

Dr R. Bhatt

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

SUMMER SEMESTER EXAMINATION- 2018

B.Tech (VIII) Semester

COURSE CODE: 17B1WCI814

MAX. MARKS: 50

COURSE NAME: Design and Analysis of Real World Algorithms

COURSE CREDITS: 3

MAX. TIME: 2 Hr

Note: All questions are compulsory.

1. [10 Marks]

Explain the ID3 and candidate elimination algorithm with following:

Origin	Manufacturer	Color	Decode	Type	Example Type
Japan	Honda	Blue	1980	Economy	Positive
Japan	Toyota	Green	1970	Sports	Negative
Japan	Toyota	Blue	1990	Economy	Positive
USA	Chrysler	Red	1980	Economy	Negative
Japan	Honda	white	1980	Economy	Positive

2. [10 Marks]

- Explain how the distribution of secret keys is facilitated by public key cryptography.
- Write notes on the following.
 - MAC
 - Hash function

3. [10 Marks]

- What is the need for digital signatures? Explain important properties of digital signatures.
- What is the role of a function approximation algorithm? How does learner system estimate training values and adjusts weights while learning?

4. [10 Marks]

- Write the algorithm steps for Schnorr signature scheme.
- Explain Diffie Hellman key exchange algorithm.

5. [10 Marks]

- Explain elliptic curve cryptography.
- Explain Authentication protocols for symmetric cipher system.