Quiz I

Principles of Information Security
IIIT Hyderabad, Spring 2025

January 30, 2025

There are 4 questions. Maximum Marks: 30. Time: 45 min

---

1. Which of the following is/are negligible function(s)? Prove your answers. $1 \times 6 = 6$

    1. $\frac{1}{(\log n)!}$
    2. $\frac{1}{(\log \log n)!}$
    3. $f(n) + g(n)$, where f, g are negligible functions in n.
    4. $f(n) \times g(n)$, where f, g are negligible functions in n.
    5. $\frac{f(n)}{g(n)}$, where f, g are negligible functions in n.
    6. $\frac{1}{n^{100}}$

2. Prove the following are hard-core predicates for DLP ($f(x) = g^x \bmod p$) in $\mathbb{Z}_p^*$ for a prime p, if $(p-1) = s2^r$ for some odd s: (a) the `msb` and (b) the $(r+1)^{th}$ `lsb` (that is the bit that says if $x \bmod 2^{r+1}$ is $\geq 2^r$). Using any of these, design a provably secure PRG assuming DLP is hard in $\mathbb{Z}_p^*$. $4 + 5 + 5 = 14$ marks

3. Consider a variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is not CPA-secure. 5 marks

4. Write in detail about any *one* among: 5 marks

    - Breaking historical ciphers.
    - Shannon's perfect secrecy.
    - One-way functions