

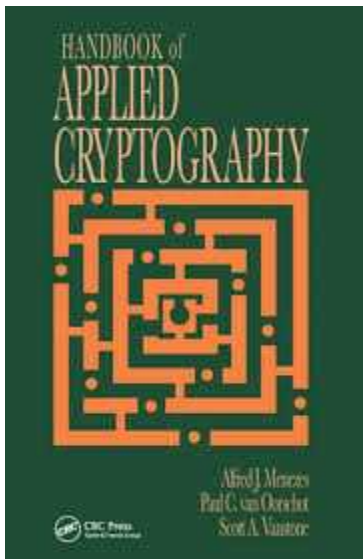
□ **교과목명: 현대암호론 (전북대학교 홍득조 교수)**

○ **교과목의 개요**

[수업 목표]

우리는 일상 생활에서 정보 통신의 발달로 인한 다양한 서비스를 제공받고 있다. 그러나 그러한 서비스에 불편함을 초래하거나 중요한 자산 및 프라이버시와 직결되는 보안 사고를 유발하는 사이버 공격 기술 또한 함께 발달하고 있다. 사이버 공격으로부터 우리를 보호하기 위한 다양한 보안 장치의 기본이 되는 것이 바로 암호시스템이다. 본 강의에서는 현대암호시스템을 구성하는 암호 알고리즘의 기본 원리를 이해하고, 최신 암호 기술이 어디까지 도달하였는지 파악한다.

[주요 교재]



- 교재명 : Handbook of Applied Cryptography
- 저 자 : Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
- 책소개 : Handbook of Applied Cryptography는 총 15장으로 구성되어있으며, 암호시스템에서 사용되는 기본 지식들을 공부하기에 알맞은 책이다.