عنوان درس	فارسی	الگوریتم ومحاسبه									
	انگلیسی	Algorithm and Computation									
نوع واحد								تعداد واحد	تعداد ساعت	دروس پیش‌نیاز	
پایه		اصلی		تخصصی		اختیاری		۳	۴۸	ندارد	
نظری	عملی	نظری	عملی	نظری	عملی	نظری	عملی				
حل تمرین: ندارد						نیاز به اجرای پروژه عملی: ندارد					

هدف: هدف این درس آشنایی دانشجو با مفاهیم اصلی نظریه محاسبه مرتبط با زمینه‌های رمز و کد در ایجاد سختی الگوریتم یا سهولت محاسبات الگوریتم‌هاو یا امکان تجزیه و تحلیل پیچیدگی الگوریتم‌های مورد استفاده است.

سرفصل‌های درس:

- ارائه تعریف دقیق پیچیدگی محاسبه در مدل‌های قطعی (deterministic) و غیرقطعی (non-deterministic).
- تعریف دقیق کلاس‌های P و NP، تعریف دقیق مسائل NP-تمام با ارائه مثال.
- اهمیت مدل NP در تحلیل حمله به سامانه‌های رمزنگاری و اینکه الگوریتم مهاجم اساساً مسأله‌ای در کلاس NP را حل می‌کند.
- بحث در مورد اهمیت کلاس مسائل به طور کارا حل‌پذیر و اینکه مدل‌های مختلفی وجود دارند. نامناسب بودن کلاس P از دیدگاه رمزنگاری برای این منظور.
- تعریف کلاس‌های پیچیدگی تصادفی، بالاخص BPP. بحث در مورد مسأله $\mathbf{NP} - \mathbf{BPP} \stackrel{?}{=} \emptyset$ و ارتباط آن با مفهوم امنیت.
- تحلیل چند سامانه رمزنگاری در مدل‌های مختلف حمله از این دیدگاه و ارائه تعریف دقیق امنیت معنایی (Semantic Security). بحث در مورد ارتباط این مطلب با تمایزناپذیری (Indistinguishability).
- تعریف دقیق ماشین تورینگ اوراکل‌دار و چگونگی عملکرد آن. ارائه تعریف دقیق مدل پاسخ‌گوی تصادفی (Random Oracle) و ارائه یک اثبات امنیت ساده در این مدل.
- بحث در مورد سامانه‌های اثبات تعاملی (Interactive Proof Systems) و قضایای اصلی مرتبط با آن‌ها، بالاخص بحث در مورد طرح اثبات $\mathbf{IP} = \mathbf{PSpace} = \mathbf{AM}$، اهمیت این قضیه و ارتباط با قضیه PCP.

منابع:

[1] J. Talbot and D. Welsh, Complexity and Cryptography: An Introduction, Cambridge University Press, 2006.

[2] S. Arora and B. Barak,Computational Complexity: A Modern Approach, Cambridge University Press, 2009.