Indian Institute of Information Technology, Allahabad
Department of Information Technology

Program Code & Semester: B.Tech (IT)- 6^{th} Semester.

Paper Title: Network Security
Tutorial and Practical Assignment - 1 (Component 1)

Important Note: The group members have to prepare the report and presentation

1. **Tutorial: Browser** - Refer the paper "The Security Architecture of the Chromium Browser" and identify the security requirements for the web browsers. Also compare chrome with firefox with respect to only security parameters (or requirements).
2. **Practical: ICMP** - Analyze the different vulnerabilities of the ICMP protocol with respect to Packet Internet Groper (PING) [use Wireshark, packeth, etc. as per your available infrastructure]
3. **Tutorial: Perfect Secrecy** - An example for the perfect secrecy? What is the limitation of perfect secrecy? Can we link semantic security with perfect secrecy?
4. **Tutorial: Entropy** - Analyze the entropy and provide example to quantify the uncertainty. Give the need of entropy in cryptography.
5. **Tutorial: Oracle Machine** - Why the cryptanalyst need oracle machine? How it works? What are the alternates to the Oracle Machine?
6. **Tutorial: Unicity Distance** - Analyze the Unicity distance with the perspective of Substitution cipher.
7. **Tutorial: Birthday Problem** - Analyze the birthday problem. Prove that a hash algorithm with output size N can get the collision with the chance of 50% when $2^{\frac{N}{2}}$ attempt is made.
8. **Practical: Brute-force** - Analyze the Rainbow Table and Dictionary attack.
9. **Tutorial: Encryption Algorithm Criteria** - How to estimate the following.
   - The cost of breaking the cipher exceeds the value of the encrypted information.
   - The time required to break the cipher exceeds the useful lifetime of the information.
10. **Tutorial: Number Theory** - Group, Ring, Field, Fermat's Little Theorem, Euler Theorem and analyze the usage in Cryptography.
11. **Tutorial: Active and Passive Attack** - Categorize the different Network attacks.
12. **Tutorials: Attackers** - Assume a larger application and list out the inside and outside attackers.