



بسمه تعالی
دانشگاه جامع انقلاب اسلامی
معاونت آموزش

کاربرگ طرح درس: رمزنگاری، امنیت اطلاعات و حریم خصوصی

استاد: دکتر سیدعلی لاجوردی

مقطع: ارشد

تعداد واحد: ۳

رشته: شبکه

اهداف کلی				
آشنایی با اصول رمزنگاری آشنایی با الگوریتم ها و دستورالعمل های رمزنگاری و تنظیمات آن چگونگی ایجاد ارتباط ایمن در محیط ناامن آشنایی با اصول حریم خصوصی و قوانین مرتبط				
جلسه	موضوع کلی	موضوع جزئی	اهداف جزئی	تکالیف دانشجو در این جلسه توضیحات
1	معرفی درس و استاد			
2	مقدمه	آشنایی اولیه با رمزنگاری	آشنایی با رمزنگاری قدیمی و جدید	فصل ۱ (یک نفر) *
3	رمزنگاری	تئوری شانون و محدودیت ها	آشنایی با چگونگی الگوریتم رمزنگاری	فصل ۲ (یک نفر) *
4	کلید خصوصی	رمزنگاری مبتنی بر کلید خصوصی	آشنایی با چگونگی ایجاد کلید خصوصی	فصل ۳ (دو نفر)
5	احراز هویت	احراز هویت پیام و الگوریتم CBC	آشنایی با احراز هویت امن و تئوری MAC	فصل ۴ (دو نفر)
6	رمزنگاری احراز هویت	حمله CCA و روش مقابله	آشنایی با الگوریتم های رمزنگاری احراز هویت	فصل ۵ (یک نفر) *

7	توابع هش	توابع هش و کاربرد آن	آشنایی با انواع توابع هش (درهم ساز) و کاربرد آن در امنیت	حل تمرین و ارائه کلاسی	فصل ۶ (دو نفر)
8	رمزنگاری متقارن ۱	الگوریتم ساختار متقارن و ساختار آن	آشنایی با ساختار کلید متقارن و الگوریتم های آن	حل تمرین و ارائه کلاسی	فصل ۷ (دو نفر)
9	رمزنگاری متقارن ۲	تئوری ساختار متقارن و توابع	آشنایی با پایه های نظری ساختار کلید متقارن	حل تمرین و ارائه کلاسی	فصل ۸ (دو نفر)
10	رمزنگاری نامتقارن ۱	تئوری اعداد و مفروضات سختی رمزنگاری	آشنایی با پایه های نظری مورد نیاز برای طراحی الگوریتم های رمزنگاری عمومی	حل تمرین و ارائه کلاسی	فصل ۹ (دو نفر)
11	رمزنگاری نامتقارن ۲ و ۳	الگوریتم های فاکتورینگ و محاسبات گسسته مدیریت کلید و طراحی کلید عمومی	آشنایی با محاسبات گسسته، قضایا و تئوری ها آشنایی الگوریتم های توزیع کلید عمومی	حل تمرین و ارائه کلاسی	فصل ۱۰ (یک نفر) فصل ۱۱ (یک نفر)
12	رمزنگاری نامتقارن ۴	رمزنگاری کلید عمومی	آشنایی با الگوریتم های کلید عمومی KEM/DEM, CDH/DDH	حل تمرین و ارائه کلاسی	فصل ۱۲ (دو نفر)
13	امضای دیجیتال	اصول امضای دیجیتال و TLS	آشنایی با TLS و الگوریتم RSA	حل تمرین و ارائه کلاسی	فصل ۱۳ (دو نفر)
14	رمزنگاری پساکوانتوم و حریم خصوصی	رمزنگاری در پساکوانتوم قوانین حریم خصوصی در آمریکا	آشنایی با مشکلات رمزشکنی در پساکوانتوم آشنایی با آخرین قوانین حریم خصوصی	حل تمرین و ارائه کلاسی	فصل ۱۴ (یک نفر) حریم خصوصی (یک نفر)
15	رمزنگاری بیومتریک	آشنایی با رمزنگاری بیومتریک	بررسی روش های مختلف و نقاط ضعف و قوت	حل تمرین و ارائه کلاسی	مقاله بیومتریک (یک نفر)
16	جمع بندی	رفع اشکال و حل تمرین			

۲. قوانین کلاسی و بارم بندی آزمون پایان ترم:

۱- حضور به موقع و فعال دانشجو در کلاس

۲- ارائه تمرینات و پروژه های درسی به موقع و بر مبنای تقویم کلاس

۳- بارم بندی: ۲۰ درصد نمره کلاسی، ۲۰ درصد پروژه پایانی، ۲۰ درصد میان ترم، ۴۰ درصد پایان ترم

۳. ابزارهای آموزشی و کمک آموزشی مورد نیاز:

ویدئو پروژکتور جهت ارائه اسلاید

۴. منابع مطالعاتی درس

فرعی	اصلی
1. Ruth J.A., et al. (2024). Innovative Machine Learning Applications for Cryptography 2. Bertaccini M. (2022). Cryptography Algorithms 3. Radhakrishnan S. ,Travieso C.M. (2024). Biometrics and Cryptography 4. Mammeri Z. (2024). Cryptography Algorithms, Protocols, and Standards for Computer Security	1. Jonathan Katz, J. & Lindell, Y. (2021). Introduction to Modern Cryptography 2. Paar C. & Pelzl J. & Güneysu T. (2024). Understanding Cryptography From Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms 2ed 3. Data Protection Laws and Regulations USA (2024) 4. Biometrics for Internet-of-Things Security: A Review (2021). Wencheng Yang

۵. تکالیف

یادگیری	عملکردی
---------	---------

ارائه اسلاید در هر جلسه در موضوع همان جلسه توسط دانشجویان
حل تمرینات بر اساس موضوعات جلسه

ارائه پروژه نهایی بر مبنای ارائه اسلایدهای انجام شده بر مبنای آخرین تحقیقات پژوهشی
در موضوعات ارائه شده

۶. راهبرد های ارزشیابی:

ارزشیابی در طول ترم موثرترین روش در ارزیابی تحصیلی می باشد که با ارائه کلاسی، تمرینات و پروژه پایانی انجام می گردد (مجموعاً ۴۰ درصد نمره).
در نهایت نیز با توجه به اهمیت مطالعه متون علمی، آزمون میان ترم و پایان ترم از منابع اصلی انجام می گردد (مجموعاً ۶۰ درصد نمره).
به جهت اهمیت کار عملی، مهارتی و پژوهشی در روند کلاس هر هفته یکی از دانشجویان ارائه کلاسی از موضوع همان جلسه خواهند داشت که با انجام پروژه پایانی مبتنی بر تحقیق در یکی از موضوعات جلسات درس و ارائه آخرین تحقیقات به روز جمع بندی انجام خواهد شد.

تاریخ و امضا:

۳۰ شهریور ۱۴۰۳