CS641: Midsem Examination

February 27, 2022

Submission Deadline: March 1, 2022, 23:55hrs **Maximum Marks**: 50

Question 1. (25 marks) Consider a variant of DES algorithm in which all the S-boxes are replaced. The new S-boxes are all identical and defined as follows.

> Let $b_1, b_2, \cdots, b_6$ represent the six input bits to an S-box. Its output is $b_1 \oplus (b_2 \cdot b_3 \cdot b_4)$, $(b_3 \cdot b_4 \cdot b_5) \oplus b_6$, $b_1 \oplus (b_4 \cdot b_5 \cdot b_2)$, $(b_5 \cdot b_2 \cdot b_3) \oplus b_6$.

Here '$\oplus$' is bitwise XOR operation, and '$\cdot$' is bitwise multiplication. Design an algorithm to break 16-round DES with new S-boxes as efficiently as possible.

Question 2. (25 marks) Suppose Anubha and Braj decide to do key-exchange using Diffie-Hellman scheme except for the choice of group used. Instead of using F_p^* as in Diffie-Hellman, they use S_n, the group of permutations of numbers in the range $[1, n]$. It is well-known that $|S_n| = n!$ and therefore, even for $n = 100$, the group has very large size. The key-exchange happens as follows:

> An element $g \in S_n$ is chosen such that g has large order, say ℓ. Anubha randomly chooses a random number $c \in [1, \ell - 1]$, and sends g^c to Braj. Braj chooses another random number $d \in [1, \ell - 1]$ and sends g^d to Anubha. Anhuba computes $k = (g^d)^c$ and Braj computes $k = (g^c)^d$.

Show that an attacker Ela can compute the key k efficiently.