



رمزنگاری، امنیت اطلاعات و حریم خصوصی

ارائه: دکتر سیدعلی لاجوردی
بخش آشنایی



سلام

چراغی در دستم، دری در پیش رو

من و جستجوی یک ذره روشنایی!



سیدعلی لاجوردی

- کارشناسی مکانیک امیرکبیر
- کارشناسی ارشد فناوری اطلاعات تربیت مدرس
- دکتری فناوری اطلاعات تربیت مدرس
- استادیار دانشگاه جامع انقلاب اسلامی
- توسعه دهنده راه حل های سازمانی
- علاقمند به الگوریتم، برنامه نویسی و کتاب
- سخت گیر نیستم اما دقیقم!
- شما چطور؟



راه های ارتباطی

- ایمیل: L8026070@gmail.com و sa.lajevardi@cuir.ac.ir
- شماره همراه: ۰۹۱۲۷۰۱۲۴۷۱
- ایتا، واتساب، تلگرام، پیامک
- طرح درس و منابع مطالعاتی: <https://learn.lajevardi.id.ir>
- مطالعه منابع معرفی شده جدا توصیه می شود
- اطلاع رسانی در گروه کلاس
- حضور در دانشگاه
- دوشنبه (آموزشی)
- چهارشنبه (پژوهشی)



حضور در کلاس

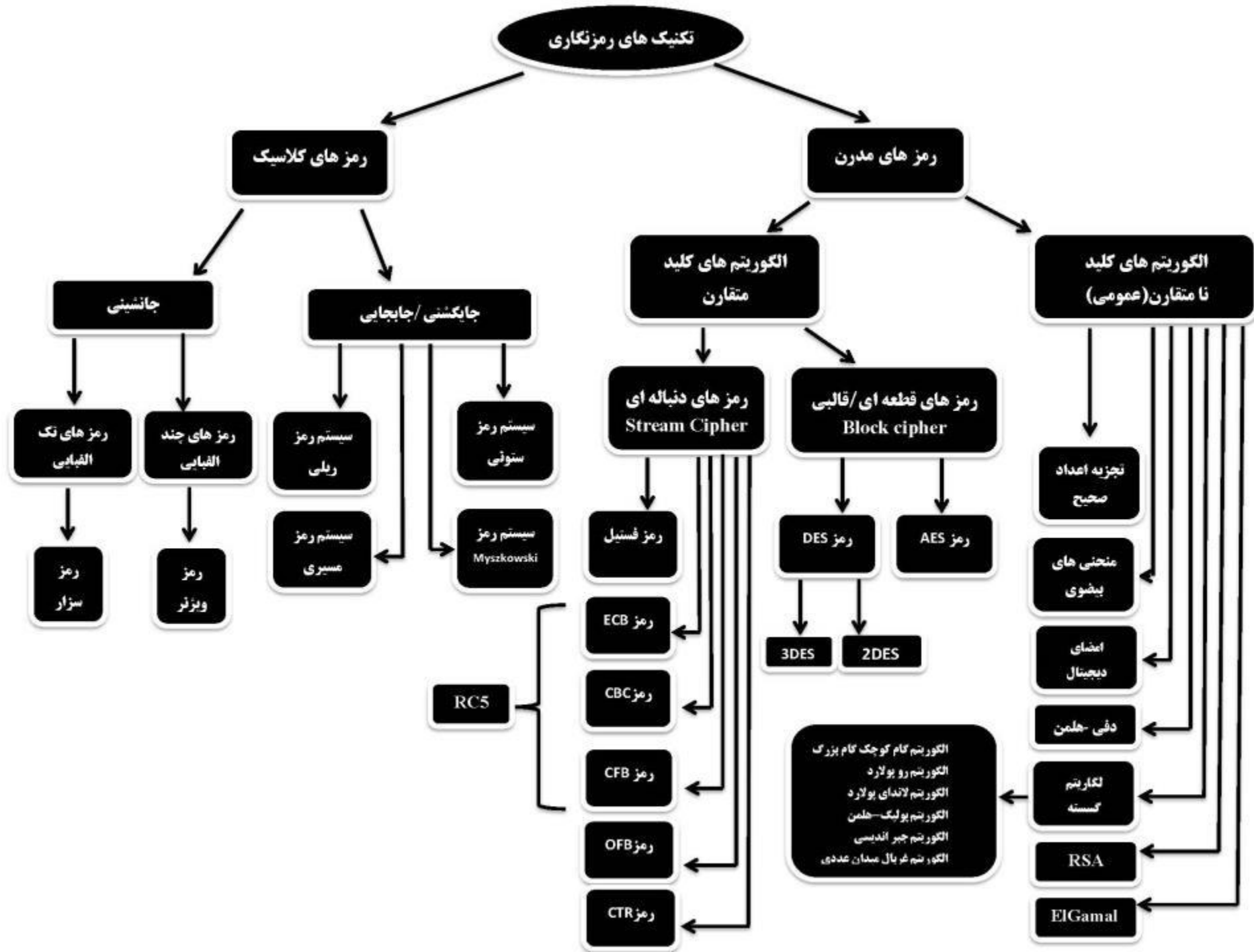
- حضور به موقع و فعال در کلاس (۵٪)
 - حضور و غیاب
 - تاخیر
 - جبرانی
 - مجازی و حضوری
 - بدون گوشی!
- تحویل تمرینات به صورت کاغذی (زمان دو هفته) (۵٪)
 - بدون تقلب و کپی!
 - استفاده از هوش مصنوعی
 - مردود، ناقص e، کامل E، جامع E+
 - حل تمرین در صورت ضرورت



تکالیف دانشجویان

- ارائه اسلاید به صورت هفتگی دانشجویان به مدت ۴۵ دقیقه (۱۰٪)
- انتخاب فصول به صورت انفرادی و به ترتیب انتخاب
- رعایت اصول ساخت اسلاید
- حداکثر ۴۰ صفحه
- آزمون میان ترم: هفته ۱۰ ترم (۲۰٪)
- در صورت نمره قابل قبول حذفی خواهد بود
- پروژه پایانی (مقاله ای از اسلاید ارائه شده مبتنی بر مقالات روز)
- ارسال به ایمیل تا روز آزمون پایانی به صورت فایل pdf و word به همراه اسلاید ارائه (۲۰٪)
- آزمون پایانی کتاب باز بدون اینترنت و گوشی همراه (۴۰٪)
- ۴۰ درصد مفاهیم و تعریف
- ۶۰ درصد مساله و تحلیلی







پیش نیاز

نظریه اعداد، الگوریتم، مجموعه، گزاره، احتمال، دنباله، کدینگ، امنیت

نظريه اعداد

- عدد
- عدد در پایه
- جمع و تفریق
- ضرب و تقسیم
- XOR
- MOD



الگوریتم

- تعریف
- اجرای الگوریتم
- بدترین حالت
- بهترین حالت
- مفهوم O بزرگ
- جستجو
- مرتب سازی
- انتخاب



مجموعه

- مفهوم مجموعه
- مجموعه اعداد (N, Z, W, Q, R, I)
- جبر مجموعه
 - اجتماع
 - اشتراك
 - منها
- زیر مجموعه
- مجموعه اصلی
- تساوی



گزاره

- گزاره
- فرض
- حکم
- اثبات
- استنتاج
- جبر بول



گروه

- تعریف گروه
- جبر گروه
- تعریف عمل
- جابجایی
- اشتراک پذیری
- تعدی
- بسته بودن



احتمال

- شمارش
- ترکیب
- ترتیب
- احتمال
- احتمال شرطی (قانون بیز)
- توزیع احتمالی
- یکسان Uniform
- نرمال



دنباله

- دنباله اعداد
- جمله عمومی
- دنباله بازگشتی
- دنباله فیبوناتچی
- گروه دنباله



اعداد تصادفی

- عدد تصادفی
- ساخت عدد تصادفی
 - سخت افزاری
 - نرم افزاری
- مولد عدد تصادفی
- اعداد شبه تصادفی
 - بذر اولیه Seed
 - رشته اعداد خروجی



امنیت

- Confidence : محرمانگی
- Integrity : یکپارچگی
- Availability : دسترس پذیری

CIA

- Attack : حمله
- انواع حملات



کدینگ

• کد Code

• Encode

• Decode

• رمز Cipher

• Encrypt

• Decrypt

