جمهوری اسلامی ایران

وزارت علوم، تحقیقات و فناوری

شورای عالی برنامه‌ریزی آموزشی

برنامه درسی رشته

ریاضی کاربردی

Applied Mathematics

مقطع کارشناسی ارشد ناپیوسته

گرایش

Cryptography and Coding	رمز و کد

گروه علوم پایه

پیشنهادی کارگروه تخصصی علوم ریاضی

باسمه تعالی

نام رشته: ریاضی کاربردی | **عنوان گرایش: رمز و کد**

گروه تحصیلی: علوم پایه | **دوره تحصیلی: کارشناسی ارشد ناپیوسته**

زیرگروه تحصیلی: علوم ریاضی | **نوع مصوبه: بازنگری**

پیشنهادی: کارگروه تخصصی علوم ریاضی | **تاریخ تصویب: ۱۴۰۲/۰۴/۱۲**

برنامه درسی بازنگری شده دوره کارشناسی ارشد ناپیوسته رشته ریاضی کاربردی گرایش رمز و کد، در جلسه شماره ۱۷۱ تاریخ ۱۴۰۲/۰۴/۱۲ کمیسیون برنامه‌ریزی درسی، محتوا و سرفصل رشته‌های تحصیلی به شرح زیر تصویب شد:

ماده یک- این برنامه درسی برای دانشجویانی که پس از تصویب این برنامه درسی در دانشگاه‌ها و موسسات آموزش عالی پذیرفته می‌شوند، قابل اجرا است.

ماده دو – این برنامه درسی، جایگزین برنامه درسی رشته ریاضی کاربردی گرایش رمز و کد مصوب جلسه ۷۰ تاریخ ۱۳۹۵/۰۳/۲۳ کمیسیون برنامه‌ریزی آموزشی می‌شود.

ماده سه- این برنامه درسی در سه فصل: مشخصات کلی، جدول‌های واحدهای درسی و سرفصل دروس تنظیم شده است و برای اجرا در دانشگاه‌ها و موسسات آموزش عالی پس از اخذ مجوز پذیرش دانشجو از شورای گسترش آموزش عالی و سایر ضوابط و مقررات مصوب وزارت علوم، تحقیقات و فناوری، ابلاغ می‌شود.

ماده چهار- این برنامه درسی از شروع سال تحصیلی ۱۴۰۳-۱۴۰۲ به مدت ۵ سال قابل اجرا است و پس از آن، در صورت تشخیص کارگروه تخصصی مربوطه، نیاز به بازنگری دارد.

دکتر رضا نقی‌زاده
مدیر کل دفتر برنامه ریزی آموزش عالی
و دبیر کمیسیون

دکتر قاسم عموعابدینی
معاون آموزشی و رئیس کمیسیون

وزارت علوم، تحقیقات و فناوری
شورای عالی برنامه ریزی و آموزش عالی

جمهوری اسلامی ایران

وزارت علوم، تحقیقات و فناوری

شورای عالی برنامه‌ریزی

گروه علوم پایه

کمیته تخصصی علوم ریاضی

برنامه آموزشی دوره کارشناسی ارشد ریاضی کاربردی

گرایش رمز و کد

فصل اول

مشخصات دوره کارشناسی ارشد ریاضی کاربردی

گرایش رمز و کد

مقدمه

دوره کارشناسی ارشد «رمز و کد» یک دوره تحصیلی میان رشته‌ای با تاکید بر دو زمینه تخصصی «رمز» و «کد» است. هدف از این دوره تربیت دانش‌آموختگانی است که علاوه بر آشنایی بر جنبه‌های کاربردی این دو زمینه تخصصی، با تسلط بر مبانی نظری این مباحث توانایی تجزیه و تحلیل مسایل را نیز به طور اصولی داشته باشند. همچنین فارغ التحصیلان می‌توانند به عنوان کارشناسی ارشد در سازمان‌ها، شرکت‌ها یا موسسات مرتبط و یا با ادامه تحصیل در مقاطع بالاتر به عنوان متخصص در زمینه مربوطه به فعالیت حرفه‌ای بپردازند.

تعریف

دوره کارشناسی ارشد«رمز و کد» یکی از دوره‌های آموزشی وپژوهشی در سطح تحصیلات تکمیلی از نظام آموزش عالی است که بعد از دوره کارشناسی آغاز و به اعطای مدرک رسمی دانشگاهی در دوره کارشناسی ارشد ریاضی کاربردی گرایش «رمز و کد» می‌انجامد و از نظر اجرایی، تابع ضوابط، مقررات و آیین نامه‌های مصوب شورای برنامه‌ریزی وزارت علوم، تحقیقات و فنآوری است

اهداف

- تربیت پژوهشگرمتخصص درحوزه رمز و کد
- تامین نیازهای تخصصی شرکت‌های خصوصی و دولتی در زمینه‌های امنیت داده و اطلاعات و فناوری‌های ارتباطاتی و مخابراتی
- توسعه علم و فناوری در حوزه فناوری اطلاعات و ارتباطات با تاکید برمبانی بنیادی و ریاضی آنها

نقش وتوانایی

فارغ التحصیلان دوره کارشناسی ارشد«رمز و کد» میتوانند:

به عنوان متخصص امنیت داده، اطلاعات و ارتباطات در مراکز داده، مدیریت شبکه‌های اطلاعاتی و ارتباطی، ... در شرکت‌های خصوصی، مراکز مالی، شرکت‌های مخابراتی، شرکت‌های فناوری اطلاعات، دانشگاه‌ها، مراکزآموزشی و ... فعالیت کنند.

به عنوان پژوهشگردر زمینه امنیت اطلاعات و یا متخصص سامانه‌های ارتباطی در شرکت‌ها و مراکز تحقیقاتی به پژوهش، نوآوری و توسعه فناوری‌های نوین حوزه رمز و کد بپردازند.

ضرورت و اهمیت

عصر جدید، عصر فناوری‌های نوین اطلاعاتی و ارتباطی است. سرعت نوآوری در این حوزه نیازمندی‌های علمی و عملی خاصی را طلب می‌کند. حجم داده‌های فراوان در این حوزه که نیازمند امنیت و محرمانگی هستند و نیاز به پردازش و ارسال سریع اطلاعات حجیم که نیازمند فناوری‌های نوین ارتباطی هستند، تربیت متخصصین و کارشناسان خبره و مسلط بر دانش رمز و کد را طلب می کند. شاخه رمز و کد یک دوره بین رشته‌ای، بین رشته‌های مهندسی برق، کامپیوتر، فیزیک، علوم کامپیوتر و ریاضی است، که بخش اعظم آن بر بنیاد دانش ریاضی بنا شده است و لازم است به تربیت دانشجویان در این حوزه پرداخته شود تا بتوان پاسخگوی نیازمندی‌های کشور در حال حاضر و آینده بود.

کلیات برنامه

عنوان دوره: کارشناسی ارشد ریاضی کاربردی- گرایش رمز و کد

پیشنیاز ورود : دارا بودن مدرک کارشناسی در یکی از رشته‌های مجموعه علوم ریاضی، فیزیک و یا مهندسی

آزمون ورودی: آزمون ورودی مطابق برنامه کنکور سراسری کارشناسی ارشد که توسط سازمان سنجش برگزار می گردد می باشد و مواد آزمون عمومی، مشترک و تخصصی این گرایش مطابق جدول مواد درسی و ضرایب مربوطه که همه ساله توسط کارگروه برنامه ریزی علوم ریاضی وزارت تعیین و به سازمان سنجش اعلام می گردد خواهد بود.

طول دوره و شکل نظام

دوره کارشناسی ارشد مطابق با آیین نامه جاری دوره کارشناسی ارشد وزارت عتف است.

تعداد و نوع واحدهای درسی

توزیع واحدها

نوع دروس	تعداد واحد
دروس تخصصی	**۸**
دروس اختیاری	**۱۶ – ۱۳**
سمینار	**۲**
پایان‌نامه	**۶**
جمع	**۳۲ – ۲۹**

نحوه انتخاب درس ها

تعداد واحدهای درسی دوره کارشناسی ارشد ریاضی کاربردی- گرایش رمز و کد حداقل ۲۹ واحد و حداکثر ۳۲ واحد به قرار زیر است:

درس های تخصصی: ۸ واحد، شامل ۲ درس به صورت زیر است:

- اانتخاب درس اول از جدول دروس اصلی تخصصی (سرشاخه) گرایش رمز و کد (جدول شماره ۱) (انتخاب درس **رمز نگاری ۱** برای زیر گرایش رمز یا **کدگذاری ۱** برای زیر گرایش کد الزامی است).
- انتخاب درس دوم از جدول دروس تخصصی(جدول شماره ۲) و یا درس کذرانده نشده جدول شماره ۱

درس های اختیاری: شامل ۴ درس به صورت زیر است:

- انتخاب حداقل ۲ درس از جدول درس های اختیاری گرایش رمز و کد (جدول شماره ۳)

سایر درس های باقیمانده اختیاری با نظر استاد راهنما می تواند به روش های زیر انتخاب شود:

- از دروس اخذ نشده جداول شماره های ۱ و ۲ و ۳
- از دروس تخصصی یا اختیاری سایر گرایش های کارشناسی ارشد رشته های ریاضیات و کاربردها ، ریاضی کاربردی و یا رشته های مرتبط با نظر استاد راهنما و گروه
- از دروس دوره دکتری ریاضی زیربرنامه های کد و رمز

سمینار: ۲ واحد

پایان نامه: ۶ واحد

تبصره ۱: اخذ درس سمینار و پایان نامه در نیمسال اول تحصیلی مجاز نیست. برای اخذ درس سمینار نیاز به گذراندن دست کم ۸ واحد درسی و برای اخذ پایان نامه دست کم ۱۲ واحد (که شامل درس های الزامی باشد) و موافقت گروه الزامی است.

تبصره ۲: دانشجویان دوره کارشناسی ارشد ریاضیات و کاربردها گرایش کد و رمز با اخذ دست کم ۶ واحد تمام وقت محسوب می شوند.

تبصره ۳: دانشجو در طول تحصیل خود نمی تواند بیش از یک درس با عنوان مباحث ویژه اختیار کند.

تبصره ۴: گذراندن دروس پیش نیاز برای دانشجویانی که این دروس را در دوره کارشناسی نگذرانده اند با موافقت گروه و دانشکده بر اساس مقررات دانشگاه بلامانع است.

تبصره ۵: دروس تخصصی می توانند همزمان با ارایه درس دارای کلاس حل تمرین باشند. برای سایر دروس بر اساس نیاز و صلاحدید و موافقت گروه ، ارایه کلاس حل تمرین بلامانع است.

تبصره ۶: گروههای مجری می توانند حداکثر یک درس جدید را به عنوان درس اختیاری مطابق با روال جاری دانشگاه مصوب و به جدول شماره ۳ اضافه نمایند. البته لازم است معاون آموزشی دانشگاه درس مربوطه به همراه سرفصل را حداکثر یک ماه پس از تصویب به کارگروه برنامه ریزی وزارت اعلام نماید.

فصل دوم

جدول‌های دروس

جدول شماره ۱ : دروس اصلی تخصصی (سرشاخه) گرایش رمز و کد

شماره درس	نام درس	تعداد واحد	ساعت			پیشنیاز	هم نیاز
			جمع	نظری	عملی		
۱	رمز نگاری ۱	٤	٦٤	٦٤		----	
۲	کدگذاری ۱	٤	٦٤	٦٤		----	

جدول شماره ۲ : درس‌های تخصصی گرایش رمز و کد

شماره درس	نام درس	تعداد واحد	ساعت			پیشنیاز	هم نیاز
			جمع	نظری	عملی		
۱	نظریه اطلاع و کاربرد	٤	٦٤	٦٤			-----
۲	الگوریتم و محاسبه	٤	٦٤	٦٤			-----
۳	جبر پیشرفته	٤	٦٤	٦٤			-----

جدول شماره ۳ : درس های اختیاری گرایش رمز و کد

شماره درس	نام درس	تعداد واحد	ساعت			پیش نیاز	هم نیاز
			جمع	نظری	عملی		
۱	رمزنگاری ۲	٤	٦٤	٦٤		رمزنگاری ۱	
۲	امنیت شبکه	٤	٦٤	٦٤		شبکه‌های کامپیوتری، رمزنگاری ۱	
۳	روش‌های آماری در رمزنگاری	٤	٦٤	٦٤		رمزنگاری ۱	
٤	پنهان‌سازی اطلاعات	٤	٦٤	٦٤		نظریه اطلاع و کاربرد	
٥	امنیت پایگاه داده	٤	٦٤	٦٤		رمزنگاری ۱	
٦	نظریه اعداد محاسباتی	٤	٦٤	٦٤		نظریه اعداد، برنامه‌سازی C	
۷	پروتکل‌های رمزنگاری	٤	٦٤	٦٤		رمزنگاری ۱	
۸	روش‌های صوری در رمزنگاری	٤	٦٤	٦٤		رمزنگاری ۱	
۹	مباحث ویژه در رمزنگاری	٤	٦٤	٦٤		اجازه گروه	
۱۰	کدگذاری ۲	٤	٦٤	٦٤		کدگذاری ۱	
۱۱	کدگذاری شبکه	٤	٦٤	٦٤		کدگذاری ۱	
۱۲	الگوریتم‌های کدگشایی تکراری	٤	٦٤	٦٤		کدگذاری ۲	
۱۳	کدگذاری فضا-زمان	٤	٦٤	٦٤		کدگذاری ۱	
۱٤	کدگذاری منبع	٤	٦٤	٦٤		نظریه اطلاع و کاربرد	
۱٥	نظریه اطلاع و کدگذاری کوانتومی	٤	٦٤	٦٤		کدگذاری ۱	

۱٦	**کدهای حلقه مبنا**	٤	٦٤	٦٤		**کدگذاری ۱ , مبانی جبر**	
۱۷	**کدشبکه خطی تصحیح کننده خطا**	٤	٦٤	٦٤		**کدگذاری شبکه**	
۱۸	**مباحث ویژه در کدگذاری**	٤	٦٤	٦٤		اجازه گروه	

فصل سوم

سرفصل درس های دوره

کارشناسی ارشد ریاضی کاربردی گرایش رمز و کد

عنوان درس	فارسی	رمزنگاری ۱								
	انگلیسی	Cryptography I								
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی			تخصصی		اختیاری			
		نظری	عملی		نظری	عملی	نظری	عملی	۴	۶۴	
آموزش تکمیلی عملی:	دارد □	ندارد ■								
سفر علمی:	دارد □	ندارد ■								
کارگاه:	دارد □	ندارد ■								
آزمایشگاه:	دارد □	ندارد ■								
سمینار:	دارد □	ندارد ■								
حل تمرین: دارد	نیاز به اجرای پروژه عملی: ندارد									

هدف درس: بیان اهمیت رمزنگاری در ارتباطات و نقش ریاضیات پیشرفته در توسیع آن، معرفی رمزنگاری کلاسیک و سپس انواع سیستم‌های رمزنگاری متقارن و نامتقارن، امضای دیجیتال و . . . به نحوی که دانشجو بر اصول و مفاهیم پایه ای رمزنگاری مسلط شده و با مثال‌های لازم در این زمینه آشنا شود.

سرفصل‌های درس:

- اهمیت رمزنگاری، تاریخچه، معرفی سرفصل‌های مهم ریاضی مرتبط با رمزنگاری و درصورت لزوم تدریس و یادآوری نکات کلیدی ریاضی مورد لزوم نظیر، میدان‌های متناهی، نظریه اعداد، پیچیدگی و ....
- رمزنگاری کلاسیک، معرفی سیستم‌های رمز مشهور (نظیر سزار، آفین و...) و نحوه شکستن آنها
- یادآوری قضیه شانون، امنیت کامل، نحوه اندازه گیری امنیت و محرمانگی (با استفاده از روش هایی نظیر آنتروپی، نظریه پیچیدگی و ...)، بررسی انواع امنیت
- رمزنگاری متقارن (قالبی و جریانی)، انواع، امنیت و معرفی بعضی از حملات به آنها (حمله تفاضلی، حمله خطی، حملات جبری و...)
- معرفی توابع چکیده ساز، انواع آنها (CBC، MAC، HMAC و ...)، امنیت و حملات محتمل به آنها، الگوریتم تبادل کلید دیفی-هلمن
- سامانه‌های رمزنگاری کلید عمومی مشهور (RSA، الجمال، رابین و ...)، تحلیل امنیت آنها
- طرح‌های امضای دیجیتال مشهور (RSA، الجمال و ...)
- معرفی مقدماتی مفهوم امنیت اثبات پذیر
- معرفی رمزگذاری پسا کوانتمی و مسائل مرتبط با آن

مراجع:

١- Kiayias, A., Kohlweiss, M., Wallden, P. and Zikas, V., ٢٠٢٠. Public-Key Cryptography-PKC ٢٠٢٠. Springer International Publishing.

٢- Easttom, C, ٢٠٢١. Modern Cryptography. Applied mathematics for encryption and information security. McGraw-Hill Publishing.

٣- J. Hoffstein, J. Pipher and J.H. Silverman, An Introduction to Mathematical Cryptography, Springer, ٢٠٠٨.

٤- Josef Pieprzyk, Thomas Hardjono, Jennifer Seberry: “Fundamentals of Computer Security”, Springer Verlag, ٢٠٠٣.

٥- Christof Paar, Jan Pelzl: “Understanding Cryptography, A Textbook for Students and practitioner”, Springer Verlag, ٢٠١٠.

٦- Jonathan Katz, Yehuda Lindell: “Introduction to Modern Cryptography”, Editor: Douglas Stinson, Chapman and Hall/CRC, Taylor & Francis Group, ٢٠٠٨.

٧- Andreas Klein, Stream Ciphers, Springer Verlag, ٢٠١٣.

٨- Thomas Cover, Joy A. Thomas: “Elements of Information Theory”, ٢nd Ed. Wiley Series, ٢٠٠٦.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="6">کدگذاری ۱</td></tr>
<tr><td>انگلیسی</td><td colspan="6">Coding I</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="5"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td colspan="2">پایه</td><td colspan="2">اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="8">ندارد</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="2">آموزش تکمیلی عملی:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سفر علمی:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">کارگاه:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">آزمایشگاه:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سمینار:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">حل تمرین: دارد</td><td colspan="8">نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: شناخت مفاهیم اساسی ساخت کد و انتقال اطلاعات از کانال نویزدار، روش‌های تشخیص و تصحیح خطا، آشنایی با چند کد مهم و دارای ساختار.

سرفصل‌های درس:

- مرور سامانه مخابراتی و کانال های مخابراتی و معرفی مختصر کانال های AWGN, BEC, BSC و بعضی از مدولاسیون های معروف
- کد های بلوکی، کد های خطی: تعریف، پارامترهای کلیدی ; ماتریس مولد و ماتریس توازن آزما ; تشخیص و تصحیح خطا
- دوگان کد خطی توزیع وزن کدهای بلوکی
- احتمال های تشخیص و تصحیح خطا ; کدگشایی کمترین فاصله و کد گشایی بیشترین درستنمایی ; آرایه استاندارد وکد گشایی مشخصه (سندرم)
- کد همینگ , ساخت خواص و پارامترها
- به دست آوردن کد جدید از کد مفروض ;اصلاح کدها (بسط, الحاق, کوتاه کردن و...)
- کران های پوششی و بسته بندی کره ها و سینگلتون; کد کامل, کدهای بیشترین فاصله جدایی پذیری(MDS)
- میدانهای متناهی روش ساخت و توسیع ; تجزیه چند جمله ایها ; محاسبات روی میدان های متناهی
- کد های دوری و نحوه ساخت آنها با کمک میدان های متناهی

- کدهای BCH دودویی و غیردودویی، کدگذاری و کدگشایی خواص و پارامترها
- کدهای رید-سالمون ، کدگذاری و کدگشایی خواص و پارامترها
- کد های رید-مولر و اتواع آن
- کد های مانده مربعی , گلی و هادامارد
- کدهای رید-سالمون تعمیم یافته ,کدهای متناوب (آلترننت) و کدهای گپا

مراجع:

۱- S.B. Wicker, Error control systems for Digital communication and storage, Prentice Hall Englewood cliffs, NJ, ۱۹۹۵.
۲- Shu Lin and Daniel Castello, Error Control Coding, Pearson Pr. Hall, NJ, ۲۰۰۵
۳- F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North- Holland Mathematical Library, ۱۹۷۷.
٤- S. Romann, Coding and Information Theory, Springer Verlag, ۱۹۹٦.
٥- San Ling and Chaoping Xing, Theory A First Course, Cambridge University Press, ۲۰۱۰.
٦- Berlekamp, E.R., Algebraic coding theory (revised edition). World Scientific, ۲۰۱٥.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="5">نظریه اطلاع و کاربرد</td></tr>
<tr><td>انگلیسی</td><td colspan="5">Information Theory and its Application</td></tr>
<tr><td colspan="2">نوع واحد</td><td>تعداد واحد</td><td>تعداد ساعت</td><td colspan="2">دروس پیش‌نیاز</td></tr>
<tr><td colspan="2">پایه / اصلی / تخصصی / اختیاری</td><td>۴</td><td>۶۴</td><td colspan="2" rowspan="6">ندارد</td></tr>
<tr><td colspan="2">نظری ■ / عملی □ | نظری ■ / عملی □ | نظری ■ / عملی □ | نظری □ / عملی □</td><td colspan="3"></td></tr>
<tr><td colspan="2">آموزش تکمیلی عملی:</td><td colspan="3">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سفر علمی:</td><td colspan="3">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">کارگاه:</td><td colspan="3">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">آزمایشگاه:</td><td colspan="3">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سمینار:</td><td colspan="3">دارد □ ندارد ■</td><td></td></tr>
<tr><td colspan="2">حل تمرین: ندارد</td><td colspan="3">نیاز به اجرای پروژه عملی: ندارد</td><td></td></tr>
</table>

هدف درس: ارائه مفاهیم آنتروپی به‌صورت تحلیلی و بیان کاربرد آن در کدگذاری منبع و کانال، ظرفیت کانال، قضیه های شانون، بررسی خواص آماری و احتمالاتی آنتروپی و نقش نظریه اطلاعات در رمزنگاری

سرفصل‌های درس:

- آنتروپی، آنتروپی شرطی و توام، آنتروپی نسبی، اطلاعات متقابل، نامساوی ینسن(Jensen)، فانو . . .
- خاصیت افراز مجانبی یکنواخت و خواص و اهمیت آن
- نرخ آنتروپی یک فرآیند تصادفی، آنتروپی و قدم زدن تصادفی
- فشرده سازی داده ها، نامساوی کرفت (Kraft)، کدهای بهینه، کدهای هافمن(Huffman)، کدگذاری شانون،
- ظرفیت کانال، انواع کانال‌ها و خواص آنتروپیک آنها، خواص ظرفیت کانال، نامساوی فانو و عکس قضیه کدگذاری، قضیه های شانون
- کانال گوسی، خواص، انواع نویزها
- رمزنگاری از دیدگاه نظریه اطلاع، مدل شانون برای امنیت، امنیت کامل و . . .
- موضوعات در فناوری اطلاعات چند کاربره: ظرفیت یک کانال با دسترسی چندگانه. مساله Gelfand-Pinsker، کانال های تداخل.

مراجع:

١- T.M.Cover and J.A.Thomas , *Elements, of Information T heory*, John Wiley, New York, ٢٠٠٦.

٢- R. McEliece, *The Theory of Information and Coding*, Cambridge Univ. Press, ٢٠٠٤.

٣- Y. Liang, H. V. Poor and S. Shamai , *Information Theoretic Security*, Now publishers Inc.

٢٠٠٩: ISBN-١٠: ١٦٠١٩٨٢٤٠٢.

٤- Yockey, H.P., ٢٠٠٥. *Information theory, evolution, and the origin of life*. Cambridge University Press.

٥- MacKay, D.J. and Mac Kay, D.J., ٢٠٠٣. *Information theory, inference and learning algorithms*. Cambridge university press.

عنوان درس	فارسی	الگوریتم و محاسبه										
	انگلیسی	Algorithm and Computation										
نوع واحد									تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی			تخصصی			اختیاری				
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی		۴	۶۴		
آموزش تکمیلی عملی:	دارد □ ندارد ■											
سفر علمی:	دارد □ ندارد ■											
کارگاه:	دارد □ ندارد ■											
آزمایشگاه:	دارد □ ندارد ■											
سمینار:	دارد □ ندارد ■											
حل تمرین: ندارد	نیاز به اجرای پروژه عملی: ندارد											

هدف درس: هدف این درس آشنایی دانشجو با مفاهیم اصلی نظریه محاسبه مرتبط با زمینه‌های رمز و کد در ایجاد سختی الگوریتم یا سهولت محاسبات الگوریتم‌ها و یا امکان تجزیه و تحلیل پیچیدگی الگوریتم های مورد استفاده است.

سرفصل‌های درس:

- ارائه تعریف دقیق پیچیدگی محاسبه در مدل‌های قطعی و غیرقطعی.
- تعریف دقیق کلاس‌های P و NP، تعریف دقیق مسائل NP-تمام با ارائه مثال.
- اهمیت مدل NP در تحلیل حمله به سامانه‌های رمزنگاری و اینکه الگوریتم مهاجم اساساً مساله‌ای در NP را حل می‌کند.
- بحث در مورد اهمیت کلاس مسائل به طور کاراً حل‌پذیر و اینکه مدل‌های مختلفی وجود دارند. نامناسب بودن کلاس P از دیدگاه رمزنگاری برای این منظور.
- تعریف کلاس‌های پیچیدگی تصادفی، بالاخص BPP. بحث در مورد مساله $\boldsymbol{NP - BPP \stackrel{?}{=} \emptyset}$ و ارتباط آن با مفهوم امنیت.
- قضیه PCP و سختی تقریب
- درختان تصمیم
- تحلیل چند سامانه رمزنگاری در مدل‌های مختلف حمله از این دیدگاه و ارائه تعرف دقیق Semantic Security. بحث در مورد ارتباط این مطلب با Indistinguishability .
- تعریف دقیق ماشین تورینگ اوراکل دار و چگونگی عملکرد آن. ارائه تعریف دقیق مدل Random Oracle و ارائه یک اثبات امنیت ساده در این مدل.

- بحث در مورد Interactive Proof Systems و قضایای اصلی مرتبط با آن‌ها، بالاخص بحث در مورد طرح اثبات $\boldsymbol{IP = PSpace = AM}$، اهمیت این قضیه و ارتباط با قضیه PCP.
- محاسبات کوانتمی

مراجع:

۱. Wegener, I., ۲۰۰۵. Complexity theory: exploring the limits of efficient algorithms. Springer Science & Business Media.

۲. S. Arora and B. Barak, *Computational Complexity: A Modern Approach*, Cambridge University Press, ۲۰۰۹.

عنوان درس	فارسی	جبر پیشرفته								
	انگلیسی	Advanced Algebra								
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی		تخصصی		اختیاری		۴	۶۴	ندارد
		نظری	عملی	نظری	عملی	نظری	عملی			
آموزش تکمیلی عملی:	دارد □ ندارد ■									
سفر علمی:	دارد □ ندارد ■									
کارگاه:	دارد □ ندارد ■									
آزمایشگاه:	دارد □ ندارد ■									
سمینار:	دارد □ ندارد ■									
حل تمرین: ندارد	نیاز به اجرای پروژه عملی: ندارد									

هدف درس: آشنایی دانشجویان با ساختارهای مهم جبری

سرفصل‌های درس:

- مفاهیمی از نظریه رسته ها: تعاریف رسته، ضرب و هم‌ضرب، شئی آزاد به همراه مثال در هر قسمت، ضرب و جمع مستقیم در رسته گروه‌ها، گروه‌های آزاد و مفاهیم ضرب آزاد و مولد و رابطه در آنها، گروه‌های آبلی آزاد
- مفاهیمی از نظریه مدول‌ها: تعریف مدول و مثال‌های متنوع ار آن، جمع و ضرب خانواده مدول‌ها، همریختی و خواص مرتبط در مدول ها، دنباله‌های دقیق و دنباله های دقیق شکافته شده و خواص آنها، مدول‌های آزاد، مدول‌های تصویری و خواص آن‌ها و بررسی وجود آن‌ها، مدول‌های انژکتیو و بررسی خواص آن‌ها (قضایای وجود مدول‌های انژکتیو به صورت مختصر ارائه شود)، ضرب تانسوری مدول‌ها
- مفاهیمی از نظری حلقه‌های جابجایی: شرط‌های زنجیری، حلقه و مدول های نوتری و آرتینی و قضایای اصلی آن‌ها، قضیه کرول، لم ناکایاما، قضیه پایه هیلبرت

مراجع:

۱. Thomas W. Hungerford, Algebra. Graduate Texts in Mathematics, ۷۳. *Springer-Verlag, New York-Berlin,* ۲۰۰۳.

۲. Serge Lang, Algebra. Revised third edition. Graduate Texts in Mathematics, ۲۱۱. *Springer-Verlag, New York,* ۲۰۰۲.

۳. Joseph J. Rotman, Advanced Modern Algebra. Part ۱. Third edition. Graduate Studies in Mathematics, ۱۶۵. *American Mathematical Society, Providence, RI,* ۲۰۱۵.

٤. Joseph J. Rotman, Advanced Modern Algebra. Part ۲. Third edition. With a foreword by Bruce Reznick. Graduate Studies in Mathematics, ۱۸۰. *American Mathematical Society, Providence, RI,* ۲۰۱۷.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="8">رمزنگاری ۲</td></tr>
<tr><td>انگلیسی</td><td colspan="8">Cryptography II</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="5">تعداد واحد</td><td colspan="2">تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td rowspan="2">پایه</td><td>اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td colspan="5" rowspan="2">۴</td><td colspan="2" rowspan="2">۶۴</td><td rowspan="9">رمزنگاری ۱</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="2">آموزش تکمیلی عملی:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سفر علمی:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">کارگاه:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">آزمایشگاه:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سمینار:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">حل تمرین: ندارد</td><td colspan="7">نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: معرفی و آشنایی با جنبه‌های مختلف از کاربرد رمزنگاری، مولدهای تصادفی و نقش حیاتی آنها در ایجاد امنیت، معرفی سیستم‌های رمزنگاری جدید، سیستم‌های رمزنگاری آینده و چالش‌های موجود

سرفصل‌های درس:

- تعریف دقیق اولیه های رمزنگاری به ویژه مولدهای شبه تصادفی، توابع یک طرفه، توابع چکیده ساز و ارائه قضایای اصلی
- تعریف دقیق طرح شناسایی و احراز اصالت، روش ساخت و اثبات امنیت.
- پرتکل دیفی- هلمن، الگوهای توزیع کلید
- مدل امنیت پاسخگویی تصادفی و تحلیلی آن
- تعریف دقیق توابع چکیده ساز، روش‌های ساخن و تحلیل آن‌ها
- الگوریتم های امضای رقمی با کلید عمومی، روش‌های طراحی و اثبات آنها
- آموزش حملات استاندارد نظیر حملات خطی، تفاضلی، جبری و نظایر آن بر روی یک سامانه ساده رمزنگاری (با انتخاب استاد)
- معرفی مفاهیم و اصول موضوعات پیشرفته‌تر در رمزنگاری با تاکید بر مثال، نظیر: اثبات‌های هیچ دانشی، رمزنگاری کوانتومی (معرفی محاسبات کوانتومی، محدودیت¬های کامپیوترهای کوانتومی و ...)، رمزنگاری مشبکه مبنا، رمزنگاری کدمبنا، رمزنگاری مبتنی بر خم بیضوی، رمزنگاری چکیده مبنا، رمزنگاری چند متغیره
- روش‌های شناسایی
- تبادیل کلید احراز اصالت شده
- محاسبات چند جانبه امن

مراجع:

۱- Katz, J. and Lindell, Y., ۲۰۲۱. Introduction to modern cryptography. CRC press.

۲- D.R. Stinson, Cryptography: Theory and Practice, Chapman & Hall / CRC; ۳nd edition, ۲۰۰٦.

۳- W. Mao, Modern Cryptography: Theory and Practice, Prentice Hall, ۲۰۰۳.

٤- A. Menezes , P. Oorschot , S Vanstone, Handbook of Applied Cryptography, CRC Press; ۱ edition, ۱۹۹٦.

٥- Bernstein Daniel J., Johannes Buchmann, Erik Dahmen: "Post-quantum Cryptography", Springer Verlag, ۲۰۰۹.

٦- Micciancio Daniele, Shafi Goldwasser: "Complexity of Lattice Problems: A Cryptographic Perspective", Springer Verlag, ۲۰۰۲.

۷- Steven D. Galbraith: "Mathematics of public key cryptography", Cambridge University Press, ۲۰۱۲.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="7">پنهان سازی اطلاعات</td></tr>
<tr><td>انگلیسی</td><td colspan="7">Information Hiding</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="5"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td rowspan="2">پایه</td><td>اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="9">نظریه اطلاع و کاربرد</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="8">آموزش تکمیلی عملی: دارد □ ندارد ■</td></tr>
<tr><td colspan="8">سفر علمی: دارد □ ندارد ■</td></tr>
<tr><td colspan="8">کارگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="8">آزمایشگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="8">سمینار: دارد □ ندارد ■</td></tr>
<tr><td colspan="8">حل تمرین: ندارد نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: آشنا سازی دانشجو با تکنیک‌ها و روش‌های پنهان سازی اطلاعات در داده‌ها و محتواها، همچنین معرفی بعضی از روش‌های نهان‌کاوی و معرفی آخرین روش‌های مورد استفاده در پنهان سازی اطلاعات.

سرفصل‌های درس:

- مبانی پنهان سازی اطلاعات (information hiding) و کاربردهای اصلی آن: نهان نگاری (steganography) و نشان‌گذاری (watermarking)
- بررسی ساختاری اطلاعات چندرسانه‌ای (ویدیو، تصویر ، صوت باند پهن و صحبت)
- تحلیل سیگنال‌های حامل (cover) و بررسی الگوریتمیک آن‌ها در محیط فشرده به منظور درج پیام (covert)
- مطالعه تحلیلی روش‌های پنهان سازی شامل نهان نگاری و نشان‌گذاری (مقاوم، شکننده و نیمه شکننده)
- شناسائی و تحلیل حملات عمدی و غیرعمدی در نشان‌گذاری
- نهان‌کاوی (Steganalysis) و معرفی بعضی از تکنیک‌های نهان‌کاوی مشهور نظیر ماشین‌های فراگیری و تحلیل‌های آماری
- آشکارسازی و استخراج پیام در نشان‌گذاری و نهان‌نگاری
- مطالعه اثر ویژگی‌های ادراکی انسان در پنهان سازی اطلاعات
- آخرین فنون نهان‌نگاری

مراجع:

۱- Wu, Z., ۲۰۱۴. Information Hiding in Speech Signals for Secure Communication. Syngress.

۲- Pan, J.S., Tsai, P.W. and Huang, H.C., ۲۰۲۰. Advances in intelligent information hiding and multimedia signal processing. Springer Singapore.

۳- S. Katzenbeisser, P. Fabien, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, ۲۰۰۰.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="8">نظریه اعداد محاسباتی</td></tr>
<tr><td>انگلیسی</td><td colspan="8">Computational Number Theory</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="6"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td rowspan="2">پایه</td><td>اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="8">نظریه اعداد،
برنامه‌سازی C</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="2">آموزش تکمیلی عملی:</td><td colspan="6">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سفر علمی:</td><td colspan="6">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">کارگاه:</td><td colspan="6">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">آزمایشگاه:</td><td colspan="6">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سمینار:</td><td colspan="6">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">حل تمرین: ندارد</td><td colspan="6">نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: آشنایی با روش‌های محاسباتی در نظریه اعداد با هدف تحلیل عددی و کاهش پیچیدگی محاسبات برای الگوریتم‌ها در نظریه اعداد که کاربردهای متعددی در رمزنگاری، علوم کامپیوتر و ... دارند.

سرفصل‌های درس:

- مروری کوتاه بر مقدمات نظریه اعداد و جبر چون قضیه باقیمانده چینی، قضیه کوچک فرما، تابع اویلر، دنباله Lucas، نماد Jacoby و ...
- مقدمه ای بر نظریه اعداد محاسباتی کوانتمی
- الگوریتم‌های کارای ضرب، جمع، تقسیم، توان رساندن و ... در حلقه‌های متناهی و الگوریتم‌ها مختلف پیمانه گرفتن چون Montgomery reduction، و Barrett reduction
- الگوریتم‌های غرباگری اعداد مرکب Table-Lookup، Bit-Array و Constructive Methods
- الگوریتم‌های آزمون اول بودن: آزمون‌های احتمالی Miller-Rabin، Solovay-Srassen، Ballie-PSW و آزمون قطعی Agrawal-Kayal-Saxena و مقایسه آنها از لحاظ پیچیدگی زمانی و حافظه مصرفی
- الگوریتم‌های تجزیه اعداد و مطالعه پیچیدگی محاسباتی آنها
- حساب منحنی Elliptic
- بکارگیری کتابخانه اعداد بزرگ زبان C++ برای پیاده‌سازی الگوریتم‌های ارائه شده در درس

مراجع:

۱- R. Crandall, C. Pomerance, Prime Numbers, A Computational Perspective, Springer, ۲۰۰۰.

۲- Victor Shoup, Computational Introduction to Number Theory.

۳- and Algebra, Cambridge University Press, ۲۰۰۵.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="7">پروتکل‌های رمزنگاری</td></tr>
<tr><td>انگلیسی</td><td colspan="7">Cryptographic Protocols</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="5"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td colspan="2">پایه</td><td colspan="2">اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="8">رمزنگاری ۱</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="3">آموزش تکمیلی عملی:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="3">سفر علمی:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="3">کارگاه:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="3">آزمایشگاه:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="3">سمینار:</td><td colspan="7">دارد □ ندارد ■</td></tr>
<tr><td colspan="3">حل تمرین: ندارد</td><td colspan="7">نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: در این درس پروتکل‌های امنیتی مختلف توصیف شده، همچنین حملات و دفاع‌های مختلف در مقابل آنها مطرح می‌گردد. پروتکل‌های مختلف مانند پروتکل‌های تصدیق اصالت و امضا، مدیریت حقوق دیجیتال، پروتکل‌های امنیتی در شبکه های توزیع شده، بدون سیم و باسیم، رای‌گیری الکترونیکی، پروتکل‌های پرداخت الکترونیکی، تکنیک‌های رمزنگاری بصری و ...

سرفصل‌های درس:

- مقدماتی بر پروتکل‌ها، پروتکل‌های امن و انواع آن، کلاس‌های حملات به پروتکل‌های امن و مدل‌های امنیتی، امضا و تصدیق اصالت و هویت، پروتکل‌ها و مکانیزم‌ها، مدیریت و برقراری کلید و گواهی)
- بلوک‌های سازنده پروتکل(تعریف پروتکل، ارتباط با استفاده از رمزنگاری متقارن، توابع یک طرفه، ارتباط با استفاده از رمزنگا نامتقارن، امضاهای دیجیتالی، چارچوبی برای مکانیزم‌های دیجیتالی، RSA و طرح‌های امضای مربوطه، طرح امضای فیات شامیر، DSA و طرح های امضای مربوطه، طرح های امضای دیجیتالی یکبار مصرف، طرح‌های امضای دیجیتالی حکم‌دار، طرح‌های امضای دیجیتالی کور، طرح‌های امضای دیجیتالی غیرقابل انکار، طرح‌های امضای رد-توقف)
- پروتکل‌های ساده (مبادله کلید، احراز اصالت، احراز اصالت و مبادله کلید، تحلیل فورمال مبادله کلید و احراز اصالت، رمزنگاری با کلید عمومی چندگانه، تقسیم راز، اشتراک راز، محافظت رمزنگارانه از پایگاه‌های داده.
- پروتکل‌های متوسط (سرویس‌های مهر زمانی، کانال نهان، امضای دیجیتالی غیرقابل انکار، امضای با تاکید کننده مشخص، امضاهای نیابتی، امضاهای گروهی، محاسبه با اطلاعات رمزشده، طرح‌های Bit Commitment، طرح‌های سکه اندازی عادلانه، پوکر ذهنی، جمع کننده های یک طرفه، افشای همه یا هیچ راز، برون سپاری کلید)
- پروتکل‌های پیشرفته (اثبات های هیچ دانشی، اثبات‌های هیچ دانشی هویت، امضاهای کور، رمزنگاری کلید عمومی مبتنی بر هویت، انتقال بی خبر، امضاهای بی خبر، امضای قرارداد توامان، نامه دیجیتالی سفارشی، مبادله همزمان رازها)

- پروتکل های خاص (انتخابات امن، محاسبات چندطرفه امن، پخش بدون نام پیام، اسکناس دیجیتال)
- مدیریت کلید (تولید کلید، فضای غیرخطی کلید، انتقال کلید، تایید کلید، استفاده از کلید، ذخیره کلید، تازه کردن کلید، ازبین بردن کلید، مدیریت کلیدهای عمومی)
- الگوریتم های مبادله کلید (طرح دیفی هلمن، پروتکل های ایستگاه به ایستگاه، پروتکل های شامیر، مبادله کلید رمزشده، توزیع کلید کنفرانس و پخش راز)
- طرح‌های شناسایی
- پروتکل‌ها خاص (انتخاب امن، محاسبات چند طرفه امن، پخش بدون نام پیام و اسکناس رقمی).

مراجع:

۱- Ramkumar, M., ۲۰۱٤. Symmetric Cryptographic Protocols. Springer.

۲- B.Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, ۱۹۹٦.

۳- P.Ryan, S.Schneider, M.Goldsmith, G.Lowe and B.Roscoe, modelling and Analysis of Security Protocols, Addison-Wesley, ۲۰۰۱.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="6">امنیت پایگاه داده</td></tr>
<tr><td>انگلیسی</td><td colspan="6">Database Security</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="4">تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td rowspan="2">پایه</td><td>اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۶۴</td><td rowspan="2">رمزنگاری ۱</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="2">آموزش تکمیلی عملی:</td><td colspan="4">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سفر علمی:</td><td colspan="4">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">کارگاه:</td><td colspan="4">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">آزمایشگاه:</td><td colspan="4">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سمینار:</td><td colspan="4">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">حل تمرین: ندارد</td><td colspan="4">نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: این درس به نکات منطقی در رابطه با امنیت پایگاه داده ها می‌پردازد. رویه های صحت و محرمانگی اطلاعات در زمینه پایگاه داده ها مرور شده و مدل سازی پایگاه های داده بررسی می شود. طراحی پایگاه داده امن، امنیت در پایگاه داده های آماری، رویکردهای امنیت برای پایگاه داده های شی گرا، و جمع آوری و استفاده از پایگاه داده های بازرسی همراه با تشخیص نفوذ مطرح می گردد.

سرفصل‌های درس:

- مقدمه ای بر پایگاه داده ها(مفاهیم،اجزا، معماری ها، انواع و ....)
- خواسته های امنیتی (یک‌پارچگی داده و صحت المان ها، قابلیت بازرسی، کنترل دست یابی، تصدیق اصالت کاربر، دسترس پذیری، قابلیت اعتماد)
- اطلاعات حساس (عوامل حساس سازی، تصمیم های مختلف در مورد دسترسی، دسترس پذیری داده ها، اطمینان از اصالت، انواع افشای اطلاعات)
- مدل‌های امنیتی
- کنترل دسترسی
- مساله استنتاج و کانال های نهان
- خط مشی باز در مقابل بسته
- کنترل دسترسیاختیاری در مقابل اجباری
- مدل‌های کنترل دسترسی اختیاری
- مدل‌های ماتریس مبنا

- مدل‌های گراف مبنا
- مدل‌های کنترل دسترسی اختیاری خاص پایگاه داده ها
- مدل‌های کنترل دسترسی اجباری
- مدل‌های حفظ محرمانگی
- مدل‌های حفظ صحت
- مدل‌های کنترل دسترسی چندسطحی
- معماری DBMS امن چند سطحی
- مدل‌های کنترل دسترسی نقش مبنا و انواع آنها
- امنیت در پایگاه داده آماری، تکنیک‌های مختلف
- مدل‌های امنیتی نسل‌های نو و بعدی پایگاه داده ها (کنترل دسترسی در پایگاه داده‌های شی گرا، مبتنی بر XML، آنتولوژی و ...)
- مدل‌های کنترل دسترسی قیدی و الزامی
- محصولات تجاری و پروتوتایپ های تحقیقاتی
- ارزیابی و تعبیر داده مطمئن
- مکانیزم ها و مدل های صحت
- بازرسی در پایگاه داده رابطه ای
- امنیت اراکل
- تشخیص نفوذ در پایگاه های داده
- امنیت پایگاه های داده در فضای ابری و فضای گرید
- امنیت داده ها در حالت داده های حجیم Big Data

مراجع:

۱- Mustafa, O. and Lockard, R.P., ۲۰۱۹. Oracle Database Application Security. Apress.

۲- Michael, G. and Sushil, J., ۲۰۱۰. Handbook of Database Security: Applications and Trends

.۳- M. Bishop, Computer Security: Art and Science, ۲nd ed: Addison-Wesley, ۲۰۰۳.

٤- R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based Access Control Models", IEEE Computer, vol. ۲۹, pp. ۳۸-٤۷, ۱۹۹٦.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="7">امنیت شبکه</td></tr>
<tr><td>انگلیسی</td><td colspan="7">Network Security</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="5"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td colspan="2">پایه</td><td colspan="2">اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="8">شبکه‌های کامپیوتری، رمزنگاری ۱</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="2">آموزش تکمیلی عملی:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سفر علمی:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">کارگاه:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">آزمایشگاه:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">سمینار:</td><td colspan="8">دارد □ ندارد ■</td></tr>
<tr><td colspan="2">حل تمرین: ندارد</td><td colspan="8">نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: این درس به ارائه مباحث مورد نیاز برای امنیت سیستم‌های کامپیوتری در شبکه ها می‌پردازد. در این درس سازوکارهای ایجاد محرمانگی، صحت و دسترس‌پذیری برای برقراری سرویس‌های مختلف امنیت شبکه مورد توجه قرار می‌گیرد.

سرفصل‌های درس:

- مقدمه‌ای بر مباحث شبکه
- تهدیدات امنیتی، انواع حملات و راههای مقابله با آنها (DOS، بدافزارها، ویروس‌ها، کرم‌ها، شبکه های بات، جاسوس افزارها، فیشینگ و . . .)
- معرفی اجمالی سیستم‌های رمزنگاری متقارن، نامتقارن، توابع چکیده ساز و ...
- امنیت لایه دسترسی به شبکه، سرویس‌های امنیتی ATM، پروتکل‌های PPP، PAP، CHAP، EAP، ECP و پرتکل‌های L۲TP
- امنیت لایه اینترنت، فیلترهای بسته، NAT، IPSec، VPN
- فایروال و اصول طراحی آن، نحوه قرار گیری در شبکه
- سیستم‌های تشخیص نفوذ، محل قرارگیری در شبکه، false positive/negative، NIDS وHIDS و ترکیب آنها، موتورهای همبستگی سنج
- امنیت لایه حمل، Socks V۵، SASL، ISAKMP
- امنیت لایه کاربرد،فیلترهای محتوی، مجوزدادن و کنترل دسترسی، امنیت پست الکترونیکی، امنیت وب، SSL، SET، امنیت جاوا، امنیت مدیریت شبکه و SNMP
- مونیتورینگ، مراکز مدیریت امنیت (SOC)
- گمنامی در شبکه

- پروتکل‌های امن درشبکه‌های کامپیوتری (رای گیری الکترونیکی، پرداخت الکترونیکی و ...)
- مفاهیم کلیدی فارنزیکس، مولفه‌ها و تکالیف
- امنیت شبکه های بی سیم، WPA/WEP
- امنیت VOIP
- طرح و معرفی مباحث جدید و به روز در زمینه امنیت شبکه
- امنیت اطلاعات برونسپاری شده
- امنیت در رایانش ابری

مراجع:

۱- Doherty, J., ۲۰۲۱. Wireless and mobile device security. Jones & Bartlett Learning.
۲- William Stallings, Cyptography & Network Security: principles and practice, ۵th ed., Pearson, ۲۰۱۱.
۳- B. Forouzan, Cyptography & Network Security, McGraw-Hill, ۲۰۰۸.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="5">روش‌های آماری در رمزنگاری</td></tr>
<tr><td>انگلیسی</td><td colspan="5">Statistical Methods in Cryptography</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="3">تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td rowspan="2">پایه</td><td rowspan="2">اصلی</td><td rowspan="2">تخصصی</td><td rowspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="8">رمزنگاری ۱</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="6">آموزش تکمیلی عملی: دارد □ ندارد ■</td></tr>
<tr><td colspan="6">سفر علمی: دارد □ ندارد ■</td></tr>
<tr><td colspan="6">کارگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="6">آزمایشگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="6">سمینار: دارد □ ندارد ■</td></tr>
<tr><td colspan="6">حل تمرین: ندارد نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: هدف اصلی این درس آشنایی دانشجو با تکنیک‌ها و ابزار موجود در علم آمار برای تحزیه و تحلیل سامانه‌های رمزنگاری است.

سرفصل‌های درس:

- یادآوری اصول اولیه آمار و احتمال بالاخص احتمال شرطی و قانون بیز.
- مولدهای شبه تصادفی و پیاده‌سازی آن‌ها. تحلیل آماری این مولدها. اصول طراحی تست‌های آماری و مسائل مرتبط. جهانی بودن Next Bit Test. تست‌های NIST و تست‌های آماری پیشرفته‌تر.
- استفاده از روش‌های بیزی در تجزیه و تحلیل سامانه‌های رمز. ارائه چند مثال در تحلیل و حمله (با نظر استاد). تأکید بر حمله‌های خطی و دیفرانسیلی از این دیدگاه.
- ارائه اصول طراحی مدل‌های گرافیک، بالاخص روش HMM و مدل‌های پیشرفته‌تر. اصول نظری مرتبط و چگونگی نگرش و به کارگیری این مدل‌ها به عنوان مسائل بهینه سازی پیچیده. بررسی کارآیی و پیاده‌سازی با ارائه چند مثال (با نظر استاد).

مراجع:

١- Neuenschwander, D., ٢٠٠٤. Probabilistic and statistical methods in cryptology: an introduction by selected topics (Vol. ٣٠٢٨). Springer Science & Business Media.

٢- Kiayias, A., Kohlweiss, M., Wallden, P. and Zikas, V., ٢٠٢٠. Public-Key Cryptography-PKC ٢٠٢٠. Springer International Publishing.

٣- D. Koller and N. Friedman, Probabilistic Graphical Models: Principles and Techniques, MIT Press, ٢٠٠٩.

٤- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press ١٩٩٦.

٥- S. Murphy, F. Piper, M. Walker, P. Wild, Likelihood Estimation for Block Cipher Keys, Technical Report, RHUL, ١٩٩٥.

٦- D. Neuenschwander, Probabilistic and Statistical Methods in Cryptology, LNCS ٣٠٢٨, Springer ٢٠٠٤.

٧- H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, SIAM, ١٩٩٢.

٨- M. Stamp, R.M. Low, Applied Cryptanalysis: Breaking Ciphers in the Real World, John Wiley and Sons Inc, ٢٠٠٧.

عنوان درس	فارسی	روش‌های صوری در رمزنگاری										
	انگلیسی	Formal Methods in Cryptography										
نوع واحد									تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی			تخصصی			اختیاری				
نظری	عملی	نظری	عملی		نظری	عملی		نظری	عملی	۴	۶۴	رمزنگاری ۱
آموزش تکمیلی عملی:		دارد □		ندارد ■								
سفر علمی:		دارد □		ندارد ■								
کارگاه:		دارد □		ندارد ■								
آزمایشگاه:		دارد □		ندارد ■								
سمینار:		دارد □		ندارد ■								
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد										

هدف درس: استفاده از روش‌های صوری در مدل سازی و تحلیل پروتکل‌ها و الگوریتم‌های رمزنگاری

سرفصل‌های درس:

- نظریه مجموعه ها و منطق از مرجع [۱]
- سه روش صوری اصلی
- وارسی‌گر مدل (چون ابزار Scyther) از مرجع [۲]
- درستی‌یابی خودکار (چون منطق BAN)از مرجع [۳]
- جبر پردازه‌ای از مرجع [۴]
- مدلسازی (description) چند پروتکل معروف امنیت و توزیع کلید (چون دیفی-هلمن) به وسیله یکی از روشهای صوری سه‌گانه معرفی شده در درس
- توصیف (specification) چندتا از خواص عمده امنیت چون احراز اصالت، محرمانگی، کنترل دسترسی، گمنامی، عدم انکار با یکی از روشهای صوری سه گانه معرفی شده در درس
- درستی‌یابی (verification) خواص امنیت توصیف شده برای پروتکل‌های مدل‌سازی شده

مراجع:

۱- Michael Huth and Mark Ryan, Logic in Computer Science modeling and reasoning about systems, Cambirdge University Press, ۲۰۰٤.
۲- C. Cremers, S. Mauw, Operational Semantics and Verification of Security Protocols, Springer, ۲۰۱۲.
۳- G. Bella, Formal Correctness of Security Protocols, Springer, ۲۰۰۷.
٤- Wan Fokkink, Introduction to Process Algebra, Springer, ۲۰۰۷.

عنوان درس	فارسی	کدگذاری ۲										
	انگلیسی	Coding II										
نوع واحد									تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری			۴	۶۴	کدگذاری ۱	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی					
آموزش تکمیلی عملی:		دارد □		ندارد ■								
سفر علمی:		دارد □		ندارد ■								
کارگاه:		دارد □		ندارد ■								
آزمایشگاه:		دارد □		ندارد ■								
سمینار:		دارد □		ندارد ■								
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد										

هدف درس: ارائه مفاهیم پیشرفته در نظریه کدگذاری نظیر بررسی و تحلیل پارامترهای ریاضی و کلیدی کدها، تکنیک‌های کدگشایی و کدگذاری کدهای جدید و بررسی خواص آنها، معرفی آخرین دستاوردها در خصوص کدهای جدید و بررسی خواص آنها.

سرفصل‌های درس:

- کدهای ساخته شده با هندسه متناهی و کدهای Majority-Logic decodable
- کدهای روی Zm (مطالعه موردی برای Z_4) معرفی کدهای دارای ساختار هندسه جبری (خواص و پارامترها)
- کدهای تصحیح کننده خطای پاک کننده کپه ای
- کدهای پیچشی و انواع و روشهای ساخت
- کدگذاری کدهای پیچشی
- کانالهای خطای پاک کننده کپه ای
- ارائه یک نوع روش کدگشایی (به عنوان مثال، روشهای کدگشای داربست-مبنا و الگوریتم ویتربی)
- کدهای توربو انواع و روشهای ساخت و معرفی جایگشت دهندها
- ارائه یک نمونه الگوریتم کدگشای مشهور برای این دسته از کدها
- تحلیل کارایی کدهای توربو
- کدهای LDPC
- کدگذاری کدهای LDPC و QC-LDPC
- انواع و روشهای ساخت دارای ساختار منظم و نامنظم، دوری، شبه دوری و دودویی و غیر دودویی (با استفاده از ماتریسهای جایگشت گردشی، با استفاده از طرحهای ترکیبیاتی، با استفاده از هندسه متناهی، پورتوگرافها (گراف های پایه) و PEG، و شبه تصادفی مک کی ..) گلاگر.

- ارائه دو نمونه الگوریتم کدگشای تکراری تصمیم سخت و نرم (الگوریتم جمع-ضرب یا کمینه-جمع و Bit flipping) برای این دسته از کدها در حالت دودویی, توانایی درک کدگشایی کدهای LDPC بر روی سه کانال BSC ، BEC و AWGN .
- تحلیل کارایی کدهای LDPC
- تکامل چگالی Density evolution
- خواص کدهای ساخته شده و تحلیل کارایی آنها
- الحاق کدها، ضرب کدها،بر هم نهش کدها (Superposition) ، و ... با استفاده از کدهای توصیف شده بندهای فوق (پیچشی، توربویی LDPC نحوه کدگشایی مزایا و معایب
- کدهای مبتنی بر گراف گسترنده (Expander)
- معرفی کدهای قطبی ، کدهای جدید (رپتور، فوارهای و ....)،
- معرفی مقدماتی از کدگذاری شبکه، کدهای جدید

مراجع:

١- T. Richardson, R. Urbanke, Modern Coding Theory, Cambridge University Press, ٢٠٠٨.
٢- S. Lin, D.J. Costello, Error Control Coding, ٢٠٠٤.
٣- J.H Van Lit, Introduction to Coding Theory (Graduate Texts in Mathematics), Springer, ١٩٩٨.
٤- W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge, ٢٠٠٣.
٥- Handbook of Coding Theory, Volume I, Volume II, North Holland; ١ edition, ١٩٩٨.
٦- William E. Rayan and Shu Lin, Channel Codes, Classical and Modern, Cambridge University Press, ٢٠٠٩.
٧- Kelbert, M. and Suhov, Y., Information theory and coding by example. Cambridge University Press, ٢٠١٣
٨- Berlekamp, E.R., Algebraic coding theory (revised edition). World Scientific و٢٠١٥.
٩- Zamir, R., Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory. Cambridge University Press, ٢٠١٤.

عنوان درس	فارسی	کدگذاری شبکه									
	انگلیسی	Network Coding									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۴	۶۴	کدگذاری۱	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
آموزش تکمیلی عملی:		دارد □		ندارد ■							
سفر علمی:		دارد □		ندارد ■							
کارگاه:		دارد □		ندارد ■							
آزمایشگاه:		دارد □		ندارد ■							
سمینار:		دارد □		ندارد ■							
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد									

هدف درس: هدف این است که دانشجو به توان تحلیل شبکه و کدگذاری آن دست یابد و بتواند با توجه به کاربرد زیادی که کدگذاری شبکه در مسائل اقتصادی، طراحی ارتباط همتا-به-همتا، شبکه‌های بیسیم و ... دارد دانش و توان علمی خود را مورد استفاده قرار دهد.

سرفصل‌های درس:

- تعریف و مقدمات ریاضی مورد نیاز، شبکه پروانه‌ای، ارتباطات بیسیم و ماهواره‌ای، شبکه‌های ارتباطی نقطه به نقطه، کران برای بیشترین جریان
- کدگذاری شبکه برای شبکه‌های منبع منفرد چند-پخشی، مدل شبکه‌های ارتباطی، شبکه‌های غیردوری، تعریف کدهای شبکه، نظریه کدگذاری برای شبکه‌های منبع منفرد چند-پخشی، بهره (gain)کدگذاری شبکه برای شبکه های ترکیبی
- کدگذاری شبکه به‌صورت خطی، تعاریف کدهای شبکه خطی، قضیه Koetter و Medart برای کدهای شبکه خطی، خواص مطلوب برای کدهای شبکه خطی
- تکنیک‌های کدگذاری شبکه، کدگذاری متمرکز (localized)، کدگذاری تصادفی
- کدگذاری شبکه منبع-منفرد به‌صورت خطی، شبکه‌های دوری، شبکه‌های دوری بدون تاخیر، کدهای پیچشی (convolutional) شبکه، کدگذاری و کدگشایی
- معرفی مفهوم کدگذاری کوانتومی شبکه

مراجع:

۱- Shang, T. and Liu, J., Secure Quantum Network Coding Theory. Berlin: Springer, ۲۰۲۰.
۲- Al-Kofahi, O.M. and Kamal, A.E., Resilient Wireless Sensor Networks: The Case of Network Coding. Springer International Publishing, ۲۰۱۵.
۳- Médard, M. and Sprintson, A., Network Coding: Fundamentals and Applications, ser. ۲۰۱۲.
٤- Fragouli, C. and Soljanin, E., Network coding applications. now Publishers Inc, ۲۰۰۸.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="6">کدگذاری فضا- زمان</td></tr>
<tr><td>انگلیسی</td><td colspan="6">Space-Time Coding</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="4"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td colspan="2">پایه</td><td colspan="2">اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="8">کدگذاری۱</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="10">آموزش تکمیلی عملی: دارد □ ندارد ■</td></tr>
<tr><td colspan="10">سفر علمی: دارد □ ندارد ■</td></tr>
<tr><td colspan="10">کارگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="10">آزمایشگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="10">سمینار: دارد □ ندارد ■</td></tr>
<tr><td colspan="10">حل تمرین: ندارد نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: مطالعات بنیادی درخصوص ظرفیت کانال های MIMO۱ برای مخابرات بدون سیم و دست یابی به حداکثر کارایی پیش بینی شده توسط نظریه‌های مختلف ریاضی. معرفی مفاهیم آنتن های انتقال/دریافت چندگانه، معرفی فنون کدگذاری فضا-زمان، مطالعه فنون آنالیز کدهای فضا-زمان و معرفی الگوریتم های مختلف کدگشا برای کدهای فضا-زمان

سرفصل‌های درس:

- مرور دوره
- معرفی کانال های بی سیم
- ظرفیت کانال های MIMO
- محک طراحی کد فضا-زمان
- کدهای بلوکی متعامد فضا-زمان
- کدهای بلوکی شبه متعامد فضا-زمان
- کدهای ترلیس۲ فضا زمان و انواع آن
- کدگشایی کدهای فضا-زمان
- مدلولاسیون مختلف فضا-زمان
- روش های مختلف تشخیص برای آنتن های چندگانه
- روش ها و فنون جدید و به روز دنیا درخصوص کدهای فضا-زمان

---

۱ Multiple-Input Multiple-Output (MIMO)

۲ Trellis

- کدهای پیچشی، توربو و LDPC و .... و کاربرد آنها در کدهای فضا-زمان
- سایر مفاهیم جدید در کدهای فضا-زمان

مراجع:

۱- H. Jafarkhan, Space-Time Coding: Theory and Practice Cambridge University Press, ۲۰۰۵.

۲- Branka Vucetic, Jinhong Yuan, Space-Time Coding, John Wiley, ۲۰۰۳.

عنوان درس	فارسی	کدگذاری منبع									
	انگلیسی	Source Coding									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۴	۶۴	نظریه اطلاع و کاربرد	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
آموزش تکمیلی عملی:		دارد □		ندارد ■							
سفر علمی:		دارد □		ندارد ■							
کارگاه:		دارد □		ندارد ■							
آزمایشگاه:		دارد □		ندارد ■							
سمینار:		دارد □		ندارد ■							
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد									

هدف درس: فناوری های دیجیتال کنونی به مرحله ای از رشد رسیده اند که به خلق، تبادل و مصرف اطلاعات می‌پردازند. این دامنه وسیع استفاده از داده و اطلاعات، پهنای باند مورد استفاده در ارتباطات را با مسائل جدی روبرو نموده است و هسته اصلی این فناوری ها برای مدیریت داده، اطلاعات و نرخ آن روش های کدگذاری منبع است که موضوع این سرفصل درسی است. مبتنی بر اصول نظریه اطلاع و نرخ اعوجاج۳ مواردی نظیر کدگذاری آنتروپی، تدریج۴، کدگذاری تبدیل۵ و کدگذاری پیشگویانه۶ در این درس مورد توجه قرار خواهند گرفت. همچنین الگوریتم های کدگذاری صوت و ویدئو بررسی و مطالعه خواند شد.

سرفصل‌های درس:

- مقدماتی بر نظریه اطلاع، آنتروپی، نامساوی کرفت، آنتروپی نسبی،شرطی، نرخ افزونگی، اطلاعات متقابل و ..
- کدکذاری بدون اتلاف، کدهای نامنطبق: شانون، هافمن، کدهای حسابی. کدهای فراگیر و منطبق. کدهای Ziv-Lempel.
- نظریه نرخ-اعوجاج، تابع نرخ-اعوجاج، کران پایین شانون، توزیع نرخ روی متغیرهای مستقل، معکوس آبشار، الگوریتم بالاهوت
- کوانتیزاسیون نرخ-بالا، تدریج Constrained-resolution و constrained-entropy. تدریج بردار در مقابل اسکالر. Practical high-rate-theory-based quantizers
- تدریج نرخ-پایین، الگوریتم Lloyd training (k-means) برای حالت های constrained-resolution و constrained-entropy. تدریج برداری دارای ساختار و انواع آن، روش های جستجوی سریع

---

۳ Distortion
۴ Quantization
۵ Transform
۶ Predictive

- بانک های تبدیل و فیلتر
- پیشگویی خطی

مراجع:

۱- T. Wiegand and H. Schwarz, Source Coding: Part I of Fundamentals of Source and Video Coding, Now Publishers, ۲۰۱۱.
۲- T.M. Cover and J.A. Thomas: Elements of Information Theory, ۲nd Edition, John Wiley & Sons, NJ, ۲۰۰٦.
۳- R.M. Gray: Source Coding Theory, Springer, ۱۹۸۹.
٤- Le Ruyet, D. and Pischella, M., Digital communications ۱: source and channel coding (Vol. ۱). John Wiley & Sons, ۲۰۱٥.
٥- Safieh, M., Algorithms and architectures for cryptography and source coding in non-volatile flash memories. Springer Nature, ۲۰۲۱.

عنوان درس	فارسی	نظریه اطلاع و کدگذاری کوانتومی									
	انگلیسی	Information Theory and Quantum Coding									
نوع واحد					تعداد واحد	تعداد ساعت	دروس پیش‌نیاز				
پایه	اصلی				تخصصی			اختیاری		۴	۶۴	کدگذاری ۱
	نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
آموزش تکمیلی عملی:	دارد □ ندارد ■											
سفر علمی:	دارد □ ندارد ■											
کارگاه:	دارد □ ندارد ■											
آزمایشگاه:	دارد □ ندارد ■											
سمینار:	دارد □ ندارد ■											
حل تمرین: ندارد	نیاز به اجرای پروژه عملی: ندارد											

هدف درس: دانشجو در این درس با مکانیزم‌های کوانتومی، الگوریتم‌های کوانتومی و کدهای تصحیح کننده خطای کوانتومی آشنا می‌شود.

سرفصل‌های درس:

- مرور جبرخطی و نماد دیراک (ضرب داخلی فضاها، ماتریس‌های نرمال، ضرب تنسوری فضاهای برداری، تجزیه مقدار تکین، تجزیه اشمیت و ...)
- فرض‌های مکانیزم‌های کوانتوم (فضای حالت، تکامل یکتایی، اندازه‌گیری، ماتریس‌های چگالی، رد جزئی)
- اصل عدم قطعیت هایزنبرگ، پارادوکس ERP و نامساوی‌های بل
- بعضی از پروتکل‌ها و و الگوریتم‌ها شامل کدگذاری فوق چگال، teleportation، الگوریتم Duetsch-Jozsa، الگوریتم تجزیه شور، الگوریتم گرورز، پروتکل توزیع کلید BB۸٤
- فاصله ها روی فضاهای حالت
- نقشه‌های کوانتوم (نقشه‌های حفاظت-رد به طور کامل مثبت، بازنمایش Kraus، بازنمایش Choi-Jamiolkowski)
- نظریه تصحیح خطای کوانتومی کدها و محاسبه کوانتومی (کد شور، قضیه Knill-Laflame، کدهای CSS،کدهای پایدارساز)

مراجع:

۱- Michael A. Nielsen, Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, ۲۰۱۱.

۲- *Ivan Djordjevic*, Quantum Information Processing and Quantum Error Correction, Academic Press, ۲۰۱۲.

۳- Wilde, M.M., Quantum information theory. Cambridge University Press, ۲۰۱۳.

٤- Hayashi, M., Quantum information theory. New York: Springer, ۲۰۱٦.

٥- Shang, T. and Liu, J., Secure Quantum Network Coding Theory. Berlin: Springer, ۲۰۲۰.

عنوان درس	فارسی	کدهای حلقه مبنا									
	انگلیسی	Coding based on the Rings									
نوع واحد						تعداد واحد	تعداد ساعت	دروس پیش‌نیاز			
پایه		اصلی		تخصصی		اختیاری		۴	۶۴	مبانی جبر (کارشناسی)، کدگذاری ۱	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
آموزش تکمیلی عملی:		دارد □		ندارد ■							
سفر علمی:		دارد □		ندارد ■							
کارگاه:		دارد □		ندارد ■							
آزمایشگاه:		دارد □		ندارد ■							
سمینار:		دارد □		ندارد ■							
حل تمرین: ندارد		نیاز به اجرای پروژه عملی: ندارد									

هدف درس: شاخه جدیدی از نظریه کدگذاری در زمینه ساخت کدهای خطی رو حلقه‌های متناهی ایجاد شده است که هدف این درس آشنایی دانشجو با نظریه های جدید این حوزه است.

سرفصل‌های درس:

- حلقه چندجمله‌ای‌ها و الگوریتم تقسیم اقلیدس
- تجزیه چندجمله‌ای‌ها روی میدان‌های متناهی و خواص چندجمله‌ای‌ها نظیر تحویل ناپذیری، ارائه محک‌های بررسی تحویل ناپذیری، بررسی وجود ریشه و ...
- لم هنسل و قضیه ترفیع هنسل۷
- حلقه‌های گالوا شامل ارائه مثال‌هایی از حلقه‌های گالوا، ارائه ساختار و بررسی قضایای کلیدی، بررسی شباهت‌های میان حلقه‌های گالوا و میدان‌های گالوا و ...
- معرفی حلقه‌هایی که شرایط طراحی کد روی آنها وجود دارد نظیر حلقه‌های آرتینی و نوتری، حلقه‌های فروبنیوس، حلقه‌های زنجیری۸ و ... (اختیاری)
- کدهای خطی روی $\mathbb{Z}_4$ و ارائه ماتریس مولد
- چندجمله‌ای‌های شمارنده وزن، تعریف تابع وزن روی یک حلقه و ارائه وزن‌های مختلفی که روی کدهای حلقه مبنا تعریف می‌شود نظیر وزن همینگ، وزن لی و ...

Hensel Lift
Chain ring

- معرفی نگاشت گری[۹] که رابطه میان کدهای حلقه مبنا و کدهای مبتنی بر میدان‌ها را بیان می‌کند.
- کدهای دوری روی حلقه‌ها و بررسی رده‌های خاص نظیر کدهای کردوک و پریپرتا و تعمیم‌های آنها
- ارتباط میان کدهای چهارتایی[۱۰] و مشبکه‌ها، بررسی کدهای چهارتایی خود دوگان و ارائه چندجمله‌ای شمارنده وزن برای آنها (اختیاری)
- ارائه کدهای مبتنی بر حلقه‌های فروبنیوس و حلقه‌های زنجیری

مراجع:

۱- Zhe-Xian Wan, Quaternary Codes, Series On Applied Mathematics, World Scientific Pub Co Inc, ۱۹۹۷.

۲- Zhe-Xian Wan, Lectures on finite fields and Galois rings, World Scientific Pub Co Inc, ۲۰۰۳

۳- Bernard R. McDonald, Finite Rings with Identity, Pure and Applied Mathematics, a series of monograph and textbooks, ۱۹۷٤.

[۹] Gray isometry
[۱۰] Quaternary Codes

عنوان درس	فارسی	الگوریتم‌های کدگشایی تکراری								
	انگلیسی	Iterative Decoding Algorithms								
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز
پایه		اصلی		تخصصی		اختیاری		۴	۶۴	کدگذاری ۲
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی			
آموزش تکمیلی عملی:	دارد □ ندارد ■									
سفر علمی:	دارد □ ندارد ■									
کارگاه:	دارد □ ندارد ■									
آزمایشگاه:	دارد □ ندارد ■									
سمینار:	دارد □ ندارد ■									
حل تمرین: ندارد	نیاز به اجرای پروژه عملی: ندارد									

هدف درس: این درس به بررسی و تحلیل الگوریتم‌های کدگشایی کدهای خطی می‌پردازد که برای کدگشایی از روش‌های تکراری و گراف‌ها بهره می‌برند. این رده از کدها از جدیدترین خانواده‌های کدها بوده و دارای کاربردهای فراوانی در سیستم‌های مخابراتی فعلی هستند.

سرفصل‌های درس:

- مقدمه‌ای بر کدها، کانال‌ها، ظرفیت و مفاهیم گرافی مورد نیاز (آنتروپی، ظرفیت، انواع کانال، کدها و کدگشایی و اندازه گیری کارایی)
- کدهای LDPC
  - معرفی مختصر (روش های ساخت دارای ساختار، شبه تصادفی)
  - کدگذاری (اختیاری)
  - کدگشایی (انواع روش های تکراری نرم و سخت برای کدهای دودویی و غیر دودویی و برای انواع کانال های مخابراتی)، بررسی پیچیدگی محاسباتی
  - معرفی مجموعه های ترکیبیاتی اثر گذار بر کدگشایی تکراری، کمرگراف، دور در گراف
  - تحلیل نمودارهای کارایی،
  - معرفی کدهای خوب LDPC و قواعد تولید آنها مبتنی بر نتایج کدگشایی
- کدهای پیچشی
  - معرفی مختصر و نحوه ساخت
  - کدگذاری کدهای پیچشی (اختیاری)

- کدگشایی BCJR ، کدگشایی Log MAP، Viterbi برای انواع کانال های مخابراتی، بررسی پیچیدگی محاسباتی

- کدهای توربو
  - معرفی مختصر و نحوه ساخت
  - کدگذاری کدهای توربو (اختیاری)
  - کدگشایی کدهای توربو برای انواع کانال های مخابراتی، بررسی پیچیدگی محاسباتی
- الحاق سریالی و کدهای RA
  - الحاق سریالی کدهای توربو
  - کدهای Repeat–accumulate(RA)
  - کدگذاری کدهای RA (اختیاری)
  - کدگشایی کدهای RA
  - طراحی کد
- نمودارهای EXIT
  - نمودارهای EXIT برای کدهای توربو (اختیاری)
  - نمودارهای EXIT برای کدهای RA (اختیاری)
  - نمودارهای EXIT برای کدهای LDPC
  - طراحی و آنالیز کد بر اساس نمودارهای EXIT
- تحلیل خطای کف
  - معرفی
  - تحلیل بیشترین درست نمایی
  - تحلیل خطای کف برای کدهای LDPC
  - ملاک ها و معیارهای طراحی کدها برای غلبه بر خطای کف و پارامترهای موثر

مراجع:

۱- S.B. Wicker, S. Kim, FUNDAMENTALS OF CODES, GRAPHS, AND ITERATIVE DECODING, Kluwer Academic Publishers, ۲۰۰۳.

۲- S. J. JOHNSON, Iterative Error Correction Turbo, Low-Density Parity-Check and Repeat–Accumulate Codes, Cambridge University Press, ۲۰۱۰.

۳- T. Richardson , R. Urbane, *Modern Coding Theory*, Cambridge University Press, ۲۰۰۸.

٤- S. Lin, D.J. Costello, *Error Control Coding*, Pearson-Prentice Hall, ۲۰۰٤.

٥- *Handbook of Coding Theory*, *Volume I*, *Volume II*, North Holland; ۱ edition, ۱۹۹۸.

٦- William E. Rayan and Shu Lin, Channel Codes, Classical and Modern , Cambridge University Press, ۲۰۰۹.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="8">مباحث ویژه در رمزنگاری</td></tr>
<tr><td>انگلیسی</td><td colspan="8">Special Topics in Cryptography</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="6"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td rowspan="2">پایه</td><td>اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="9">اجازه گروه</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="9">آموزش تکمیلی عملی: دارد □ ندارد ■</td></tr>
<tr><td colspan="9">سفر علمی: دارد □ ندارد ■</td></tr>
<tr><td colspan="9">کارگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="9">آزمایشگاه: دارد □ ندارد ■</td></tr>
<tr><td colspan="9">سمینار: دارد □ ندارد ■</td></tr>
<tr><td colspan="9">حل تمرین: ندارد نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

درسی است در سطح کارشناسی ارشد یا بالاتر در زمینه رمز نگاری که سرفصل و ریز موارد درسی مربوطه قبل از ارائه بایستی به تصویب شورای تحصیلات تکمیلی گروه یا دانشکده برسد. این درس در نوبت بعدی می تواند با سرفصل تصویب شده قبلی ارایه گردد و یا سرفصل جدید باشد که مجددا باید بایستی به تصویب شورای تحصیلات تکمیلی گروه یا دانشکده برسد.

عنوان درس	فارسی	مباحث ویژه در کدگذاری								
	انگلیسی	Special Topics in Coding								
نوع واحد							تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری				
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی	۴	۶۴	
آموزش تکمیلی عملی:	دارد □ ندارد ■									
سفر علمی:	دارد □ ندارد ■									
کارگاه:	دارد □ ندارد ■									
آزمایشگاه:	دارد □ ندارد ■									
سمینار:	دارد □ ندارد ■									
حل تمرین: ندارد	نیاز به اجرای پروژه عملی: ندارد									

درسی است در سطح کارشناسی ارشد یا بالاتر در زمینه کدگذاری که سرفصل و ریز موارد درسی مربوطه قبل از ارائه بایستی به تصویب شورای تحصیلات تکمیلی گروه یا دانشکده برسد. این درس در نوبت بعدی می تواند با سرفصل تصویب شده قبلی ارایه گردد و یا سرفصل جدید باشد که مجددا باید بایستی به تصویب شورای تحصیلات تکمیلی گروه یا دانشکده برسد.

<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="7">کدشبکه خطی تصحیح کننده خطا</td></tr>
<tr><td>انگلیسی</td><td colspan="7">Linear Error Correcting Network Codes</td></tr>
<tr><td colspan="2">نوع واحد</td><td colspan="6"></td><td>تعداد واحد</td><td>تعداد ساعت</td><td>دروس پیش‌نیاز</td></tr>
<tr><td colspan="2">پایه</td><td colspan="2">اصلی</td><td colspan="2">تخصصی</td><td colspan="2">اختیاری</td><td rowspan="2">۴</td><td rowspan="2">۶۴</td><td rowspan="8">کدگذاری شبکه</td></tr>
<tr><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td><td>نظری</td><td>عملی</td></tr>
<tr><td colspan="8">آموزش تکمیلی عملی:</td><td colspan="2">دارد □ ندارد ■</td></tr>
<tr><td colspan="8">سفر علمی:</td><td colspan="2">دارد □ ندارد ■</td></tr>
<tr><td colspan="8">کارگاه:</td><td colspan="2">دارد □ ندارد ■</td></tr>
<tr><td colspan="8">آزمایشگاه:</td><td colspan="2">دارد □ ندارد ■</td></tr>
<tr><td colspan="8">سمینار:</td><td colspan="2">دارد □ ندارد ■</td></tr>
<tr><td colspan="10">حل تمرین: ندارد نیاز به اجرای پروژه عملی: ندارد</td></tr>
</table>

هدف درس: با توجه به اینکه در بسیاری از موارد کاربردی کانال های یک شبکه ارتباطی خطا دار هستند لازم است در طراحی کد های مورد نیاز در شبکه به قابلیت تصحیح خطای کد نیز توجه نمود و از این جهت طراحی کدهای با قابلیت تصحیح خطا اجتناب ناپذیر است.

سرفصل‌های درس:

- مدل شبکه تصحیح خطا
- وزن و فاصله، توانایی کشف تصحیح و تصحیح خطا
- توصیف موضعی کدشبکه تصحیح خطا، وزن و فاصله، کدگشایی
- کران همینگ، کران یکانی و کدهای MDS
- ساخت کدهای MDS
- کدشبکه‌های تصادفی تصحیح خطا

مراجع:

۱- Xuan Guang and Zhen Zhang, Linear Network Error Correction Cod ۲۰۰۸.

۲- S. Lin, D.J. Costello, *Error Control Coding*, Pearson-Prentice Hall, ۲۰۰٤.

۳- *Handbook of Coding Theory*, *Volume I, Volume II*, North Holland; ۱ edition, ۱۹۹۸.

۴- William E. Rayan and Shu Lin, Channel Codes, Classical and Modern , Cambridge University Press, ۲۰۰


وزارت علوم، تحقیقات و فناوری
شورای عالی برنامه ریزی و آموزشی