**Quiz 4**

109550135 范恩宇

1. Answer : **(A)**

Since ciphertexts tend to look like random strings , the only opportunity for compression should be prior to encryption.

1. Answer : **(D) (E) (F)**

Because the outputs of these answers will be random

1. Answer : **0.25**

For a random string x , we have Pr[A(x)=1]=1/2 . But for a pseudorandom string G′(k1,k2) , we should have Prk1,k2[ A( G′(k1,k2) )=1 ] =1/4 = 0.25.

1. Answer : **(C)**

Executives 1&2 can be decrypted using k1&k1’ , executives 1&3 can be decrypted using k2&k2’ , and executives 2&3 can be decrypted using k2&k2’ . Besides , a single executive has no information about

p1 = ( k1 , k2 ) , p2 = ( k1’ , k2 ), = ( k2’ ) .