Exercise_06

516030910555

1.

Answer: 80-bit = 64-bit + 16-bit. Use DES to encrypt the former 64-bit, and then take the latter 48-bit of the ciphertext with the rest 16-bit of original plaintext to form a new 64-bit. Encrypt the new 64-bit, combine the result with rest 16-bit ciphertext. Do the same to AES.

2.

Answer: C_i is the original ciphertext. $C_i^{'}$ is the error ciphertext.

$$P_i = D_k(C_i^{'}) \oplus C_{i-1}$$
$$P_{i+1} = D_k(C_{i+1}) \oplus C_i^{'}$$

So only two plaintext blocks will be affected if an error is in ciphertext block.

3.

Answer: Pseudo-random number generator is a one way function. Because when you get a random number, it's hard to get the input to generate the number. I think