Cryptography (BITS F463) Comprehensive Exam (2017)

There are 4 questions in all and total marks is 45. Please show all steps in computations or proofs. This is an **open book exam**. You can use books or notes (only hard copies). Calculators are allowed. Time: 180 minutes.

1. If an encryption function E_K is identical to the decryption function D_K, then the key K is said to be an *involutory key*.

   (a) Prove that a permutation π in the *Permutation Cipher* of alphabet size m is an involutory key if and only if $\pi(i) = j$ implies $\pi(j) = i$, for all $i, j \in \{1, ..., m\}$. [5]

   (b) Determine the number of involutory keys in the *Permutation Cipher* for $m = 2, 3, 4, 5$, and 6. [5]

2. Prove that if $\mathtt{P} = \mathtt{NP}$ then one-way functions do not exist. [10]

3. Consider the following variation of the ElGamal signature scheme. Alice chooses a large prime p and a primitive root α of Z_p^*. She also chooses a function $f(x)$ that, given an integer x with $0 \leq x < p$, returns an integer $f(x)$ with $0 \leq f(x) < p-1$. (For example, $f(x) = x^7 - 3x + 2 (\text{mod } p-1)$ for $0 \leq x < p$ is one such function.) She chooses a secret integer a and computes $\beta \equiv \alpha^a (\text{mod } p)$. The numbers p, α, β and the function $f(x)$ are made public.
   Alice wants to sign a message m:
   (1) Alice chooses a random integer k with $\mathtt{gcd}(k, p-1) = 1$.
   (2) She computes $r \equiv \alpha^k (\text{mod } p)$.
   (3) She computes $s \equiv k^{-1}(m - f(r)a)(\text{mod } p-1)$.
   The signed message is (m, r, s).
   Bob verifies the signature as follows:
   (1) He computes $v_1 \equiv \beta^{f(r)} r^s (\text{mod } p)$.
   (2) He computes $v_2 \equiv \alpha^m (\text{mod } p)$.
   (3) If $v_1 \equiv v_2 (\text{mod } p)$, he declares the signature to be valid.

   (a) Show that if all procedures are followed correctly, then the verification equation is true. [5]

   (b) Suppose Alice is lazy and chooses the constant function satisfying $f(x) = 0$ for all x. Show thet Eve can forge a valid signature on every message m_1 (for example, give a value of k and of r and s that will give a valid signature for the message m_1). [5]

4. (a) Alice and Bob are following the *Diffie Hellman Secret Key Exchange Protocol* with $p = 101$ (the prime number p), and $g = 2$ (the generator of Z_p^*). Alice sends Bob the message 14, and Bob sends Alice the message 44. Find the shared secret key between Alice and Bob showing all computations. [5]

   (b) n people $A_1, A_2, ..., A_n$ want to agree on a common secret key. They publicly choose a large prime p and a primitive root α of Z_p^*. They privately choose random numbers $r_1, r_2, ..., r_n$ respectively. Generalize the *Diffie Hellman Secret Key Exchange Protocol* so that the n people can compute the common private key $K = \alpha^{r_1 r_2 \cdots r_n} (\text{mod } p)$ securely (ignore active intruder in the middle attacks) using minimum possible message exchanges (if X sends a message to Y, it is counted as one message; if X brodcasts a message, it is counted as $n-1$ messages). [10]