۱ برنامه زمانی

در جدول ۱ می‌توانید موضوعات مرتبط با هر جلسه و تطابق آن‌ها با کتاب را پیدا کنید.
جدول ۲ نیز برای برای تطابق این موضوعات با لکچرنوت‌ها و ویدیوهای موجود کلاس تهیه شده است.
مرجع اصلی درس **کتاب** می‌باشد، و ویدیوها و لکچرنوت‌ها **فقط** برای کمک به روند دنبال‌کردن مباحث آماده شده‌اند.

تاریخ	موضوع	شماره فصل/بخش کتاب
۳ اسفند	مقدمه	۱.۱، ۲.۱، ۳.۱(بخش اول)، ۴.۱
۵ اسفند	اصل کرشهف، رمز متقارن، مدل‌های حمله، رمزهای کلاسیک	۲.۱، ۳.۱، ۱.۴.۱
۱۰ اسفند	امنیت کامل، OTP، آزمایش تمایزناپذیری، قضیه شانون	۲، ۱.۲.۳
۱۲ اسفند	رویکردهای تعریف امنیت در رمزنگاری، مولد شبه‌تصادفی	۱.۳، ۳.۳
۱۷ اسفند	رمزهای دنباله‌ای، کاربرد LFSR در رمزهای دنباله‌ای، رمزهای دنباله‌ای معروف	۱.۱.۶، ۲.۱.۶
۱۹ اسفند	امنیت چندپیامی، CPA	۴.۳
۲۴ اسفند	توابع شبه‌تصادفی، رمزهای دنباله‌ای با بارگذاری اولیه	۵.۳
۲۶ اسفند	جایگشت شبه‌تصادفی و رمزهای قالبی	۱.۲.۶، ۲.۲.۶
۱۵ فروردین	روش‌های طراحی رمزهای قالبی، AES، DES	۳.۲.۶، ۵.۲.۶
۱۷ فروردین	مدهای عملکرد رمز قالبی، CCA	۲.۶.۳، ۱.۷.۳
۲۲ فروردین	کد اصالت‌سنجی پیام	۱.۴، ۲.۴
۲۴ فروردین	ساخت کد اصالت‌سنجی پیام، CBC-MAC	۳.۴، ۴.۴
۲۹ فروردین	تعریف و ساخت توابع چکیده‌ساز	۱.۵، ۲.۵، ۱.۳.۵
۳۱ فروردین	رمزنگاری تصدیق‌شده (Authenticated Encryption)	۵.۴
۵ اردیبهشت	Random Oracles ،HMAC	۲.۳.۵، ۵.۵
۷ اردیبهشت	تبادل کلید، پازل مرکل، پروتکل دیفی–هلمن	۱.۱۰، ۲.۱۰، ۳.۱۰
۱۲ اردیبهشت	سیستم رمز نامتقارن و امنیت آن‌ها، KEM	۱.۱۱، ۲.۱۱، ۳.۱۱
۱۹ اردیبهشت	مقدمه‌ای بر نظریه اعداد، مسائل سخت و فرضیات رمزنگاری	۱.۸، ۲.۸، ۱.۳.۸
۲۱ اردیبهشت	سیستم رمز الگمال	۱.۴.۱۱
۲۶ اردیبهشت	سیستم رمز RSA	۱.۵.۱۱، ۲.۵.۱۱
۲۸ اردیبهشت	امضای مبتنی بر RSA و لگاریتم گسسته	۱.۱۲، ۲.۱۲، ۴.۱۲، ۱.۵.۱۲
۲ خرداد	تسهیم راز	۱.۳.۱۳
۴ خرداد	رمزنگاری توزیع‌شده و رأگیری‌الکترونیکی	۲.۱۳، ۳.۱۳
۹ خرداد	اثبات دانش‌صفر، پروتکل سیگما و رأی‌گیری الکترونیکی	–

جدول ۱: برنامه زمانی کلاس

تاریخ	شماره ویدیو	شماره لکچرنوت
۳ اسفند	۱(موجود نیست)	۱
۵ اسفند	۲	۲، ۳(به‌جز امنیت کامل)
۱۰ اسفند	۳، ۴	۳(امنیت کامل)، ۴، ۵
۱۲ اسفند	۵، ۶(به‌جز قسمت‌های LFSR)	۶، ۱۱
۱۷ اسفند	۶(قسمت‌های LFSR)، ۷، ۸	۷، ۸، ۹، ۱۰
۱۹ اسفند	۹	۱۲(تا ابتدای بخش ۲)، ۱۳(تا ابتدای ۳.۲)
۲۴ اسفند	۱۰	۱۲(بخش ۲)، ۱۳(بخش ۱ و ۳)
۲۶ اسفند	۱۱	۱۴(۱۴آ: رمزهای قالبی)
۱۵ فروردین	۱۲	۱۴(۱۴ب: AES، DES)
۱۷ فروردین	۱۳	۱۳(از بخش ۳.۲)، ۱۵
۲۲ فروردین	۱۳	۱۶(تا بخش ۴)
۲۴ فروردین	۱۴،۱۵	۱۶، ۱۷(تا ابتدای توابع چکیده‌ساز)
۲۹ فروردین	۱۵، ۱۶	۱۷، ۱۸
۳۱ فروردین	۱۶، ۱۷	۱۸(۱۸ب: از بخش ۳)
۵ اردیبهشت	۱۷	۱۸(۱۸ب: از بخش ۶)
۷ اردیبهشت	۱۸، ۱۹	۱۹
۱۲ اردیبهشت	۲۰	۲۰(بخش ۱)
۱۹ اردیبهشت	۲۰، ۲۱	۲۰(از بخش ۲)، ۲۱
۲۱ اردیبهشت	۲۲	۲۲(از بخش ۳)، ۲۳(بخش ۱)
۲۶ اردیبهشت	۲۲	۲۲(تا بخش ۳)
۲۸ اردیبهشت	۲۳، ۲۴	۲۳(از بخش ۲ تا ابتدای ۱.۲)
۲ خرداد	۲۴	۲۳(از بخش ۲)، ۲۴
۴ خرداد	۲۴	۲۴
۹ خرداد	۲۴	۲۴

جدول ۲: تطابق موضوعات کلاس با لکچرنوت‌ها و ویدیوها