

# Key Escrowing Systems and Limited One Way Functions

William T. Jennings  
Southern Methodist University  
& Raytheon E-Systems, Greenville Div.  
(903) 457-6756  
wtj1@esygv1.com

## KEY ESCROW SYSTEMS

Characterized by  
Many Deposits, Few Withdrawals

Write BW >> Read BW

## KEY ESCROW SYSTEMS

- Only legitimate to make withdrawals one at a time.
- Should never need to read entire database.

## KEY ESCROW SYSTEMS

- Requires strong encryption protection
- May require secret sharing/splitting techniques

## KEY ESCROW SYSTEMS

- Requires Central, Trusted Authority
- Requires strong encryption protection
- May require secret sharing/splitting techniques

## LIMITED ONE WAY FUNCTIONS

- Feasible but costly to invert. Requires both time and computational resources.

## PROPOSED ALGORITHM

- Example of Limited One-Way Function.
- Alice generates pairs of cryptograms and decryption keys.
- Each cryptogram conveys a token.

## PROPOSED ALGORITHM

- Bob selects one at random and performs the decryption.
- Bob takes the token, adds randomization and signature information, then re-encrypts.
- Alice uses retained secret keys to recover token.

## PROPOSED ALGORITHM

- Carol represents a passive observer of the channel recording the transaction.
- Withdrawals occur by either breaking the underlying cryptosystems (intractable), or solving large numbers of simple puzzles (built-in front door).

## Why Apply Limited One-Way Functions?

- Addresses class of problems not adequately resolved by conventional cryptographic means.
- Withdrawal bandwidth can be adjusted to fit available bandwidth.
- Built In Work Function discourages excessive withdrawals. Makes abuse infeasible provided resources physically limited.
- Patterns of abuse may be detectable due to systemic (measurable) use of resources.