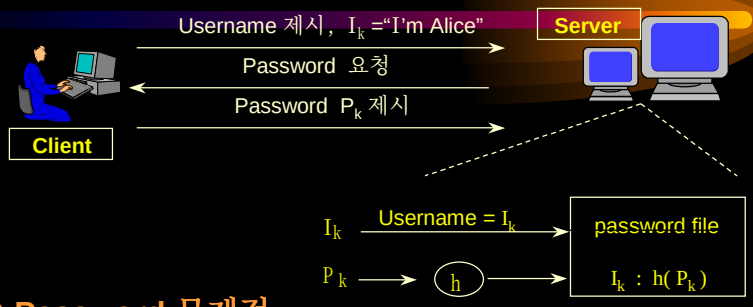
❑ 개인식별, 실체인증

- ❒ Identification, Entity Authentication
- ❒ Access to Computer System, Entry to Building, Withdrawing from ATM
- ❒ Server's authenticating Client

❑ 개인식별 방식

- ❒ 사용자 고유의 물리적 특성 (voice, fingerprint, 홍채)
- ❒ 사용자가 알고 있는 정보 (password)
- ❒ 사용자가 소지하고 있는 것 (smart card, token card)

❑ Password 방식



❑ Password 문제점

- ❒ password에 대한 불법적 도청
- ❒ password에 대한 추측의 용이함
  - online / offline guessing
  - short password, no password, username=password
- ❒ password file에 대한 공격 가능성

❑ Password 보호 전략

❑ Password Control

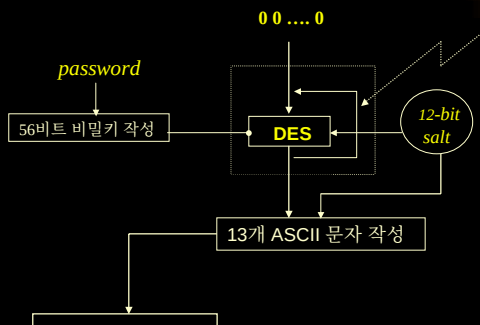
- Limited Attempts (잘못된 로그인 회수 제한)
- Password Aging (패스워드 노화기법)
- Minimum Length (패스워드 최소 길이 제약)
- Lockout of Dormant Account (장기 유휴 account 폐쇄)

❑ Password Checking for Good Password

- Reactive Password Checking - "CRACK"
- Proactive Password Checking

❑ UNIX Password SYSTEM

❑ Password 생성

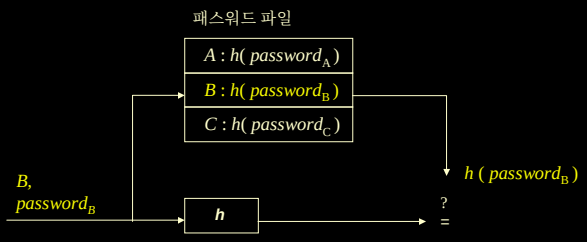


- 중복된 password 문제
- dictionary attack (key search)

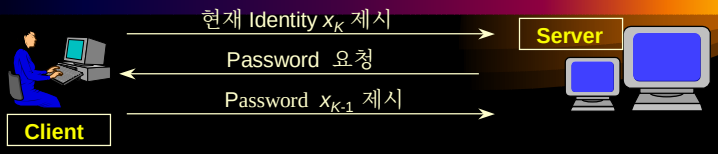
cspark : **eH5/.mj7NB3dx** : 181: 100 : Chang-Seop Park: /u/cspark: /bin/csh

❑ UNIX Password SYSTEM

❑ Password 확인

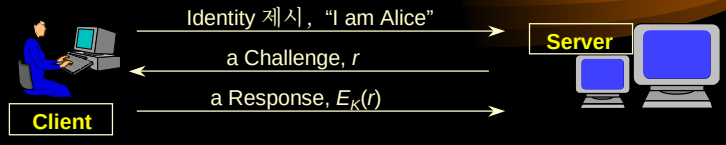


❑ One-Time Password



- ❑ 각각의 System 접근마다 서로 다른 Password 사용
- ❑ Client와 Server 간의 공유된 Secret 없음
- ❑ **One-way Function *h*( )** 사용
- ❑ Client에 의해 x_0 와 $x_i = h(x_{i-1})$ for $i = 1,2,3,.. k$ 선택 { *k* access tickets }
- ❑ password x_k는 다음번 access 때의 user identity
- ❑ System 접근회수의 제한
- ❑ Sequence x_i를 System 접근마다 다시 계산

❑ Challenge-Response 개인식별 프로토콜

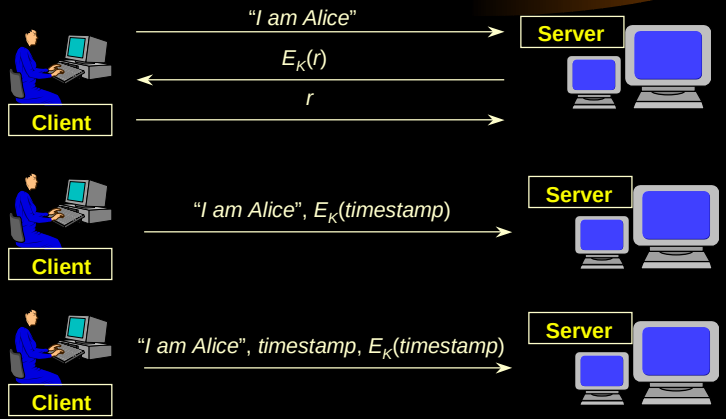


- ❑ 시도-응답 개인식별 프로토콜
- ❑ Client와 Server가 공통된 secret key *K* 를 공유
- ❑ ***E*** is a public encryption function e.g. DES ; hash function
- ❒ 비밀정보(secret information)의 상호교환은 없음
- ❒ key database 보호
- ❒ 매번 상이한 Response 값; ***E*** 함수의 안전성에 기반

암호이론과 보안 개인식별시스템

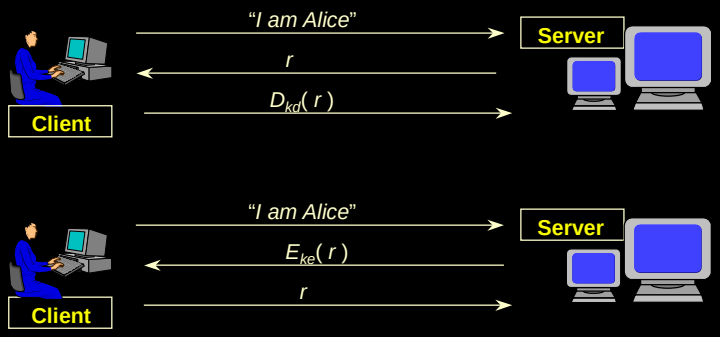
❑ Challenge-Response 개인식별 프로토콜

❑ Symmetric Key

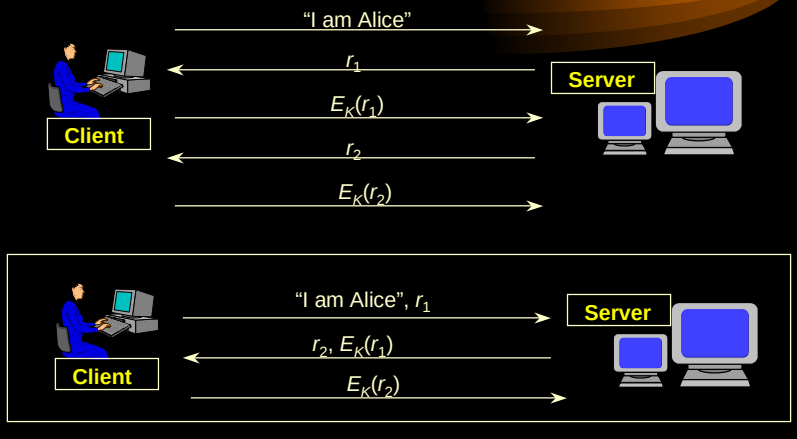


❑ Challenge-Response 개인식별 프로토콜

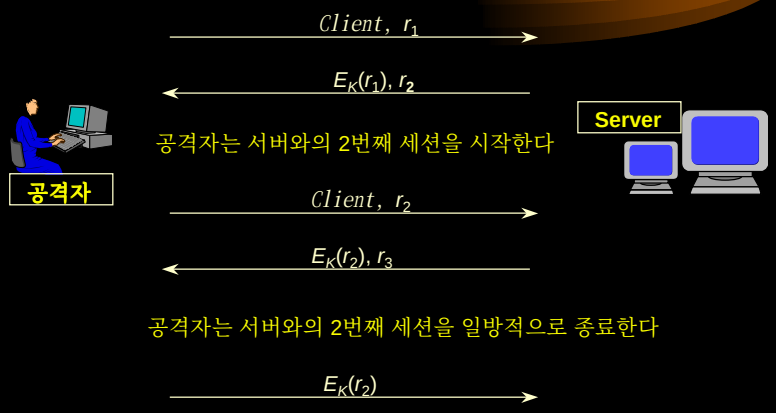
❑ Public Key



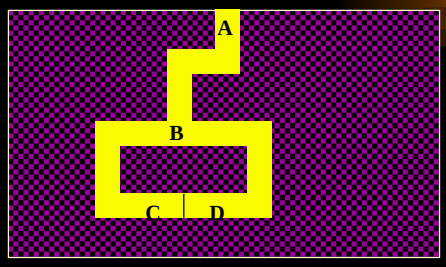
❑ Mutual Identification (상호 개인식별)



❑ Reflection Attack (반사공격)

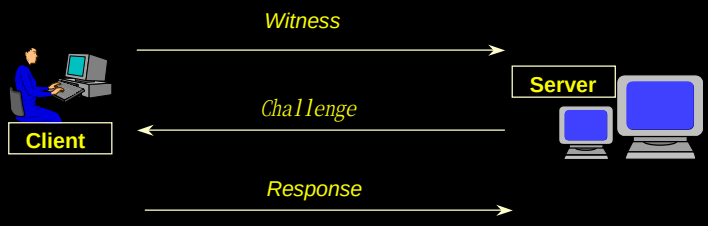


❑ Zero-Knowledge Proof



❑ Zero-Knowledge Proof of Identity

❑ 대화형 영지식 개인식별 프로토콜



❑ Quadratic Residues modulo a prime

- p is a prime
- If $(v,p) = 1$ and $x^2 \bmod p = v$ has a solution, then
  v is called a "**quadratic residue**" of modulo p.
  x is a "**square root**" of quadratic residue v.

- e.g.
  p=7, $x^2 \bmod p = v$, $(v,p) = 1$
  $1^2 \bmod 7 = 1$, $2^2 \bmod 7 = 4$, $3^2 \bmod 7 = 2$
  $4^2 \bmod 7 = 2$, $5^2 \bmod 7 = 4$, $6^2 \bmod 7 = 1$
  {1,2,4} = a set of quadratic residues of modulo 7
  {3,5,6} = a set of quadratic non-residues

❑ Quadratic Residues modulo a prime

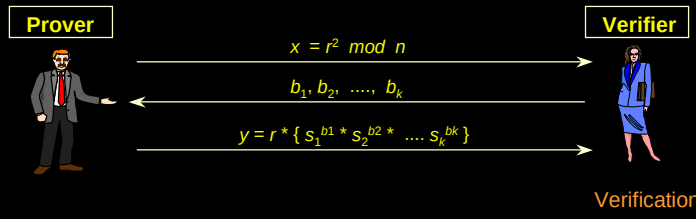
- Let $s = (p - 1) / 2$, where $p > 2$ is a prime
- $S_p = \{ x^2 \bmod p : 0 < x \leq s \}$
- The elements of S_p are quadratic residues modulo p
- There are s quadratic residues and s quadratic non-residues

- Let $s = (p - 1) / 2$, where $p > 2$ is a prime
- Let v be a quadratic residue modulo p
- v has exactly two **square roots modulo p** in Z_p^*
- one in (0, s] and the other in (s, p-1]

암호이론과 보안 영지식 개인식별

❑ Feige-Fiat-Shamir Interactive Identification

- a public modulus $n = p*q$
- choose a random v_i such that $x^2 \bmod n = v_i$, where $i = 1,2, ..., t$ and $v_i^{-1} \bmod n$ exists
- compute $s_i = \text{sqrt} (v_i^{-1}) \bmod n$



Verification

❑ *Schnorr* 영지식 개인식별 프로토콜