# Encryption, continued

## Public Key encryption and Digital Signatures

# Public Key encryption

- Eliminates the need to deliver a key
- Two keys: one for encoding, one for decoding
- Known algorithm
  - security based on security of the decoding key
- Essential element:
  - knowing the encoding key will not reveal the decoding key

# Effective Public Key Encryption

- Encoding method E and decoding method D are inverse functions on message M:
  - D(E(M)) = M
- Computational cost of E, D reasonable
- D cannot be determined from E, the algorithm, or any amount of plaintext attack with any computationally feasible technique
- E cannot be broken without D (only D will accomplish the decoding)
- Any method that meets these criteria is a valid Public Key Encryption technique