1. A) Compress then encrypt.
   It is because that if you choose to encrypt first, then after it is later compressed, the data may be out of order, and can never be decrypted. However, if you choose to compress first, then after decryption, you'd get the compressed data.

2. DEF
   A) is not secure because we can use the 0 at the last position as a line to guess the plaintext. The Adv of the last bit to be 0 is 1/2.
   B) is not secure because we can use the first half to predict the last half.
   C) is not secure because it becomes only one key.
   D) is secure because it is just the key becomes (key'), G(key') must still be OK.
   E) is secure because it is just the original G(k) to become (G(k)'), it's still OK.
   F) is secure because it is still unpredictable.

3. 0.25
   Pr(A(G(r))) is 0.5. Also, for AND operation, we only get 1 when both bits are 1, so Pr(A(G'(k1, k2))) is 0.25, so Adv is |0.25-0.5|=0.25.

4. C
   For A, we can do nothing when getting p2 and p3.
   For B, only B itself can solve it.
   For C, it is correct.
   For D, we can do nothing when getting p2 and p3.
   For E, we can do nothing when getting p1 and p2.