<table>
<tr><td rowspan="2">عنوان درس</td><td>فارسی</td><td colspan="10">روش‌های آماری دررمزنگاری</td></tr>
<tr><td>انگلیسی</td><td colspan="10">Statistical Methods in Cryptography</td></tr>
<tr><td colspan="8">نوع واحد</td><td>تعداد واحد</td><td>تعداد ساعت</td><td colspan="2">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">۳</td><td rowspan="2">۴۸</td><td rowspan="3" colspan="2">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="5">حل تمرین: ندارد</td><td colspan="5">نیاز به اجرای پروژه عملی:ندارد</td></tr>
</table>

هدف: هدف اصلی این درس آشنایی دانشجو با روش‌ها و ابزار موجود در علم آمار برای تجزیه 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 آزمون‌های آماری و مسائل مرتبط. جهانی بودن Next Bit Test. آزمون‌های NIST و آزمون‌های 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 تفاضلی 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 بهینه‌سازی پیچیده. بررسی کارایی و پیاده‌سازی با ارائه چند مثال (با نظر استاد).

منابع:

[1] L. Chen and G. Gong, Communication System Security, CRC Press, 2012.
[2] J. E. Gentle, Computational Statistics, Springer 2009.
[3] D. Koller and N. Friedman, Probabilistic Graphical Models: Principles and Techniques, MIT Press, 2009.
[4] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press 1996.
[5] S. Murphy, F. Piper, M. Walker, P. Wild, Likelihood Estimation for Block Cipher Keys, Technical Report, RHUL, 1995.
[6] D. Neuenschwander, Probabilistic and Statistical Methods in Cryptology, LNCS 3028, Springer 2004.
[7] H. Niederreiter, Random Number Generation and Quasi-Monte Carlo Methods, SIAM, 1992.
[8] M. Stamp, R.M. Low, Applied Cryptanalysis: Breaking Ciphers in the Real World, John Wiley and Sons Inc, 2007.