

یا ذالامن والامان

مبانی امنیت اطلاعات و ارتباطات



معرفی درس

توسط: حمید رضا شهریاری

دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر

<https://www.aut.ac.ir/shahriari>

<https://atlas.aut.ac.ir>

معرفی درس

□ عنوان: مبانی امنیت اطلاعات [و ارتباطات]

□ مدرس: حمید رضا شهریاری

<http://www.aut.ac.ir/shahriari/>

<http://courses.aut.ac.ir>

[Email:shahriari@aut.ac.ir](mailto:shahriari@aut.ac.ir) with subject: #ICTSec ...



@hshahriari

معرفی درس

روش مراجعه برای رفع اشکال:

■ تماس با دفتر کار ۰۶۴۵۴۲۷۱۶:

□ شنبه و دوشنبه ۰۹:۰۰-۱۰:۳۰

■ تماس از طریق google meetings
(hshahriari@gmail.com)

□ <https://meet.google.com/pba-kahm-erh>

■ ارسال ایمیل به shahriari@aut.ac.ir

معرفی درس

هدف:

- آشنایی با مبانی امنیت اطلاعات و ارتباطات
- نیازمندیهای امنیتی
- آشنایی با تهدیدها و حملات
- آشنایی با اصول و روشهای رمزنگاری
- آشنایی با مشکلات و راهکارهای امنیتی در لایه های شبکه
- آشنایی با امنیت در سیستمها و نرم افزارها

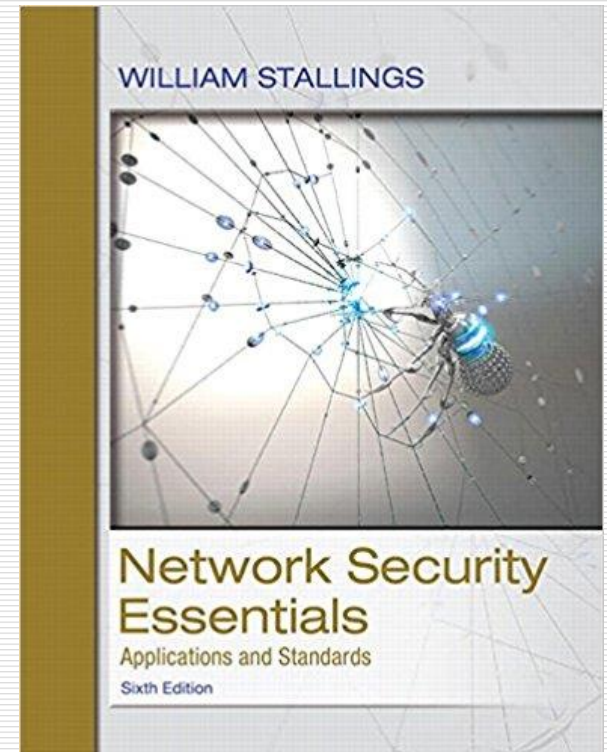
معرفی درس

□ ساختار درس:

- مفاهیم اساسی امنیت
- مکانیزمهای پایه‌ای امنیت (رمزنگاری، احراز هویت و)
- جنبه های کاربردی امنیت شبکه در لایه های مختلف
- ابزارها و مکانیزمهای امنیت رایانه

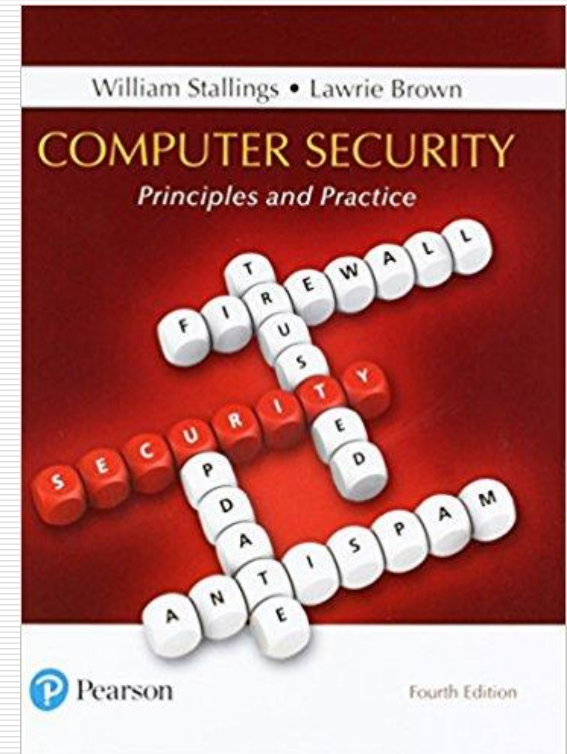
مرجع اصلی درس (Text book)

- William Stallings, **Network Security Essentials, Application and Standard**, 6th Ed., Prentice-Hall, 2016.
 - <http://www.williamstallings.com/NetworkSecurity>



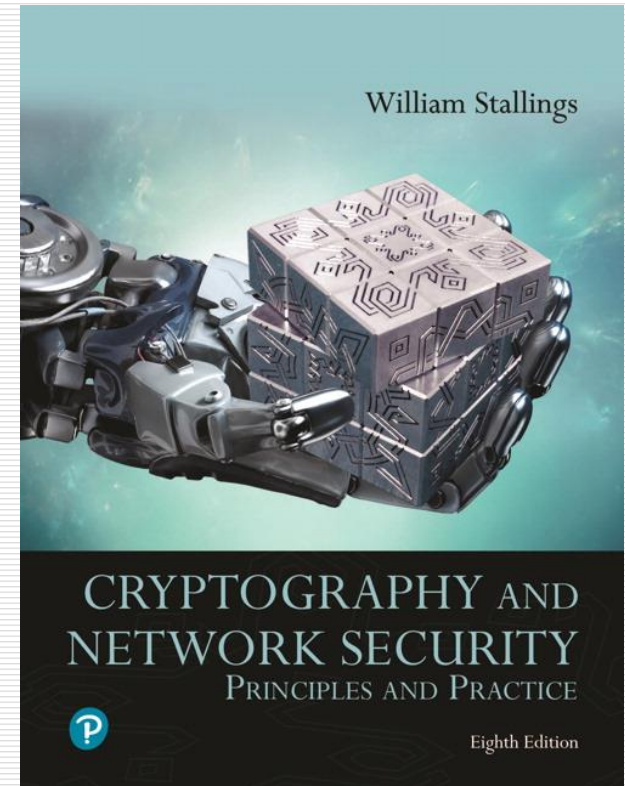
مرجع دیگر

- ❑ William Stallings, Lawrie Brown, **Computer Security: Principles and Practice** , 4th Ed., Prentice-Hall, 2017.
 - <http://williamstallings.com/ComputerSecurity/>



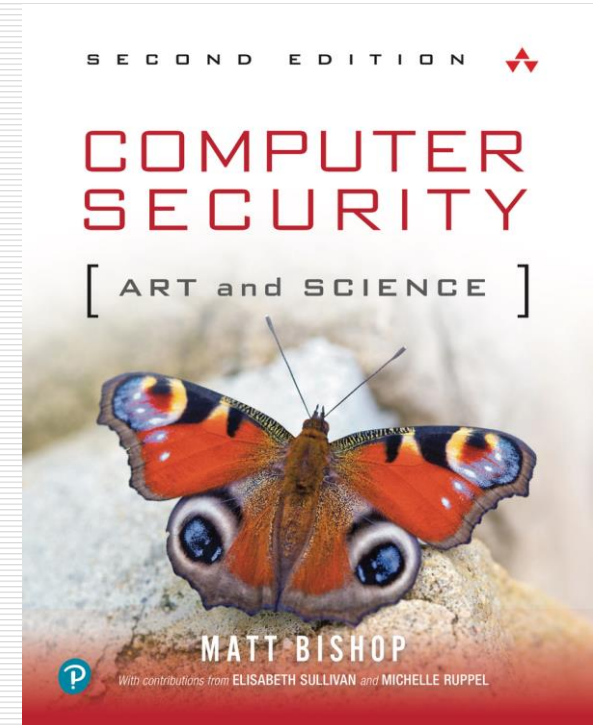
کتاب دیگر استالینگز

- William and Stallings,
Cryptography and
Network Security:
Principles and Practice,
8th ed., Prentice Hall,
2020



مرجع کمکی

- ❑ Matt Bishop, [Computer Security: Art and Science](#) Second edition, 2019
- ❑ <http://nob.cs.ucdavis.edu/book/>
- ❑ Related Papers and RFCs which will be delivered according to the topics.



سرفصل‌های درس

□ مقدمه: معرفی، محتوای درس، قوانین، ...

■ مفاهیم اولیه امنیت: جنبه های امنیت، انواع و ماهیت تهدیدها و حملات

■ رمزنگاری مرسوم (متقارن) و محرمانگی پیام

■ رمزنگاری با کلید عمومی و احراز هویت پیام

سرفصلهای درس

- احراز هویت
 - روشهای پایه
 - پروتکلهای (X.509 و Kerberos)
- امنیت پست الکترونیکی و پیام رسانی
- امنیت پروتکل اینترنت (IPSec)
- امنیت لایه انتقال
- سیستمهای تشخیص نفوذ و حفاظتها (Firewalls)
- بدافزارها و نرم افزارهای مخرب
- امنیت در برنامه های تحت وب

ارزیابی دانشجویان

نحوه ارزیابی (درصدها ممکن است کمی تغییر یابند)

- تمرین کتبی : ۱۰ درصد
- فعالیت‌های کلاسی و خواندنی‌ها: ۵ درصد
- پروژه‌های برنامه نویسی: ۱۵ درصد
- کویزها: ۱۵ درصد
- امتحان میان ترم: ۲۰ درصد
- امتحان پایان ترم: ۳۵ درصد
- شرط گذراندن درس کسب حداقل نصف تمرین و پروژه، و کسب حداقل نصف امتحانها و کویزها است.

خط مشی / Policy

- تمرینات در مودل تحویل گرفته خواهد شد.
- <http://courses.aut.ac.ir>
- تاخیر تا ۳ روز موجب کسر حداقل ۲۵ درصد از نمره تمرین خواهد شد.
- تاخیر بیش از ۳ روز تحویل گرفته نمی شود.
- کپی کردن تمرین و پروژه نه تنها باعث **از دست رفتن نمره** تمرین یا پروژه خواهد شد، بلکه باعث **کسر نمره** نیز خواهد شد.
- شرط گذراندن درس کسب حداقل نصف تمرین و پروژه، و کسب حداقل نصف امتحانها و کویزها است.