1. What is the output of the first round of the DES algorithm when the plaintext and the key are both all zeros? (5 points)

> IP has no effect on 0s, so plaintext is 64-bits 0. Then divide them to x and y, each of which is 32 bits.
>
> As all the bits are 0, the extension of x is 48-bits 0s. k is 48-bit 0, then $x \oplus k = 0$ with a length of 48 and goes to S-boxes.
>
> The output S-boxes: 1110, 1111, 1010, 0111, 0010, 1100, 0100, 1101.
>
> After mixing permutation: we have

1	**1**	**0**	**1**	**1**	**0**	**0**	**0**
1	1	0	1	1	0	0	0
1	1	0	1	1	0	1	1
1	0	1	1	1	1	0	0

> Therefore $F(k_1, x) = 11011000110110001101101110111100$
>
> Then we have $(y, x \oplus f(y)) = (y, x \oplus 0) = (y, 0))$, so the output of the first round is two 32-bit 0s, i.e., 64-bit 0s.

2. Suppose you are told that the one-time pad encryption of the message "attack at dawn" is 09e1c5f70a65ac51626bc3d25f28 (the plaintext letters are encoded as 8-bit ASCII and the given ciphertext is written in hex). What would be the one-time pad encryption of the message "attack at dusk" under the same OTP key? (5 points)

> A = 01100001. K1 = 00010100. D = 01110101
>
> W = 01110111. K2 = 00000100. S = 01110011
>
> N = 01101110. K3 = 00000101. K = 01101011
>
> So Δ = $K1K2K3 = 000101000000010000000101 = hex140405$
>
> Ciphertext = $09e1c5f70a65ac51626bc3d25f28 \oplus 140405 = 9e1c5f70a65ac51626bc3c65b2d$