II. Digital Signatures

- Just like “real” signatures
  - Authentic, Unforgeable
  - Verifiable, Non-repudiable
- To sign a message M, Alice encrypts message with her own private key
  - Signed message: [M, $K_{Apriv}(M)$]
  - Anyone can verify, using Alice’s public key, that Alice signed it
- To make it more efficient, use a one-way hash function, e.g., SHA-1, MD-5, etc.
  - Signed message: [M, $K_{Apriv}(Hash(M))$]
  - Efficient since hash is fast and small; don’t need to encrypt/decrypt full message