**계산 보안성**

계산 보안성은 주어진 암호를 적당한 시간과 적당한 자원안에 깰 수 없으면 안전하다고 간주한다. 계산 보안성은 암호 또는 임의의 암호화 알고리즘 보안성을 정량화하는 한 수단으로 암복호화 알고리즘 공략의 난이도 상한을 제시한다. 계산 보안성은 다음 두 값으로 표현한다. t: 공격자가 수행할 연산 횟수의 한계, ε : 한 공격의 성공 확률 한계(0 이상 1 이하)

어떤 암호 또는 암복호화 방안에 대해 공격자가 최대 t회의 연산을 수행할 수 있고 성공확률이 ε을 넘지 않을 때 그러한 암호를 (t, ε)-보안 이라 부른다. 어떤 암호가 (t, ε)-보안이라는 것은 그 어떤 공격자라도 이 암호를 깨려면 적어도 t회의 연산을 수행해야 하며, 그런 경우 공격 성공 확률은 ε을 넘지 않는다. t회의 연산을 수행한다고 공격에 성공하는 것은 아니며 실제 필요 연산 횟수는 t보다 클 수 있다. 보안을 깨는데 필요한 최소 연산 횟수 t를 필요한 계산 노력의 하계라 한다. 정확히 t회의 연산과 ε의 성공 확률로 암호를 깨는 공격이 존재한다고 할 때, (t, ε)-보안은 하나의 엄밀한 한계를 제공한다 할 수 있다.

안전하다고 간주되는 암호가 주어졌을 때 파악할 것은 암호가 어느 정도의 공격 노력을 견딜 수 있는지 수치를 평가하는 것이다. n비트 보안은 암호 알고리즘을 깨는데 2ⁿ회의 연산이 필요하다는 뜻이다. 암호를 깨는데 필요한 연산횟수를 대략적으로나마 알 수 있다면, 연산 횟수의 이진 로그를 취해 암호의 보안 수준을 파악할 수 있다. n비트 키를 사용하는 암호는 모든 가능한 2ⁿ개의 키를 시도하는 무차별 대입 공격으로 항상 뚫리므로, 그런 암호의 최대 보안 수준은 n비트이다. 키의 크기가 항상 보안 수준과 일치하지는 않는다. 키의 크기는 보안 수준보다 높을 수 없는 한계 수준을 말할 뿐이다. 보안 수준이 n 비트(키 크기)보다 작을 수 있는 경우가 2가지 있다. 어떤 공격이 예상한 것보다 더 적은 수의 연산 즉 모든 2ⁿ개의 키가 아니라 일부만 사용해 키를 복원하는 경우, 그리고 보안 수준을 일부러 n 비트(키 크기)와 다르게 설정한 경우로서 공개 키 알고리즘 비밀 키의 비트와 보안 수준의 비트가 다르다.