Lecture 8 — Cryptolite

8.1 Authenticated encryption

- Good to achieve both secrecy and integrity
- Secure authenticated encryption
  - Made of
    - CPA-secure: $\Pi_E = (Enc, Dec)$
    - Secure MAC: $\Pi_M = (Mac, Vrf)$
    - Instantiated using indep. keys, ke and km
- Generic AE constructions
  1. encrypt-and-authenticate
     - $Enc_{ke}(m) \to c; Mac_{km}(m) \to t$ send ciphertext (c, m)
     - if $Dec_{ke}(c) = m \neq$ fail and $Vrf_{km}(m, t)$ accepts, output m; else output fail
     - Not secure
  2. Authenticate then encrypt
     - Not secure
  3. Encrypt then authenticate
     - Encrypt to get c, Mac to get t and ciphertext is (c, t)
     - Vrf (c, t) then output Dec(m), else fail
     - secure scheme generally
- Possible attacks
  - re-ordering attacks
  - reflection attacks
  - replay attacks

8.4 The RSA algorithm

-