Overview: Question 1 [5 Marks]
These are short-answer questions. Please answer in 2-4 lines and not in paragraphs. ***Explain your reasoning behind the answer.*** *Yes/no answers will not fetch you marks.*

1. Mallory has given a bunch of messages (ciphertext) to Alice for her to sign using the RSA signature scheme, which Alice does without looking at the messages and without using a one-way hash function. What kind of attack is Mallory using here to recover the key? Assume same key is used for encryption and signature.

Chosen cipher-text attack since attacker is chosing the cipher and is obtaining the corresponding message.

2. Why can't Bob use the pair (6, n) as an RSA public key, where n = pq, for two large primes p and q?

   p and q are primes, therefore totient function (=(p-1)(q-1)) will be an even number.
   e needs to be relative prime to the totient function;
   since e = 6 is an even number it cannot be relative prime to totient function and hence cannot be used.

3. What pad sequence (vectors V_i) is generated by OFB (block mode) with a weak DES key. A weak key k is its own inverse, i.e., for any block b: $E_k(b) = D_k(b)$.

   The pad sequence is $E_k(V_0)$, $E_k(E_k(V_0)$, $E_k(E_k(E_k(V_0))$ *etc*
   But since $E_k(b) = D_k(b)$, $E_k(E_k(V_0) = D_k(E_k(V_0) = V_0$
   So, the pad sequence is $E_k(V_0)$, V_0, $E_k(V_0)$, V_0 *etc*

4. Can AES with fixed key (i.e. key is fixed for all and made public) be used as a hash function? Why or why not?

   This is not pre-image resistant i.e. in this case given hash, one can find the message m.
   Partial credit: hash will be the same size as the message

5. Can a MAC provide non-repudiation? Explain. (Non repudiation: Signer cannot deny the authenticity of their signature on a document)

   No. Since the key is shared with another. One can claim, the other signed it.

Question 2: RSA [2 Marks]
Given RSA signatures on messages m_1 and m_2, how can one compute signature on message $m_1^j . m_2^k$ for any positive integers j and k?

Let s1 be the signature on message m1 and s2 be the signature on message m2.

$(s1)^j \cdot (s2)^k \bmod n$ will be the signature of $m_1^j \cdot m_2^k$

(straightforward proof)

Question 3: DES [3 Marks]

a) In DES, how many plaintext blocks, on the average, are encrypted to the same ciphertext block by a given key?

DES has 56-bit keys, 64-bit plaintext blocks, and 64-bit ciphertext blocks.
The number of ciphertext blocks equals the number of plaintext blocks.
DES is a 1-1 mapping between ciphertext blocks and plaintext blocks. Otherwise one cannot decrypt without ambiguity.

So 1 plaintext block is mapped to a given ciphertext block by any given key

b) In DES, how many keys, on the average, encrypt a particular plaintext block to a particular ciphertext block?

There are 2^{56} possible keys and 2^{64} possible ciphertext blocks for a particular plaintext block. So only about $2^{(56-64)} = 1/256$ of the possible ciphertext blocks can be obtained with a DES key.

Another explanation:
Each key maps 2^{64} plaintext blocks to 2^{64} ciphertext blocks.
So it has a $1/2^{64}$ chance of mapping a plaintext block b to a ciphertext block c.
There are 2^{56} keys, so the total probability of mapping p to c is $(1/2^{64}) * 2^{56} = 1/256$.