Cryptography (BITS F463) Mid Sem Exam (2017)

There are 3 questions in all and total marks is 35. Please show all steps in computations or proofs. This is an **open book exam**. You can use books or notes (only hard copies). Time: 90 minutes.

1. Consider a special case of a *Permutation Cipher*. Let m, n be positive integers. Write out the plaintext, by rows, in $m \times n$ rectangles. Then form the ciphertext by taking the columns of these rectangles. For example, if $m = 3, n = 4$, then we would encrypt the plaintext "`cryptography`" by forming the following rectangle:
   `cryp`
   `togr`
   `aphy`
   The ciphertext would be "`CTAROPYGHPRY`" $[5 + 5 = 10]$

   (a) Describe how Bob would decrypt a ciphertext string (given values for m and n).

   (b) Decrypt the following ciphertext, which was obtained by using this method of encryption:
   `IRUITRTRHICITONOCOOYOAYTONHRTDTNCPGPWHDGEY`

2. Consider the following DES-like encryption method. Start with a message of $2n$ bits. Divide it into two blocks of length n (a left half and a right half): M_0M_1. The key K consists of k bits, for some integer k. There is a function $f(K, M)$ that takes an input of k bits and n bits and gives an output of n bits. One round of encryption starts with a pair M_jM_{j+1}. The output is the pair $M_{j+1}M_{j+2}$, where
   $M_{j+2} = M_j \oplus f(K, M_{j+1})$.
   ($\oplus$ means XOR, which is addition mod 2 on each bit). This is done for m rounds, so the ciphertext is M_mM_{m+1}. $[5 + 5 + 5 = 15]$

   (a) If you have a machine that does the m-round encryption just described, how would you use the same machine to decrypt the ciphertext M_mM_{m+1} (using the same key K)? Prove that your decryption method works.

   (b) Suppose K has n bits and $f(K, M) = K \oplus M$, and suppose the encryption process consists of $m = 2$ rounds. If you know only a ciphertext, can you deduce the plaintext and the key? If you know a ciphertext and the corresponding plaintext, can you deduce the key? Justify your answers.

   (c) Suppose K has n bits and $f(K, M) = K \oplus M$, and suppose the encryption process consists of $m = 3$ rounds. Why is this system not secure?

3. Let R be the field of real numbers, and C be the field of complex numbers. Let $R[x]$ be the ring of polynomials with real coefficients. Let $R[x]/(x^2+1)$ be the ring of polynomials modulo (x^2+1), in which addition and multiplication are done modulo (x^2+1). Let F_1 and F_2 be fields. A mapping $h : F_1 \to F_2$ is called a *homomorphism* from F_1 to F_2 if $\forall a, b \in F_1$:
$h(a+b) = h(a) + h(b)$, and
$h(a.b) = h(a).h(b)$.
The operations on the left sides of the above equations are in the field F_1, and the operations on the right sides of the above equations are in the field F_2. An *isomorphism* is a *one-to-one* homomorphism. We say that F_1 is isomorphic to F_2 if there exists an isomorphism from F_1 to F_2 which is *onto* F_2. $[5 + 5 = 10]$

(a) Prove that $R[x]/(x^2+1)$ is a field.

(b) Prove that $R[x]/(x^2+1)$ is isomorphic to C.