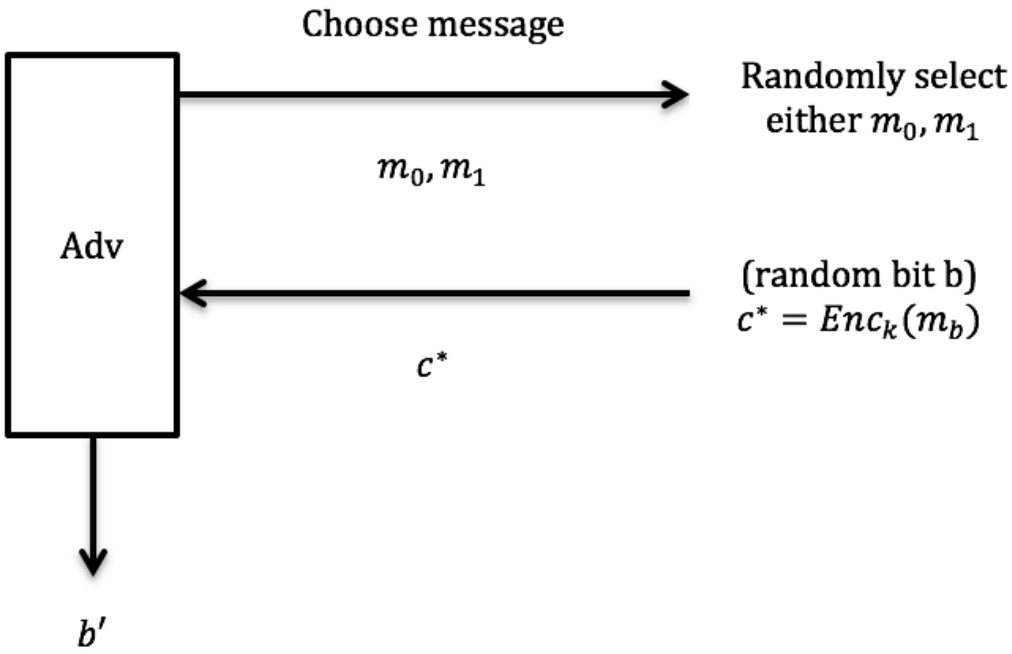
Review:

- Schemes
  - One-time-pad
  - AES-CBC mod (AES plays role of PRP)
  - 1-bit encryption with OTP
  - Arbitrary length message encryption
- **Attacks on Encryptions:**
  - Key recovery – adversary outputs secret key
    [Most difficult attack: can get other two attacks, once key recovery attack successfully]
  - Recovery of plaintext – adversary outputs plaintext
  - Indistinguishability

  * Knowing that my system can prevent key recovery doesn't mean my system can stand indistinguishability attack.

Cipher Schemes:

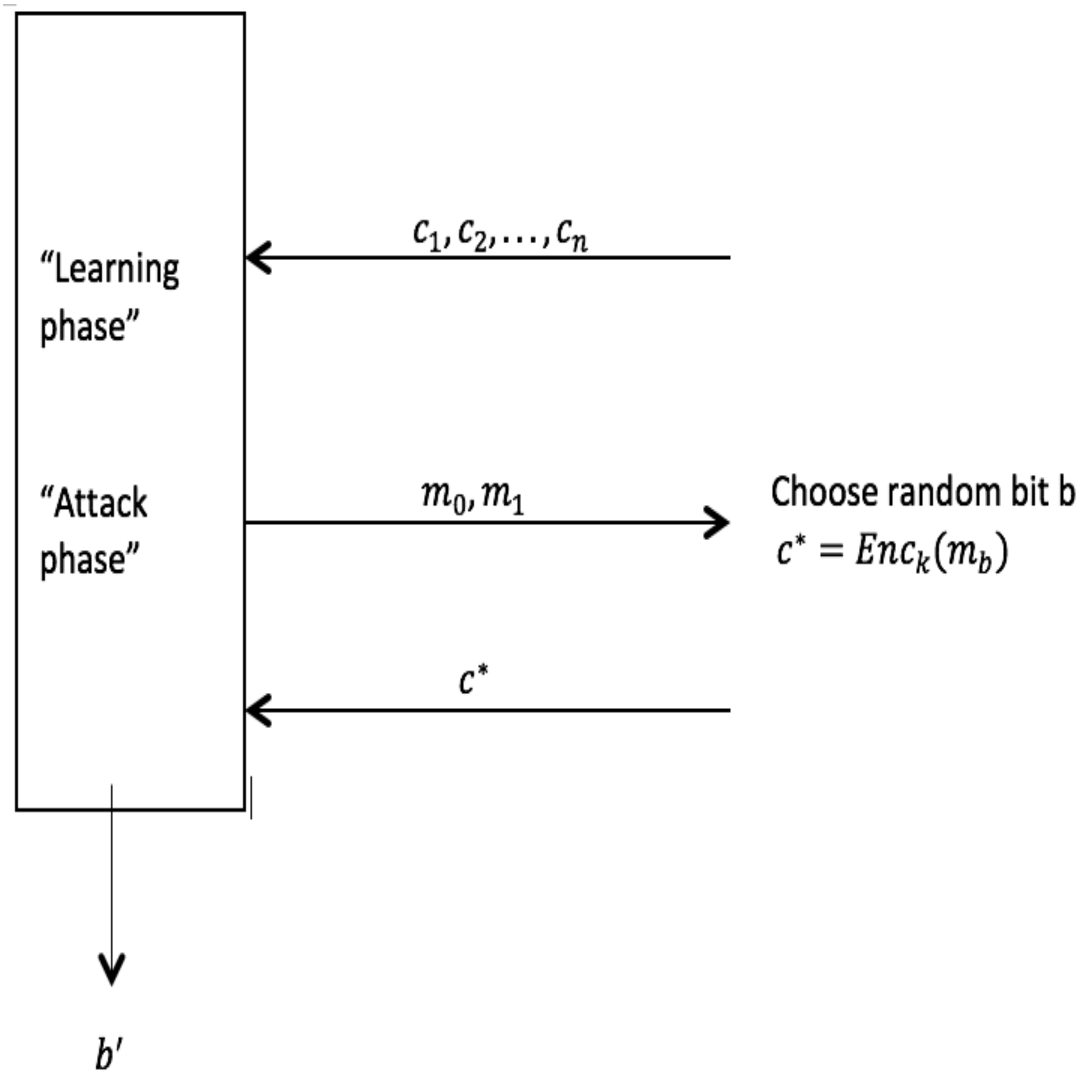
1.



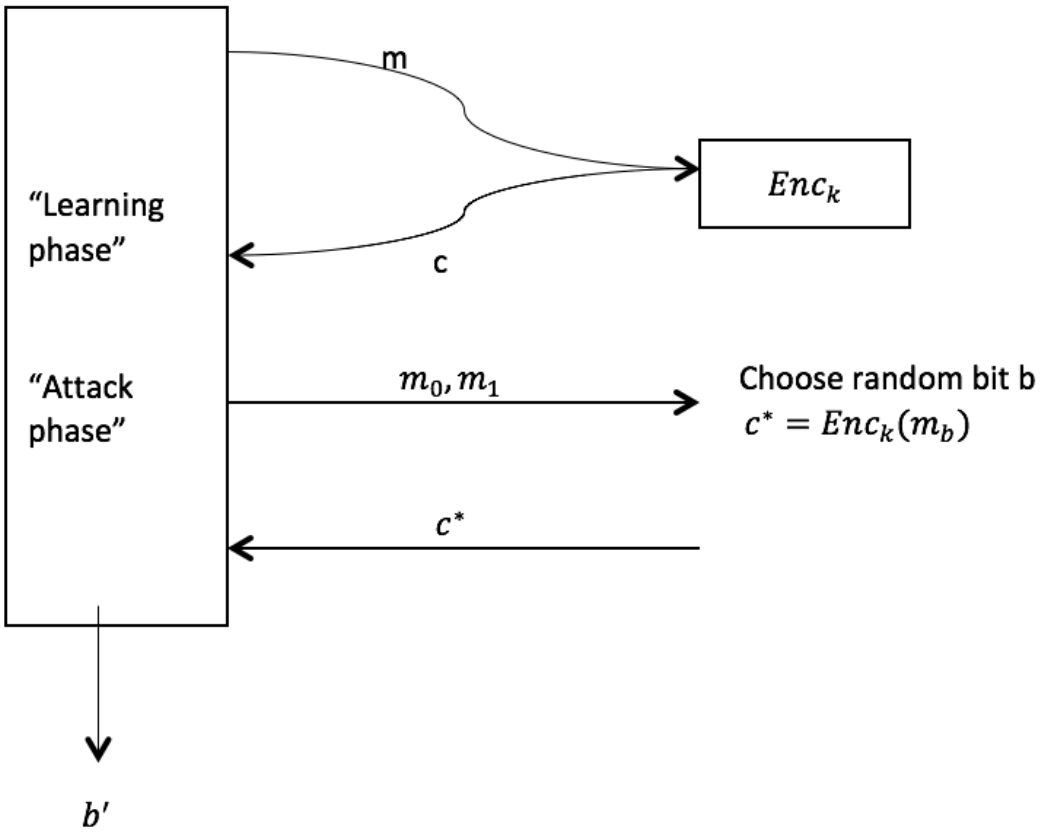
2. Known Ciphertext Attack – KCA, IND-KCA

independent indistinguish ~ Definition of Security

In real life, adversary can observe ciphertext, like through Wi-Fi or sitting on conversation



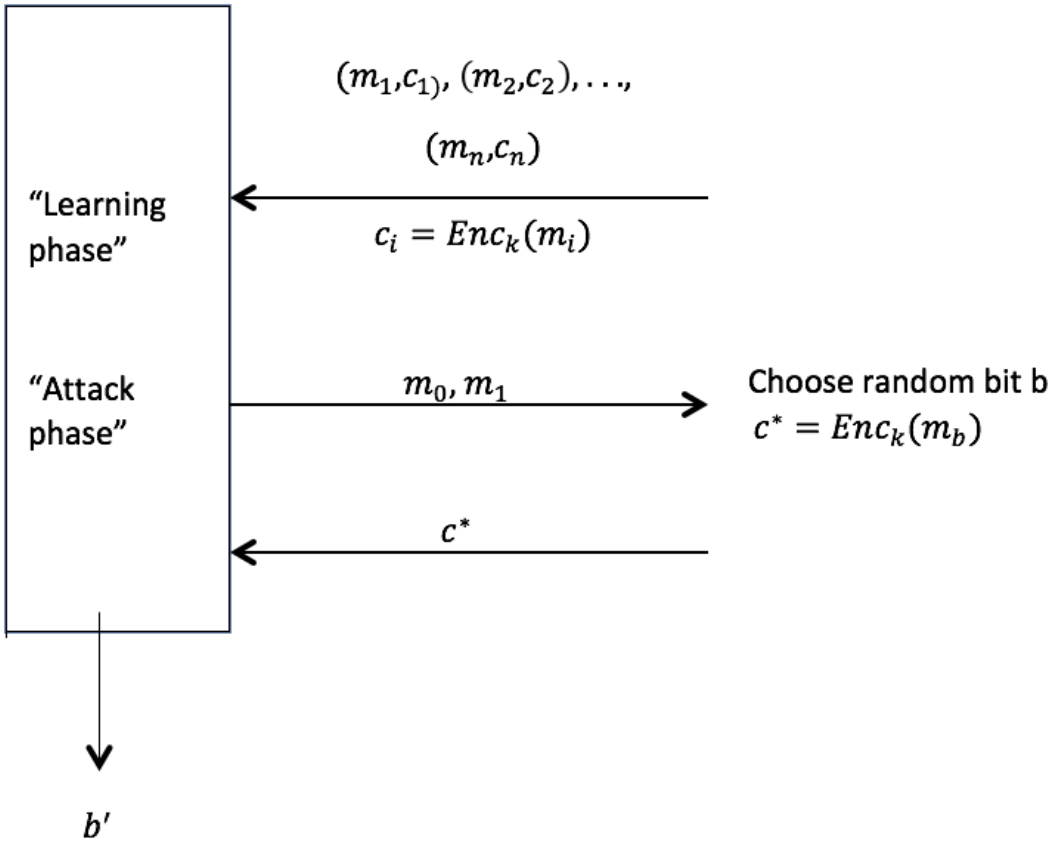
3. Chosen Plaintext Attack – CPA ~ "Encryption create"



Note: m_0 and m_1 may be queried during the learning phase. By defining security this way, rule out deterministic encryption scheme, i.e. satisfying CPA security.

* Adversary can choose m_0 and m_1 and get c_0 and c_1, but still use m_0 and m_1 to do this attack, and adversary still can't know b'. Even though m_0 and m_1 encrypt multiple times, c_0 and c_1 are different time to time. Like the penguin example, the same plaintext can't result the same ciphertext.

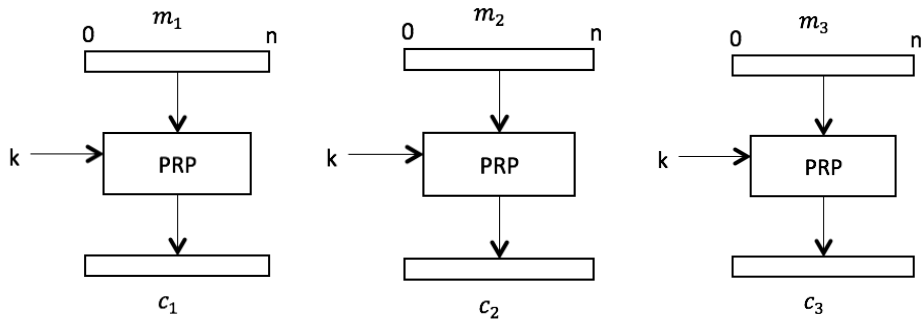
4. Known Plaintext Attack – KPA



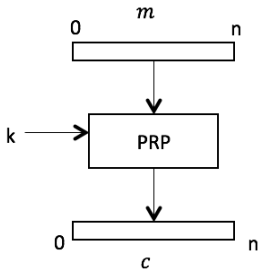
(Need to stand CPA)

E.g. EBM doesn't stand CPA, because the same plaintext always has the same ciphertext.

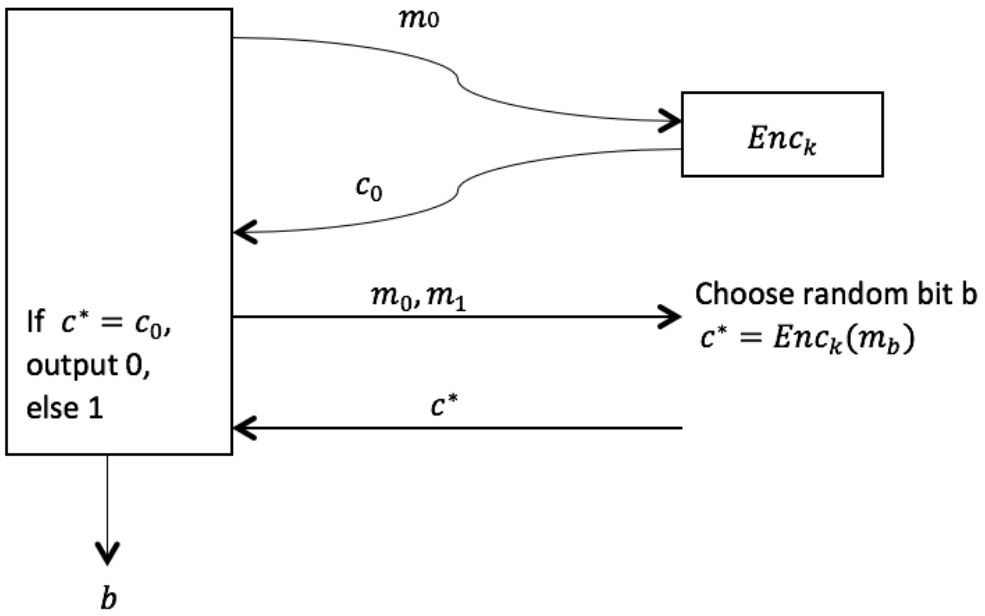
Recall EBM scheme.



Show $Enc_k(m)$ doesn't stand CPA.



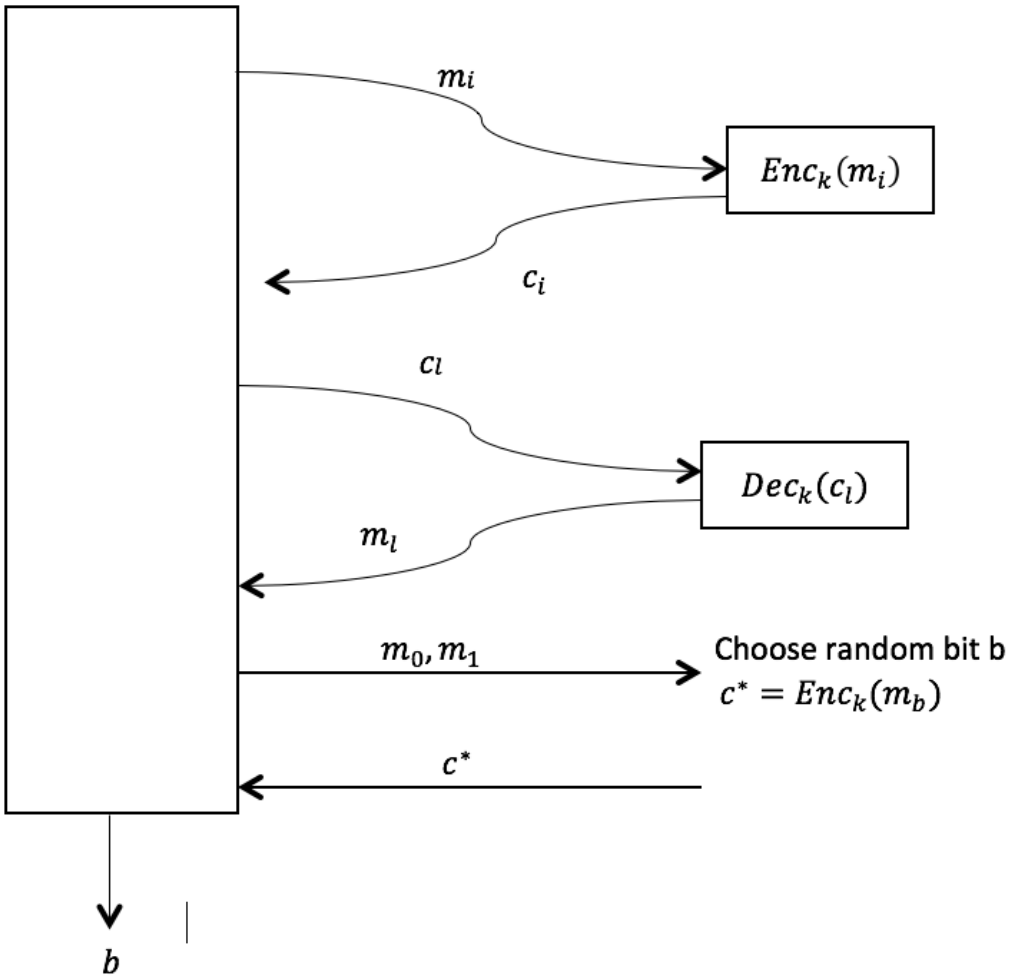
Prove:



* How to show a scheme isn't secure: giving a scenario which can break the security / showing an attack.

In real life, actual attack: Adversary could choose a certain plaintext as an advertisement and plant it on Google, and sit on the encrypted connection between users and Google. In this way, adversary will know the ciphertext. So defining our system that should stand for KPA isn't unreasonably hard requirement.

5. Chosen Ciphertext Attack – CCA



Can't ask for c^*.

* Given more information than CPA, could give ciphertext and get plaintext.

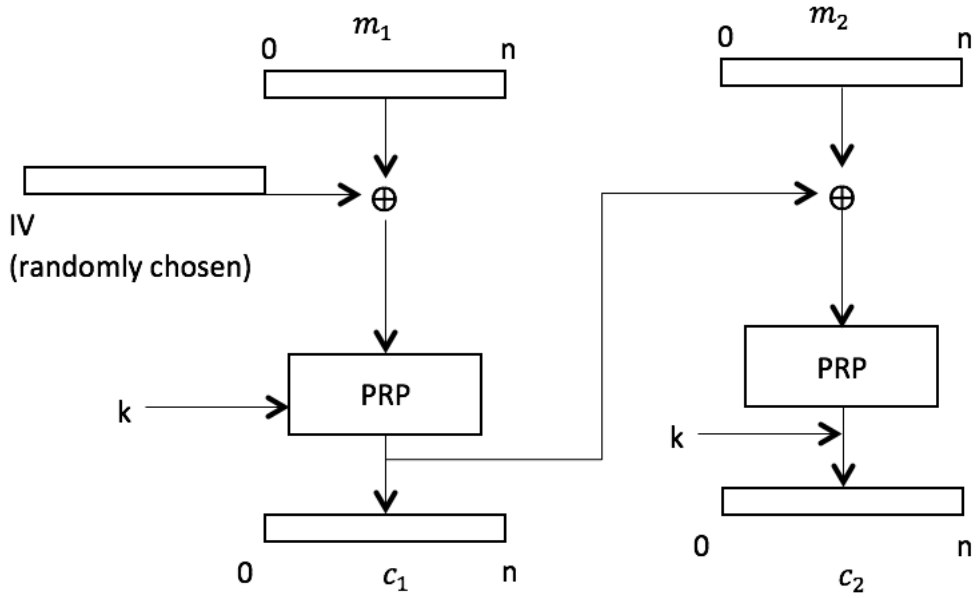
Summary:

Easiest for Adv:

CCA
CPA
KPA
Hardest for Adv: KCA

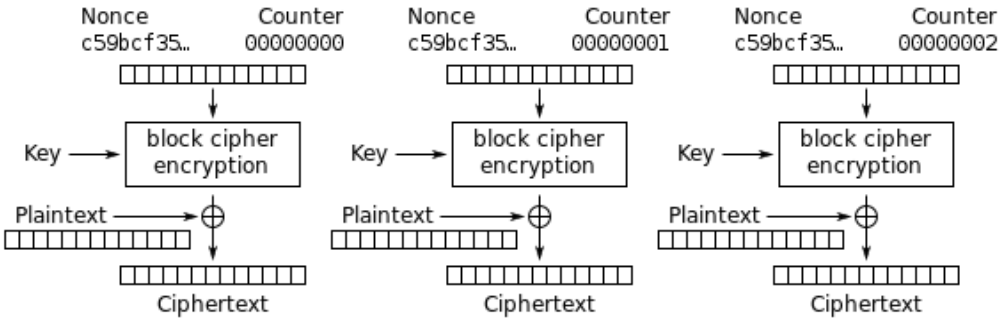
↑ more security for encryption scheme

Recall CBC:

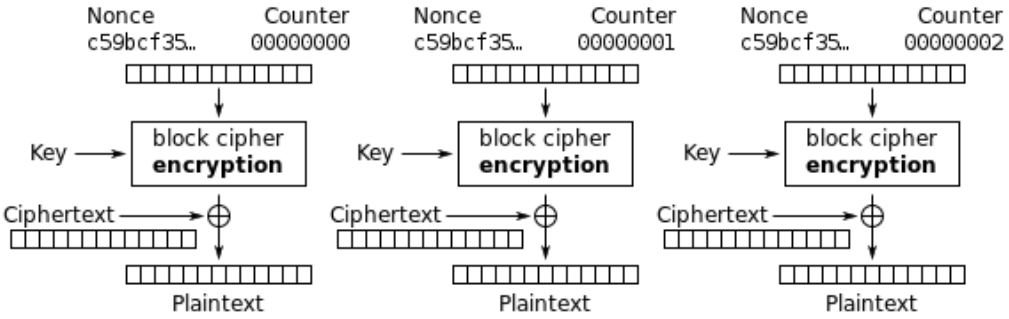


* If IV could be chosen by attacker, then CBC scheme is vulnerable.
If AES is a secure PRP (sand), then AES-CBC mode is TND-CPA secure (castle, have mathematical proof).

- Counter Mode (3-block message encrypted)



Counter (CTR) mode encryption



Counter (CTR) mode decryption

- Malliability:
  - The encryption scheme is malleable if I can alter bits in ciphertext and still have valid plaintext.
  - All schemes we've seen are malliable for now.
  - e.g. Transfer 0000000001 $ to Mom
    flip first number bit
    → Transfer 1000000001 $ to Mom → still valid