۱ برنامه زمانی

در جدول ۱ می‌توانید موضوعات مرتبط با هر جلسه و تصابق 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 برای کمک به روند دنبال‌کردن مباحث آماده شده‌اند.

تاریخ	موضوع	شماره فصل/بخش کتاب
۱ مهر	مقدمه	۱.۱، ۲.۱، ۳.۱(بخش اول)، ۴.۱
۶ مهر	اصل کرشهف، رمز متقارن، مدل‌های حمله، رمزهای کلاسیک	۲.۱، ۳.۱، ۱.۴.۱
۸ مهر	امنیت کامل، OTP، آزمایش تمایزناپذیری، قضیه شانون	۲، ۱.۲.۳
۱۳ مهر	رویکردهای تعریف امنیت در رمزنگاری، مولد شبه‌تصادفی	۱.۳، ۳.۳
۱۵ مهر	رمزهای دنباله‌ای، کاربرد LFSR در رمزهای دنباله‌ای، رمزهای دنباله‌ای معروف	۱.۱.۶، ۲.۱.۶
۲۰ مهر	امنیت چندپیامی، CPA	۴.۳
۲۲ مهر	توابع شبه‌تصادفی، رمزهای دنباله‌ای با بارگذاری اولیه	۵.۳
۲۷ مهر	جایگشت شبه‌تصادفی و رمزهای قالبی	۱.۲.۶، ۲.۲.۶
۲۹ مهر	روش‌های طراحی رمزهای قالبی، AES، DES	۳.۲.۶، ۵.۲.۶
۶ آبان	مدهای عملکرد رمز قالبی، CCA	۲.۶.۳، ۱.۷.۳
۱۱ آبان	کد اصالت‌سنجی پیام	۱.۴، ۲.۴
۱۸ آبان	ساخت کد اصالت‌سنجی پیام، CBC-MAC	۳.۴، ۴.۴
۲۰ آبان	تعریف و ساخت توابع چکیده‌ساز	۱.۵، ۲.۵، ۱.۳.۵
۲۷ آبان	**میانترم اول**	**تا انتهای مباحث ۲۰ آبان**
۲ آذر	رمزنگاری تصدیق‌شده (Authenticated Encryption)	۵.۴
۴ آذر	HMAC، Random Oracles	۲.۳.۵، ۵.۵
۹ آذر	تبادل کلید، پازل مرکل، پروتکل دیفی_هلمن	۱.۱۰، ۲.۱۰، ۳.۱۰
۱۱ آذر	سیستم رمز نامتقارن و امنیت آن‌ها، KEM	۱.۱۱، ۲.۱۱، ۳.۱۱
۱۶ آذر	مقدمه‌ای بر نظریه اعداد، مسائل سخت و فرضیات رمزنگاری	۱.۸، ۲.۸، ۱.۳.۸
۱۸ آذر	سیستم رمز الگمال	۱.۴.۱۱
۲۳ آذر	**میانترم دوم**	**تا انتهای مباحث ۱۸ آذر**
۲۵ آذر	سیستم رمز RSA	۱.۵.۱۱، ۲.۵.۱۱
۳۰ آذر	امضای مبتنی بر RSA و لگاریتم گسسته	۱.۱۲، ۲.۱۲، ۴.۱۲، ۱.۵.۱۲
۲ دی	تسهیم راز	۱.۳.۱۳
۷ دی	رمزنگاری توزیع‌شده و رأگیری‌الکترونیکی	۲.۱۳، ۳.۱۳
۹ دی	اثبات دانش‌صفر، پروتکل سیگما و رأی‌گیری الکترونیکی	–

جدول ۱: برنامه زمانی کلاس

تاریخ	شماره ویدیو	شماره لکچرنوت
۱ مهر	۱(موجود نیست)	۱
۶ مهر	۲	۲، ۳(به‌جز امنیت کامل)
۸ مهر	۳، ۴	۳(امنیت کامل)، ۴، ۵
۱۳ مهر	۵، ۶(به‌جز قسمت‌های LFSR)	۶، ۱۱
۱۵ مهر	۶(قسمت‌های LFSR)، ۷، ۸	۷، ۸، ۹، ۱۰
۲۰ مهر	۹	۱۲(تا ابتدای بخش ۲)، ۱۳(تا ابتدای ۳.۲)
۲۲ مهر	۱۰	۱۲(بخش ۲)، ۱۳(بخش ۱ و ۳)
۲۷ مهر	۱۱	۱۴(۱۴آ: رمزهای قالبی)
۲۹ مهر	۱۲	۱۴(۱۴ب: AES، DES)
۶ آبان	۱۳	۱۳(از بخش ۳.۲)، ۱۵
۱۱ آبان	۱۳	۱۶(تا بخش ۴)
۱۸ آبان	۱۴،۱۵	۱۶، ۱۷(تا ابتدای توابع چکیده‌ساز)
۲۰ آبان	۱۵، ۱۶	۱۷، ۱۸
۲۷ آبان	**میانترم اول**	**تا انتهای مباحث ۲۰ آبان**
۲ آذر	۱۶، ۱۷	۱۸(۱۸ب: از بخش ۳)
۴ آذر	۱۷	۱۸(۱۸ب: از بخش ۶)
۹ آذر	۱۸، ۱۹	۱۹
۱۱ آذر	۲۰	۲۰(بخش ۱)
۱۶ آذر	۲۰، ۲۱	۲۰(از بخش ۲)، ۲۱
۱۸ آذر	۲۲	۲۲(از بخش ۳)، ۲۳(بخش ۱)
۲۳ آذر	**میانترم دوم**	**تا انتهای مباحث ۱۸ آذر**
۲۵ آذر	۲۲	۲۲(تا بخش ۳)
۳۰ آذر	۲۳، ۲۴	۲۳(از بخش ۲ تا ابتدای ۱.۲)
۲ دی	۲۴	۲۳(از بخش ۲)، ۲۴
۷ دی	۲۴	۲۴
۹ دی	۲۴	۲۴

جدول ۲: تطابق موضوعات کلاس با لکچرنوت‌ها و ویدیوها