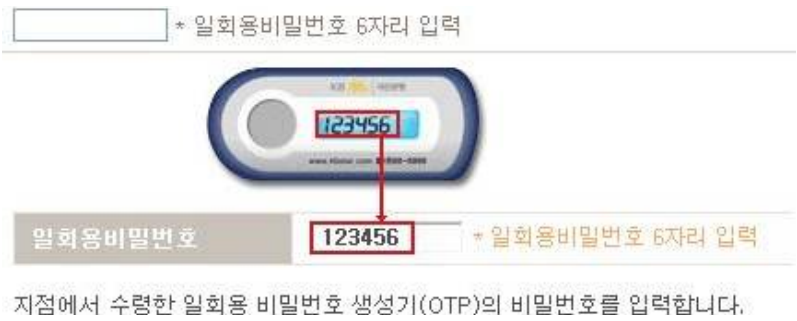
3. OTP(One Time Password)

• OTP는 **일회용비밀번호**를 필요할 때 생성하여 인증하는 기술이다.
• OTP는 **사용자** 인증에 사용된다.(클라이언트 인증)

◈ One Time Password 생성기



◈ OTP(One Time Password) 생성 흐름 - 한국정보통신기술협회 참조

연계정보 생성
• 연계정보는 OTP 생성키와 연산하여 OTP 생성에 필요한 정보이다.
• 연계정보는 OTP 생성 방식에 따라 다양하다.**(시각, 이벤트 정보 등)**

⇓

생성 알고리즘
• OTP 생성에 사용하는 암호 알고리즘이다.(HIGHT, AES, HMAC-SHA256 등)
• 생성 알고리즘에서 연계정보를 암호화하여 **암호문을 생성**한다.

⇓

추출 알고리즘
• 추출 알고리즘은 OTP를 추출하는 알고리즘이다.
• 생성 알고리즘에서 생성된 암호문에서 OTP를 추출한다.
• OTP는 **숫자** 또는 **문자**로 구성될 수 있다.

• OTP는 높은 수준의 보안을 유지하며, 사용자를 인증할 필요가 있을 때 사용된다.
• OTP는 세션 또는 통신시마다 매번 변경되며, 단 한번만 사용 가능한 패스워드이다.
• OTP 생성 및 인증 방식은 여러 가지가 있다.
• **예** : S/KEY 방식, 시간 동기화 방식, 이벤트 동기화 방식, **도전-응답 방식**

◈ S/KEY 방식

• **해시체인**에 기반한 OTP 생성 알고리즘이다.(해시함수의 역연산은 어렵다는 점)

클라이언트에서 임의의 비밀키를 결정하여 서버로 보낸다.

↓

서버는 **해시체인** 방식으로 이전 결과 값에 대한 해시값을 구하는 작업을 n번 반복한다.
첫 번째 값은 클라이언트에서 받은 비밀키를 사용한다.

↓

해시체인 방식으로 생성된 n개의 OTP를 서버에 저장한다.

• 서버에 저장된 OTP 목록이 유출되면 보안에 취약해지는 단점이 있다.
• 생성한 OTP를 모두 소진하면 새로 설정을 해야 한다.
• 벨 연구소에서 개발한 OTP 생성 알고리즘이다.
• S/KEY 방식은 **유닉스** 계열 운영체제에서 사용자 인증에 사용되고 있다.

◈ 시간 동기화 방식

• OTP 생성을 위한 입력 값으로 **현재 시각**을 사용하는 방식이다.(임의의 입력값 불필요)
• 시간 동기화 방식은 RSA사에서 만든 "**시큐어 ID**"에 적용되었다.
• 클라이언트는 현재 시각을 입력값으로 OTP를 생성하여 서버로 보낸다.
• 서버도 같은 방식으로 OTP를 생성하여 클라이언트가 보낸 값의 유효성을 검사한다.
• 클라이언트와 서버의 **시간 동기화**가 정확하지 않으면 인증에 실패하게 된다.(단점)
• 이를 보완하기 위해 1~2분 정도를 OTP 생성 간격으로 둔다.**(시간오차범위 허용)**
• 클라이언트와 서버가 통신하는 횟수가 비교적 적다.(입력값을 주고받을 필요 없음)
• 스마트폰 같은 모바일 기기를 클라이언트로 사용하기 적합하다.(별도 추가 장비 필요 없음)
• 다른 OTP 생성 원리에 비해 피싱 등에 안전하다.

◈ 이벤트 동기화 방식

• OTP 토큰과 OTP 인증서버가 **동일한 카운트 값**을 입력값으로 OTP를 생성하는 방식이다.
• 서버와 클라이언트는 카운트 값을 동일하게 증가시켜 가면서 OTP를 생성한다.
• 사용자가 인증을 요청할 때마다 OTP 값을 생성한다.

〈OTP 메커니즘〉

① 클라이언트는 OTP 토큰에서 생성한 OTP를 서버 측에 보낸다.
→ 서버와 클라이언트 사이에 미리 약속된 규칙에 의해서 OTP를 생성된다.
② 서버도 같은 규칙에 의해 OTP를 생성하여, 서로 비교한다.
→ 서버는 데이터베이스에서 사용자의 비밀값을 가져온 후, OTP를 생성한다.

• 인증이 필요할 때 OTP만 주고받으므로 토큰과 서버는 물리적인 연결이 필요 없다.
• 토큰에서 생성된 OTP를 사용자가 키보드를 통해 입력하는 형태로 동작한다.

기출문제 분석

1. OTP(One Time Password)에 대한 설명으로 옳지 않은 것은? [2018년 국회 9급]

① OTP는 비밀번호 예측 공격을 막기 위한 방법으로 사용 가능하다.
② 패킷 스니핑을 통한 비밀번호 재사용 공격의 대응책으로 활용 가능하다.
③ 동기화 방식 OTP에서는 시간과 인증 횟수를 기반으로 비밀번호를 동기화 한다.
④ 비동기화 방식 OTP는 인증서버에서 전송된 난수를 기반으로 비밀번호를 생성한다.
⑤ 시간 동기화 방식 OTP는 인증서버와 OTP 생성기의 시간오차범위를 허용하지 않는다.

♤ OTP(One Time Password)

- 시간 동기화 방식 OTP는 인증서버와 OTP 생성기의 시간오차범위를 허용하지 않는다.(×)
  → 클라이언트와 서버의 시간 동기화가 정확하지 않으면 인증에 실패하게 된다.(단점)
  → 해서, 일반적으로 1~2 분정도를 OTP 생성 간격으로 둔다.
- 시간 동기화 방식은 OTP 생성을 위해 시각을 사용하는 방식이다.

정답 : ⑤

2. 사용자 인증을 위한 접근방법으로 사용자가 알고 있는 것, 사용자가 가지고 있는 것, 사용자 자신의 특성을 이용하는 것 등이 있다. 최근 사용이 증가하고 있는 OTP(One Time Password)에 대한 설명으로 옳은 것은? [2016년 국가 7급]

① 어떤 패스워드가 일정 유형으로 반복해서 생성된다.
② 사용자가 알고 있는 정보에 의한 인증 기법이다.
③ 일반적으로 사용자 자신의 특성을 이용하는 기법들에 비하여 식별 오류 발생 가능성이 높다.
④ 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.

♤ 사용자 인증 – OTP(One Time Password)

- OTP는 생성 방식에 따라 사용자나 인증 서버의 관리 부담이 발생할 수 있다.(????)
  → 이유 : 인증을 위해 서버-클라이언트 사이에 통신 요구 횟수가 많을 수 있다.**(방식에 따라)**

정답 : ④