Many-Time Pad: Theme and Variations
Dorothy Denning
SSP 1983

- Method of attack, not security
- Unlike one-time pad, it can be used over and over 😊

Applications
- George Davida’s attack on RSA
- Tracker attacks on statistical DB
- Covert channels

Overview
- Attacker wants $f(X)$ for some $X$
- Security blocks its release
- Attacker gets it anyway
Step 1 of attack

• Attacker pads X with pad P
Step 2 of attack

- Attacker gets $f(P)$
- Attacker gets $f(P \circ X)$
Step 3 of attack

- Attacker computes $f(X)$
  
  $f(X) = f(P)^{-1} \cdot f(P \circ X)$

Requirements

Input/output domains are groups

$f$ is a homomorphism

$f(P \circ X) = f(P) \cdot f(X)$