Identification

1. 4 ~ 6-digit PIN(Personal Identification Number) at ATM(Automatic Teller Machine)
2. Purchase by credit card
3. Asking a service by telephone card or membership cards
4. Remote access to host under Client /Server environment
5. Access to restricted areas, etc

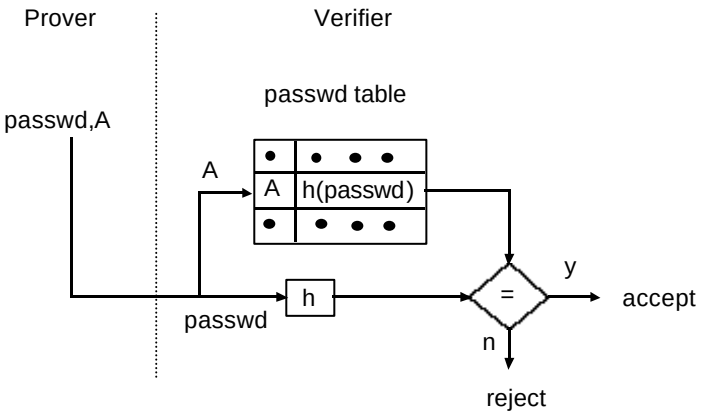
Way of Identification

- Password-based scheme (weak authentication)
  - crypt passwd under UNIX
  - one-time password
- Challenge-Response scheme (strong authentication)
  - Symmetric cryptosystem
  - Asymmetric cryptosystem
- Cryptographic Protocols
  - Fiat-Shamir identification protocol
  - Schnorr identificatoin protocol, etc

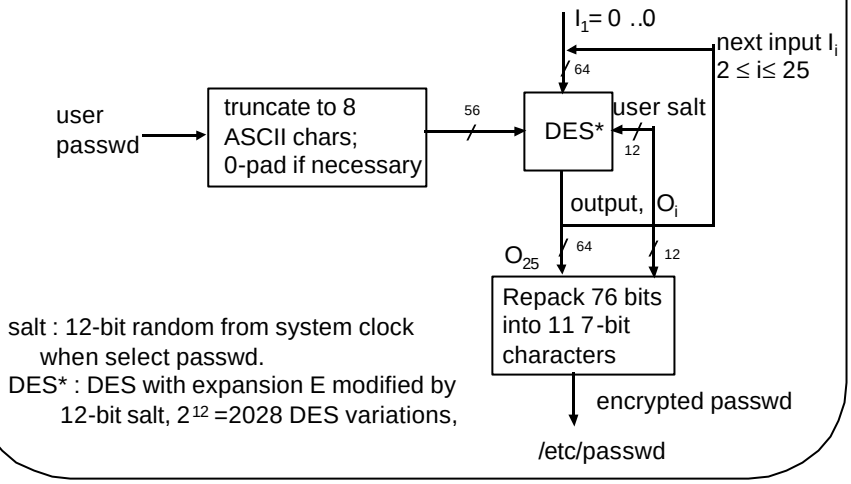
Identification by personal information

Method	Secret info.	Reliability	Security	Cost
What you remember	Password Telephone No. Reg. no	M/L	M(theft) L(imperso-nation)	Cheap
What you have	Registered Seal Magnetic Card IC Card	M	L(theft) M(imperso-nation)	Reason-able
Biometric Character-stics	Fingerprint, Eye, DNA, face, Voice etc	H	H(theft) H(Imperso-nation)	Expen-sive

Identification by Password



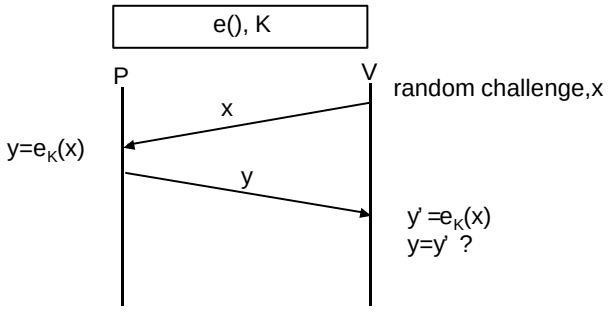
crypt passwd in UNIX



salt : 12-bit random from system clock
when select passwd.
DES* : DES with expansion E modified by
12-bit salt, 2^{12} =2028 DES variations,

Challenge-Response Scheme(I)

- ✓ **Using Symmetric Cryptosystem**



Challenge-Response Scheme(II)

- ✓ **Using Asymmetric Cryptosystem**

  P can prove to have secret information in either way :

  (1) P decrypts a challenge encrypted under P' s public key.

  (2) P digitally signs a challenge.

Cryptographic Protocol

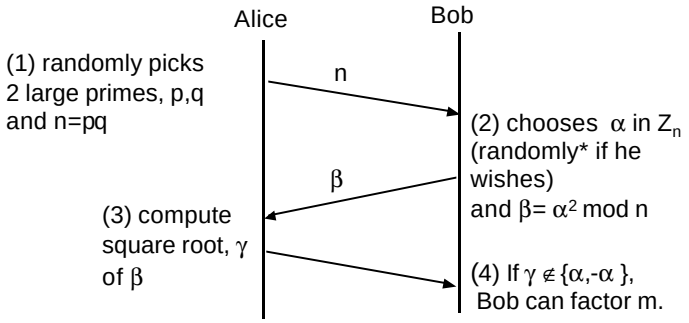
2 or more entities involved :
- Easy in face-to-face situation, but
- Extremely difficult non face-to-face situation over communication like Internet

$\Rightarrow$ magic protocol

- Coin Flipping by telephone
- Comparison-asset protocol
- Mental Poker
- Electronic Voting
- Electronic Contract
- Electronic Cash
- Remote Entity Authentication, etc

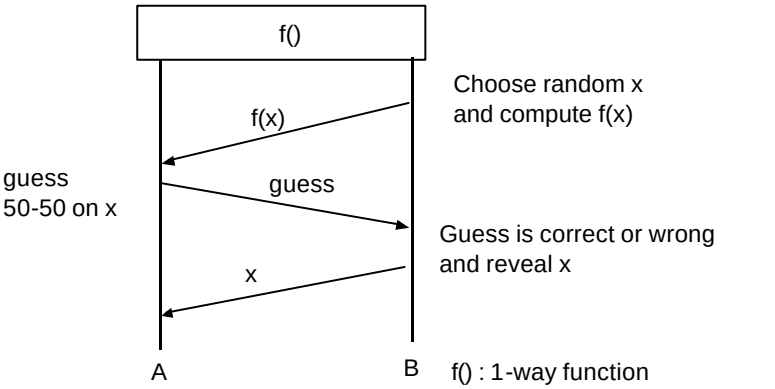
Coin Flipping(I)

- **Rules : Bob wins if he can factor n at the end (and prove this by sending p or q); otherwise Alice wins.**



(Basic Concept) Only who knows p, q can compute square root of n.
* If Bob chooses randomly, then the game is fair for himself.

Coin flipping (II)



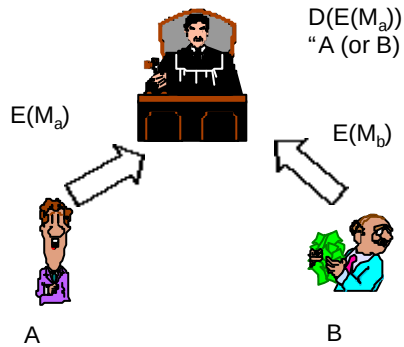
Comparison-asset protocol(I)

- **(Problem) Without informing his own asset (or age), any communication protocol to compare who have more or who is older**

(1) Using TTP
(2) Using random number
(3) Using PKC

Comparison-asset protocol(II)

(1) Using TTP

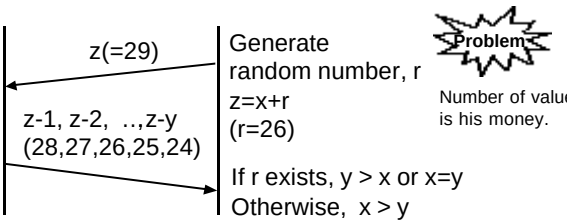


(1) Collaboration A (or B) and TTP
(2) Malicious Acts by TTP

Comparison-asset protocol(III)

(2)Using random number

(Assumption)
- x and y has a unit in 1 to 10.
- No one is a liar.
- What a claimer knows is that he is richer than other ?
- If both have same, claimer is a looser.



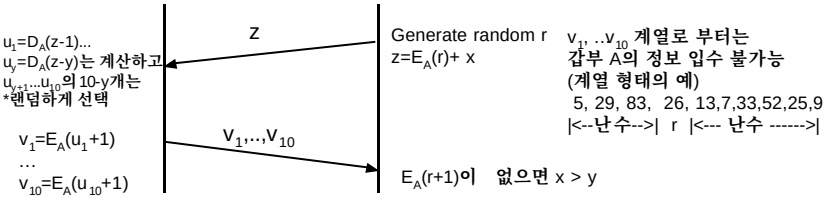
Problem

Number of values A has sent is his money.

Comparison-asset protocol(IV)

(3)Using PKC

(Assumption)
- x and y has a unit in 1 to 10.
- No one is a liar.
- What a claimer knows is that he is richer than other ?
- If both have same, claimer is a looser.



v_1, ..v_{10} 계열로 부터는 갑부 A의 정보 입수 불가능
(계열 형태의 예)
5, 29, 83, 26, 13,7,33,52,25,9
|<--난수-->| r |<--- 난수 ------>|

*랜덤 선택 값 중 $D_A(z-1),D_A(z-10)$이 되지 않도록 주의.

$u_x = D_A(z-x)=D_A(E_A(r)+x-x)) = r$
$v_x = E_A(ux+1)=E_A(r+1)$

Zero-Knowledge Interactive Proof

- **GMR(Goldwasser, Micali, Rackoff) : Proposed 1985 at first.**
- **ZKIP (Zero Knowledge Interactive Proof) : Between Prover and Verifier**
  - **Completeness : Only true P can prove V.**
  - **Soundness : False P' can' t prove V.**
  - **0-Knowledge : No knowledge transfer to V.**

Concept of ZKIP

By Quisquater and Guillou
P knows the secret, but he doesn' t want to reveal his secret.
1. V stands at point A.
2. P walks all the way into the cave, either C or D.
3. After P disappeared into the cave, V walks to point B.
4. V shouts to P asking him either to:
(a) come out of the left passage or (b) come out of the right passage
5. P complies, using the magic words to open secret door if he has to.
6. P and V repeat step (1) -(5) t times

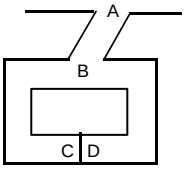
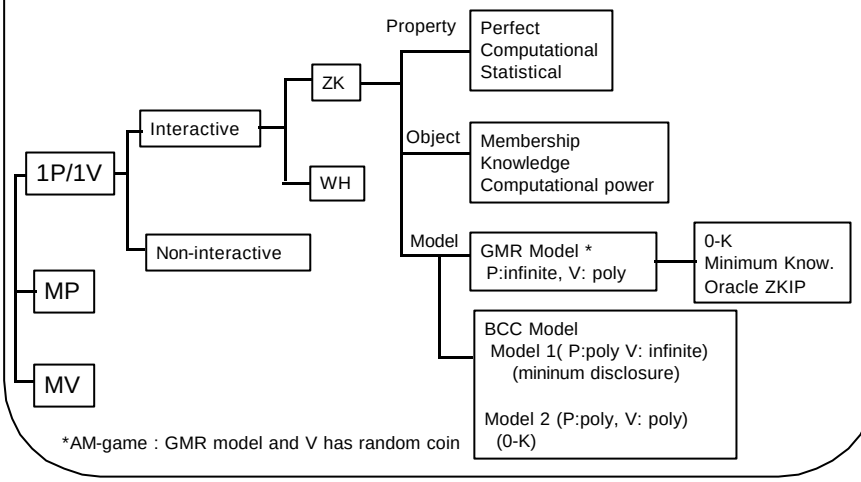


Fig.
0-knowledge cave

P knows the magic words
to open the secret door between
C and D.

Classification of ZKPS



Way of ZKIP

There are many ways to prove the truth of a proposition like "I know the modular square root of V" (or any other PSPACE problem):

1. **To give the proof (i.e., to tell the square root to the verifier)**
2. **Zero-knowledge proof : to convince the verifier that the claim holds without giving him any information on the proof (and thus he cannot compute the square root).**

ZKIPs are used in identification scheme, in which a user (called the prover) proves to the verifier that he knows a certain secret, without revealing the secret, or any information on the secret.

F-S Identification(I)

- **(Preparation)**

(1) Unlike in RSA, a trusted center can generate a universal *n*, used by everyone as long as none knows the factorization.

(2) P has an RSA modulo *n=pq* whose factorization is secret.

(3) secret key : P chooses random value *S*, s.t. gcd(*S*,*n*)=1.(1 < *S* < *n*)

public key : P computes $I=S^2$ mod *n*, and publishes (*I*,*n*) as public

F-S Identification(II)

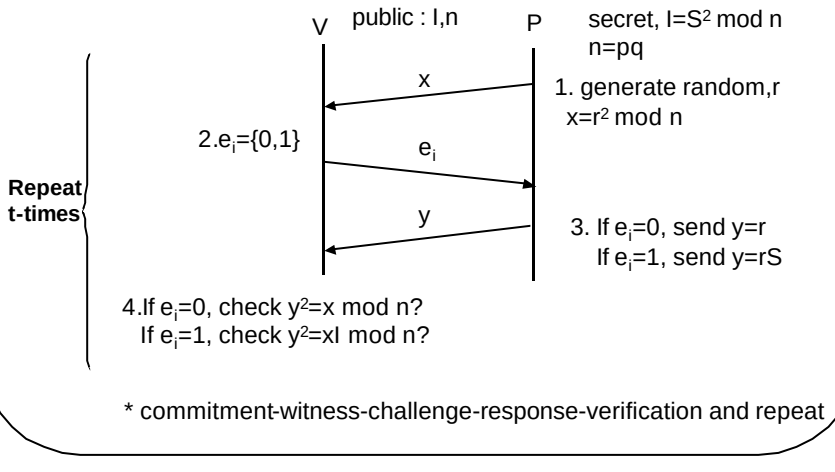
(Goal)

P has to convince V that he knows secret key *S* corresponding public key (*I*,*n*) (i.e., to prove that he knows a modular square root of *I* mod *n*), without revealing *S*.

F-S Identification(III)

1. P chooses random value r ($1<r<n$) and computes $x=r^2 \bmod n$. then sends x to V.
2. V requests from P one of the following request at random
   (a) r or (b) $rS \bmod n$
3. P sends the requested information to V.
4. V verifies that he received the right answer by checking whether
   (a) $r^2 = x \bmod n$ or (b) $(rS)^2 = xI \bmod n$
5. If verification fails, V concludes that P does not know S, and thus he is not the claimed party.
6. This protocol is repeated t (usually 20 or 30) times, and if in all of them the verification succeeds, V concludes that P is the claimed party.

F-S Identification(IV)



* commitment-witness-challenge-response-verification and repeat

Security of F-S scheme

(1) It is assumed that computing S is difficult, actually the difficulty is equivalent to that of factoring *n*.

(2) Since P doesn' t know in advance (when he chooses *r* or *rS* mod n) which question V will ask, he can' t choose the required choice. He can succeed in guessing V' s question with prob. 1/2 for each question, and thus V can catch him in half of the times, and fails to catch him in half of the times. The protocol is repeated t times,and thus the prob. that V fails to catch P in all the times is only 2^{-t}, which is exponentially reducing with *t*. (*t*=20 or 30)

F-S scheme is ZKIP

- ✓ **The F-S protocol convinces V that P knows the square root of *I*, without revealing any information on *S*. However, V gets <u>one bit</u> of information : <u>he learns that *I* is a quadratic residue</u>**

Other Identification scheme

- Feige-Fiat-Shamir scheme
- Guillou-Quisquarter scheme
- Schnorr scheme
- Okamoto scheme etc.