Thursday, February 2, 2017

CS558 Lecture Notes

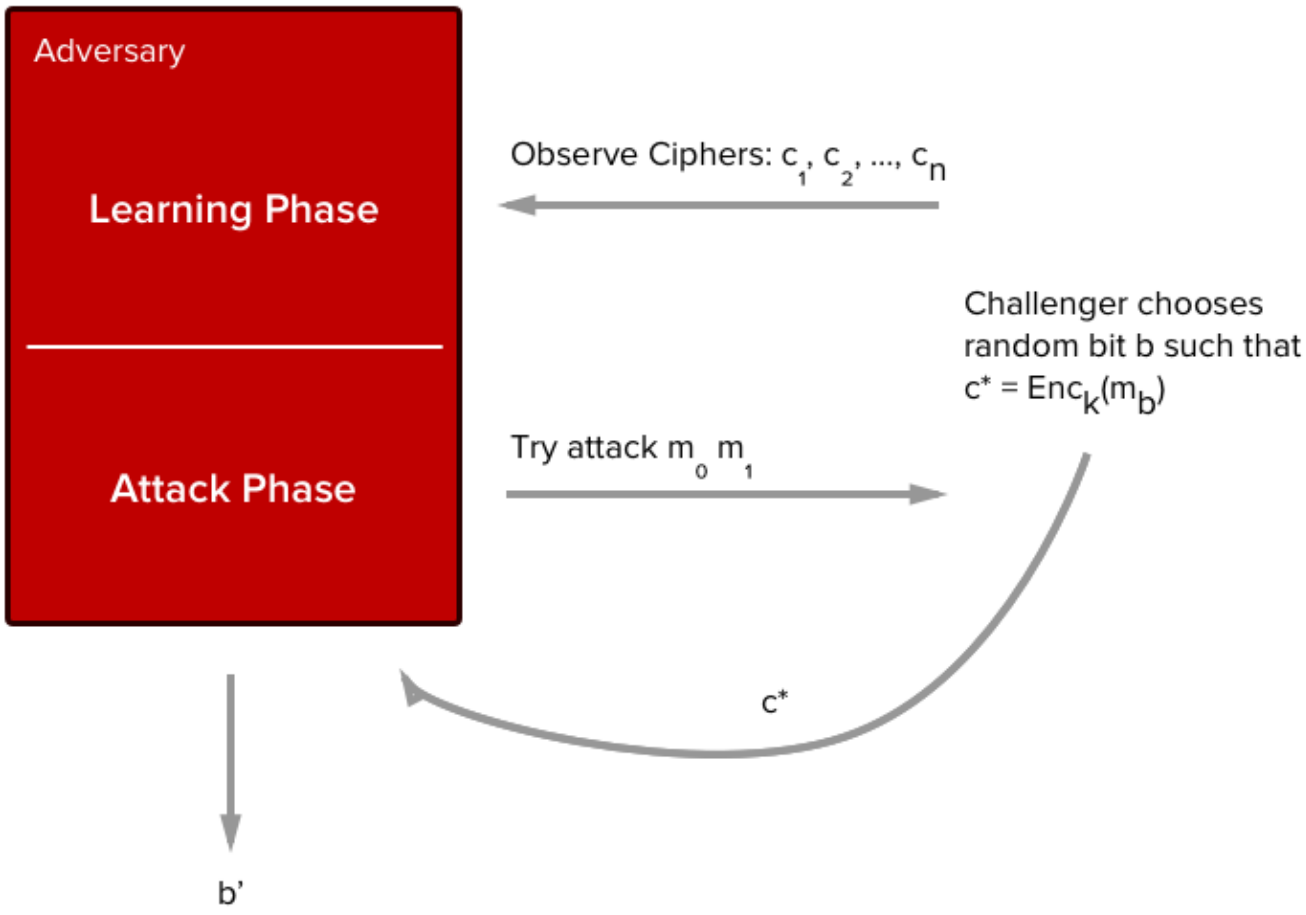
Review from Last Lecture

- Possible attacks on encryption schemes
  - Key Recovery
    - Adversary outputs the security key
  - Recovering the plain text
    - Adversary outputs the plain text
  - Indistinguishability
    - Adversary chooses either message m_0 or m_1. Challenger chooses a random bit b and outputs c*. The adversary then outputs a b' depending on whether m_0 was encrypted or m_1.
- Key recovery is the most difficult attack here
  - If successful at a key recovery, the adversary can potentially succeed in the other two attacks

Known Cipertext Attack (KCA)

- Important: we need a scheme that is secure even if the adversary has the ciphertext
- How this method is helpful to the adversary depends on the encryption scheme used
- See diagram on next page

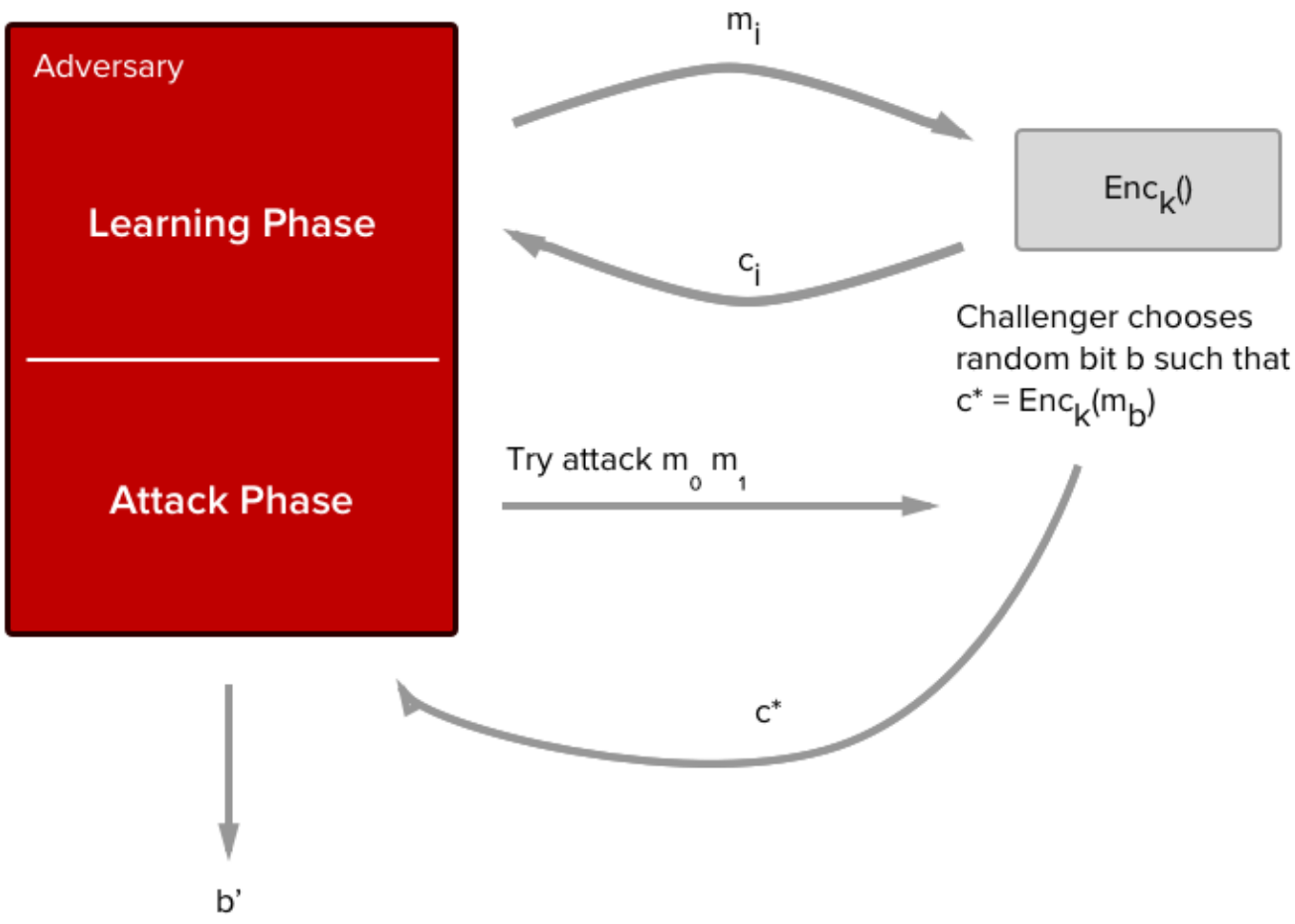
Known Cipertext Attack (KCA) - Continued



Chosen Plaintext Attack (CPA)

- Important: m_0 and m_1 may be queried during the learning phase (rules out electronic codebook mode)
- In order to satisfy Chosen Plaintext Security, we cannot have deterministic encryption. i.e. If we encrypt m_0 twice, the results better be different
- Adversary chooses an m_i and gets back a c_i. They can use the plaintext/ciphertext pairs to make inferences
- Easier to attack than KCA since the adversary has more information
- See diagram on next page

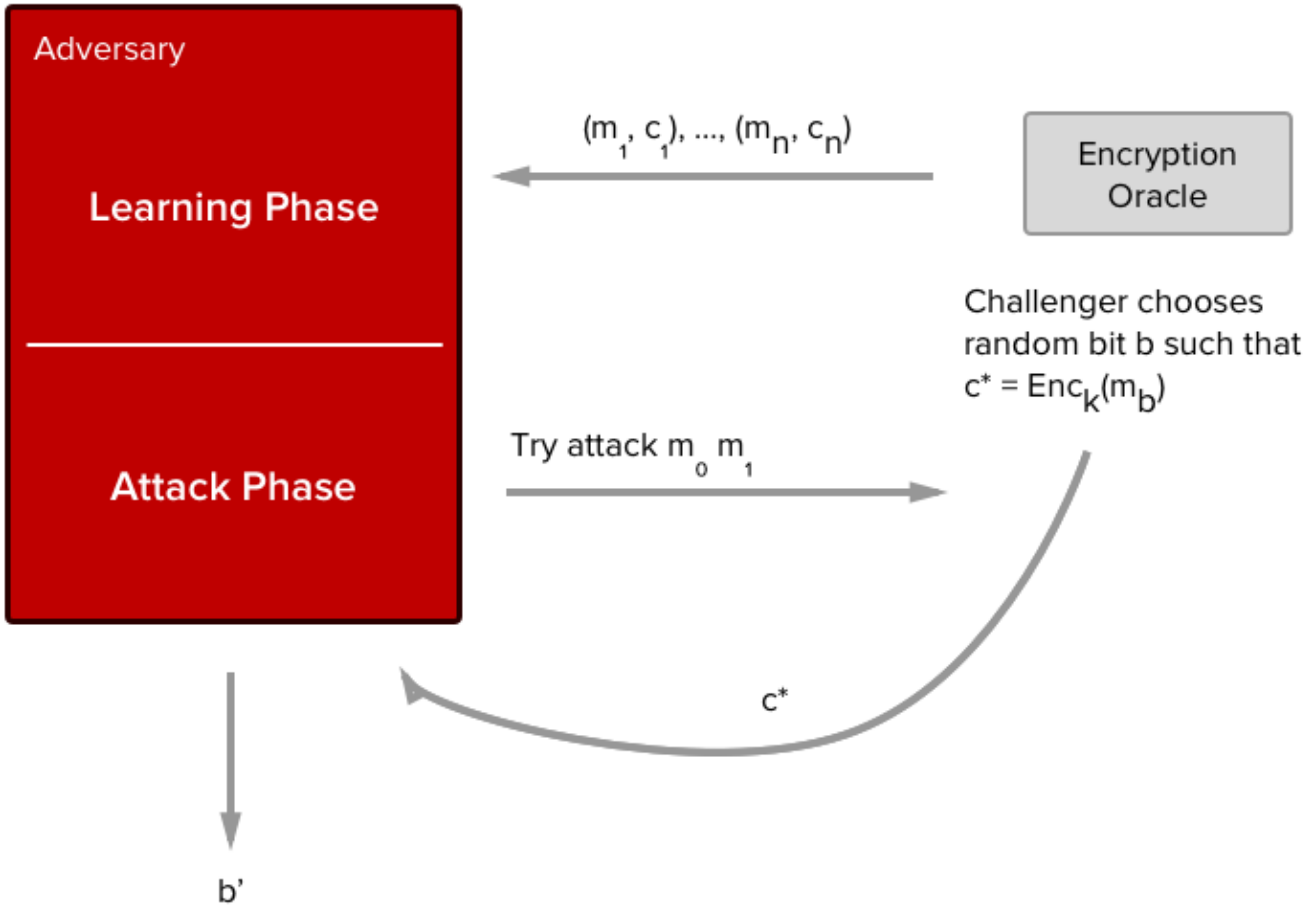
Chosen Plaintext Attack (CPA) - Continued



Known Plaintext Attack (KPA)

- Includes an “Encryption Oracle” that knows the secret key
- See diagram on next page

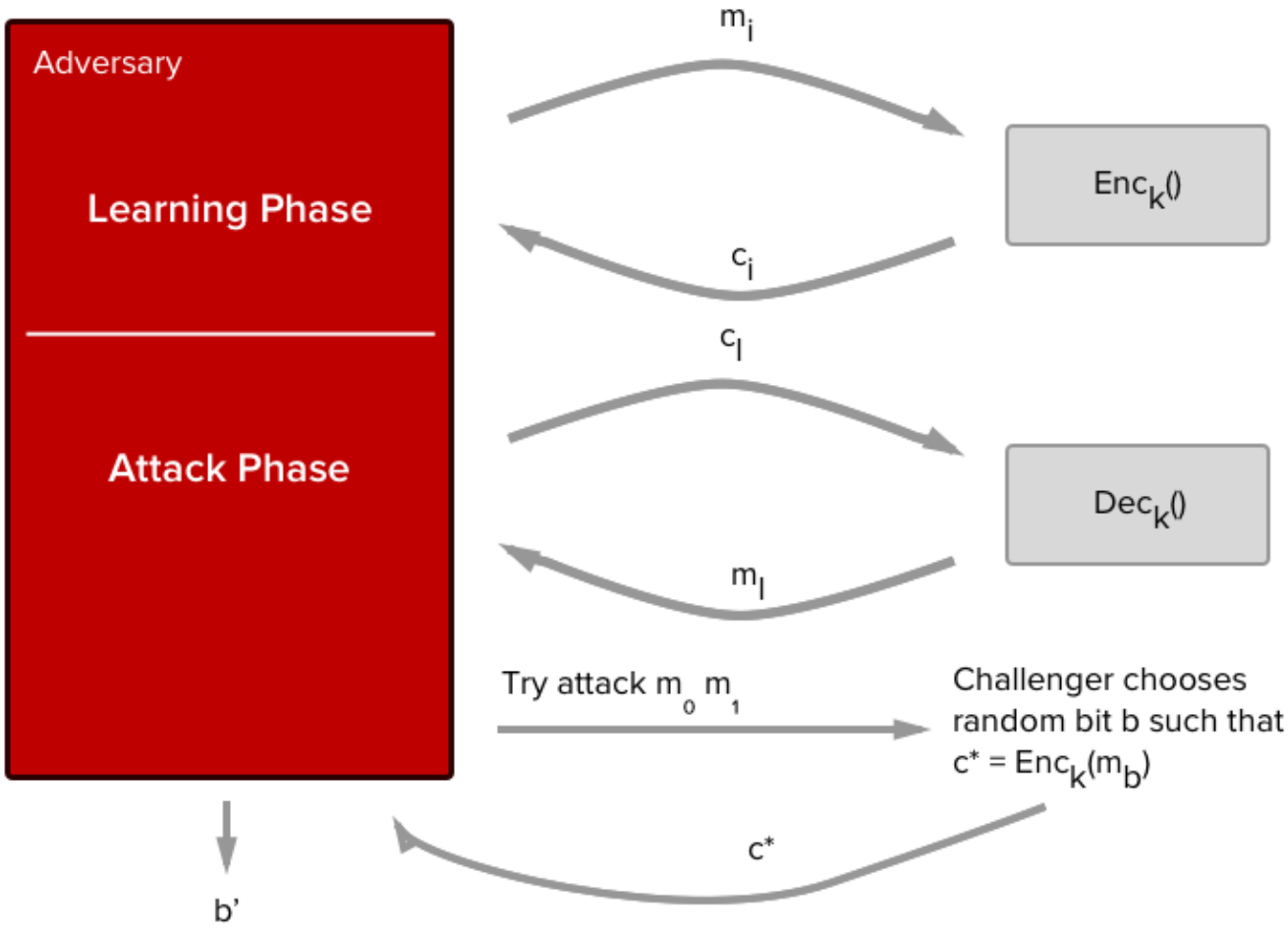
Known Plaintext Attack (KPA) - Continued

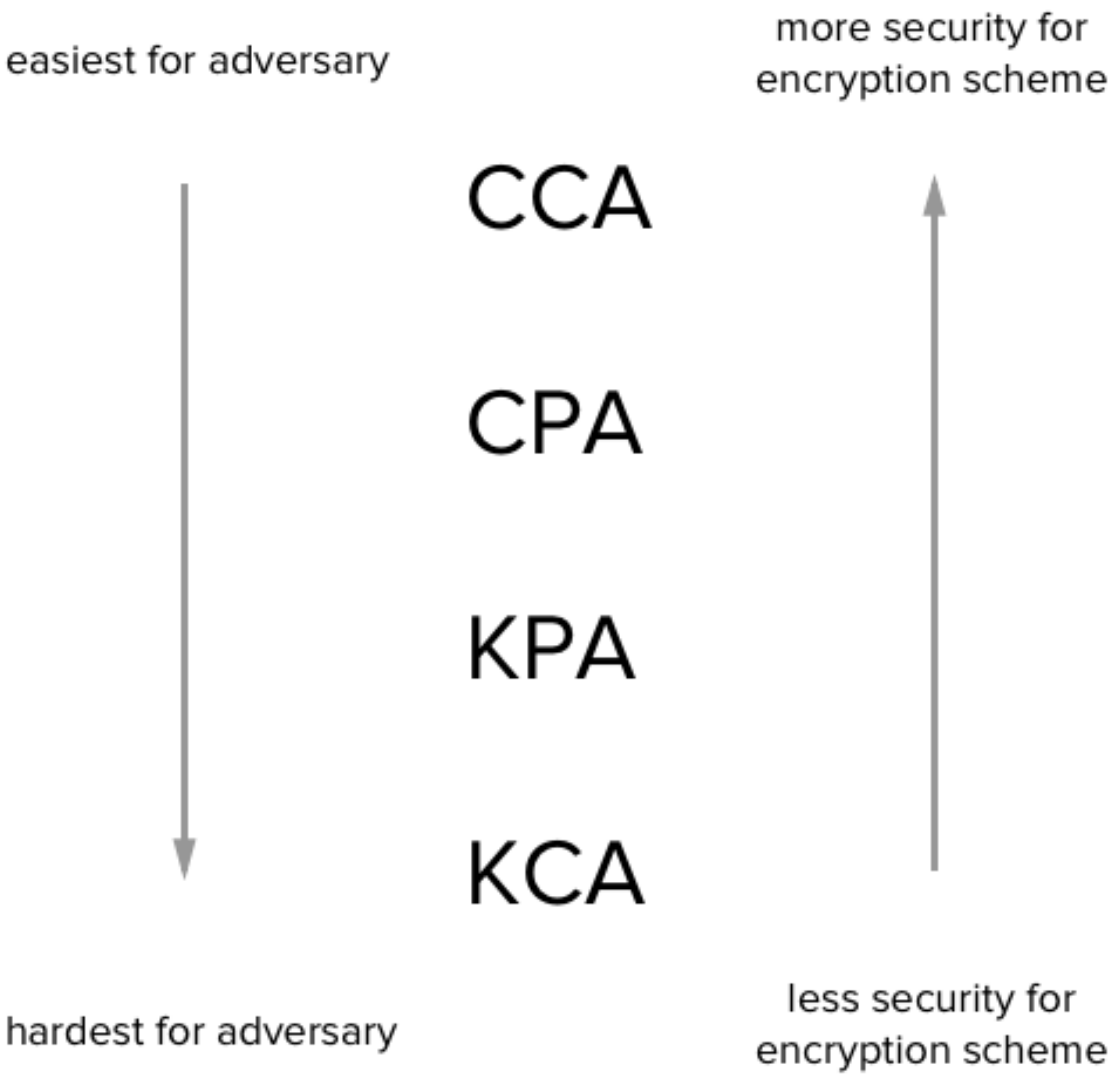


Chosen Ciphertext Attack (CPA)

- Includes an “Encryption Oracle” and a “Decryption Oracle”
- Attacker cannot ask for c* to be decrypted in the Decryption Oracle
- See diagram on next page

Chosen Ciphertext Attack (CPA) - Continued





Counter Mode (CTR)

- Malleability: An encryption scheme is malleable if someone can alter bits in the cipher text and still have valid plaintext
- Counter Mode has malleability: Flipping the first bit in ciphertext c actually flips the first bit in plaintext m
- See: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Counter_.28CTR.29 for diagram of counter mode