송 정 환 (한양대학교)

암호학과 수학

암호학(Cryptology)과 수학(Mathematics)은 인류가 문자를 사용하면서 부터 매우 중요한 부분으로서의 역할을 수행해왔다. 고대 이집트에서부터 현대까지의 암호학의 변천사를 고찰하여 수학이 암호학에 얼마나 영향을 주었는지를 기술한다. 암호학은 정보보호를 위한 기밀성(Confidentiality)과 인증성(Authetication)을 실현시키기 위한 암호기술(Cryptography)과 그에 대한 안전성 및 효율성을 입증하기 위한 암호분석(Cryptanalysis)으로 크게 두가지로 분류할 수 있다. 암호기술과 암호분석에 수학이론들이 도입됨으로 해서 암호학이 학문영역으로 자리를 잡아가고 있다.

과거의 암호학은 주로 국가안보 및 군사적 목적에 의하여 소수 연구자들에 의해서 연구되어 왔으나 상거래 공간이 인터넷 등 통신망의 발달로 인하여 가상공간으로 옮겨짐에 따라 상업적 목적으로의 암호기술 사용이 급증하고 있기에 전자공학,전산학 등 다양한 분야에서 암호학에 대한 참여가 활발하다. 현대 암호학에서 다루고 있는 암호기술은 대칭키암호알고리즘(Symmetric key cryptographic algorithm)과 공개키암호알고리즘(Public key cryptographic algorithm) 두가지로 분류되며 이에 대한 안전성 및 효율성을 입증하기 위한 암호분석이 이루어 지고 있다.

산업사회에서 정보화사회로 변환기에 놓여 있는 현실태에서 가상공간에서의 정보보호는 필수적이다. 정보보호를 위한 가장 좋은 방법은 신뢰성 있는 암호기술 사용이고 신뢰성 있는 암호기술에 대한 이론적 안전성 및 효율성을 입증하기 위한 암호분석에 수학적 이론과 수학자들의 참여가 절대적이다.