

Reg. No.:

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Question Paper Code : 20428

B.E./B.Tech. DEGREE EXAMINATIONS, APRIL/MAY 2022.

Sixth/Seventh Semester

Computer Science and Engineering

CS 8792 — CRYPTOGRAPHY AND NETWORK SECURITY

(Common to : Computer and Communication Engineering/Electronics and
Communication Engineering/Electronics and Telecommunication
Engineering/Information Technology)

(Regulations 2017)

Time : Three hours

Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What are the two types of passive attacks?
2. Perform encryption for the plain text "AUTHENTICATION AND INTEGRITY" using single columnar transposition technique and the key is 614352.
3. Compare differential and Linear cryptanalysis.
4. Find $\text{gcd}(45, 6)$ using Euclidean algorithm.
5. Find the value of $6^{24} \text{ mod } 35$ using Euler's theorem.
6. What are the various ways to distribute the keys?
7. List the properties of hash function.
8. Why do we need digital signature?
9. List the five services provided by PGP.
10. Mention the difference between virus, worm and Trojan horse.

