Syllabus

- موارد مهم کاربرد رمزنگاری (بدون جزئیات)
- رمزنگاری کلاسیک
  - رمزنگار Caesar
    - تعریف رمزنگار و خواص آن
    - اصطلاحات رمزنگاری
    - مدل‌سازی ریاضی و معیارهای سنجش یک رمزنگار
    - حملات مرسوم و حملات ویژه سزار (Frequency Analysis)
  - رمزنگار Affine
    - روند بررسی یک رمزنگار
    - مزایا و معایب نسبت به سزار
    - نتیجه گیری

جلسه ۱

  - سیر تکاملی رمزنگارهای کلاسیک و رمزهایدارای ویژگی‌های بارز
    - رمزهای ابتدایی مانند Pigpen, Nihilist, Skytale
    - رمزهای Transposition
      - تعریف Substitution و Permutation
      - رمزهای Rail Fence, Route, Columnar, Double, Myskowski, Disrupted
      - تعریف آنتروپی اطلاعات
    - رمزهای مربعی
      - تعریف Fractionation
      - رمز Alberti
      - رمزهای Two-Square, Four Square
      - رمزهای Polybius, Playfair

جلسه ۲

- رمزهای پخش کننده و ماتریسی
  - رمز Hill
  - تعریف Diffusion , Confusion
- رمزهای جدولی و چندحرفی
  - رمز معروف ویگنر (Vigenere)
  - متدهای شکستن ویگنر (Kasiski و IoC)
  - رمزهای Autokey
- از رمزنگاری کلاسیک به رمزگذاری مدرن

جلسه ۳

- کلاد شانون و معجزه One-Time Pad
- دستگاه Enigma
- رمزها و دستگاه‌های رمزنگاری در جنگ جهانی دوم و تاثیرات آنها
- رمزگذاری عملی و مولد اعداد تصادفی
  - مولد LCG و ضعف آن، مولد Mersenne Twister, LFG و ...

جلسه ۴

- رمزهای جریانی (Stream Cipher)
- رمزنگاری مدرن
  - رمزنگاری متقارن
- Lucifer و رمزنگاران در ابهام و سردرگمی
- DES، استانداردی قابل اطمینان
- رقابت AES و کمال رمزگذاری با برنده شدن Rijndael
- تکامل نهایی و حملات Linear و Differential

جلسه ۵

  - رمزنگاری نامتقارن
- تعریف، استفاده و لزوم رمزنگاری نامتقارن
- مدل‌سازی و تعاریف ریاضی (قفل دو کلیده)

جلسه ۶

- رمز رابین و الگوریتم اشتراک کلید Diffie-Hellman
- RSA و فتح رمزنگاری نامتقارن
  - پیاده‌سازی و موانع
  - حملات مرسوم

جلسه ۷

- نقاط ضعف
- لگاریتم گسسته و ElGemal
  - حملات و نقاط ضعف
- میدان‌های محدود جمعی و خم‌های بیضوی، تحولی عظیم

جلسه ۸

- پیاده‌سازی و مشکلات امروزه رمزنگاری نامتقارن (سرعت، دقت)
  - توابع چکیده‌ساز
- CRC-32 و تضمین صحت پیام
- MD5 و تضمین امنیت پیام
  - نقاط ضعف و سردرگمی
  - شکسته شدن ناباورانه MD5
- SHA-1 و امضاهای دیجیتالی مبتنی بر چکیده‌پیام

جلسه ۹

- حمله روز تولد و SHA-2
  - امضاهای دیجیتال و کدهای اهراز هویت پیام و فرستنده
- امضای دیجیتال مبتنی بر رمزنگاری نامتقارن
- امضای دیجیتال مبتنی بر کدهای اهراز هویت
- امضای دیجیتال مبتنی بر چکیده
- امضای دیجیتال مستقل
  - استاندارد DSS

جلسه ۱۰