

## Meet-in-the-middle-attack (P, C, keys)

Initial  $M_1, M_2$  are dictionary (hash table) with {middle-text : key}  
Initial Possible-keys is dictionary to store tuple {id : (text, key1, key2)}  
id = 0

Do Encryption to P with all possible keys  
and store it into a Dictionary (Hash table) called  $M_1$  }  $O(n)$

Do Decryption to C with all possible keys  
and store it into a Dictionary (Hash table) called  $M_2$  }  $O(n)$

For  $m$  in  $M_2.m$  :  $\xrightarrow{\quad} O(n)$   
if  $m$  in  $M_1.m$  :  $\xrightarrow{\quad} O(1)$  (hash table dictionary)  
store  $(m_1, m_2[m], M_1[m])$  into Possible-keys }  $\Rightarrow O(1)$   
id++

return Possible-keys

Total time complexity:  $O(n) + O(n) + O(n)$   
 $= O(n)$