1 2 128비트 블록암호알고리즘 SEED 표준화

정보보호 산업 활성화의 씨앗 SEED

정보화 사회가 고도화될수록 전자상거래, 개인정보 등 민감한 정보를 보호할 수 있는 안전성과 신뢰성이 검증된 암호알고리즘의 중요성이 날로 높아지고 있다. 이에 한국정보보호센터(KISA)에서는 1998년 12월 국내 암호전문가들과 공동으로 128비트 블록암호알고리즘 SEED를 개발하였다. 블록암호알고리즘이란 암호화 키와 복호화 키가 동일한 대칭암호화 방식의 일종으로, 암호문을 만들기 위해 암호화 키와 알고리즘이 64비트, 128비트 등의 블록단위의 평문에 적용되는 암호화 방식이다.

개발된 SEED는 4개월여 간의 공개검증과정을 거쳐 1999년 2월 26일 최종 개발결과를 발표하였다. 이후 의견수렴과 공청회를 개최하여 128비트 블록암호알고리즘 표준(안)으로 TTA에 제안하였고, 1999년 9월 28일 정보통신단체표준으로 제정되었다. 순수 국내 기술로 개발된 128비트 블록암호알고리즘은 정보보호 산업 활성화의 씨앗이 되라는 의미에서 'SEED(씨앗)'라 명명되었으며, 국내의 전자상거래, 금융, 무선통신 등에서 전송되는 중요정보를 보호하는 역할을 담당하게 되었다. 단체표준으로 제정된 SEED는 TTA 표준 중 가장 높은 활용도를 보이게 되었다. 실제 TTA에서 실시한 정보통신표준 활용실태 조사결과에 따르면, SEED는 2000년부터 2003년까지 국내 2,000여 TTA 표준 중 4년 연속 활용도 1위를 차지했다.

이후 SEED는 2005년 국제 표준화 기구인 ISO/IEC로부터 미국의 AES(Advanced Encryption Standard)와 일본의 Camellia와 함께 국제블록암호알고리즘 표준으로 제정되었다. 또한 같은 해 IETF 표준으로도 제정되었다.

이와 함께 SEED 암호알고리즘 자체에 대한 표준 외에도 SEED를 사용하기 위한 다양한 국내외 표준들이 제정되었다. 대표적인 사례로는 TTA에서 제정된 블록암호알고리즘 SEED의 운영모드인 TTAS.KO-12.0025가 있으며, 국제표준으로는 보안전자우편에서의 메시지 암호화를 위한 SEED 사용표준인 IETF RFC 4010과 TLS를 위한 SEED 알고리즘 사용표준 IETF RFC 4162, 그리고 IPsec을 위한 SEED 알고리즘 사용표준인 IETF RFC 4196가 있다.

SEED의 특징과 활용

SEED는 대칭키 암호알고리즘으로 블록 단위로 메시지를 처리하는 블록암호알고리즘이다. 대칭키 블록암호알고리즘은 비밀성을 제공하는 암호시스템의 가장 중요한 요소로, 본 표준이 규정하는 128비트 블록암호알고리즘 SEED는 128비트 암호 키를 이용하여 메시지를 128비트 블록 단위로 암·복호화하는 알고리즘으로 데이터의 기밀성과 같은 기능을 제공하기 위해 사용될 수 있다.

SEED의 전체 구조는 Feistel 구조로 이루어져 있으며, 128비트의 평문 블록 단위당 128비트 키로부터 생성된 16개의 64비트 라운드 키를 입력으로 사용하여 총 16라운드를 거쳐 128비트 암호문 블록을 출력한다. SEED는 128비트 입력 평문블록을 2개의 64비트 블록으로 나누어 16개의 64비트 라운드키를 이용하여 16라운드를 수행한 후, 최종 128비트 암호문 블록을 출력한다.

SEED 표준을 활용할 수 있는 범위는 기밀성 기능을 제공하는 정보보호시스템 및 암호제품에 다양하게 활용될 수 있으며, 이를 통해 국내 정보통신망의 안전성·신뢰성을 제고할 수 있다.

기본적으로 SEED는 민간분야의 암호사용을 촉진하기 위해 개발된 암호알고리즘이다. 따라서 개인 및 기업에서 중요정보를 보호하기 위해 필요한 경우 누구나 SEED를 사용할 수 있다.

현재 SEED는 국내 금융 및 인터넷 산업 전반에 걸쳐 널리 사용되고 있으며, TTA 표준을 통해 SEED에 대한 알고리즘 소개, 구현 가이드 및 테스트 벡터를 제공함으로써, SEED를 탑재한 정보보호제품 개발에도 중요한 역할을 담당하고 있다.