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.

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?

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: $E_k(b) = D_k(b)$.

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?

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

Question 2: RSA [2 Marks]

Given RSA signatures on messages m_1 and m_2, how can one compute signature on message $m_1^j \cdot m_2^k$ for any positive integers j and k?

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?

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