Thursday, February 2nd

Methods of Attack

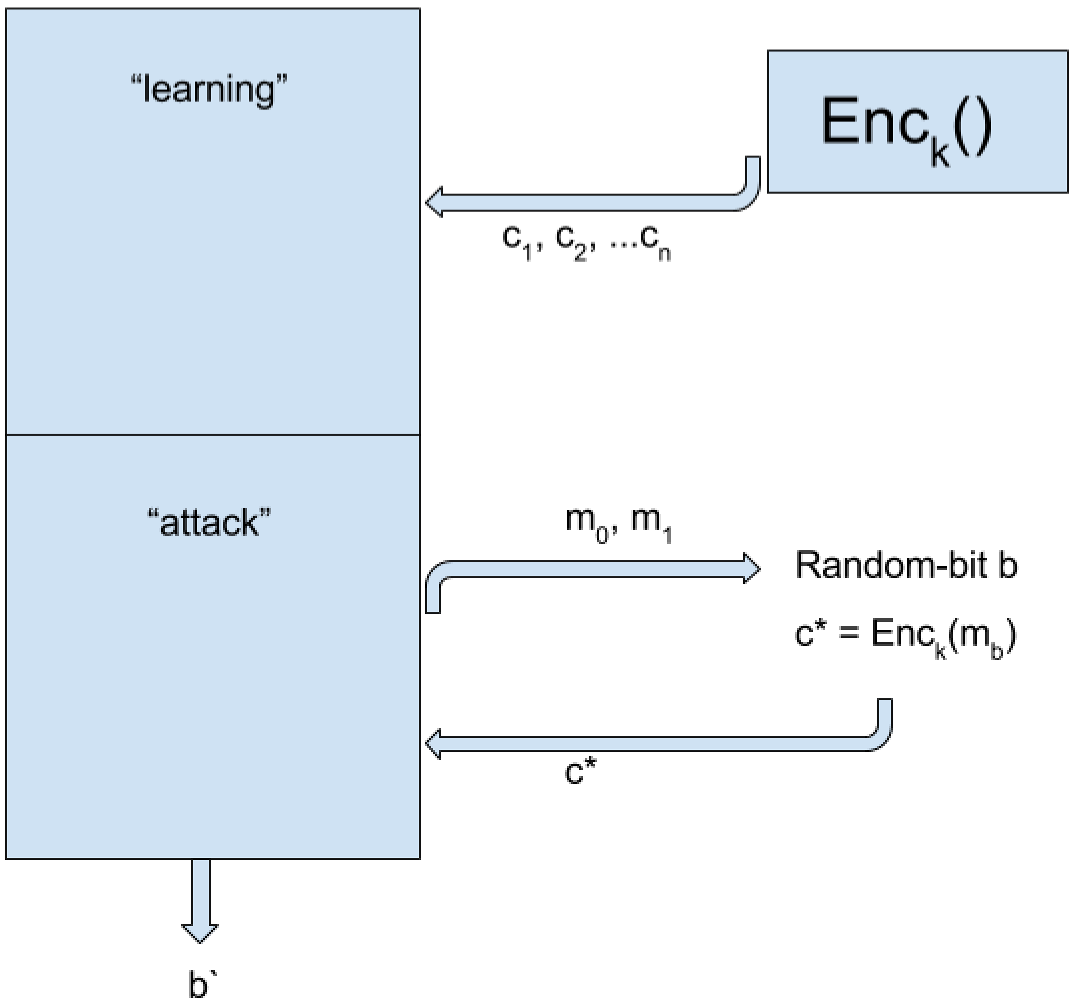
Schemes from Tuesday:

- OTP
  - 1 bit encryption mode
- AES-CBC mode (plays the role of PRP)
  - Arbitrary bit-length encryption mode

Possible attacks on an encryption:

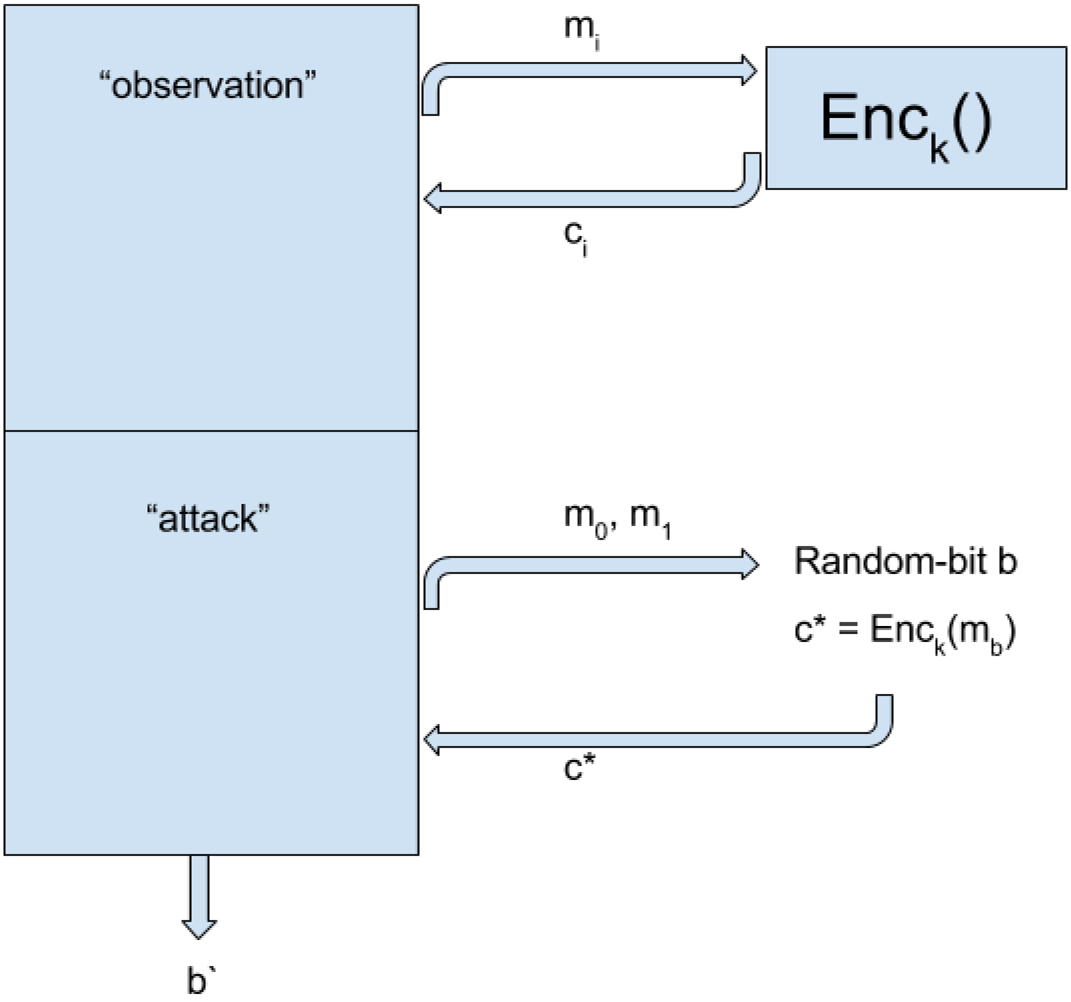
- Key recovery
  - Most difficult attack
  - Adversary outputs the secret key
- Recovering the plaintext
  - Adversary outputs the plaintext
- Indistinguishability
  - Adversary chooses m_0, m_1, and challenger randomly selects one of these (with random bit b) and encrypts them, sending back c_0 = enc(m_0) or c_1 = enc(m_1)
  - Your scheme is “strong” if it can always protect against indistinguishability

KNOWN CIPHERTEXT ATTACK



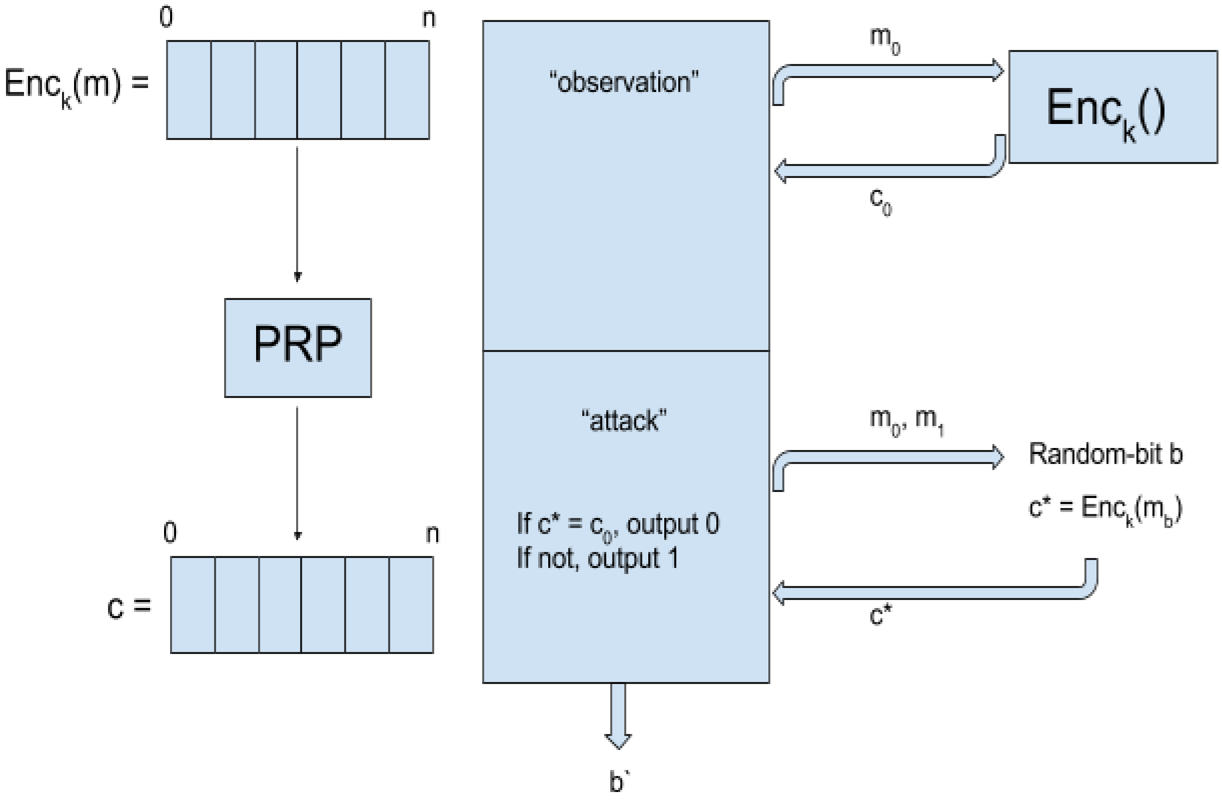
- For indistinguishability, it’s much more likely that the adversary will be looking at multiple encrypted messages c_2, c_3, …...c_n before sending m_0, m_1 to the server
- So we want to protect our system from an adversary that is able to observe out ciphertext

CHOSEN PLAINTEXT ATTACK



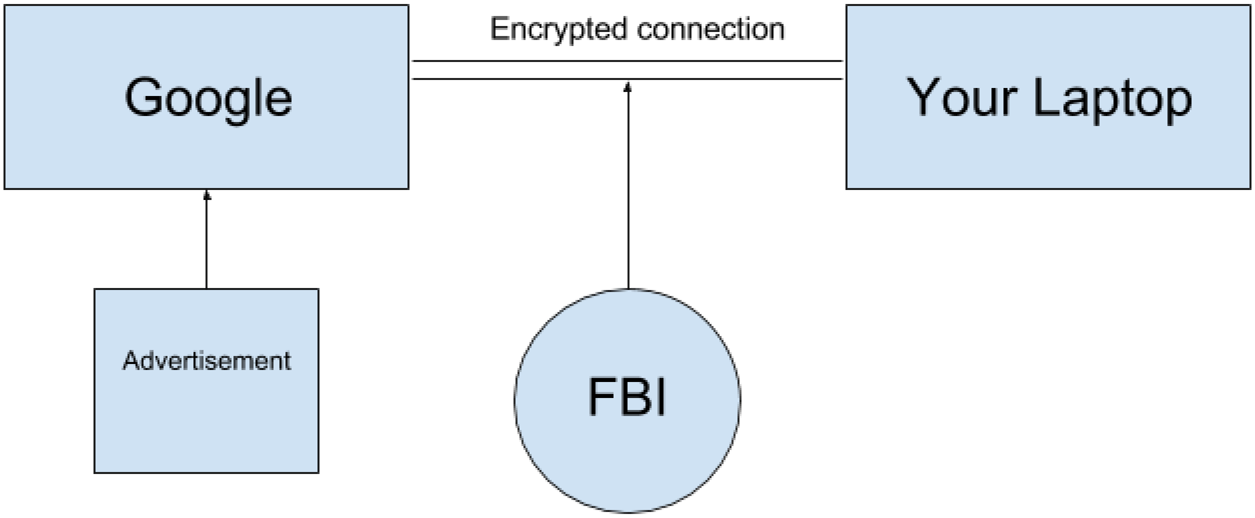
- We want to be able to protect against Plaintext Security because it gives the adversary the most information.
- Note: m_0, m_1 may be queried during the learning phase
    - By defining security this way, we rule out any deterministic encryption scheme as satisfying CPA security
- In order to prevent the adversary from learning m_0, m_1 before attacking, we must make sure that even if the same message is being sent, it is *sent with different outputs each time*

EXAMPLE OF WHY THIS IS INSECURE



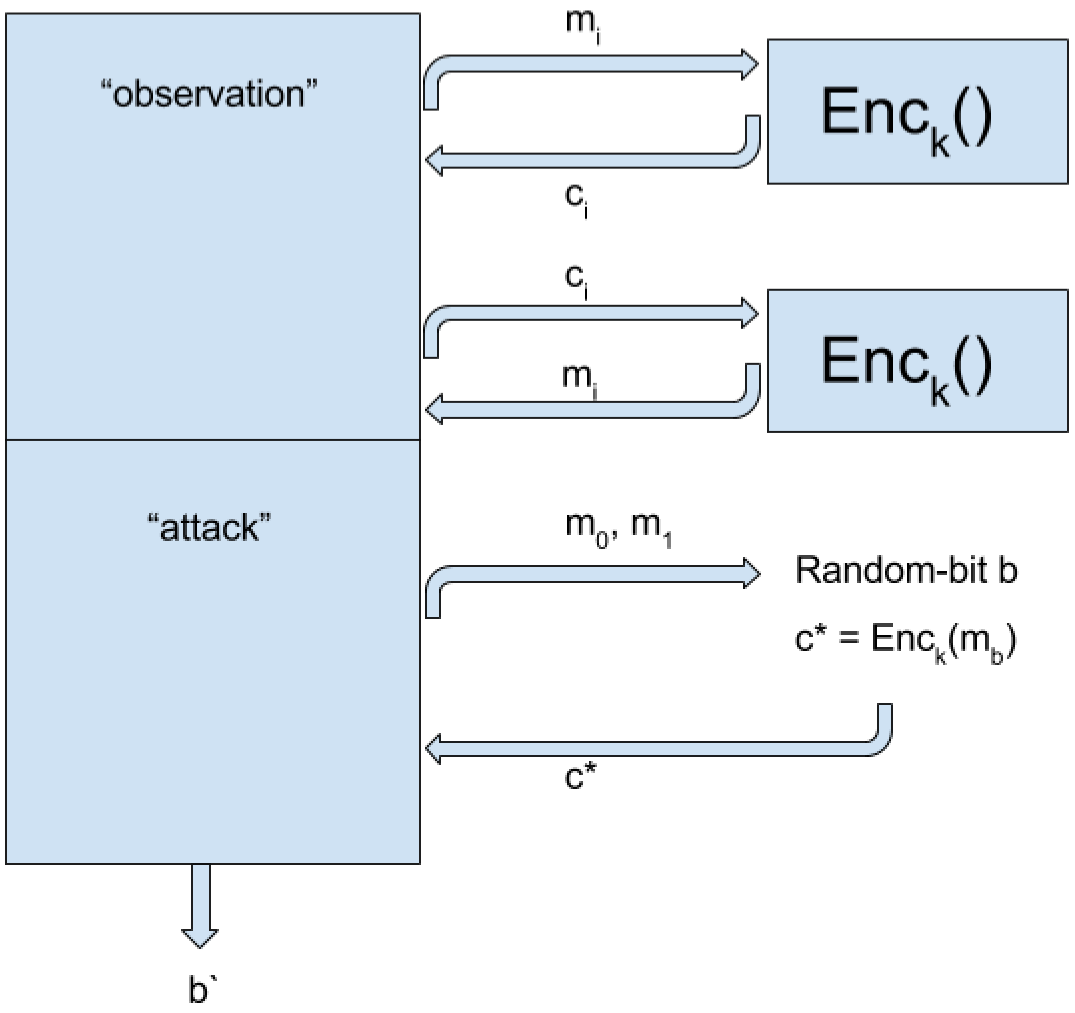
- Relies on the fact that if you send m_0 twice, you receive the same c_0
- So when you attack, send m_0 and m_1
  - If $c^* = c_0$, then output o
  - If not, then output 1
- The probability of winning is always 100%

Example of chosen plaintext attack:



- FBI is eavesdropping on your activity on Google
- FBI also owns an ad agency and they're telling you to "take a vacation in Florida"
- Since the FBI knows that Google is going to encipher your data, including the text "take a vacation in Florida", they know some of the plaintext being sent back

CHOSEN CIPHERTEXT ATTACK

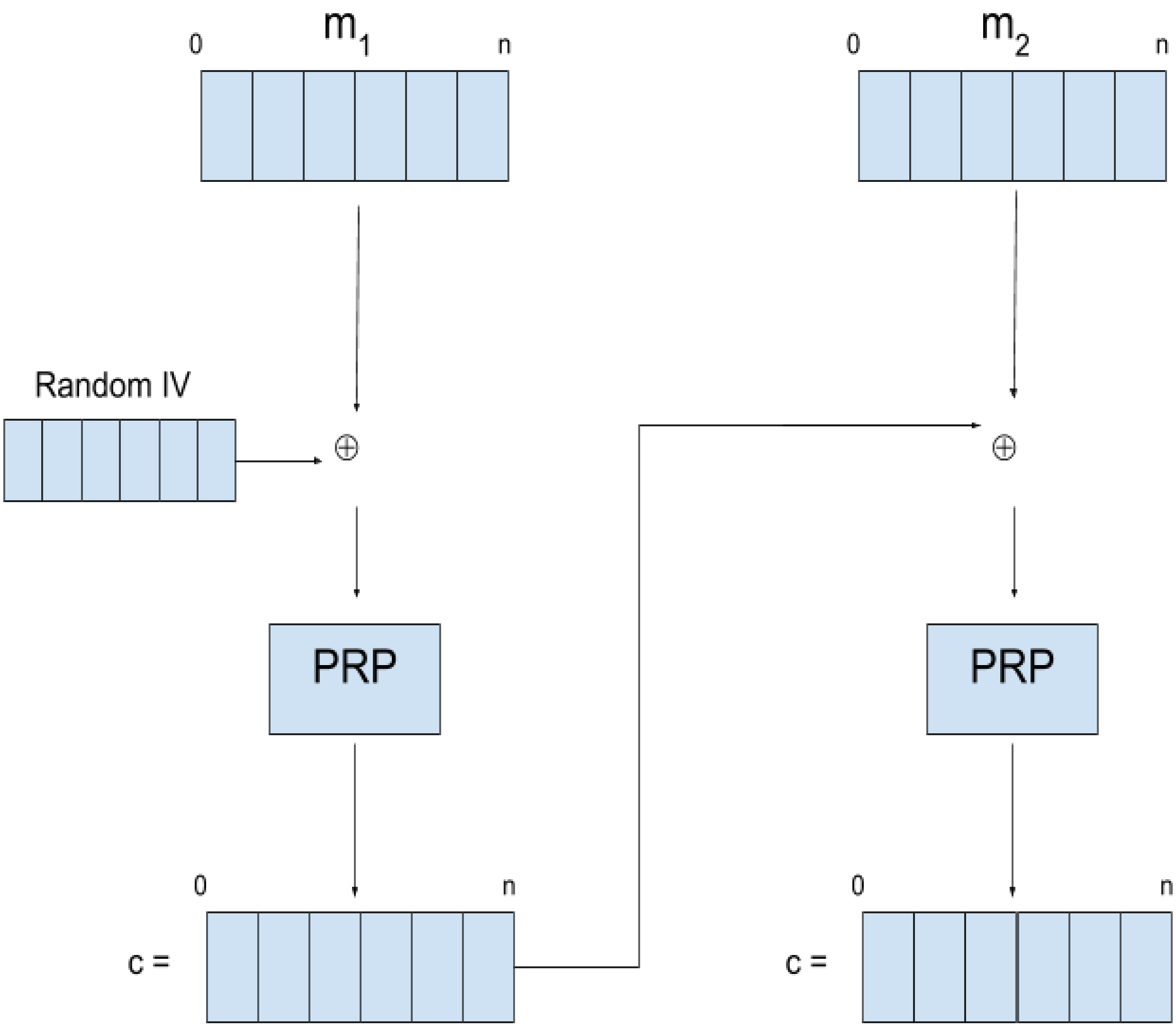


Ranked ease of encryptions

- CCA (chosen ciphertext) [easiest for adversary]
- CPA (chosen plaintext)
- KPA (known plaintext)
- KCA (known ciphertext) [hardest for adversary]

The easier the attack is for the adversary, the more secure the system is if it is protected from that method of attack

Review of CVC mode



- If adversary can control the IV (because IV needs to be random) then CVC is vulnerable to attack

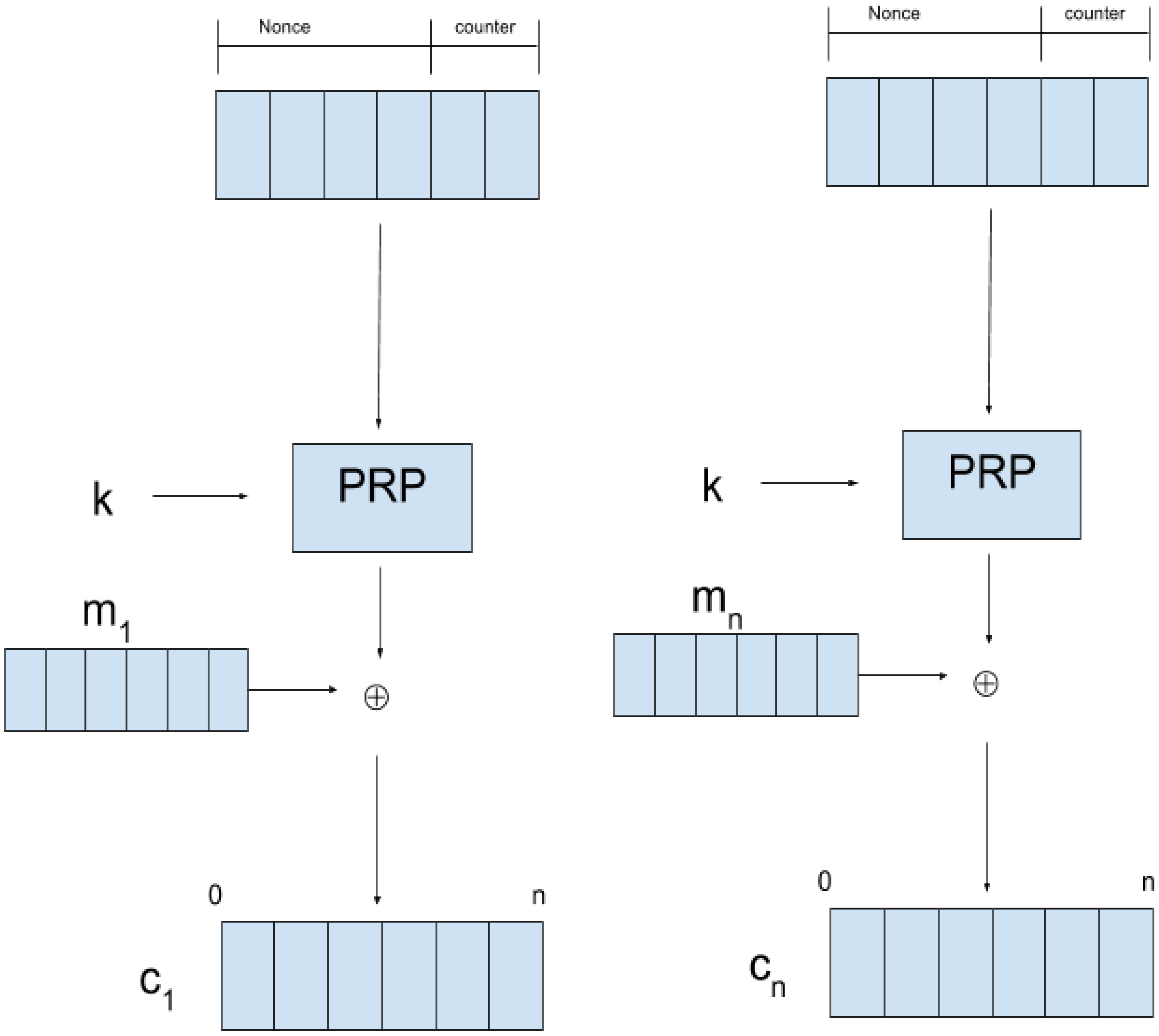
Counter mode

- If *AES is a secure PRP*, then AES-CBC mode is TND-CPA secure.
    - Note: have faith that AES is a secure PRP - proof is *long* and covered in a Crypto class
- But, AES-CBS mode is not CCA secure

Malleability

- A scheme is **malleable** if you can alter bits in the ciphertext and still get valid text in the plain text
    - Doesn’t have to be the same message it started with but it is something that could potentially be decrypted

Example



- This is a malleable code because if you are able to flip one bit in the ciphertext, the plaintext is also altered

Ending Thoughts

- ALL schemes we’ve looked at so far are malleable, so they are not secure.
- How do we fix that??
- Tune in next week to find out…..