Quiz 4

Question 1

Answer : A

Compression uses patterns in data to reduce its size. Encryption shuffles data in such a way that one can't find any patterns in data. Specifically, encryption produces output that appears random with high entropy, while compression doesn't really work on data that appears random with high entropy. So if encryption comes first, compression will be useless. Therefore, the answer is compress then encrypt.

Question 2

Answer : DEF

A secure PRG should be able to generate a sequence of pseudorandom data that are indistinguishable from truly random data.

A) a zero is added in the end : The output bit stream of this generator will change the distribution of 0 and 1, which is not secure.

B) a same bit stream is added in the end : The output bit stream of this generator will appear two equal patterns, which is not secure.

C) always uses 0 as the key : The output bitstream of this generator appears not random since its key remains the same, which is not secure.

D) XOR the key with 1 : The output bitstream of this generator will remain secure since the operation is applied to the key instead of the output of secure PRG.

E) XOR the output with 1^n : The output bitstream of this generator will remain secure since the operation result in 0->1 and 1->0, which will not change the distribution of 0 and 1.

F) reverse the output : The output bitstream of this generator will remain secure since the operation will not change the distribution of 0 and 1.

Question 3

Answer : 0.25

Truth table of A and B is :

A	B	A and B
0	0	0
0	1	0
1	0	0
1	1	1

The attacker can know the bit is 0 with the chance of 3/4 = 0.75

The advantage of attacker is 0.75 - 0.5 = 0.25

Question 4

Answer : C

A) p2 and p3 cannot decrypt.

B) p2 can decrypt by itself.

C) p1 and p2 can decrypt by using k1 and k1'. p1 and p3 can decrypt by using k2 and k2'. p2 and p3 can decrypt by using k2 and k2'. no single piece can decrypt by itself.

D) p2 and p3 cannot decrypt.

E) p1 and p2 cannot decrypt.