

Week 4

Dictionary Attack

Dictionary Attack

- If keys are poorly chosen, attacks can be very simple
 - Often the user's password is converted to the key
 - The attacker tries passwords from a dictionary, rather than all possible keys
 - For a 20,000-word dictionary, one trial/second will crack a poor password in less than 6 hours



School of Information Studies
SYRACUSE UNIVERSITY