**인증 암호화**

인증 암호는 암호와 MAC 조합의 대안이다. 보통의 암호와는 달리 인증 암호는 암호문과 함께 인증값도 돌려준다. 인증 암호의 암호화 연산은 AE(K, P) = (C,T)로 정의된다. AE는 인증 암호화 함수이다. 이 함수는 키(K)와 평문(P)을 입력받아 암호문(C)과 인증값(T)을 반환한다.

복호화는 AD(K, C, T) = P로 정의된다. AD는 인증 복호화 함수이다. 이 함수는 키(K), 암호문(C), 인증값(T)을 입력받아 평문(P)을 반환한다. 암호문(C) 또는 인증값(T)이 유효하지 않으면 인증 복호화 함수(AD)는 오류를 반환해 수신자가 위조되었을 수도 있는 평문을 처리해서 생기는 위험을 방지한다. AD가 평문을 반환하면 인증이 성공한 것이다. 따라서 AD가 복호화 한 값이 비밀 키를 아는 누군가가 보낸 암호문인 것이 증명된다. 인증 암호는 비밀 키를 가진 시스템이 인증값이 유효할 때만 암호문을 복호화해 일반 암호보다 강하다. 인증값이 유효하지 않으면 암호문은 폐지된다. 인증 암호화는 공격자가 암호문을 만들어서 시스템에 평문을 요청하는 선택된 암호문 공격을 방지한다.

인증 암호가 처리하는 자료 중 인증만 수행하고 암호화를 적용하지 않은 자료는 연관 자료라 부른다. 인증 암호에 입력되는 모든 평문은 암호화와 인증을 거친다. 그러나 하나의 메시지 전체를 인증하되 일부만 암호화 하는 경우가 있다. 대표적으로 통신 패킷 암호화가 이런 경우다. 암호가 헤더와 페이로드(데이터)로 구성된 패킷을 처리하면 보호해야할 메시지를 담은 페이로드는 암호화한다. 그러나 패킷을 수신자에게 전달하는데 필요한 정보를 담은 헤더는 암호화 하지 않아야 한다. 라우터, 스위치 등의 통신기기가 헤더를 확인해 목적지IP, MAC는 무엇인지, 사용하는 포트는 무엇인지 등을 알아야 하기 때문이다. 그리고 패킷 헤더가 변조되지 않고 목적지에 도착했는지 알아야 해 헤더의 자료를 인증해야한다. 그래서 AEAD(연관 자료가 있는 인증 암호화)가 탄생했다. 전송자는 평문을 암호문에 부착해 보낸다. 만약 평문이 손상되면 수신자 인증값 검증을 실패하게되어 암호문을 복호화하지 않고 폐지한다. AEAD 암호화 연산은 AEAD(K, P, A) = (C, A, T)로 정의된다. AEAD 함수는 키(K), 평문(P), (연관 자료(A)를 암호화해 암호문(C), 암호화되지 않은 연관자료(A), 인증값(T)을 반환한다. 연관자료는 변환 없이 그대로 출력되며 암호문은 평문을 암호화한 결과이다. 인증값은 평문(P)와 연관자료(A) 모두에 의존하며 암호문(C)과 연관자료(A) 둘 다 수정되지 않았을 때만 유효하다. 인증값이 연관자료(A)에 의존하므로 수신자의 복호화는 연관자료가 관여한다. 복호화는 ADAD(K, C, A, T) = (P, A)로 정의된다. 복호화 함수는 키(K), 암호문(C), 연관자료(A), 인증값(T)을 복호화해 평문(P)과 연관자료(A)를 반환한다. 만약 암호문(C)과 연관자료(A)가 손상되었다면 오류를 반환한다.