



## وصف مادة

رقم المتطلب السابق	اسم المادة	رقم المادة
1506341	نظرية التشفير	1506344

يقدم هذا المساق مقدمة لفهم تقنيات التشفير الكلاسيكية: الاستبدال ، والتبديل ، وأصفار المنتج ، وفحص خوارزميات التشفير التقليدية ومبادئ التصميم بما في ذلك تقنيات التحويل والاستبدال مثل DES ، وفهم تقنيات التشفير الحديثة مثل RSA ، AES ، RC4 ، توزيع المفتاح ، Diffie-Hellman ، التوقيع الرقمي ، تحديد الهوية والمصادقة ، ومفاتيح المشاركة. ويتضمن المساق تنفيذ الطلاب لمشروع بحث أو تطبيق برمجي لقياس مهارات استخدام تقنيات التشفير المختلفة.