دانشگاه علم و صنعت ایران

دفتر برنامه‌ریزی درسی

مشخصات کلی برنامه و سرفصل دروس

دوره کارشناسی ارشد مهندسی فناوری اطلاعات

گرایش مهندسی مخابرات امن

گروه فنی مهندسی

معاونت آموزشی
دانشگاه علم و صنعت ایران
۱۳۸۸
دفتر برنامه‌ریزی درسی

مصوب نهمین جلسه شورای برنامه‌ریزی درسی دانشگاه مورخ ۱۳۸۱/۷/۱۶

معاونت آموزشی دانشگاه

بسم الله الرحمن الرحیم

برنامه آموزشی دوره کارشناسی ارشد مهندسی فنآوری اطلاعات

گرایش مخابرات امن

گروه: فنی و مهندسی　　کمیته تخصصی:

رشته: مهندسی فنآوری اطلاعات　　گرایش: مخابرات امن

دوره: کارشناسی ارشد　　کد رشته:

شورای برنامه ریزی درسی دانشگاه علم و صنعت ایران در نهمین جلسه مورخ ۸۱/۷/۱۶ بر اساس طرح دوره کارشناسی ارشد مهندسی فنآوری اطلاعات گرایش مخابرات امن که توسط مرکز فن آوری اطلاعات و دانشکده مهندسی برق تهیه و به تایید رسیده است، برنامه آموزشی این دوره را در سه فصل (مشخصات کلی، برنامه و سرفصل دروس) به شرح پیوست تصویب کرد و مقرر می‌دارد:

ماده ۱) برنامه آموزشی دوره کارشناسی ارشد مهندسی فنآوری اطلاعات (مخابرات امن) از تاریخ تصویب برای این دانشگاه می تواند اجرا شود.

ماده ۲) این برنامه از تاریخ　　برای دانشجویانی که از این تاریخ به بعد وارد دانشگاه می‌شوند لازم الاجرا است.

ماده ۳) مشخصات کلی، برنامه درسی و سرفصل دروس دوره کارشناسی ارشد مهندسی فنآوری اطلاعات (مخابرات امن) با سه فصل مشخصات کلی، برنامه و سرفصل دروس برای اجرا به دفتر تحصیلات تکمیلی دانشگاه ابلاغ می شود.

ابوالفضل واحدی
رئیس شورای برنامه ریزی درسی دانشگاه

محسن سریانی
دبیر شورای برنامه ریزی درسی

معاونت آموزشی
دفتر برنامه ریزی درسی

دوره آموزشی کارشناسی ارشد

مخابرات امن

یا

Secure

Communcations

بسم الله الرحمن الرحیم

فصل اول

مشخصات دوره کارشناسی ارشد مخابرات امن

۱- تعریف و هدف :

دوره کارشناسی ارشد مخابرات امن مرکب از دروس نظری و کار تحقیقاتی در زمینه‌های مخابرات امن است. هدف از ایجاد این دوره ، تربیت دانش آموختگانی است که با فعالیت در زمینه‌های برنامه‌ریزی، مدیریت یا بهره‌برداری، طراحی و پیاده کردن پروژه‌های تولیدی، مخابراتی، شبکه‌های کامپیوتری و حفاظت آنها بتواند بنحو موثری پاسخگوی نیازها و کمبودهای کشور باشند. فارغ‌التحصیلان این دوره می‌توانند علاوه بر کار آموزشی و یا پژوهشی در دانشگاهها در سطح مراکز تحقیقاتی و یا وزارتخانه‌ها و سازمانها مسئول اجرای طرحهای صنعتی بویژه آنهایی که با امنیت و حفاظت داده‌ها، سیستمها و مدیریت آنها که در سطح وسیع با مسائل تکنولوژی اطلاعات روبرو هستند، فعالیت نمایند.

۲- طول دوره و شکل نظام :

حداقل طول این دوره ۴ نیمسال است، بدین معنی که دانشجویانی که ناچار به گرفتن دروس جبرانی نیستند، چنانچه کار درسی و تحقیقاتی خود را به نحو مطلوبی انجام دهند، می‌توانند دوره را در ۴ نیمسال به پایان برسانند، نظام آموزشی آن واحدی است و هر واحد نظری ۱۶ ساعت است.

۳- تعداد واحدهای درسی :

دانشجو برای دوره کارشناسی ارشد مخابرات امن باید حداقل ۳۲ واحد درسی و تحقیقاتی بشرح زیر با موفقیت بگذراند.

اصلی و تخصصی ۲۴ واحد

سمینار ی	۲ واحد
پروژه تحقیق	۶ واحد
جمع	۳۲ واحد

علاوه بر موارد فوق، هر دانشجوی این دوره که قبلاً در دوره کارشناسی یا لیسانس، دروس جبرانی نگذرانده باشد، باید با موفقیت آنها را بگذراند از دروس جبرانی واحدی به دانشجو تعلق نمیگیرد.

۱-۳- دروس جبرانی :

دروس جبرانی از دوره کارشناسی تکنولوژی اطلاعات، با نظر کمیته تحصیلات تکمیلی، به عنوان دروس جبرانی دوره محسوب میشوند :

۴- شرایط گزینش دانشجو :

۱-۴- دوره‌های کارشناسی پیشنیاز : این دوره در اساس برای فارغ‌التحصیلان کارشناسی " تکنولوژی اطلاعات " برنامه‌ریزی شده است، لیکن فارغ‌التحصیلان دیگر دوره‌های کارشناسی برق، کامپیوتر، علوم کامپیوتر و ریاضیات کاربردی میتوانند در آن شرکت نمایند، مشروط بر آنکه دروس " جبرانی " ، تعیین شده را با موفقیت بگذرانند.

۲-۴- آزمون ورودی : آزمون ورودی بطور کتبی از دروس پایه و اصلی تکنولوژی اطلاعات بعمل می‌آید، لیکن بنحوی تنظیم میگردد که کسانیکه دروس تخصصی تکنولوژی اطلاعات را نگذرانده‌اند اما پایه قوی در یکی دیگر از دوره‌های کارشناسی فوق‌الذکر را دارند، امکان موفقیت در آنرا داشته باشند.

۳-۴- دانستن یک زبان خارجی علمی : تسلط به یک زبان خارجی علمی بنحوی که دانشجو بتواند بسهولت از متون علمی تکنولوژی اطلاعات آن زبان استفاده نماید ضروری است.

۴-۴- مصاحبه تخصصی : گروه آموزشی ممکن است در صورت تشخیص با کسانیکه در آزمون ورودی موفق شده‌اند، در زمینه‌های تخصصی، مصاحبه شفاهی بعمل آورد.

فصل دوم

بـــرنـامـــه

برنامه‌های آموزشی و پژوهشی :

۱- دروس اصلی : هر دانشجو باید حداقل سه درس (۹واحد) از مجموعه زیر را بگذراند :

شماره	نام درس	واحد
۱	شبکه های مخابره داده ها	۳
۲	اصول رمزنگاری	۳
۳	پردازش سیگنال دیجیتالی	۳
۴	ریاضیات پیشرفته (در زمینه امنیت و رمزنگاری)	۳
۵	شبکه‌های کامپیوتری پیشرفته	۳
۶	مخابرات سیار	۳
۷	مبانی امنیت اطلاعات	۳

تبصره ۱: سه درس اجباری اخذ نشده را میتوان به عنوان دروس اختیاری انتخاب نمود.

۲- دروس تخصصی : دانشجو باقیمانده واحدهای درسی خود را، بـا موافقـت اسـتاد راهنمـا و کمیته تحصیلات تکمیلی، از لیست دروس تخصصی اختیاری گزینش و حداکـثر تـا دو درس از دروس اصلی و تخصصی اختیاری سایر گرایش‌های کارشناسی و کارشناسی ارشد تکنولوژی اطلاعـات و دروس تخصصی کارشناسی و کارشناسی ارشد سایر رشته‌ها را میتواند اخذ نماید.

۳- سمینار مخابرات امن :

سمینار مخابرات امن شامل قسمتهای زیر می‌باشد :

معرفی فعالیتـهای جـاری، مشـکلات و مسـائل کشـور در زمینـه امنیـت و حفـاظت، معرفـی زمینه‌های تحقیقاتی که دانشجویان ممکن است پروژه خود را از میان آنها برگزینند.

تهیه یک گزارش توسط هر دانشجو و ارائه آن.

دروس تخصصی اختیاری مخابرات امن

شماره	نام درس	واحد
۱	طیف گسترده	۳
۲	کد کننده‌های صوتی	۳
۳	سیستم عامل پیشرفته	۳
۴	امنیت پایگاه داده‌ها	۳
۵	سیستم های ارتباطی امن	۳
۶	دفاع و جنگ الکترونی	۳
۷	موضوعات پیشرفته در امنیت شبکه‌های کامپیوتری	۳
۸	تکنولوژی اینترنت	۳
۹	برنامه‌نویسی در محیط یونیکس	۳
۱۰	مدیریت سیستمهای امن	۳
۱۱	سیستمهای هوشمند	۳
۱۲	تجزیه و تحلیل الگوریتم‌ها	۳
۱۳	پایگاه داده پیشرفته	۳
۱۴	امنیت شبکه های کامپیوتری	۳
۱۵	سیستم های کامپیوتری امن	۳
۱۶	پروتکلهای امنیتی	۳
۱۷	تئوری اطلاعات و کدینگ	۳
۱۸	طراحی و تجزیه و تحلیل سیستمها	۳
۱۹	سیستمهای کامپیوتری توزیع شده	۳

شبکه های مخابره داده ها

تعداد واحد: ۳ نوع واحد: نظری ساعت درس: ۴۸ ساعت

سرفصل دروس:

مخابرات داده ای نقطه به نقطه: مخابرات داده ای آسنکرون و سنکرون – مدم ها – مولتی پلکس زمان- مولتی پلکس فرکانس- متمرکز کننده ها اطلاعات قراردادی و انواع آن – کدهای تشخیص یا تصحیح خطا روش انتقال مجدد خبر برای کنترل خطا.

شبکه های مخابرات داده ای: سوئیچینگ خط، سوئیچینگ پیام و سوئیچینگ بسته خبر نمونه هائی از شبکه های سوئیچینگ پیام و بسته خبر- اصول سوئیچینگ دتا- کاربرد تئوری اطلاعات ، تئوری صفها و تئوری بهینه سازی خطی و غیرخطی در مطالعه مسائل مربوط به : اطلاعات قراردادی خط و شبکه تمرکز ترافیک در گره ها محاسبه بهینه ظرفیت خطوط و حافظه گره ها- روشهای مسیریابی پویا و ایستا کنترل ترافیک و پیشگیری از راه بندان مدیریت متمرکز و گسترده در شبکه .

مروری بر استانداردهای *CCITT* – بررسی نمونه ای از مسائل مخابرات داده ای در کشور

1. *Schwartz, "Computer Communication Network Design & Analysis"*
2. *Davis & Barber, " Communication Networks For C Computers"*
3. *Martin J. " Teleprocessing Network Organization"*
4. *Kleinrock, L., "communication Nets, Stochastic Massage Flow And Delay"*

رمزنگاری

تعداد واحد : ۲ نوع واحد : نظری تعداد ساعت : ۴۸

سر فصل مطالب:

۱- مقدمه (نیاز به سرویس های امنیتی در سیستم های کامپیوتری و ارتباطی و مفاهیم پایه معماشناسی)

۲- پیش زمینه های لازم (تئوری اعداد – تئوری اطلاعات – تئوری پیچیدگی)

۳- معما شناسی کلاسیک (سیستم های رمز تک الفبائی جانشینی و جایگشتی و تحلیل آنها- سیستم های رمز چند الفبائی و تحلیل آنها)

۴- سیستم های رمزنگاری مدرن (سیستم های رمزنگاری دنباله ای و قطعه ای، سیستم های رمزنگاری متقارن و نامتقارن، معرفی *DES* و ویژگی های آن ، معرفی *AES*)

۵- مقدمه ای بر تحلیل خطی و تحلیل تفاضلی، تحلیل خطی و تحلیل تفاضلی *DES*

۶- رمزنگاری با کلید عمومی (توصیف الگوریتمهای با کلید عمومی *KNAPSACK* ، دیفی هلمن، *RSA*، رمز ویلیامز، *RC5*، رمزنگاری منحنی بیضوی و تحلیل آنها)

۷- تصدیق اصالت و صحت داده ها (مفاهیم پایه طرح تصدیق اصالت فیات- شامیر ، الجمال،.....- مسئله زندانبان و کانال نهان- طرحهای کانال نهان – توابع *HASH, MAC* و تحلیل آنها و پارادوکس روز تولد)

۸- امضای رقمی(انواع پروتکل های امن- مفاهیم پایه امضاء رقمی- طرحهای امضای رقمی ساده- طرح رابین – طرح ماتیاس – امضای *RSA* و انواع آن ونقاط ضعف- طرح امضای *DSS*)

۹- تبادل کلید و مدیریت (پروتکل های توزیع کلید بر سیستم رمز متقارن و نامتقارن – تولید کلید واعداد *random* – مدیریت کلید ومدول های امن و کلید گذاری چند لایه – طرحهای *Key escrow* – دفترچه راهنمای کلیدعمومی – گواهی و قبولی گواهی – مدیریت گواهی ها- *PKI*)

1- B.Schneier Applied Cryptography : Protocols, Algorithms and Source Code in C, John – Wiley & Sons Inc., 1996.

2- J.Seberry and J. Pieprzyk, Cryptography: An Introduction to Coputer Security, Perntice-Hall,1992.

3- C.Meyer, S.Metyas, Cryptography: A New Dimension in Computer Data Security, John-Wiley & Sons Inc. 1982.

4- A .Menezes, Elliptic Curve Public Key Cryptosystem , Kluwer Academic Publishers

پردازش سیگنالهای دیجیتال

تعداد واحد: ۳ نوع واحد: نظری ساعت درس : ۴۸

سر فصل مطالب:

مقدمه، آنالیز حوزه زمان آنالیز حوزه فرکانس (آنالیز فوریه)، آنالیز حوزه فرکانس (تبدیل Z) ، تبدیل گسسته فوریه وتبدیل سریع فوریه، طراحی فیلترهای رقمی غیر برگشتی، طراحی فیلترهای رقمی برگشتی، آنالیز طیف و تخمین طیف قدرت، فیلتر کردن به کمک کانولوشن سریع، آنالیز هوموفیک، تبدیل هیلبرت، آنالیز پیشگوئی خطی و ساختارهای نردبانی، پردازش سیگنالهای رقمی دو بعدی.

منابع:

1- Proakis,J.G & Manolokis, D.G., Digital Signal Processing Prentice-Hall,1996.
2. Oppenheim , A.V. & Schafer, R.W. Discrete-Time Signal Processing , Prentice-Hall, 1989.
3. Lynn, P.A.& Fuerst, W., Digital Signal Processing With Computer Applications, Wiley,1994.

ریاضی پیشرفته:

تعداد واحد: ۳ نوع درس : نظری تعداد ساعت ۴۸

محتوای درسی :

۱- طبقه بندی مسائل از دید محاسباتی به

الف – مسائل خوش خیم *(well- Posed prob)*

ب- : مسائل بد خیم *(Ill- Posed Problems)*

ج- مسائل خوش وضع *(Well Conditioned //)*

د: مسائل بد وضع *(Ill Canditioned //)*

روشهای محاسبات کار آمد ماتریس در داده های تصادفی ، سفید کردن و ابلاغ تجزیه ماتریس *Covariance* فرآیندهای تصادفی و الگوریتمهای مربوط به ماتریسهای زیر

L, U, D, Tridiagonal Sparse, dense, diagonally, dominant matrix, Hermitian matrix, Hessenberg

توابع متعامد و ارتباط آنها با نظریه کد *(Coding & Decoding)*

توابع متعامد و پیوسته و کاربرد آنها در *Vocoder* و *Encryption* و *Image* توابع پیوسته ثابت، توابع متعامد *Wavelet* و کاربرد آن

حل مسائل غیر خطی در رمز نگاری ، نظریه آشوب*(chaos)* و رمز نگاری تعریف آشوب و شرایط ایجاد پدیده آشوب، سیستمهای آشوبگونه بیان چند الگوریتم رمزنگاری بر اساس آشوب

ریاضیات پیشرفته در مهندسی کامپیوتر

تعداد واحد: ۳ نوع واحد: نظری ساعت درس: ۴۸ ساعت

سرفصل درس

- مروری بر معادلات خطی، فضاهای برداری، تبدیل های خطی، نمایش تبدیلات خطی توسط ماتریس.
- سری فوریه و انتگرال فوریه، توابع متعامد ، بسط توابع بر حسب توابع متعامد.
- فرآیندهای تصادفی و کاربرد آنها ، تئوری گراف و کاربرد آنها.
- توزیع مسئله صف، ساختار فرایند، صف، زمینه های کاربرد نظریه صف، سیستمهای صف با پارامترهای غیر احتمالی *(Deterministic)* ، فرآیند پواسن و توزیع نمائی.
- خصوصیت مارکوفی توزیع نمائی، سیستم *M/M/1* ، رابطه بین طول صف، زمان و آهنگ ورود مشتری، روابط لیتل *(Little)* سیستمهای صف چند سرویس *M/M/K*، *M/M/* ∞، فرآیند تولید و مرگ *(Birth- Death)* سیستمهای صف چند سرویس دهنده، سیستم صف *M/M/C* و سیستمهای صف *M/M/C/K* و *M/M/C/C* و زنجیره های مارکوف روابط *Chapman- Kolaogorov*، مدلهای صف با توزیع ارلانگ *(Erlang)*.

شبکه های کامپیوتری پیشرفته

تعداد : ۳ نوع واحد: نظری پیش نیاز: شبکه های کامپیوتری

سرفصل مطالب:

این درس شامل موضوعات جدید و مطرح روز در زمینه شبکه های کامپیوتری میباشد. مطالب درس شامل مباحث ۱ الی ۴ و مباحث انتخابی از مبحث ۵ به بعد میباشد.

۱- اصول *B-ISDN* و تکنولوژیهای جایگزین نظیر *IPng, ATM*

۲- روشهای انتقال اطلاعات نظیر *Cell Switching,Packet Switching, Circuit Switching* و تکنولوژیهای پیشتیبان آنها همچون *IP Switching ,MPLS, MPOA* اصول کار و ارزیابی آنها،

۳- مسیر دهی *(routing)* ، مسیر دهی با هدف کنترل کیفیت خدمات *(QoS routing)* ، مسیر دهی برای انتقال موازی *(multicast routing)*

۴- روشهای کنترل کیفیت خدمات *(Qos)* : تعریف خدمات شبکه *(Controlled bitrate, CBR,ABR)* روشهای مدیریت و کنترل ترافیک و ارزیابی آنها، روشهای زمانبندی *(Scheduling)* و تاثیر آنها بر کیفیت خدمات ، روشهای تخصیص منابع شبکه *(Resource Sharing)*

۵- مدل کردن ترافیک نظیر مدلهای *Self Similar,Fluid Flow, MMPP* و الگوریتم های متناظر جهت کنترل برقراری ارتباط *(CAC)*

۶- ساختمان واصول کار سوئیچها در *B-ISDN* ، سوئیچهای مبتنی بر *Banian Networks* ، سوئیچهای مبتنی بر حافظه ، مسائل مربوط به بافرهای ورودی – خروجی

۷- پروتکل *TCP* و فرمهای جدید آن، طراحی پارامترها و ارزیابی عملکرد آن بااستفاده از تکنولوژیهای مختلف در لایه های زیرین

۸- شبکه های نوری ، تکنولوژی *SONET* و مسائل مربوط به *WDM*

۹- شبکه های بی سیم، طراحی اپتیم توپولوژی شبکه، تعیین ظرفیت خطوط در یک محیط چند خدماتی، طراحی منطقی شبکه *VP(Virtual Path)*

۱۱- امنیت شبکه *(Network Security)* شناسایی کاربران، کنترل درستی اطلاعات

۱۲- مدیریت و کنترل شبکه، شبکه های هوشمند و موضوعات مطرح دیگر

مراجع :

S.Keshav, An Engineering Approach to Computer Networking. Addison-Wesley.

2- M.Schwartz, Broadband Integrated Networks, Prentice- Hall PTR, 1996.
3- A.Tanenbaum. Computer Networks. Prentice Hall,1996.
4- T.G. Robertazzi, Performance Evaluation of High Speed Switching Fabrics and Networks.
5- J-P. Leduc, Digital Moving Pictures: Coding and Tronsmission on ATM Networks. Amsterdam.
6- M.E.Steenstrup, Routing in Communication Networks,Prentice-Hall Int..., 1995.
7- U.Black , ATM, Vol. III, Prentice-Hall,1998.
8- A.Kershenbaum, Telecommunication Network Desing Algorithms, McGraw-Hill, 1993.
9- ACM/EEE Transaciton on Networking.
10- IEEE Journal of Selected Areas in Communication.
11- Proceedings of IEEE INFOCOM (a conference on Comuter Communication).
12- Procedings of IEEE ICC (International Conference on Communication.

مخابرات سیار

تعداد واحد : ۳ نوع واحد : نظری تعداد ساعت : ۴۸ ساعت

سر فصل مطالب:

- اصول و ویژگیهای مخابرات سیار سلولی و مخابرات انفرادی شامل تاریخچه مخابرات سیا، روند رشد و تکامل و دورنمای آن، ساختار یک سیستم سلولی و پارامترهای مربوطه، روشهای ارسال و مالتیپلکس، بررسی ظرفیت سیستمهای سلولی و میکرو سلولی، بررسی مقایسه ای سیستمهای مختلف موجود و پیشنهادی مخابرات سیار در جهان.
- انتشار امواج در محیطهای سیار سلولی شامل بررسی مدلهای مربوط به پیش بینی افت سیگنال در حد وسیع و تعیین نواحی پوشش، بررسی فیدینگ سریع شامل خواص پوش و فاز سیگنال، بررسی انتشار امواج دیجیتال در محیطهای فیدینگ چند مسیره و مدلهای مربوط، اثر فیدینگ در کاهش سرعت ارسال و کیفیت.
- بررسی روشهای مختلف دایورسیتی از جمله دایورسیتی فضائی فرکانسی، زمانی، پلاریزاسیون و زاویه دریافت، روشهای ادغام شاخه های دایورسیتی، مقایسه ادغام قبل و بعد از آشکار سازی، بررسی مقایسه ای سیستمهای دایورسیتی در بهبود عملکرد سیستمهای مخابرات سیار.
- سیستم های *GSM*، امنیت در این سیستمها، تهدیدات و راه حل ها
- امنیت در سیستم های *GSM*

مراجع :

1. *W.C. Jakes, Jr., Microwave Mobile Communications, John Wiley, 1974.*
2. *W.C. Y. Lee, Mobile Communications Engineering, McGraw-Hill Book Company, 1982.*
3. *R.V. Sutton, Secure Communications Applications and Managememt, John-Wiley8 Sons Inc. 2002.*
4. *D. J. Torrieri, Princles of Secure Communication Systems, Artech House, 1992.*

مبانی امنیت اطلاعات

تعداد واحد : ۲ نوع واحد: تعداد ساعت : ۴۸

اهداف فصل : هدف از این فصل تفهیم موضوعاتی است که در تکنولوژی امنیت اطلاعات مطرح می‌شود، بدینصورت که خلاصه نسبتاً جامعی (فراگیری) در مورد موضوعات این زمینه و نیز ارتباط بین زمینه ها را به دانشجویان انتقال دهد. بدین منظور در این درس مفاهیم خمله به سیستمهای اطلاعاتی و چگونگی دفاع در مقابل آن مطرح می شود.

سر فصل مطالب:

۱- تعریف امنیت اطلاعات و فرآیند بودن امنیت
۲- تهدیدات به سیستم های کامپیوتری، درخت های تهدید، طبقه بندی حملات، برنامه های مخرب کامپیوتری ویروس و اسب تروا، روش های متداول حمله.
۳- سرویس های امنیتی
۴- برچسب امنیتی، لاتیس برچسب های امنیتی، رویه امنیتی، مدل افشای اطلاعات *BLP* و بحث و تحلیل آن
۵- امنیت عدم استنتاج و عدم تداخل، مدل صحت *Biba*، مدل صحت کلارک- ویلسون، ممانعت از سرویس
۶- اقدامات مقابله کننده محافظ ایمنی، بازرسی، تشخیص نفوذی، تصدیق اصالت و تشخیص هویت، کلمات عبور، رمزنگاری و مدیریت کلید، کنترل دستیابی، کانال های نهانی، نقش ها و امتیازات، هسته عامل امنیتی
۷- امنیت شبکه
۸- امنیت پایگاه داده ها
۹- ارزیابی امنیتی سیستم ها

مراجع :

1. Edward Amoroso, Fundamentals of Computer Security Technology, Prentic-Hall, 1994.
2. Eric Mainwald, Network Security : A Beginners Guide, Osborne/McGraw-Hill, 2002.
Charles Pfleeger, Security in Computing, Prentice-Hill, 1997.

3. *Marshall Abrams, et. Al. (eds.) Information Securit : An Inregrated Collection of Essays, IEEE Compyter Society Press, 1995.*
4. *Peter Denning, Computers Under Attack, Addison-Wesley, 1990.*

طیف گسترده

تعداد واحد : ۳ نوع واحد : نظری تعداد ساعت : ۴۸ ساعت

سر فصل مطالب:

طیف گسترده به نوعی مدولاسیون میشود که پهنای طیف سیگنال ارسالی خیلی بیشتر از پهنای باند مورد نیاز برای ارسال سیگنال است و همچنین برای دمدولاسیون باید از همبستگی بین سیگنال دریافتی و نسخه ای از سیگنال مورد استفاده در فرستنده برای گستراندن طیف استفاده شود. تئوری طیف گسترده طی تحقیقاتی که در زمان جنگ جهانی دوم برای تامین مخابرات امن انجام می شد گسترش یافت و کاربردهای آن در مخابرات از آن زمان مورد توجه بود. با این همه طیف گسترده زمانی مورد توجه بسیار زیاد قرار گرفت که مخابرات سلولی با کمبود ظرفیت مواجه شد. هدف از ارائه این درس تامین تئوری لازم برای طیف گسترده و ایجاد زمینه لازم برای مطالعه و تحقیق بیشتر و یا طراحی سیستمهای طیف گسترده میباشد.

مباحث درس :

۱. تئوری طیف گسترده و انواع آن (دنباله مستقیم و جهش فرکانسی و جهش زمانی و ترکیبات آنها)
۲. کاربردهای طیف گسترده
۳. دنباله های شبه تصادفی
۴. مخابرات در کانالهای با فیدینگ
۵. ردیابی و ردگیری دنباله شبه تصادفی
۶. سیستمهای مخابراتی دسترسی چندگانه با تقسیم کد
۷. آشکار سازی چند-کاربره
۸. معرفی استانداردهای *IS-95* , *W-COMA* و *UMTS-2000*

مراجع :

1. *Introduction to Spread Spectrum Communications by : Peterson, Ziemer and Borth 1995 Prentice Hall*
2. *Spreced Spectrum Communication (V.1,2 and 3) by : Simon, Omura, Scholtz and Levitt 1985 Computer Sciense Press.*
3. *Principles of Secure Communication System by : D.J. Torrieri 1985 Artech House.*

4. *spruced Spectrum Communicatios Handbook by : Simon, Omura and Scholtz 1994 Mc. Grow Hill*

پایگاه داده پیشرفته

تعداد واحد: ۳ ساعت درس : ۴۸ ساعت

نوع واحد: نظری

پیشنیاز:طراحی و پیاده سازی پایگاه داده ها

سر فصل دروس:

ترمیم- یکپارچگی – همزمانی – حفاظت- مدلسازی – نرمال سازی – داده ها- حفاظت داده ها- مدل رابطه ای گسترش یافته *RM/T* – پایگاه داده توزیع شده- ماشینهای پایگاه داده – زبانهای برنامه سازی در پایگاه داده ها شامل زبانهای نسل چهارم، شیئی گرا، استنتاجی و تابعی – پروژه

مراجع:

1- An Introduction to Data Base System, Volume II,
C.J. Date C.J. White, Addison Wesley, 1990
2- Distributed Database Systems,
D.Bell and J.Grimson A ddisonWesley,1992
3- Advances in Database Programming Languages , edited by F. Bancilhon, P. Buneman, ACM Press Books, 1990

امنیت پایگاه داده ها

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸ ساعت

سر فصل مطالب:

۱- مقدمه ای بر پایگاه داده ها (مفاهیم یک پایگاه داده، اجزاء یک پایگاه داده ، پرسش *(query)* مزایای استفاده)

۲- خواسته های امنیتی (یکپارچگی پایگاه داده و صحت المان ها، قابلیت بازرسی ، کنترل دستیابی، تصدیق اصالت کاربر، دسترسی پذیری ، قابلیت اعتماد *(reliability)*

۳- اطلاعات حساس (عوامل حساس سازی، تصمیم های مختلف درمورد دسترسی، دسترس پذیری داده ها، اطمینان از اصالت ، انواع افشاء شدن، امنیت و دقت)

۴- مسئله استنتاج

۵- کنترل دستیابی تفویضی در *DBMS* ها

۶- کنتر ل دستیابی دستوری

۷- کانال های نهان

۸- مدل رابطه ای امن چندسطحی

۹- معماری *DBMS* امن چند سطحی

۱۰- محصولات تجاری و نمونه های اولیه تحقیقاتی

۱۱- ارزیابی و تعبیر پایگاه داده مطمئن

۱۲- مکانیزم ها و مدل های صحت

۱۳- امنیت در پایگاه داده آماری

۱۴- بازرسی در پایگاه داده رابطه ای

۱۵- امنیت *Oracle9i*

۱۶- تشخیص نفوذ و *Data Mining*

۱۷- بقاء پایگاه داده ها در نبردهای اطلاعاتی

۱۸- خط مشی های اعمال کنترل دستیابی چندگانه

مراجع

1. *M. Abrams, S. Jajodia, H, Podell (eds.) Information Security : An Integrated Collection of Essays, IEEE Computer Society Press, 1995.*
2. *E. Fernandez, et al., Database Security and Integrity, Addison-Wesley, 1981.*
3. *C. Date, An Introduction to Data ase Systems, Vol.1, and Vol.2, Addison-WESLEY.*
4. *D. Denning, Cryptography and Data Security, Addison-Wesley, 1982.*
5. *C. Pfleeger, Security in Computing, Prentice-Hall, 1997.*
6. *D. Denning, A Review of Research on Statistical Data Base Secrity, Foundations of Secure Computation, Academic Press, 1978.*
7. *D. Denning, Views for Multi-level Data base Security. IEEE Trans. Software Eng., 1987.*
8. *P. Ammann. S. Jojdia, C. McCollcom, B. Blaustein, Surviving information Warfare attacks on Databases, Proc. IEEE Symposium on Research in Security and Privacy, 1997.*
9. *Oracle White Paper : Oracle 9i Database Security for e Business.*
10. *N. adam and J. Wortmann, Security- control methods for statistical databases, ACM Computing Surveys, Vol.21, No. 4, 1989.*
11. *D. Clark, D. Wilson, a comparison of Commercial and Military Computer Security Policies, Proceedings of the IEEE Symposium on Security and Privacy and Privacy, 1987.*
12. *M. Theriault and A. Near man, Oracle Security Handbook, Osborne/McGraw-Hill. 2001.*

سیستم های ارتباطی امن

تعداد واحد : ۳ نوع واحد: نظری ساعت درس: ۴۸

سرفصل مطالب:

۱- تهدیدات و راه حل ها(تهدیدات فنی به امنیت ارتباطات ، تداخل *jamming*، تشخیص توسط دشمن، استخراج اطلاعات از روی شکل موج، تصدیق اصالت، صحت، دسترس پذیری ، مقابله باتهدیدات تشعشعی)

۲- امنیت صوت در کاربردهای نظامی(رمز نگاری آنالوگ، برای ارتباطات رادیوئی *HF* برد بلند دریائی، واحد رمزنگاری دیجیتال درعملیات زمینی ، مدول رمز نگاری رادیوئی)

۳- امنیت تلفن(تهدیدات خاص برای تلفن، تکنولوژی های شبکه راه حل های امنیت تلفن، مدیریت دستیابی و کلید، پیاده سازی شبکه، توزیع کلید)

۴- سیستم های *GSM* امن (معماری پایه*GSM* ویژگی های امنیتی *GSM* استاندارد، جنبه های امنیت خاص برای کاربران *GSM*، مدیریت کلید و ابزارها، عملیات وامنیت *GPRS*)

۵- امنیت در شبکه های رادیوئی *VHF/UHF* خصوصی (کاربری و ویژگیها، تهدیدات ،اقدامات مقابله، معماری وطراحی شبکه ارتباطی، اجزاء سخت افزاری ، مدیریت کلید، بعضی ویژگیهای امنیتی خاص مانند حذف کلید از دور دست، انسداد از راه دور، و ردگیری ساکت)

۶- اقدامات حفاظت الکترونیک- خیزش فرکانس *Hopping frequency*(*EPM.EA,ESM*) کاربردهاینظامی، معماری شبکه و مراحل ماموریت، مشخصه های فرکانسی شبکه های خیزش *COMSEC* و *TRANSEC* ، ابزارها ومدیریت داده ها و کلید، اجزاء سخت افزاری)

۷- رمز نگاری *Link* (تکنولوژی پایه رمزنگاری ، پارامترهای رمزنگاری، مدیریت شبکه، امنیت *Link* نظامی)

۸- سیستم های امن(شبکه های فکسیمیلی امن، امنیت*PC*، امنیت *E-mail* ، شبکه اختصاصی مجازی امن، انتقال داده های نظامی)

مراجع:

1- R.V. Sutton, Secure Communications: Applications and Management, John-Wiley & Sons Inc,2002.

2- D.J.Torrieri, Principles of Secure Communication Systems, Artech House, 1992.

3. N.F.Jonson, Z.Duric and S. Jajodia, Information Hiding: Steganography and Watermarking – Attacks and Countermeasures, Kluwer Academic Publishers,2000.

4- I .Cox M. Miller , and Morgan Kaufman Publishers2002.

5- M.Wu, and B. Liu, Multi media Data Springer-Verlag,2002

امنیت شبکه های کامپیوتری

تعداد واحد : ۳ نوع واحد: نظری تعداد ساعت : ۴۸

سر فصل مطالب

۱- مقدمه ای بر شبکه سازی و امنیت کامپیوتر

۲- تهدیدات امنیتی، حملات مسیردهی، ردگیری

۳- محرمانگی ترافیک

۴- مروری بر رمزنگاری ، معماریهای امنیتی *PKI* ، سرویس دایر کتوری *X.509 , KERBEROS*

۵- امنیت لایه دسترسی به شبکه، سرویس های امنیتی *ATM* ، پروتکل های *EAP,CHAP,PAP,PPP -ECP* و پروتکل *L2TP*

۶ – امنیت لایه اینترنت، فیلترهای بسته، *VPN,IPSec,NAT*، فایروال و اصول آن، سیستمهای مطمئن

۷- امنیت لایه حمل، *ISAKMP, SASL V5*

۸- امنیت لایه کاربرد، فیلترهای محتوی، مجوز دادن و کنترل دستیابی، شبکه ارتباطی و تهدیدات امنیتی و برنامه مخرب (ویروس، کرم و اسب تروا)، امنیت نامه الکترونیک *S/MIME,PGP,e-mail* ، امنیت *Web,SET,SSL*، امنیت *Java* امنیت مدیریت شبکه و *SNMP*

۹- نفوزگرها، نفوذ، حملات ممانعت از سرویس ، سیستم های تشخیص نفوذ

۱۰- مونیتورینگ و *RMON*

مراجع:

1- William Stallings, Network Security Essentials: Application and Standards, Prentice-Hall,2000.

2- S.Ghosh, Preinciples of Secure Network Systems Desing, Springer- Verlag, 2002.

3- Eric Nanwald, Network Security : A Beginner's Guide, Osborne/McGraw-Hill, 2002.

4- William Stallings, Cryptography and Network Security: Principles and Practice, Prentice-Hall, 1998.

5- E.Fisch, G. White, Secure Computer and Networks. CRC Press, 2000.

6- N. Doraswamy, D.Harkins, IP Sec: The New Security Standard for the internet, interanets, and Virtual Private Network, Prentice-Hall, 1999.

7- W. Cheswick, Steven M. Bellovin, Firewalls and Internet Security, Addison- Wesley, 1994.8- D.Marchette, Computer Intrusion Detection and Network Monitoring, Springer- Verlag,2001.

8- Vesna Hessler, Communication Security, Part2 of Security Fundamentals for E-Commerce, Artech House Publishers.

تجزیه و تحلیل الگوریتم های پیشرفته

تعداد واحد : ۳ نوع واحد: نظری تعداد ساعت : ۴۸

سر فصل مطالب:

مقدمات، پیچیدگی الگوریتم ها. مسایل *NP-Complete* ، مسایل ذاتا مشکل *(Intractable)* ، نظریه ی *NP-Completeness* ، رابطه دسته مسایل *NP-Complete, NP-hard,NP,P* ، قضیه ی کوک ، روشهای اثبات *NP-Complete* بودن یک مسئله، مسایل اصلی *3D-Matching, Vertex-Cover, Clique, 3-Sat,* ، دور همیلتونی، فروشنده ی دوره گرد ، افراز.

الگوریتم های شبکه و کاربردهای آن ، شبکه ی مشاوره *(Network Flow)* (روش *Ford-Fulkerson)* الگوریتم های *Lift-to- Front , Preflow-Push)* گونه های متفاوت مسئله، کاربردهای مختلف، مسئله های تطابق *(matching)* ، مسئله ی " گمارش " *(Assignment Problem)* . مسئله های حمل ونقل *(Trans Portation Problem)* و جایابی *(Location Problem)* تطابق رشته ها، الگوریتم های *Boyer-Moore, Knuth-Morris-Pratt, Robin-Karp* ، الگوریتم های تقریبی برای برخی مسائل *NP-hard*، الگوریتم های احتمالاتی *(Probabilistic Algorithms)*

مراجع :

1. T.Cormen , C.Leiserson,R. Riverst, Introduction to Algorithms, MIT Press, 1992.

2. A.Dolan and J.Aldous, Network and Algorithms, An Introductory Approach, John Wiley, 1993.

3. Garey and Johnson, Computers and Intractibility,A Guide to Theory of NP-Completeness, W.H.Freeman And Company, 1979.

4. Dorit S.Hochbaum, Ed., Approximate Algorithms for NP-hard problems, PWS Pub. Co.,1997.

سیستمهای عامل پیشرفته

تعداد واحد: ۳ نوع واحد: نظری ساعت درس: ۴۸ ساعت

سر فصل دروس:

۱- معرفی طرح منطقی سیستمهای عامل پیشرفته
۲- زمان بندی *CPU* درمحیطهای چند پردازنده ای و چند برنامه ای
۳- مطالعه روشهای همزمانی درمحیط های چند پردازنده ای و بررسی مشکلات همزمانی و همگام سازی
۴- بررسی روشهای مدیریت حافظه و دستگاههای ورودی وخروجی و مدیریت بافر در محیطهای چند پردازنده ای و چند برنامه ای
۵- سیستم عامل توزیع شده
۶- سیستم عامل درمحیط شبکه ای
۷- تکنیکهای حفاظت منابع و تامین ایمنی سیستمهای عامل بزرگ
۸- ارزیابی کارایی سیستمهای عامل پیشرفته
۹- بررسی دو سیستم عامل پیشرفته(یک سیستم عامل متمرکز و یک سیستم عامل توزیع شده)
۱۰- طراحی و پیاده سازی هسته اصلی یک سیستم عامل پیشرفته (پروژه تیمی)

مراجع:

1- Modern Operating System, A.S.V. Tanenbaum Prentice-Hall, 1992.
2. Operating Systems : A Systematic view , William S.Davis, 4th ed. Addison – Wesley,1992.
3. Operating System Design, Dauglas Comer, Prentice-Hall,1998.
4. Distributed Operating Systems, the logical design , andrzej Goscinsri, Wesley, 1991.

دفاع و جنگ الکترونی

تعداد واحد : ۳ نوع واحد : نظری تعداد ساعت ۴۸ ساعت

محتوای درسی :

سیستم های دفاع و جنگ الکترونی – اصول معماری سیستم های *ECM* ، *SIGNT,ECCM,ESM*
اصول حاکم بر جنگ الکترونی – نقش اطلاعات و حفاظت آنها در جنگ الکترونی. مدیریت شبکه های مراقبتی و نظارت برای جمع آوری اطلاعات راداری.
مدیریت مخاطره و مدیریت وقایع طراحی زیر ساخت های نظامی و کشوری امن. روش های استفاده از جنگ جنگ الکترونی در شبکه های اطلاعاتی، ترافیک هوایی و شبکه های کامپیوتری.

1) CURTIS SCHELFHER (1986)
Introduction to Electronic Warfare.
Dedham. Artech House, 1986
2) SKOLNIK MERRILL (1980)
Introduction to Radar Systems.
McGraw-Hill, 1980.
3) Wiley R.G. (1982)
Electronic Intelligenece: ELINT
Artech House, 1986.
4) Wily R.G.(1983).
Electronic Intelligenece:The Analysis of Radar Signals.
Artech House, 1993.
5) Roe J., Gusons S., Feltham A., (1990)
Kowledge- Based Signal Processsing for Radar ESM Systems.
IEE Proceeding, Vol.137, Pt.F, No.5, OCTOBER 1990
6) US House Armed Service Committee.(1987)
News Release, 14th June 1987.
7) Whittall N.J., (1985)
Signal Sorting in ESM Systems.
IEE Proceeding, Vol.132.pt.F, No.4, JULY 1985
8) Wilkinson D.R., Watson A.W., Use of metric techniques in ESM data Processing.
IEE Proceeding, Vol.132,pt.F. No.4, JULY 1985

کد کننده های (رمزکننده های صوتی)

تعداد واحد : ۳ نوع واحد : نظری تعداد ساعت : ۴۸ ساعت

پیشنیاز : پردازش سیگناهای صوتی

سر فصل مطالب:

- نمونه برداری و کوانیزاسیئن اسکالر برداری
- تحلیل و مدل سازی سیگنال صوتی
- تحلیل طیفی زمان کوتاه
- مدل پیش بینی خطی برای سیسگنال های صحبت
- پیش بینی و آشکارسازی گام *Pctch*
- کوانیزاسیون پارامترهای *LPC* با استفاده از *LSFS*
- پیش بینی برداری *Switched-Adaption Interframe Vector Prediction (SIVP)*
- طرح کدینگ *SAVG*
- استراتژی و استانداردهای کدینگ صوتی
- کدینگ آنالیز و سنتز صحبت
- کدینگ (*MPLPC*)
- کدینگ (*CELP*)
- کدینگ با تاخیر کم
- کد کننده ها صوتی با تحریک چند باندی (*MBE*)
- کنترل خطا و انتقال صوت و کدینگ کنترل خط
- بهینه سازی منبع و کانال
- کنترل خطا در *CELP*
- مفاهیم کاربردی کد کننده ها
- پیاده سازی بلادرنگ کد کننده ها

مرجع :

1. *Digital Speech Coding for Low Bit Rate Communication Systems A.M. Kondoy, 1994. john Wiley & Sans.*

سیستمهای هوشمند

تعداد واحد: ۳ نوع درس : نظری ساعت درس ۴۸

سر فصل مطالب:

روشها و تکنیک های تولید سیستمهای هوشمند، ارائه دانش، جستجو، یادگیری و کسب دانش در سیستمهای خبره. ساختار یک سیستم خبره، روشهای ساخت اجزاء سیستم خبره، مکانیزم توصیف، مکانیزم استنتاج، انواع قوانین در مکانیزم استنتاج ، روشهای بیز، نظریه اطمینان، روشهای فازی، روشهای اعتبار سنجی اجزاء سیستم خبره، مهندسی و ساخت دانش، روشهای ساخت دانش، مقایسه وظایف مهندسی دانش و آنالیز سیستم، انواع سیستمهای کاربردی در سیستمهای خبره، روشهای تولید پایگاه دانش، اعتبار سنجی پایگاه دانش، ارزیابی دانش، تولید دانش، معرفی چندسیستم هوشمند در کاربردهای متفاوت. پیاده سازی یک سیستم هوشمند با ابزار برنامه سازی در سیستمهای هوشمند.

مراجع:

1. Lg nzioi, J.P., Introdouction to Expert Systems, The Develoment and Implementation of Rule-based Expert Systems, McGraw-Hill, 1991.

2. Jar-Liebowitz & Desalve D.A. (eds.), Structuring Expert Systems, Domain, Design, and Development, Prentice-Hall , 1989 ,

3. Gonzalez, A.J.& Ankel, D.D., The Engineering of Knowledge-Based System Theory and Practice, Prentice-Hall,1993.

4. Durkin, J., Expet Systems Design and Development, Macmillan Pub. Co.,1994.

5. Waterman,D.A., A Guide to Expert Systems, Addison –Wesley,1986.

سیستم های کامپیوتری امن

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت: ۴۸

سرفصل مطالب:

۱- اطمینان در فضای اطلاعات ، مفروضات امنیت در سیستم های کامپیوتری مدرن و ناچاری از خطا

۲- اصول طراحی سیستم های امن (حفاظت از اطلاعات در سیستم های کامپیوتری ، سخت افزار *Segmentation* برای محافظت فضای آدرس درونی)

۳- تصدیق اصالت (کلمات عبور، کارت های محافظت شده با *PIN* ، کلمات عبور یکباری ، بیومتریک، امنیت کلمه عبور ، امنیت کلمه عبور یونیکس، تحکیم کلمه عبور با حرکات ضربه به کلید)

۴- کنترل دستیابی و مجوز (کنترل دستیابی تفویضی – لیست های کنترل دستیابی و قادریت ها، پیاده سازی در *Windows NT* – کنترل دستیابی دستوری، مدل های کنترل دستیابی دستوری پیاده سازی هایشان، مدل *Bell-Lapadula* ، کنترل خط مشی روی عملیات اشیاء کنترل دستیابی مبتنی بر نقش – کنترل جریان اطلاعات، یک مدل توزیع شده برای جریان اطلاعات، خط مشی امنیتی دیوار چین و مدل کلارک- ویلسون)

۵- کانال نهان (مسئله زندان – تحلیل کانال نهان، اسب تروا)

۶- هسته های امنیتی (طراحی و پیاده سازی هسته امنیتی)

۷- امنیت سیستم های توزیع شده (تصدیق اصالت و کنترل دستیابی در سیتسم های توزیع شده ، کنترل دستیابی در محیط توزیع شده باز، جداسازی مدیریت کلید از امنیت سیستم فایل)

مراجع:

1- *Morrie Gasser, Building a Secure Computer System, Van Nostrand Reinhold Company, New York, ISBN: 0-442-23022-2,1988.*

2- *Jerome H. Sltzer, Michale D.Schroeder, The Protection of Coputer Systems, IEEE Tutorial Paper,/www.ecsl.cs.sunysb.edu/*

3- *M.Gasser, A. Goldstein, C.Kaufmann, B.Lampson, The Digital Distributed System Security Architecture, in 12 th National Computer Security conference (NIST/NCSC), Battimore,1989.*

4- *M.Zeleznik, Security Desugn in Distributed Comuting Applications,/citeseer.nj.nec.com/zelenik93 security.html.*

5- *E.Fisch,G.White, Secure computers and Networks, CRC Press, 2000.*

6- *P.Gutmann, The Design and Verifcation of a Cryptographic Security Architecture, Springer- Verlag, 2002.*

7- *S.Ames, M.Gasser,R.Shell, Security Kernel Design and Implementation: An Introduction, IEEE Coputer, Vol.16, No.1, 1983.*

8- M.Harrison, W.Ruzzo, J. Ullman, Protection in Operating Systems, Communications of the ACM, Vol.19, No.8,1976.
9- P.Denning Faut Tolerant Operating Systems, Computer Surveys, V.8.4,1976.

پروتکلهای امنیتی

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت : ۴۸

اهداف درس: در این درس پروتکلهای امنیتی مختلف توصیف شده، همچنین حملات و دفاع های مختلف در مقابل آنها مطرح می گردد. پروتکلهای مختلف مانند پروتکلهای تصدیق اصالت و امضاء. مدیریت حقوق دیجیتال، پروتکلهای امنیتی در شبکه های توزیع شده بدون سیم و با سیم، رای گیری الکترونیک، پروتکل های، پرداخت الکترونیک، تکنیکهای رمز نگاری بصری در این درس مورد توجه هستند.

سرفصل مطالب:

۱-مقدمه (پروتکل، پروتکل های امن وانواع آن ، کلاس های حملات به پروتکل های امن ومدل های امنیتی ، امضا وتصدیق اصالت و هویت، پروتکل ها ومکانیزم ها، مدیریت و برقراری کلید وگواهی)

۲- بلوک های سازنده پروتکل (تعرف پروتکل، ارتباط بااستفاده از رمزنگاری متقارن ، توابع یکطرفه، ارتباط با استفاده از رمزنگاری نامتقارن، امضاهای رقمی، چهار چوبی برای مکانیزم های امضای رقمی، *RSA* و طرحهای امضای مربوطه، طرح امضای رقمی حکم دار، طرحهای امضای فیات- شامیر، *DSA* و طرحهای امضای مربوطه، طرحهای امضا رقمی یکبار مصرف، طرحهای امضای رقمی حکم دار، طرحهای امضای رقمی کور، طراحهای امضا رقمی غیر قابل انکار، طرحهای امضای رد- توقف)

۳- پروتکل های ساده (پروتکلهای مبادله کلید، پروتکل های تصدیق اصالت، پروتکلهای تصدیق اصالت ومبادله کلید، تحلیل فورمال پروتکلهای مبادله کلید وتصدیق اصالت، رمزنگاری با کلید عمومی چند گانه ، تقسیم راز، اشتراک راز، محافظت رمزنگارانه از پایگاه داده ها)

۴- پروتکل های متوسط (سرویس های مهر زمانی، کانال نهان، امضای رقمی غیر قابل انکار، امضای باتائیدکننده مشخص ، امضاهای نیابتی، امضاهای گروهی، محاسبه با اطلاعات رمز شده، طرحهای *Bit Commitment* ، طرحهای سکه اندازی عادلانه، پوکر ذهنی، جمع کننده های یکطرفه ، افشای همه یاهیچ رازها، *KEY ESKROW*)

۵-پروتکلهای پیشرفته (اثبات های صفر- دانش، اثبات صفر- دانش هویت، امضاهای کور، رمزنگاری کلید عمومی مبتنی بر هویت، انتقال بی خبر، امضاهای بی خبر، امضای قرارداد توامان، نامه دیجیتال سفارشی، مبادله همزمان رازها)

۶- پروتکل های خاص (انتخاب امن، محاسبات چند طرفه امن، پخش بدون – نام پیام ، اسکناس دیجیتال)

۷- مدیریت کلید (تولید کلید، فضای غیر خطی کلید، انتقال کلید تائید کلید، استفاده از کلید، ذخیره کلید، تازه کردن کلید، عمر کلید، از بین بردن کلید، مدیریت کلید ، کلید های عمومی)

۸- الگوریتمهای امضای رقمی با کلید عمومی

۹- طرحهای تشخیص هویت

۱۰- الگوریتمهای مبادله کلید (طرح دیفی- هلمن، پروتکلهای ایستگاه به ایستگاه، پروتکل سه دور شامیر،

۱۱- الگوریتم های خاص برای پروتکلها

مراجع :

1- B. Schneier Applied Cryptography : Protocols, Algorithms and Source Code in C, John Wiley and Sons Inc., 1996.

2- A. Menezes, et . al., handbook of Applied Cryptography , CRC Press, 1996.

3-A. Beutelspacher et. Al., Modern Topics in Cryptography , in German, Vieweg, 1995.

4- P. Ryan, S. Schneider, M Goldsmith, G. Lowe and B. Roscoe, Modelling and Analysis of Security Protocols, Addison-WESLEY, 2001.

شماره :

تاریخ :

پیوست :

بسمه تعالی

دانشکده مهندسی برق

تکنولوژی اینترنت

تعداد واحد: ۳ نوع درس: نظری ساعت درس: ۴۸ ساعت

محتوی درس:

در این درس تاریخچه پیدایش شبکه کامپیوتری که منجر به پیدایش اینترنت گردیده است مورد بررسی و شناسایی قرار میگیرد. پروتکل TCP/IP بررسی واصول حاکم بر آن مورد تجزیه وتحلیل قرار میگیرد و نحوه عمل ICMP,UDP,TCP تشریح و تجزیه وتحلیل میگردد.

روش های مسیر یابی IGRP,OSF,BGP تشریح و تجزیه و تحلیل میگردد.

سرویس های Doma Name و سایر روش ها بحث خواهدشد.

مروری برکاربردهای شبکه اینترنت همانند تجارت الکترونی، سیستم های صوتی/تصویری الکترونی و توسعه آتی آن، آموزش الکترونی و کتابهای الکترونی در شبکه های تار عنکبوتی ارائه میگردد.

دانشکده مهندسی برق، دانشگاه علم و صنعت ایران، تهران ۱۶۸۴۴

تلفن: ۳-۷۸۰۸۰۲۲ دورنگار: ۷۴۵۴۰۵۵

مدیریت سیستم های امن

تعداد واحد: ۳ نوع واحد: نظری تعداد ساعت : ۴۸

اهداف درس: هدف از این درس اینست که درکی در مورد ملاحظات امنیتی در رابطه با مدیریت سیستم های اطلاعاتی مبتنی بر کامپیوتر برای دانشجویان فراهم آورد. از اینرو اعمال امنیتی که لازم است تایک سیستم امن رااز لحاظ عملیاتی امن نگهدار مطالعه می گردد. این زمینه شامل موضوعاتی از قبیل مدیریت مخاطرات، اعتباردهی و گواهی است . همچنین ملاحظات عملیاتی مانند گزارش دهی اعلام های خطر، بازرسی و مدیریت کلیدهای رمز نگاری راشامل می گردد.

سر فصل مطالب:

- مدیریت پیکره بندی و امنیت سیستم، اعتبار دهی و گواهی دهی
- مدیریت مخاطرات امنیتی
- مدیریت امنیت (شناسائی اجزاء تحت مدیریت، خط مشی امنیتی سازمان، خط مشی امنیتی و نرم افزارهای مورد اطمینان، اطلاعات و سیستم های پردازش اطلاعات ، زیر ساخت امنیتی سازمان، سرویس ها و مکانیزمهای امنیتی ، طبقه بندی داده هاوکنترل دسترسی، امنیت پرسنل، امنیت فیزیکی و محیطی مدیریت ارتباطات و عملیات، نگهداری و ایجاد سیستم ها ، مدیریت تداوم کار، بازیابی از فجایع طبیعی ، استانداردها)
- جنبه های قانوی امنیت
- مدیریت کلید و توافقات امنیتی
-بازرسی امنیتی
- گزارش دهی اعلام خطرهای امنیتی
- مدیریت امنیت در سیستم های *main frame* و شبکه

مراجع:

1- NIST, Guideline for computer Security Cerification and Accreditation, FIPS PUB 102,1983.

2- NIST, Guideline For the Analysis of local Area Network Security, FIPS, Pub.191-1974.

3. NIST, Guidelines for Automatic Data Processing Physical Security and Risk Mangement, FIPS PUB 31, 1974

4- ISO/IEC, Management Plan for Security JTC/SC21 SD-1.

5- ISO ,OSI Basic Reference Model, Part2.: Security Architecture, 7498-2,1989.

6- ISO/IEC, OSI Systems Management, Part7: Security Alarm Reporting Function, 10164-7,1992.
7-ISO/IEC, OSI Systems Management Part8 : Security Audit Trail Function, 10164-8, 1993.
8- ISO/IEC, OSI Systems Management Part9 : Objects and Attribute for Access Control, 10164-9, 1995.
9- ISO/IEC, OSI Security Frameworks for Open System, Part8 : Key Management, 10181-8.
10-IETF, Internet Security Association and Key Management Protocal (ISAKMP), 1997.
11-A. Blyth, and G. L. Kovacich, Information Assurance, Springer-Verlag, 2001.

تئوری اطلاعات و کدینگ

تعداد واحد : ۳ نوع واحد: نظری

تعداد ساعت ۴۸ ساعت

محتوای درس:

اندازه گیری اطلاعات انتروپی – انتروپی منبع و قضایای کدینگ بدون نویز، روشهای کدینگ منبع : هفمن الیاس، کدهای قابل دکد شدن واحد، کدهای با قابلیت همزمانی- امار نویز کانال، فاصله همینگ ، قضایای کدینگ کانال با نویز. تئوری سرعت تغییر شکل- کدهای ریدومولر- همینگ و کدهای کامل، کانولشن و ویتربی

1) Information Theory and Reliable Communication. Gallagar
2) Information theory , Ash
3) Error Correcting Codes, Peterson & wepdon

طراحی و تجزیه و تحلیل سیستمها:

تعداد واحد : ۳ نوع درس نظری ساعت درس ۴۸ ساعت

محتوای درس:

دراین درس روش ها و مراحل تجزیه و تحلیل سیستمها مورد بررسی قرار گرفته و باتاکید بر تحلیل هر واحد از سیستم اقدام به طراحی ریز سیستم ها و طراحی سیستم اصلی میگردد. طرح تشکیلاتی و تکنولوژی بکار گرفته شده در هر زیر سیستم و روابط بین زیر سیستم ها تجزیه و تحلیل میگردد.

این بررسی ها در سطوح مختلف سازمانی، ساختاری و ارتباطی و تکنولوژیکی انجام می گردد. و نیازمندیهای هر طبقه و یا هرواحد همراه با اثرات متقابل واحدها بر هم تعیین وطراحی میگردد. کاربرد تجزیه و تحلیل *RISK* و آزمایش های بحرانی درجهت پیاده سازی و شناخت واحدهای واسط یا ارتباط زیر سیستم ها در مراحل طراحی تعریف میشود. در مراحل طراحی مشخصات و مراحل، عملکرد سیستم تعریف و برنامه ریزی میگردد. در این درس تعداد زیادی از مسائل وسیستمهای موجود وتوسعه داده شده بررسی و تجزیه و تحلیل میگردد.

سیستم های کامپیوتری توزیع شده

تعداد واحد : ۳ نوع واحد : نظری تعداد ساعت : ۵۱ ساعت

سر فصل مطالب:

بررسی اصول، مفاهیم و طراحی سیستم های توزیع شده- معماری سخت افزار و نرم افزارها وسائل مخابراتی لازم برای سیستم های کامپیوتری توزیع شده – بررسی جزئیات اجزاء تشکیل دهنده – تسهیلات مربوط به زبانهای برنامه سازی لازم جهت ایجاد و کاربرد سیستم های توزیع شده – شبکه های خاص مورد نیاز – بررسی نمونه هایی از سیستم های توزیع شده و انجام پروژه های کاربردی به صورت تیمی.

مراجع :

1. Distributed Systems and computer Networks by M. Sloman and J. Kramer Prentice Hall, 1987.

2. Distributed Systems, Concepts and Design by : G. F. Coulouris and J. B. Dollimore, Addison Wesley 1988.

3. Distributed Data-based : Principles and Systems by S. Ceri and G. Pelatti, MC. Graw Hill co. 1984.