CS641A Assignment on Hash functions Semester II, 2017-18

Due Date: 2 April, 2018 **Maximum Marks: 100**

Instructions

- Submit the hard copy of the assignment at KD213 on 2 April 2018.
- Yours answers should be precise and clearly written in LATEX.
- Cheating/plagiarizing in any form will be heavily penalized.
- Late submissions will receive a mark of zero.
- Any doubts regarding the assignment can be raised in the discussion forum on moodle. PLEASE DO NOT COME TO LAB.

Consider a variant of KECCAK hash function which we will call WECCAK(WEAK-KECCAK).The following is the description of WECCAK.

1. Input to the hash function is a message M.
2. M is padded with minimum number of zero's such that bit-length of padded message is a multiple of 184.
3. The padded message is divided into block of 184 bits. Let's call them $M_1, M_2, \ldots, M_r$.
4. A state in WECCAK hash function is a $5 \times 5 \times 8$ 3-dimensional array.
5. Initial State S contains all zeros.
6. The first message block M_1 is appended with 16 zeroes to form $M_1^{'}$ and is XORed with S.(This procedure is similar to KECCAK)
7. This state is given as input to a function F(which will be defined later) and let's call it output as O_1. The output of F is also a $5 \times 5 \times 8$ 3 dimensional array.
8. The second message block M_2 is appended with 16 zeroes to form $M_2^{'}$ and is XORed with O_1 and is given to F.
9. This is continued for r times.
10. The output of WECCAK is the initial 80 bits of O_r.(This procedure is similar to KECCAK).

Let $R = \chi \circ \rho \circ \pi \circ \theta$. ($\theta, \rho, \pi, \chi$ is the same as defined in KECCAK). Please note that now in all the operations z indicies are modulo 8. Consider $H_1 = R \circ R$ and $H_2 = \underbrace{R \circ R \cdots \circ R}_{24 \text{ times}}$.

1. (40 points) Compute the inverse of χ and θ.
2. (30 points) Claim about the security of WECCAK with $F = H_1$.(Give a preimage, collision and second preimage attack)(Hint: Birthday paradox and meet in middle)
3. (30 points) Claim about the security of WECCAK with $F = H_2$.(Give a preimage, collision and second preimage attack)(Hint: Birthday paradox and meet in middle)