بسم الله الرحمن الرحیم

وزارت علوم، تحقیقات و فناوری
دانشگاه جامع علمی ـ کاربردی
دانشگاه صنایع و معادن ایران

امنیت اطلاعات و شبکه
Information and Network Security
نیمسال اول ۸۷-۱۳۸۶

امنیت اطلاعات و شبکه

Information and Network Security

۲ واحد / نظری ـ عملی
پیش‌نیاز: شبکه‌های کامپیوتری
دوشنبه، ۱۵:۰۰ تا ۱۸:۰۰

مدرس کاظم فولادی
وب‌سایت <http://kazim.fouladi.ir>, <http://khorshid.ut.ac.ir/~kfouladi>
پست الکترونیکی <kazim@fouladi.ir>, <kfouladi@ut.ac.ir>

وب‌سایت درس <http://courses.fouladi.ir/ins>

مراجع کتاب‌های مرجع

کتاب درس

[1] W. Stallings, **Cryptography and Network Security: Principles and Practices**, 4th Edition, Prentice Hall, 2005.

سایر مراجع

[2] M. Y. Rhee, **Internet Security : Cryptographic Principles, Algorithms, and Protocols**, John Wiley & Sons, 2003.

[3] M. Bishop, **Introduction to Computer Security**, Prentice Hall, 2004.

[4] C. P. Pfleeger, S. L. Pfleeger, **Security in Computing**, Prentice Hall, 2002.

[5] H. C.A. van Tilborg, **Encyclopedia of Cryptography and Security**, Springer, 2005.

[6] Internet and other useful resources.

ارزیابی نحوه‌ی محاسبه‌ی نمره‌ی درس و توضیحات لازم:

آزمون پایان‌ترم : ۱۰ نمره
تکلیف‌ها و پروژه‌ها : ۱۰ نمره

- کلیه‌ی دانشجویان این درس باید با مراجعه به وب‌سایت درس از طریق گزینه‌ی Register اقدام به ثبت‌نام در این درس نمایند.
- تمرین‌ها، کارهای مطالعاتی و آزمایشگاهی در قالب گروه‌های دو نفری انجام می‌شود.
- کلیه‌ی گزارش‌های مربوط به تمرین‌ها، کارهای مطالعاتی و آزمایشگاهی باید به صورت الکترونیکی در قالب مشخص تهیه و ارسال شود.
- قالب مربوط به گزارش‌ها در وب‌سایت درس موجود است.
- مهلت تحویل گزارش هر تکلیف، یک هفته پس از آن جلسه ساعت ۲۳:۵۹ خواهد بود.
- از آنجا که دریافت و سازمان‌دهی گزارش‌ها از طریق پست الکترونیکی به صورت خودکار انجام می‌شود، خط موضوع Subject line ایمیل‌های ارسالی مربوط به آنها حتماً باید در قالب زیر باشد وگرنه دریافت نخواهد شد:

[ins] [iuim] [شماره ی گزارش] [نام اعضای گروه] [توضیحات دیگر]

سرفصل مطالب زمان‌بندی و تکالیف

هفته‌ی ۱	۷/۹	**مقدمه‌ای بر امنیت اطلاعات و شبکه، رمزنگاری**	مطالعه: فصل ۱ تکلیف: -
هفته‌ی ۲	۷/۱۶	**رمزگذاری: تکنیک‌های استاندارد (۱)**	مطالعه: فصل ۲ تکلیف: -
هفته‌ی ۳	۷/۲۳	**رمزگذاری: تکنیک‌های استاندارد (۲)**	مطالعه: فصل ۲ تکلیف: تکلیف شماره‌ی ۱
هفته‌ی ۴	۷/۳۰	**رمزگذاری: رمزهای بلاکی**	مطالعه: فصل ۳ تکلیف:
هفته‌ی ۵	۸/۷	**رمزگذاری: استاندارد رمزگذاری داده‌ها، DES**	مطالعه: فصل ۳ و ۶ تکلیف: تکلیف شماره‌ی ۲
هفته‌ی ۶	۸/۱۴	**رمزگذاری: رمزگذاری متقارن برای محرمانگی**	مطالعه: فصل ۷ تکلیف: تکلیف شماره‌ی ۳
هفته‌ی ۷	۸/۲۱	**رمزگذاری: رمزنگاری کلید عمومی، RSA**	مطالعه: فصل ۹ تکلیف: تکلیف شماره‌ی ۴
هفته‌ی ۸	۸/۲۸	**تصدیق پیام و توابع درهم‌سازی**	مطالعه: فصل ۱۱ تکلیف: تکلیف شماره‌ی ۵
هفته‌ی ۹	۹/۵	**امضای دیجیتال و پروتکل‌های تصدیق**	مطالعه: فصل ۱۳ تکلیف: تکلیف شماره‌ی ۶
هفته‌ی ۱۰	۹/۱۲	**کاربردهای تصدیق**	مطالعه: فصل ۱۴ تکلیف: -
هفته‌ی ۱۱	۹/۱۹	**امنیت پست الکترونیکی، PGP**	مطالعه: فصل ۱۵ تکلیف: تکلیف شماره‌ی ۷
هفته‌ی ۱۲	۹/۲۶	**امنیت پروتکل اینترنت، IPsec**	مطالعه: فصل ۱۶ تکلیف: -
هفته‌ی ۱۳	۱۰/۳	**امنیت وب، SSL**	مطالعه: فصل ۱۷ تکلیف: تکلیف شماره‌ی ۸
هفته‌ی ۱۴	۱۰/۱۰	**نفوذگرها**	مطالعه: فصل ۱۸ تکلیف: تکلیف شماره‌ی ۹
هفته‌ی ۱۵	۱۰/۱۷	**نرم‌افزارهای بدخواه**	مطالعه: فصل ۱۹ تکلیف: تکلیف شماره‌ی ۱۰
هفته‌ی ۱۶	۱۰/۲۴	**دیوار آتش**	مطالعه: فصل ۲۰ تکلیف: -
آزمون			از کلیه‌ی مطالب