Authenticated encryption

安全级别 :

- 验证加密为CCA安全级别的

Constructtion based on block cipher and mac

假设 (E, D) 为一个CPA安全级别的对称加密算法, 且(S, V) 是一个安全的MAC

- SSL : 先生成MAC, 再加密
- Ipesc : 先加密, 再生成MAC

一般来说 先Encrypt - then - mac 是提供 A.E.的