رمزنگاری

Cryptography

تعداد واحد: 3 (نظری) **شماره درس: 1127011** **مقطع درس: تحصیلات تکمیلی**

پیش‌نیاز: -

هدف: آشنایی با مفاهیم و کاربردهای گوناگون رمزنگاری، معرفی سیستم‌های رمز کلاسیک، رمز قالبی، رمز دنباله‌ای، رمز کلید همگانی، آشنایی با پروتکل‌های رمزنگاری.

سرفصل مطالب درس:

مفاهیم اولیه: مرور کلی اصول و مبانی رمزنگاری، نظریه اعداد، نظریه اطلاعات، نظریه پیچیدگی

سیستم‌های رمزنگاری کلاسیک: سیستم‌های جابجایی، سیستم‌های جانشینی تک‌الفبایی، سیستم‌های جانشینی چندالفبایی، سیستم‌های جانشینی چندحرفی

سیستم‌های رمز دنباله‌ای: معرفی کلی سیستم‌های رمز دنباله‌ای، دنباله‌های شبه تصادفی، معیارهای سه‌گانه گالوب و انواع آزمون‌های آماری، تولید دنباله‌های شبه تصادفی با شیفت رجیسترهای فیدبک خطی (LFSR)، امنیت رمزهای دنباله‌ای

سیستم‌های رمز قالبی: معرفی کلی سیستم‌های رمز قالبی، استاندارد رمز داده(Data Encryption Standard (DES و Triple DES، استاندارد رمزنگاری پیشرفته (Advanced Encryption Standard (AES، سبک‌های کاری رمزهای قالبی

سیستم‌های رمزنگاری کلید همگانی: معرفی کلی سیستم‌های رمزنگاری کلیدهمگانی، امضا دیجیتال، سیستم دیفی-هلمن و سیستمRSA، سیستم‌های رمزنگاری کوله‌پشتی، حمله فرد در میانه

پروتکل‌های رمزنگاری: سیستم‌های دانایی صفر، توابع چکیده‌ساز، تسهیم راز، معرفی رمزنگاری کدمبنا، معرفی مسایل اخیر حوزه رمزنگاری (رمزنگاری سبک، رمزنگاری مشبکه‌مبنا، رمزنگاری احراز اصالت شده و..)

منابع:

[1] “Elementary Cryptanalysis: A Mathematical Approach,” By: A. Sinkov, Random House, 1968.
[2] “Cryptography and Data Security,” By: D. Robling Denning, Addison-Wesley, 1982.
[3] “Cipher System,” By: H. Beker and F. Piper, Northwood, 1982.
[4] “Cryptography and Network Security: Principles and Practice”, By: W. Stallings, 5th Edition, 2006.
[5] “Cryptography: Theory and Practice,” By: D. R. Stinson, 3rd Edition, CRC, 2006.
[6] “Introduction to Modern Cryptography,” By: J. Katz, Y. Lindell, Chapman & Hall/CRC Press, 2007.