Cryptography (BITS F463) Midsem Exam (2019)

There are 4 questions in all and total marks are $5 + 10 + (5 + 5) + 10 = 35$. Please show all steps in proofs or computations (using efficient algorithms). Calculators are not allowed. This is an **open book exam**. You can use books or notes (only hard copies). Time: 90 minutes.
Notation: $x||y$ is the concatenation of the strings x and y; $|x|$ is the length of the string x; and $x \oplus y$ is the bitwise exclusive or of the binary strings x and y.

1. Using the Vigenere cipher, encrypt the word "`cryptography`" using the keyword "`key`".

2. We associate bit strings with positive integers in some natural manner (e.g., the $n-$bit long string $x_{n-1}...x_0$ is associated with the integer $2^n + \sum_{i=0}^{n-1} x_i 2^i$). Define $f_+ : \{0,1\}^* \to \mathbb{N}$ such that
$$f_+(x||y) = x + y$$
where $|x| = |y|$. Prove that f_+ is not a one-way function (not even in the weak sense).

3. (a) Let $k = 111...111$ be the DES key consisting of all 1s. Show that if $\text{DES}_k(P) = C$, then $\text{DES}_k(C) = P$, so encrypting twice with this key returns the plaintext.
   (b) Find another key with the same property as k in part (a).

4. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a secure *Pseudo Random Permutation (PRP)*. Consider the family of permutations $E' : \{0,1\}^k \times \{0,1\}^{2n} \to \{0,1\}^{2n}$ defined for all $x, y \in \{0,1\}^n$ by
$$E'(k, x||y) = E(k, x)||E(k, x \oplus y)$$
Prove that E' is not a secure PRP.