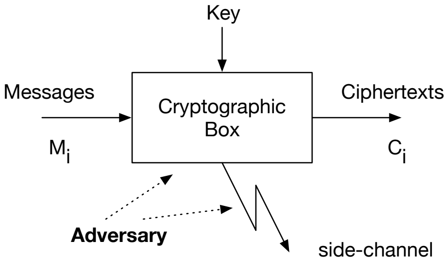
Side-Channel Attacks and Countermeasures



Side-Channel Cryptanalysis

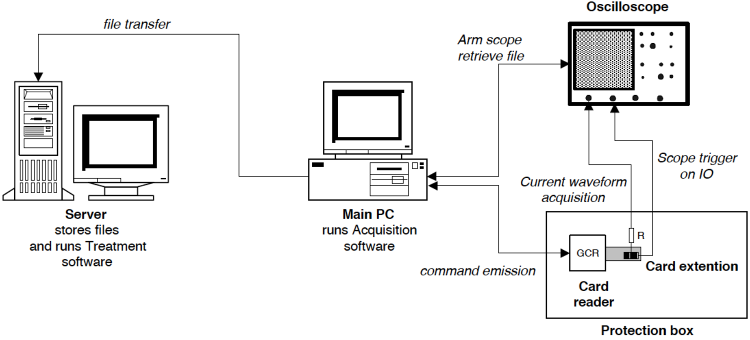
- Cryptographic algorithms must run on a real device
- Devices have physical properties
- Devices will emanate information regarding cryptographic algorithm, key, and message
- Adversary having access to these side channels will extract information
  - Timing
  - Power
  - Electromagnetic
  - Acoustic

Side-Channel Cryptanalysis

- A new area of applied cryptography
- The study of breaking cryptosystems using side-channel information

- **Timing attacks** exploit time differences occurring for various input values
- **Power attacks** exploit the instantaneous power consumption during critical phases of the cryptographic code
- **Electromagnetic attacks** exploit the instantaneous electromagnetic emanations during critical phases of the cryptographic code

Equipment Setup for Power and Timing Analysis



Smart Cards

- Side-channel attacks have been phenomenally successful at breaking the cryptosystems running on the smart cards
- A smart card is a computational device that runs a cryptographic protocol and contains a secret or private key
- Usually smart cards do not have their own power device, or battery, which makes them vulnerable to power attacks
- The card reader providing the power can monitor and record the instantaneous power curve

Smart Cards

- Smart cards are used in several applications: banking, credit cards, parking cards, ID cards, as SIM cards in mobile telephones