Cryptography (BITS F463) Midsem Exam (2022)

There are 4 questions in all and total marks are $5 + 10 + 10 + 10 = 35$. Please show all steps in proofs or computations (using efficient algorithms). Calculators are allowed. This is an **open book exam**. You can use books or notes (only hard copies). Time: 90 minutes.
Notation: $\bar{x}$ is the bitwise complement 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 plaintext "`adversary`" using the keyword "`rsa`".

2. Consider the DES key $K = 0x0101010101010101$. Using the *DES Key Schedule Algorithm*, compute C_0, D_0, C_1, D_1, and K_1 in hexadecimal notation.

3. Consider the RSA encryption function $\text{RSA}_e : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ defined by

$$\text{RSA}_e(x) = x^e (\text{mod } n).$$

   Prove that $\exists l \in \mathbb{N}$ such that $\text{RSA}^l = \text{id}_{\mathbb{Z}_n^*}$, where RSA^l is the function in which we apply the RSA function l times, and $\text{id}_{\mathbb{Z}_n^*}$ is the identity function over $\mathbb{Z}_n^*$.

4. Let $E : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^L$ be a secure *Pseudo Random Function (PRF)* family. Consider the family of functions $G : \{0,1\}^k \times \{0,1\}^l \to \{0,1\}^L$ defined for all $(K, x) \in \{0,1\}^k \times \{0,1\}^l$ by

$$G_K(x) = F_K(x) \oplus F_K(\bar{x})$$

   Prove that G is not a secure PRF family.