chap.0

2. 동전 던지기 단계 1에서 A가 매우 큰 정수를 임의로 선택한다. 만약 A가 선택하는 정수의 범위가 제한적이면 어떤 문제가 발생하는지 설명하시오.

A가 매우 큰 정수를 임의로 선택하지 않고, 제한적인 범위에서 정수를 선택한다면 B가 제한된 범위 내의 모든 정수를 함수 f에 대입하여 f(x)에 대응하는 x값을 찾아낼 수 있다. 따라서 정수의 범위가 제한적이면 함수의 특성 1(모든 정수 x에 대해 f(x)를 계산하는것은 쉽지만 f(x)로부터 그것의 원상을 얻는 것은 계산적으로 불가능(computationally infeasible)해야 한다. 특히, 원상이 짝수인지 홀수인지 구분할 수 없어야 한다.)을 제공할 수 없다.

3. 동전 던지기에서 사용한 함수 f의 출력은 균일하게 분포되어야 한다. 즉, x가 주어졌을 때 $f(x)$가 특정 출력 값을 가질 확률은 출력의 범위가 n일 때 $1/n$이어야 한다. 사용하는 함수 f가 이 조건을 만족한다고 하였을 때, $f(x)$ 출력의 범위가 작으면 특성 2를 제공할 수 없다. 그 이유를 설명하시오.

동전 던지기에서 f의 출력 범위가 작으면, 임의의 수 x에 대하여 f(x)라는 출력이 있을 때, x != y && f(x) = f(y)인 정수쌍 (x, y)를 찾는것이 계산적으로 쉬워진다. 따라서 f의 출력 범위가 작으면 함수의 특성 2(x!=y이지만 f(x) = f(y)인 정수쌍 (x, y)를 찾는 것은 불가능해야 한다.)를 제공할 수 없다.

chap.1

3. 은행 ATM기기를 제외하고 일상 생활에서 여러분이 사용하는 서비스 중 하나를 선택하여 그 서비스에서는 어떻게 개체 인증(어떤 요소를)을 하고 있는지 설명하시오.

우리가 흔히 사용하는 스마트폰에는 많은 잠금 해제 방식이 있다. 기본적으로 패스워드, 패턴, PIN등이 있고 기술의 발전에 따라 지문인식, 얼굴인식등의 기능을 추가적으로 지원하고 있다. 지문인식의 경우 "사용자만의 독특한 특징(what one is) - 지문"을 사용하여 사용자 인증을 한다. 얼굴인식의 경우도 마찬가지로 "사용자만의 독특한 특징(what one is) - 얼굴"을 사용하여 사용자 인증을 한다.

4. 본인이 직접 사용해 본 실제 암호기술이 사용되고 있는 서비스를 하나 설명하시오. 어떤 서비스에 어떤 암호 기술이 어떻게 사용되고 있는지 조사하여 간단히 서술하시오.

카카오톡의 비밀 채팅 기능이 있다. 비밀 채팅은 종단간 암호화(End to End Encryotion: 발신원부터 수신원까지 정보의 암호화를 유지한 채로 전송하는 방식. E2E암호화 라고도 부른다.)기술을 적용하여 사용자 정보 보호를 강화한 기능이다. 이 기능은 암호화된 대화 내용을 풀 수 있는 암호화 키를 개인 단말기에만 저장하기 때문에 대화를 나눈 사용자의 단말기를 압수해 분석하지 않는 이상 대화 내용을 확인할 수 있는 방법이 원천적으로 차단된다. 즉, 카카오톡 서버에 있는 정보만으로는 대화 내용을 확인할 수 없다.