به متن ساده برسیم.
- شکستن کلید: یعنی کلید را پیدا کنیم.
- شکستن الگوریتم: یعنی از یک مشکل که در الگوریتم وجود دارد استفاده کنیم.

۴-۷-۱- عملیات مورد استفاده در یک سیستم رمزگذاری

عملیات مورد استفاده در یک سیستم رمزنگاری می‌تواند یکی از موارد ذیل باشد:

- عملیات ریاضی و منطقی، گسترش بیت‌ها (مثلاً تبدیل ۳۲ بیت به ۴۰ بیت) و تقسیم^۲ و ادغام^۳

^۱Cryptanalysis

^۲Split

^۳Merge

- **جایگزینی:**^۱ جایگزینی یعنی استفاده از یک جدول برای جایگزینی کاراکترهای متن ساده. به عنوان مثالی از جایگزینی می‌توان روش‌های رمزنگاری سزار و رمزنگاری ورنام را نام برد.
- **جایگشتی:**^۲ یعنی کاراکترهای متن ساده را جابجا کنیم. مزیت این روش‌ها سادگی است و ضعف آنها این است که قابل شکستن است. به عنوان نمونه‌ای از روش‌های جایگشتی می‌توان جایگشتی ستونی را نام برد.

۶-۷-۱- اصول اساسی رمزنگاری

۱- استحکام: هر الگوریتم رمزنگاری باید علیه حملات مختلف (نظیر حمله متن ساده معلوم، متن ساده انتخابی و متن رمز معلوم) مستحکم بوده و نتیجه تلاش رمز شکن ناموفق و مایوس کننده باشد. روش‌هایی وجود دارند که در مقابل برخی از حملات مقاوم نیستند اما می‌توانند در ترکیب با سایر روش‌ها مورد استفاده قرار بگیرند.

۲- تازگی:^۳ فرض کنید آلیس مشتری یک سیستم بانکی و باب کارمند بانک است. آلیس برای باب یک پیام رمز شده بسیار مهم مبتنی بر انتقال پول از حسابش به حساب دیگری ارسال می‌کند. فرض کنید شخص ثالثی این پیام را استراق سمع کرده و به دلیل استحکام بی نظیر الگوریتم رمزنگاری هرگز موفق به شکستن رمز نمی‌شود، ولی یک هفته بعد همان پیام را از طرف آلیس برای باب می‌فرستد و باب با رمزگشایی آن؛ عمل خواسته شده را انجام می‌دهد، غافل از اینکه این پیام تکراری و دروغین است. بنابراین رمزگشایی اطلاعات گرچه لازم است ولی هرگز کافی نیست. باید مکانیزم‌هایی در کنار فرایند رمزنگاری اتخاذ شود تا تازگی پیام به اثبات برسد و از حمله تکرار پیشگیری شود. در غیر این صورت امکان هرگونه اختلال و یا سوء استفاده وجود دارد.

^۱Substitution

^۲Permutation

^۳Freshness

برای اثبات تازگی پیام‌ها می‌توان برای هر پیام تاریخ و زمان صدور و مهلت اعتبار در نظر گرفت و یا هر پیام به همراه یک شناسه یکتا، رمز شده و ارسال گردد. بدین ترتیب از حمله تکرار جلوگیری خواهد شد. بنابراین در عمل ترکیبی از مهر زمان^۱ و شناسه پیام به کار می‌رود تا گیرنده بتواند تازگی پیام را اثبات کند.

۳- افزونگی^۲: فرض کنید استاد یک درس پیامی رمز شده حاوی نمره یک دانشجو برای بانک اطلاعاتی آموزش دانشگاه ارسال می‌کند. اگر فردی در بین راه یک بیت از پیام را تغییر دهد، یک پیام معتبر به یک پیام معتبر دیگر تبدیل می‌شود و در نتیجه نمره دانشجو تغییر خواهد کرد. بنابراین پیام‌های ارسالی باید دارای افزونگی باشند و این افزونگی باید به نحوی هوشمندانه در پیام‌ها درج شود تا هر تغییر در پیام، آنرا به پیامی غیر معتبر و قابل کشف تبدیل کند. در رمزنگاری برای رفع این مشکل از چکیده پیام^۳ استفاده می‌شود.

۸-۱- سؤالات تشریحی

۱- اصطلاحات زیر را توضیح دهید؟

الف- Confidentiality ب- Asymmetric Cryptosystem

۲- شش مورد از نیازمندی‌های امنیتی یک سیستم را نام برده و توضیح دهید.

۳- در هر یک از موارد زیر مشخص کنید کدامیک از سه اصل امنیت اطلاعات به چالش کشیده شده است؟

الف- جواد تمرین‌های مریم را کپی کرد.

ب- علی سیستم مهسا را از کار انداخت.

ج- فریدون مقدار موجودی حساب زهرا را از ۱۰۰ دلار به ۱۰۰۰ دلار تغییر داد.

د- داریوش امضای خودش را به جای امضای رضا گذاشت.

ه- بهرام یک دامنه با نام Yahoo.com ثبت کرد و با استفاده از آن جلوی سرویس Yahoo Buy را گرفت.

^۱TimeStamo

^۲Redundancy

^۳Message Digest

پاسخ:

- الف) سرقت اطلاعات است و باعث عدم محرمانگی می شود .
 ب) قابلیت دسترسی را دچار چالش کرده است.
 ج) صحت را مخدوش کرده است.
 د) چون داریوش امضای خودش را به جای امضای رضا قرار داده، پس جعل اطلاعات است و در نتیجه صحت را به چالش کشیده است و در ادامه نیز می تواند اطلاعات را سرقت کند و موجب عدم محرمانگی شود. ضمناً چون مهاجم امضای خودش را به جای شخص دیگری جا زده است ولی از دیدگاه سرور تأیید هویت شده است، حتی می تواند با ارسال بسته های زیاد موجب از کار افتادن سرویس ها شده و دسترسی پذیری را نیز به چالش بکشد. بنابراین در ادامه مهاجم می تواند هر سه اصل امنیت اطلاعات را دچار چالش می شود.

۹-۱- سئوالات چهارگزینه ای

- ۱- توانایی محافظت داده از تغییر یا خرابی با دسترسی غیر مجاز یا تصادفی چه نامیده می شود؟
 الف. قابلیت اعتماد ب. محرمانگی ج. جامعیت و صحت اطلاعات د. احراز هویت
 ۲- خرابی تجهیزاتی، بلاهای طبیعی، عکس العمل های کارمندان بداندیش و حملات هکرها نمونه هایی از هستند:
 الف. تهدیدها ب. آسیب پذیری ها ج. ریسک د. خرابی های سیستم
 ۳- کدام گزینه صحیح است؟
 الف- Authentication مکانیزمی است که بر اساس آن مشخص می شود که فرد یا موجودیتی که هویت آن احراز شده است، مجوز چه کارها و عملیاتی را دارد.
 ب- Accounting مکانیزمی است که مشخص می کند فرد یا موجودیتی که هویت آن احراز شده است، مجوز چه کارهایی را دارد.
 ج- Authentication مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می شود.
 د- Authorization اهمیت بیشتری از Authentication دارد.
 ۴ - نام دیگر IP Spoofing چیست؟
 الف- IP forgery ب- IP poisoning ج- IP Attack د- همه موارد

- ۵- برای جلوگیری از حمله تکرار از چه مکانیزمی استفاده می‌شود؟
 الف- چکیده پیام ب- مهر زمان و شناسه پیام ج- رمزنگاری د- همه موارد
- ۶- Arp spoofing از حملات لایه است.
 الف- شبکه ب- لینک ج- انتقال د- کاربرد
- ۷- حمله‌ای که در آن، حمله کننده اطلاعاتی از قبیل مبداء، مقصد و اندازه پیام را می‌بیند، چه نامیده می‌شود؟
 الف. افشاء پیام ب. بدل ج. تحلیل ترافیک د. انکار سرویس
- ۸- نمونه بارز عدم رعایت اصل کرکهف کدام الگوریتم است؟
 الف- RC4 ب- RSA ج- RC2 د- DES
- ۹- بهرام یک دامنه مشابه Yahoo com ثبت کرده و با استفاده از آن جلوی سرویس yahoo Bug را گرفت. به نظر شما کدام یک از سه اصل امنیت اطلاعات به چالش کشیده شده است؟
 الف- قابلیت دسترسی ب- صحت ج- محرمانگی د- همه موارد
- ۱۰- داریوش امضای خودش را به جای امضای رضا قرار داده است. به نظر شما کدام یک از اصول امنیت اطلاعات به چالش کشیده شده است؟
 الف- قابلیت دسترسی ب- محرمانگی ج- صحت د- همه موارد
- ۱۱- کدام اصل کرکهف به اصل اساسی آن مشهور است؟
 الف- اول ب- دوم ج- پنجم د- چهارم

پاسخنامه

الف	ب	ج	د	1
الف	ب	ج	د	2
الف	ب	ج	د	3
الف	ب	ج	د	4
الف	ب	ج	د	5
الف	ب	ج	د	6
الف	ب	ج	د	7
الف	ب	ج	د	8
الف	ب	ج	د	9
الف	ب	ج	د	10
الف	ب	ج	د	11