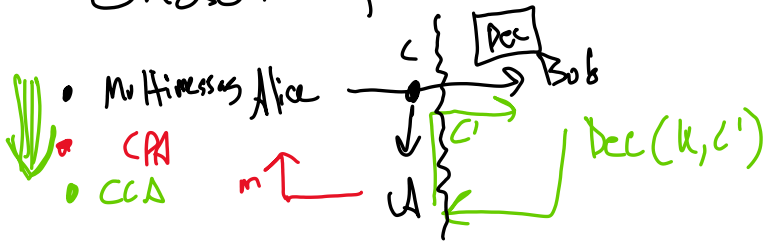
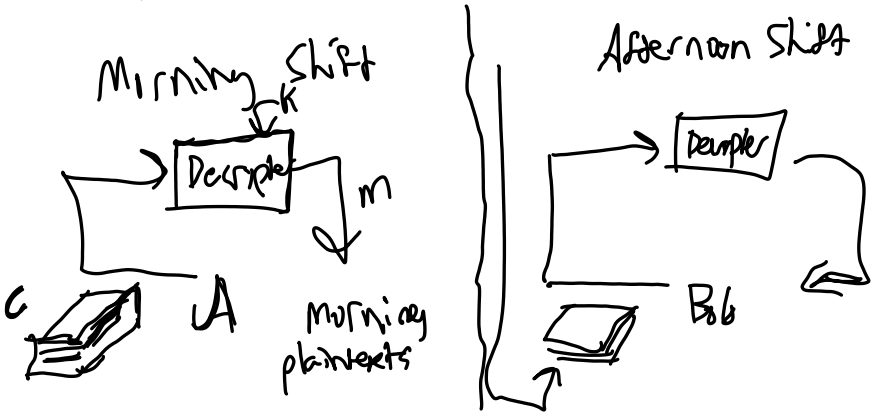
Chosen Ciphertext Attacks



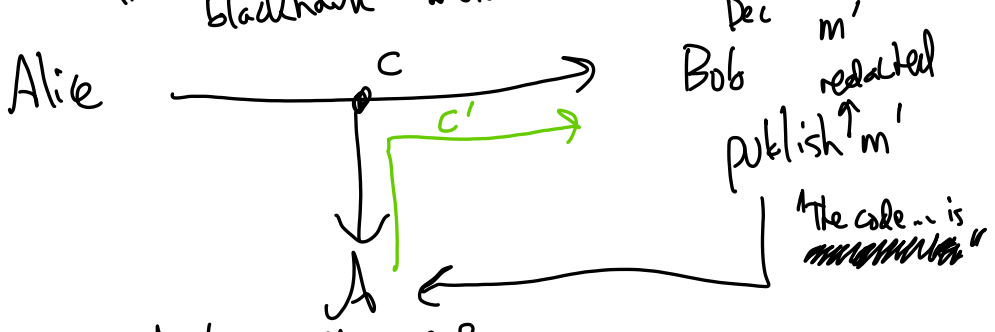
"Attacker is allowed to request decryptions of ciphertexts of its own choosing."

Examples: "lunchtime attack"



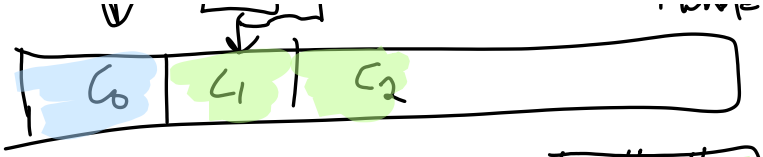
Can A decrypt afternoon ciphertexts?

Ex 2. "The code for today is blackhawk" block 1 block 2



Can A learn the code?

Above 2 questions with CBC... Alice $\vec{c}_0$ Bob



Alice's first message encrypted is $c_0 \| c_1 \| c_2$ ← $Enc(k, m)$ (today's ave)

A: asks to decrypt $c_1 \| c_2$ ← $c_1 \| c_2$ related ciphertext

Bobs decrypts c_0 c_1 c_2 + $c_0 \| c_1 \| c_2$

"The coin" "Malleability"

Bob decrypts c_1 c_2

↙ "blockchain"

Recall RPS w/ hash functions ↙ Some hash of the move

A: My move commitment is XY146...

"hiding" // at the time B commits, doesn't learn anything about A's move...

B: My move commit is also XY146...

A: reveals "rock + garbage"

B: cool me too

Defining IND-CCA:

Game Left

$S := \emptyset$ ← list of queried ciphertexts

$K \leftarrow Gen()$

• $Query(m_L, m_R)$:

assert $|m_L| = |m_R|$

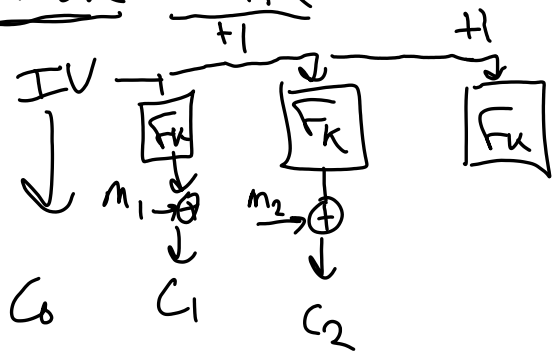
$c \leftarrow Enc(k, m_L)$

$S := S \cup \{c\}$

return c

- Decrypt(c): assert c ∉ S
  return Dec(k,c)

Attack CTR mode:



IND$-CPA ciphertexts look like uniform strings