

PURBANCHAL UNIVERSITY

2019

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO: Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

- 1(a) Explain the concept of System. Differentiate between Continuous and discrete, Deterministic and Stochastic system with example. 5
- (b) Explain the phases and steps in simulation study. 5
2. A vegetable shopkeeper is trying to determine how much green vegetable he has to purchase for selling. The probability distribution of no. of customer is as follow.

No. of customer/Day	8	10	12	14
Probability	0.35	0.30	0.25	0.10

Customer order 1,2,3 or 4 kg of vegetable as per the following probability distribution.

Kg ordered/Customer	1	2	3	4
Probability	0.4	0.3	0.2	0.1

Vegetable sells for Rs. 50 per kg. All vegetable not sold for the day are sold at half price. Based on 5 days of simulation how much vegetable the shopkeeper should purchase each day. 10

- 3(a) Discuss the basic philosophy of Monte-Carlo simulation. 5
- (b) Explain the concept of continuous system simulation. 5
- 4(a) Explain mid square random number generator. 5
- (b) Enumerate the qualities of good random number generator. Use linear congruential method to generate random numbers with full period with seed value 6 and 7. Take $a=12$, $c=5$ and $m=26$. 5

Contd. ...

(2)

5. What do you mean by testing of random numbers, why it is needed? Use Chi-Square test to test the following random numbers with confidence level 95%. 3+7
- 36, 91, 51, 02, 54, 06, 58, 06, 58, 02, 54, 01, 48, 97, 43,
22, 83, 25, 79, 95, 42, 87, 73, 17, 02, 42, 95, 38, 79, 29,
65, 09, 55, 97, 39, 83, 31, 77, 17, 62, 03, 49, 90, 37, 13,
17, 58, 11, 51, 92
6. "Simulation output has to be analyzed", Justify the statement. Explain the process of replication of runs and elimination of internal bias in the analysis of simulation output. 10
7. List out the various simulation tools. Explain GPSS in brief with suitable example. 10
8. Explain the principle of discrete system simulation. Explain feedback system with its application. 4+6
9. Write short notes on any TWO 5+5
(a) Markov Chain
(b) Application areas of simulation
(c) Kendall's notation



PURBANCHAL UNIVERSITY
2017

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO: Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

1. What do you mean by system simulation? Why do we need simulation? Explain a field of life where you would like to use simulation. 2.5+2.5+5
2. Why do you need a model for simulation? Explain the phases and steps to be followed in Simulation. 2+8
3. What are the different types of simulation? Explain each with example. Explain the concept of Monte Carlo Simulation with suitable example to calculate the value of " π (pi)" using $x^2+y^2=9$. 5+5
4. What is a queuing system? Why is it an important part of Simulation studies? Explain the Kendall's' queuing notation for different types of queues. 3+2+5
5. Explain the LCG and MCG methods of random number generation. Generate a sequence of random numbers with $X_0=37$, $a=7$, $c=29$ and $m=100$. 5+5
6. Develop poker test for the following 1000 4-digit random numbers generated during an experiment to test whether they are independent or not at 5% level of significance. ($\alpha_{0.05,2}=5.99$) 10

combination	Observed frequency
Three different digits	700
Two like digits	278
Three exactly same digits	22
7. What do you mean by analog methods? Explain the analog computer model of automobile suspensions system. 4+6

(2)

8. Discuss Markov chains with their practical areas of application.
Why are differential equations used in continuous system
simulation? 6+4
9. Write short notes on any TWO 5+5
- (a) Continuous and Discrete System
 - (b) GPSS
 - (c) Simulation Run Statistics
- ***

PURBANCHAL UNIVERSITY
2017

B.E. (Computer) / Seventh Semester / Final

Full Marks: 80 / Pass Marks: 32

Time: 03.00 hrs.

BEG473CO: Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

1. What do you mean by system simulation? What is Model?
 Explain the steps in simulation study with necessary flowchart.
 2+2+6

✓ 2. Define continuous and discrete systems. Write advantages and limitations of simulation techniques. Write its application areas.
 2+6+2

3. Discuss Monte Carlo Method. Using Monte Carlo method, calculate the integral $\int x dx$. How Monte Carlo Method differs from stochastic simulation?
 3+5+2

✓ 4. What do you mean by feedback system? What is analog method?
 Design the analog computer model for the given second order differential equation:
 $M\ddot{x} + D\dot{x} + Kx = KF(t)$
 2+3+5

5. Describe Measurement of System Performance of Queuing system with necessary formulae. What is Markov Chain? 7+3

✓ 6. What do you mean by verification and validation of simulation model? Describe the techniques for verification of simulation model.
 3+7

✓ 7. Why computer generated random numbers are called pseudo random numbers? Describe Linear Congruential Generator with example. Mention the qualities of efficient random number generator.
 2+5+3

Contd. ...

S/2015

(2)

✓ 8. Describe estimation methods for simulation output. Explain GPSS with an example. 5+5

✓ 9. Write short notes on any TWO

- (a) Hybrid Simulation
- (b) Poker Test
- (c) A pure Pursuit Problem

PURBANCHAL UNIVERSITY
2017

B.E. (Computer) / Seventh Semester / Back

Time : 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO: Simulation & Modeling (Old Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

8×10=80

1. What do you mean by continuous and discrete systems? Explain with an example of each. Describe real time simulation briefly. What are the limitations of Simulation technique? 2+2+2+4
2. Explain static mathematical model. Describe steps and phases in Simulation study. 4+6
3. State and explain qualities of an efficient random number generator. Generate 5 random numbers using LCM with $a=11$, $m=16$, $c=1$ and $X_0=7$. 5+5
4. A sequence of 1000 four-digit numbers has been generated and an analysis shows the following combinations and frequencies: 10

Combination, i	Observed frequency, O_i
Four different digits	565
One pair	392
Two pairs	17
Three like digits	24
Four like digits	2
Total	1000

Based on the poker test, test whether these numbers are independent at $\alpha=0.05$. 10

5. Distinguish analog computers with digital computers. Draw and briefly explain analog computer model of liver. 4+6
6. Explain the importance of Markov chain. Find the value of Π using Monte Carlo method. 4+6

Contd. ...

(2)

7. A baker is trying to determine how many dozens of cake to bake each day. The probability distribution of the number of cake-customers is as follows:

No. of Customers/Day	8	10	12	14
Probability	0.40	0.30	0.20	0.10

Customers order 1, 2, or 3 dozen cakes according to the following probability distribution:

No. of dozen ordered/Customer	1	2	3
Probability	0.45	0.30	0.25

Cakes sell for 540 per dozen. They cost 380 per dozen to make. All cakes not sold at the end of the day are sold at half price. Based on 6 days of simulation, how many dozen, to the nearest to 10 dozen, cakes should be baked each day? 10

8. Explain GPSS block diagram for a telephone system in detail. 10
9. Why is analysis of simulation output important? Describe estimation methods. 3+7
10. Write short notes on any TWO: 5+5
- (a) Continuous System Modeling Program version III (CSMP III)
 - (b) Pure pursuit problem
 - (c) Normally distributed random number

PURBANCHAL UNIVERSITY
2016

B.E. (Computer) / Seventh Semester / Final
Time: 09:00 hrs. Full Marks: 80 / Pass Marks: 32
BEG473CO: Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.
All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

1. What do you mean by system simulation? Why do we need simulation? Explain a field of life where you would like to use simulation. 2.5+2.5+5

2. Define and explain the concept of system. Why do you need a model for simulation? Explain the limitations and areas of applications of simulation techniques. 3+2+5

3. What are the different types of simulation? Explain each with example. Explain the concept of Monte Carlo simulation with suitable example to calculate the value of " π " using $x^2+y^2=25$. 5+5

4. What is queuing system? Why is it an important part of simulation studies? Explain different queuing disciplines. 5+5

5. Explain the LCG and MCG methods of random number generation. Generate a sequence of random numbers with $X_0=37$, $a=7$, $c=29$ and $m=100$: 0.8, 0.5, 0.9, 0.7 5+5

6. Why do we have t test Random Numbers? Explain the Chi Square test method of testing random numbers with example. 10

7. What do you mean by analog methods? Explain the analog computer model of automobile suspensions system. 4+6

8. Discuss Markov chains with their practical areas of application. Why are differential equations used in continuous system simulation? 6+4 5+5

9. Write short notes on any TWO

(a) Continuous and Discrete System

(b) Steps and Phases in Simulation Study

(c) Simulation Run statistics

PURBANCHAL UNIVERSITY
2015

B.E. (Computer) / Seventh Semester / Choice

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO. Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

1. Define Simulation. List out its advantages and disadvantages. Also deal with when the use of simulation is appropriate and when it is inappropriate. 10
2. What is discrete event simulation? Draw and explain the flowchart for the organization of discrete event simulation. 3+7
- 3(a) Differentiate between Monte Carlo Simulation with Stochastic Simulation. 4
(b) Illustrate the case of random process. Consider a game in which an unbiased coin is repeatedly flipped. For each flip you have to pay Re 1 and when the difference between heads and tails tossed becomes 3, you get Rs 8. If the required difference obtained is less than 8 flips, you win some money and if it is more than 8 flips you lose. Illustrate the simulation to decide whether to play this game or not. 6
- 4(a) What are the properties of random numbers? Why the random numbers generated by a computer are called Pseudo-random numbers? Explain. 5
(b) Write an algorithm for generating random numbers for two or more generators. Also determine its maximum period.
- 5(a) What are the methods used for testing of random numbers? Explain Poker test. 5

Contd. ...

(2)

- (b) Test whether the 2nd, 7th, 12th and so on, numbers in the sequence in the given table is auto correlated. (Use $\alpha=0.05$). 5

0.12	0.01	0.23	0.68	0.86	0.96	0.21	0.88	0.92
0.81	0.11	0.05	0.24	0.89	0.48	0.51	0.81	0.23
0.33	0.29	0.68	0.58	0.91	0.60	0.35	0.46	0.55
0.43	0.56	0.99						

6. What is feedback system? Using analog method of simulation, explain the working procedure of human liver with appropriate block diagram, 3+7

- 7(a) Explain point of estimation and confidence level estimation technique during analysis of simulation output. 5

- (b) Explain initial bias in simulation. How can it be eliminated? 5

8. Explain the different blocks used in GPSS. Draw the GPSS block diagram for the following scenario: A machine tool in a manufacturing shop is turning out parts at the rate of 1 every 7 minutes. As they are finished, the parts go to an inspector, who take 5 ± 2 minutes to examine one and rejects about 15% of the parts. 4+6

9. Write short notes on any TWO: 5+5

- (a) Static Vs Dynamic simulation
- (b) SIPOSRIPT
- (c) Validation and Verification



PURBANCHAL UNIVERSITY
2015

B.E. (Computer) / Seventh Semester / Final
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO, Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

1. What do you mean by simulation and modeling? Explain the steps in the simulation study? 3+7

2(a) Explain the analogy method of system study with suitable example. 5

(b) Explain how continuous model can be solved numerically with an example. 5

3(a) Explain the arrival and departure routine queuing model for a banking system. 5

(b) Calculate the following using Monte Carlo simulation. (Use your own random numbers): 5

$$I = \int_{-3}^{5} (x^2 - 1) dx$$

4(a) What are the properties of random numbers? Why the random numbers generated by a computer are called Pseudo-random numbers? 2+2

(b) Write the algorithm for linear congruential method. Using the multiplicative congruential method, find the period of the generators for $a=13$, $m=2^6$, and $X_0=2$ and 4. 3+3

Contd...

(2)

5(a) Explain the Mid square method for generating random numbers with an example.

(b) Consider the given sequence:

0.41 0.68 0.89 0.94 0.74 0.41 0.55 0.62 0.36 0.27
0.19 0.72 0.75 0.08 0.54 0.02 0.01 0.36 0.16 0.28
0.18 0.01 0.95 0.61 0.18 0.47 0.23 0.32 0.82 0.53
0.31 0.12 0.73 0.04 0.83 0.45 0.13 0.57 0.63 0.29

Based on run test check whether given sequence is random or not. [Given $Z_{\alpha/2} = 1.96$]

6(a) Explain feedback system with suitable example.

(b) Explain the mathematical modeling of replication of runs.

7(a) Why simulation output is analyzed? Explain estimation method for analysis of simulation output. 2+3

(b) What is initial bias in simulation output? Mention the idea of elimination of initial bias. 3+2

8(a) Draw different types of GPSS block-diagram symbols and explain with the help of GPSS block-diagram of manufacturing shop. 5

(b) State some types of Simulation languages. Illustrate the possible event interactions in Hybrid Simulation. 5

9. Write short notes on any TWO 5+5

(a) Differential equation

(b) Simulation Run statistics

(c) Markov Chain

PURBANCHAL UNIVERSITY

2014

B.E. (Computer) / Seventh Semester / Final
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO: Simulation & Modeling

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

1. Explain the ways to study a system. What are the criteria of classifying Simulation models? Brief it with suitable example. 3+7
2. What do you mean by discrete event simulation? Explain the principal approaches for advancing the simulation clock in discrete event simulation. 4+6
- 3(a) Explain the concept of Monte-Carlo simulation over stochastic simulation. 5
(b) Find the value of pi (π) by using Monte Carlo simulation using the equation $x^2+y^2= 16$? Also Calculate error when compared with its analytical value. 5
4. The computing facility of Purbanchal University has large no. of personal computers. On 50% of working days no computer fails, on 30% of the days 1 machine fails & on 20% of days 2 machines fails. There is a repairing facility, which has one-service personnel. He can fix the problem on the average 40% of the machine in 1 day, 35% in 2 days & 25% in 3 days. The service person says he is overloaded and computer waits a long time for service. He reminds that next should go for second service person. Consider the 30 days slot and verify if the service person claims is correct by computing his efficiency, the number of computers waiting for service and average waiting time for computers. 10

(2)

5. Why are differential equations so important in simulation?
Explain continuous system simulation with suitable example. 5+5
- 6(a) What are the qualities of good random number generators?
What are the methods used for testing of random numbers? 5
- (b) Test whether the 2nd, 7th, 12th and so on, numbers in the sequence in the given table are auto correlated. (use $\alpha=0.05$) 5

0.12	0.01	0.23	0.25	0.58	0.87	0.55	0.96	0.22	0.88
0.11	0.22	0.85	0.36	0.69	0.87	0.19	0.92	0.75	0.43
0.68	0.58	0.91	0.60	0.35	0.33	0.15	0.49	0.27	0.99

7. Why the output of simulation has to be analyzed? Explain
Replication of Runs method to any simulation output. 4+6

8(a) Why is simulation tool required? What is GPSS language & its
application? 3+3

(b) Explain in details of GPSS block diagram symbols. 4

9. Write short notes on any TWO:
(a) Poker test
(b) Feedback system
(c) Elimination of internal bias $2 \times 5 = 10$

~

PURBANCHAL UNIVERSITY

2013

B.E. (Computer) / Seventh Semester / Choice

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO: Simulation & Modeling

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

1. Explain the ways to study a system. What are the criteria of classifying Simulation models? Brief it with suitable example. 3+7
2. What do you mean by discrete event simulation? Explain the principal approaches for advancing the simulation clock in discrete event simulation. 4+6
- 3(a) List the entities, attributes, activities and state variables in the working of your college workshop. 5
(b) Find the value of pi (π) by using Monte Carlo simulation using the equation $x^2+y^2=25$? Also Calculate error when compared with its analytical value. 5
- 4(a) Explain Normally distributed random numbers. 3
(b) In the random walk problem the drunkard can take steps in four directions, forward, backward, to left and to right. The probabilities associated with these are 40%, 10%, 25%, and 25%. The distances covered in the forward, backward, to left and to right steps are 75 cm, 45 cm, 60 cm, and 60 cm respectively. Simulate the walk for 20 steps, and find the location at the end of 20 steps, while the starting point is (0,0) on the x-y scales. 7
- 5(a) What do you mean by a continuous system, explain pure pursuit problem to represent the continuous system. 5
(b) Represent the following equation in terms of analog computer block diagram: $Ax''+Bx'+Cx+D=0$ 5
- 6(a) What are the qualities of good random number generators? Explain any two methods of generation of random numbers. 2+3

Contd. ...

(2)

- (b) A random sequence of 10 numbers has been generated as
 $R(i)=\{0.24, 0.89, 0.11, 0.61, 0.23, 0.86, 0.41, 0.64, 0.50, 0.65\}$.
Use Kolmogorov-Smirnov test with $\alpha=0.05$ to test whether the
numbers are uniformly distributed. 5
7. Why the output of simulation has to be analyzed? Explain
Replication of Runs method to any simulation output. 4+6
8. Explain Discrete Simulation Language in brief. Explain the
system concepts of Simscript. How a program is organized in a
Simscript. 3+3+4
9. Write short notes on any TWO: 5+5
(a) Feedback system
(b) Real time simulation
(c) GPSS



PURBANCHAL UNIVERSITY

2019

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG471CO: Artificial Intelligence (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

$8 \times 10 = 80$

- 1(a) What is an artificial intelligence? Explain about PEAS any artificial intelligence agent. 2+4
- (b) Compare Blind search and Heuristic search. 4
2. What is an expert system and what are its applications? Briefly describe the various steps involved in the development of an expert system. 4+6
3. Describe the various levels of analysis used in natural language processing. 10
4. Express the following sentences into FOPL. 5×2=10
- (a) Steve only likes easy course.
 - (b) Science courses are hard.
 - (c) All apples in the basket are rotten
 - (d) Bill eats peanuts and is still alive.
 - (e) Rita eats everything Bill eats.
5. Define constraint satisfaction problem. Stating necessary conditions and assumptions solve the following crypto-arithmetic problem. SEND+MORE=MONEY. 2+8
- 6(a) What is neural network? How back propagation works for learning in multilayer network? 2+4
- (b) What is hill climbing and its problems? 4
- 7(a) What are the different types of learning. Explain the induction learning with suitable examples. 2+4

Contd. ...

(2)

(b) How does semantic network represent knowledge? Explain with suitable example.

4

8. Write the algorithm of depth-first search and explain with suitable example.

5+5

9. Write short notes on any TWO:

- (a) Genetic Algorithm
- (b) Bayesian network
- (c) Reinforcement learning



PURBANCHAL UNIVERSITY
2018

B E (Computer) / Seventh Semester / Final
Full Marks: 80 / Pass Marks: 32
Time: 03:00 hrs.

BEG471CO: Artificial Intelligence (New Course)

Candidates are required to give their answers in their own words as far as practicable
All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

$$8 \times 10 = 80$$

1. What is AI? How is it different from natural intelligence? Support with example. 2+8
2. What is heuristic function? Explain Hill climbing problems with examples. 3+7
3. Define knowledge and knowledge representation. Explain semantic networks and frames are used for knowledge representation with example. 2+8
4. What is non-linear planning? Explain MYCIN-Style probabilities and its application. 4+6
5. Explain natural language processing. Discuss different steps in language understanding and generation in brief. 4+6
6. Convert the following sentences into CNF (Conjunctive Normal Form):
(a) If Virat is a human, he can think.
(b) Salmon, Shark and Tarpon are fishes.
(c) All dogs have a tail.
(d) Everybody is good at something.
(e) John likes whatever Peter dislikes and dislikes whatever Peter likes.
5x2=10
7. Solve the following crypto-arithmetic problem:
CROSS + ROADS= DANGER
Show all the steps that you advance through constraint satisfaction. 10

Contd. ...

(2)

8. What is neural network? Explain perception and Hopfield
network in brief. 3+7

5+5

9. Write short notes on any TWO:

- (a) Simulated Annealing
- (b) Characteristics of expert-system
- (c) Bayesian networks.

~~~

# FURBANCHAL UNIVERSITY

2017

B.E. (Computer) / Seventh Semester / Final

Time 03:00 hrs.

Full Marks: 80 / Pass Marks: 32  
**BEG471CO: Artificial Intelligence (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

## Answer EIGHT questions.

8x10=80

1.(a) Why is machine learning an important in artificial intelligence? Explain inductive learning with an example.

2+4

1.(b) How does frame system represent knowledge? Explain with suitable example.

4

2. What is constraint satisfaction problem? Stating necessary conditions and assumptions solve the following crypto-arithmetic problem: EAT+THAT=APPLE.

2+8

3. What is natural language? Describe the various tasks used in natural language processing.

2+8

4. Express the following sentences into FOPL:

5x2=10

- Ram only likes easy course.
- Management courses are easy.
- All courses in the Computer department are easy.
- Bill eats peanuts and is still alive.
- Sita eats everything Ram eats.

5. What is decision support system? Briefly describe the various steps involved in the development of an expert system.

2+8

6. What is perceptron? How back propagation works for learning in multilayer network. Explain with suitable examples.

2+8

7.(a) Explain the importance of artificial intelligence and AI agent.

2+3

7.(b) Briefly explain the heuristic search with example.

5

(2)

8

Explain iterative deepening. Discuss decision tree

9

Write short notes on any TWO:

- (a) Genetic Algorithm
- (b) Forward chaining-and backward changing
- (c) Reasoning with uncertainty
- (d) Semantic Network



extra

# PURBANCHAJ UNIVERSITY

2017

B.E. (Computer) / Seventh Semester / Final

Time: 03.00 hrs.

**BEQ471CO: Artificial Intelligence (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

## Answer EIGHT questions.

$$8 \times 10 = 80$$

1. Define PEAS and its properties. Explain the challenges of AI. 7+3
2. What is depth-first search? State its algorithm. Explain how depth-limited search and iterative-deepening search solves the problem of depth-first search. 4+6
3. What do you mean by adversial search? Explain MinMax problem with example. Write the importance of game playing in AI. 2+5+3
4. State the inference theorems. Define logic and explain propositional calculus with examples. 6+4
5. How is an expert system different from natural intelligence? Explain the role of knowledge base and inference engine in expert system. 4+6
6. State back-propagation algorithm. Explain the working of Hopfield network with suitable example. 4+6
7. What are natural language understanding and natural language generation? 5
- (b) Explain case-based reasoning with proper flowchart. 5
8. How is problem formulated? Explain the types of problem with examples. 5
- (b) Solve the following cryptarithmetic puzzle by stating all the necessary assumptions that you make: 5

(2)

9. Write short notes on any TWO:

5+5

- (a) Forward-chaining vs backward-chaining
- (b) Semantic net
- (c) Reinforcement learning

# PURBANCHAL UNIVERSITY

2017

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks:

80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

## Answer EIGHT questions.

**8x10=80**

- 1.(a) Why is machine learning an important in artificial intelligence? Explain inductive learning with an example. 2+4
- (b) How does frame system represent knowledge? Explain with suitable example.
2. What is constraint satisfaction problem? Stating necessary conditions and assumptions solve the following crypto-arithmetic problem: EAT+THAT=APPLE. 2+8
3. What is natural language? Describe the various tasks used in natural language processing. 2+8
4. Express the following sentences into FOPL: 5x2=10
  - (a) Ram only likes easy course.
  - (b) Management courses are easy.
  - (c) All courses in the Computer department are easy.
  - (d) Bill eats peanuts and is still alive.
  - (e) Sita eats everything Ram eats.
5. What is decision support system? Briefly describe the various steps involved in the development of an expert system. 2+8
6. What is perceptron? How back propagation works for learning in multilayer network. Explain with suitable examples. 2+8
- 7.(a) Explain the importance of artificial intelligence and AI agent. 2+3  
(b) Briefly explain the heuristic search with example. 5

(2)

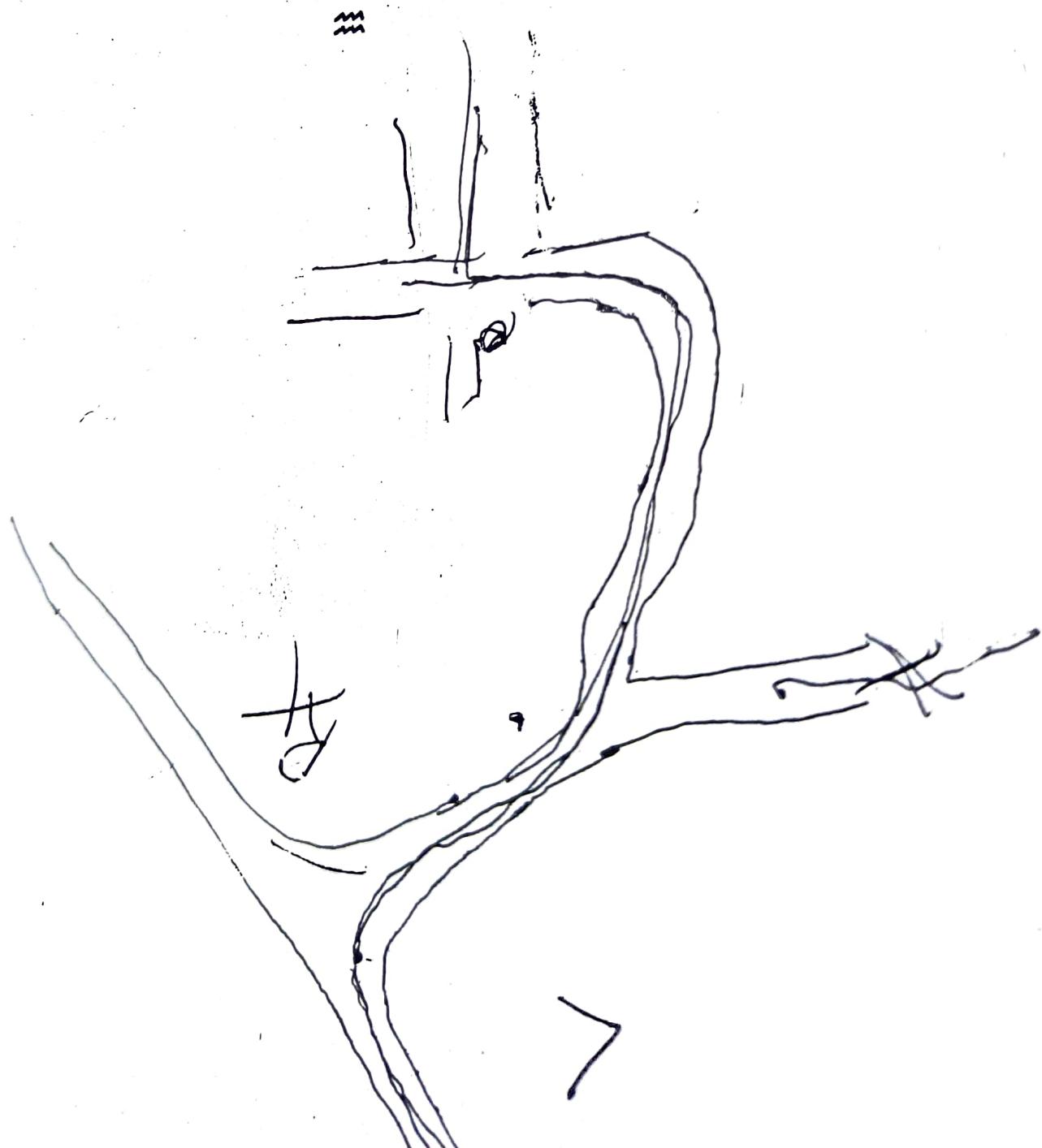
5+5

Explain iterative deepening. Discuss decision tree.

5+5

Write short notes on any TWO:

- (a) Genetic Algorithm
- (b) Forward chaining-and backward changing
- (c) Reasoning with uncertainty
- (d) Semantic Network



**PURBANCHAL UNIVERSITY**  
**2016**

E. (Computer) / Seventh Semester / Final  
Time 03.00 hrs

Full Marks: 80 / Pass Marks: 32

BEG471CO: Artificial Intelligence (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**$8 \times 10 = 80$**

**Answer EIGHT questions.**

1(a) What is an artificial intelligence. Explain with suitable example about the importance of artificial intelligence. **2+4**

(b) Compare Blind search and Heuristic search. **4**

2 Why do you need an expert system? Briefly describe the various steps involved in the development of an expert system. **2+8**

3(a) What is natural language? Describe the various levels of analysis used in natural language processing. **2+8**

4. Express the following sentences into FOPL:  **$5 \times 2 = 10$**

(a) Steve only likes easy course.

(b) Science courses are hard.

(c) All courses in the basket weaving department are easy.

(d) Bill eats peanuts and is still alive.

(e) Rita eats everything Bill eats.

5. What is constraint satisfaction problem? Stating necessary conditions and assumptions solve the following crypto-arithmetic problem. **2+8**

$$\begin{array}{r} \text{CROSS} \\ + \text{ROAD} \\ \hline \text{DANGER} \end{array}$$

6. What is neural network? How does back propagation work for learning in multilayer network?  **$2+4+4$**

7(a) Why learning is important in artificial intelligence? Explain he induction learning with suitable examples.

(2)

(b) What is a frame and a frame system? Explain. 4

7(a) Explain the importance of game-playing in AI. 5

(b) Describe explanation-based learning. 5

8(a) State and explain best-first algorithm. 5

(b) Construct a parse tree for the following sentence:  
"The beautiful lady works in central bank of the city".

$$2 \times 5 = 10$$

9. Write short notes on any TWO:

(a) Machine learning

(b) Back propagation

(c) Bayesian Network



**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer) / Seventh Semester / *Chance*

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**SEG471CO: Artificial Intelligence (Old Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer ALL questions.**

1(a) What is AI? Describe expected approaches of AI where system think and Act rationally. 1+3

(b) Define the problem as a state space search. Apply the technique and solve the following water jug Problem: "A farmer was sent to a nearby pond to fetch 2 gallons of water. He was given two pails-one 4, the other 3 gallons. How can he measure requested amount of water? (Hints: define state representation, initial state, operators and goal state as when required.)" 1+5

2(a) What is logic? Illustrate with representation of knowledge in propositional logic in the given knowledge base and draw the conclusion whether Becky comes or not from the given propositions. 1+4

Given, KB= (Mike comes to the party;

If Cathy comes to the party then Becky comes;

If Cathy doesn't come then Mike won't come to the party)

(b) What is MYCIN System? Compare the semantic networks and frames knowledge representation. 2+3

3(a) Define Natural Language Processing. Explain the steps of natural language processing. 1+4

(b) Describe the concept of learning in Neural Networks. Differentiate between pragmatic and discourse integration. 3+2

4. What are constrain satisfaction problem? Solve the following crypto-arithmetic Problem where different letters denote different integer and identical letter denote same integer. 2+8

**SEVEN+EIGHT= TWELVE**

**Contd. ...**

- 5(a) What is machine learning? Compare the analogy based and explanation based learning. (2) 2+2
- (b) Define Perceptron. Describe the concept Network Architecture in Multilayer feed forward N/Ws. 2+2
6. Write short notes on any THREE: 2+4
- (i) Genetic Algorithm
  - (ii) Boltzmann Machine
  - (iii) Bayesian networks
  - (iv) Expert system
- 3×4=12
- 7(a) What do you mean by Heuristic search. Explain in short any heuristic search. 2+2
- (b) Define inference rule. Differentiate between forward and backward chaining in Production rules system. 2+4
8. Convert the following premises into FOPL: 8
- (i) There is an X and Y that is sister of Spot and they are not the same individual.
  - (ii) Every pair of objects with property p is equal.
  - (iii) There is a king and for all kings that are similar.
  - (iv) Parents of horse are horse.
  - (v) Everyone does nothing.
  - (vi) Brothers are siblings.
  - (vii) Anyone who is not sloppy is smart.
  - (viii) Not everyone is both smart and boring.



**PURBANCHAL UNIVERSITY**

**2017**

B.E. (Computer) / Seventh Semester / Back

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (Old Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

**$8 \times 10 = 80$**

- 1.(a) Compare A\* algorithm to greedy algorithm to show how it uses heuristic cost to generate optimum solution with an example. 6
- (b) Differentiate between inference and reasoning. Why possibilities reasoning are important in the AI? Explain with suitable example. 4
2. What do you mean by frames and semantic .Net? Express the following sentence into FOPL: 10
- (a) A person is a mammal.  
(b) Shakti Gauchan is a Person.  
(c) Person has nose.  
(d) Shakti Gauchan is in Nepalese team.  
(e) Uniform color of Shakti Gauchan is Red/Blue.
3. Discuss the constraint satisfaction probleim Solve the following crypt-arithmetic problem: 10
- (a) FORTY  
TEN  
+ TEN  
SIXTY
- (b) LOGIC  
+LOGIC  
PROLOG
4. Why conjunctive normal form and Disjunctive normal form is required? Explain all the steps with example. 10
- 5.(a) What is learning system? Explain rote learning and reinforcement learning. 6
- (b) Describe MIN MAX problem with example. 4

(2)

6. Explain the different steps involved in the natural language processing (NLP) and justify that NLP requires artificial intelligence? 10
- 7(a) What is expert system? Explain the difference between Human expert vs expert system with example. 5
- (b) Describe forward chaining and backward chaining in expert system. 5
8. What is multi-layer perception? How learning and validation is done in back propagation algorithm? Explain application of neural networks? 5+5
9. Write short notes on any TWO: 5+5
- (a) Alpha-beta pruning search
  - (b) Decision tree
  - (c) Learning by Induction
  - (d) Hill-climbing search



Date \_\_\_\_\_

**PURBANCHAL UNIVERSITY**  
**2015**

B.E. (Computer) / Seventh Semester / Final

Full Marks. 80 / Pass Marks. 32

Time. 03.00 hrs.

**BED471CO: Artificial Intelligence (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary

$$8 \times 10 = 80$$

Answer EIGHT questions.

1(a) Explain with suitable examples intelligence, artificial intelligence and agent. 1+2+3

(b) Compare DFS and BFS. 4

2) Describe the structure of an expert system. Briefly describe the various steps involved in the development of an expert system. 4+6

3(a) Discuss game tree with an example. 5

(b) Explain Alpha-Beta pruning algorithm. 5

4. Express the following sentences into FOPL. 5x2=10

(a) Lipton is a tea.

(b) Lata is a child who drinks tea.

(c) Ruma dislikes children who drink tea.

(d) Ruma disliked Lata.

(e) Anything anyone eats and isn't killed by is food.

5. Define constraint satisfaction problem. Stating necessary conditions and assumptions, solve the following cryptarithmic problem. 2+8

CROSS

+ ROADS

DANGER

Contd....

(2)

6. Define ANN and its components. Explain back propagation learning mechanism in ANN. 5+5

7(a) What are the different types of learning? Explain rule learning and induction learning with suitable examples. 2+2=2

(b) How does semantic network represent knowledge? Explain, with suitable example. 4

8. Differentiate between forward chaining and backward chaining. Use truth table approach to reach the goal for the following: 5×2=10

- (a) if it rain, roads are wet
- (b) if roads are wet and driving is careless, vehicles are slippery
- (c) if vehicles are slippery, accident occurs
- (d) It is raining
- (e) Driving is careless.

Prove the goal that accident occurs.

9. Write short notes on any TWO:

- (a) Genetic Algorithm
- (b) Inference Engine
- (c) Components of NLP

# PURBANCHAL UNIVERSITY

**2015**

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80

/ Pass Marks: 32

**BEG471CO: Artificial Intelligence (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

## **Answer EIGHT questions.**

**1(a) Explain with suitable examples intelligence, artificial intelligence and agent.**

**8x10=80**

1+2+3

**(b) Compare DFS and BFS.**

**4**

**2) Describe the structure of an expert system. Briefly describe the various the steps involved in the development of an expert system.**

**4+6**

**3(a) Discuss game tree with an example.**

**5**

**(b) Explain Alpha-Beta pruning algorithm.**

**5**

**4. Express the following sentences into FOPL.**

**5x2=10**

**(a) Lipton is a tea.**

**(b) Lata is a child who drinks tea.**

**(c) Ruma dislikes children who drink tea.**

**(d) Ruma disliked Lata.**

**(e) Anything anyone eats and isn't killed by is food.**

**5. Define constraint satisfaction problem. Stating necessary conditions and assumptions, solve the following cryptographic problem.**

**CROSS**

**2+8**

**+ ROADS**

**DANGER**

**(2)**

6. Define ANN and its components. Explain back propagation learning mechanism in ANN.

7(a) 5+5

What are the different types of learning? Explain rote learning and induction learning with suitable examples.

2+2+2

(b) How does semantic network represent knowledge? Explain with suitable example.

4

8. Differentiate between forward chaining and backward chaining.

Use truth table approach to reach the goal for the following:

$$5 \times 2 = 10$$

(a) if it rain, roads are wet

(b) if roads are wet and driving is careless, vehicles are slippery

(c) if vehicles are slippery, accident occurs

(d) It is raining

(e) Driving is careless

Prove the goal that accident occurs.

$$5+5$$

9. Write short notes on any TWO:

(a) Genetic Algorithm

(b) Inference Engine

(c) Components of NLP

\*\*\*

**PURBANCHAL UNIVERSITY**  
**2015**

B.E. (Computer) / Seventh Semester / Choice  
 Time 03:00 hrs. Full Marks: 80 / Pass Marks: 32

**SEG471CO: Artificial Intelligence (New Course)**

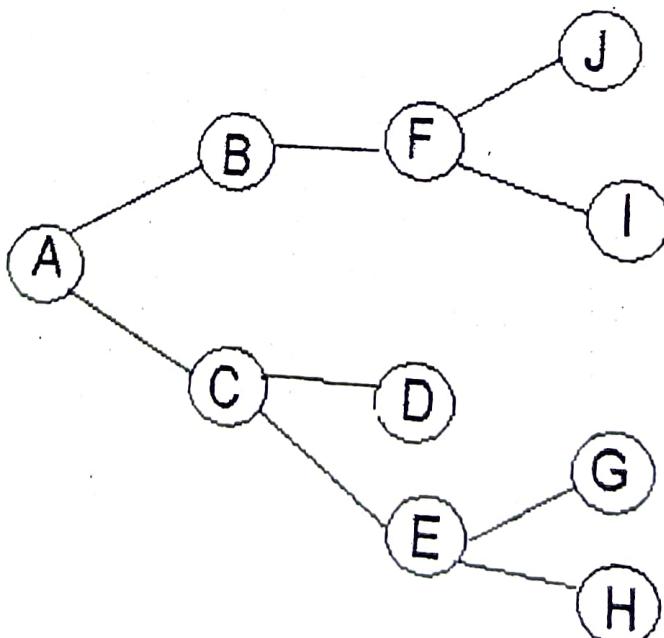
Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**$8 \times 10 = 80$**

**Answer EIGHT questions.**

- 1(a) Define Artificial intelligence and rationality. Discuss the applications of AI with examples. 5
- (b) Explain the PCAS elements of an agent with any suitable example. 5
- 2(a) Compare the Bidirectional search with depth limited search. Explain the working of iterative deepening search. 4
- (b) Starting from state A, execute BFS and DFS. The goal node is G. Show the sequence in which nodes are expanded. Note that the alphabetically smaller node is expanded first to break ties. 6



3. Explain learning system in AI. Discuss and compare the explanation based learning and reinforced learning and better of the two for different systems.

(2)

- 4(a) Compare reasoning with inferencing. Explain the Bayesian network as statistical reasoning. 6
- (b) Discuss case based reasoning. 4
5. Explain with a block diagram the expert system. Compare this system with natural intelligence. 7+3
- 6(a) What do you mean by heuristic search. Explain the hill climbing algorithm. 2+4
- (b) Briefly describe the types of agents. 4
- 7(a) Convert the following sentences into FOPL: 4×1.5=6
- (i) Anyone passing his exams and winning the lottery is happy.
  - (ii) Anyone who studies or is lucky can pass all his exams.
  - (iii) John didn't study well but he is lucky.
  - (iv) Anyone who is lucky wins the lottery.
- (b) Use resolution to prove "John is happy".
- 8(a) Compare the natural language processing with natural language generation. Describe in detail the steps of NLP. 6
- (b) Explain with necessary diagram the artificial neural network architecture. 4
9. Write short notes on any FOUR: 4×2.5=10
- (a) Forward chaining Vs backward chaining
  - (b) Semantic Nets
  - (c) Min Max problem
  - (d) Perceptron Network
  - (e) CSP problems

1  
&

**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer) / Seventh Semester / Choice

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (Old Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer ALL questions.**

- 1(a) What is AI? Describe expected approaches of AI where system think and Act rationally. 1+3
- (b) Define the problem as a state space search. Apply the technique and solve the following water jug Problem: "A farmer was sent to a nearby pond to fetch 2 gallons of water. He was given two pails-one 4, the other 3 gallons. How can he measure requested amount of water? (Hints: define state representation, initial state, operators and goal state as when required.)" 1+5
- 2(a) What is logic? Illustrate with representation of knowledge in propositional logic in the given knowledge base and draw the conclusion whether Becky comes or not from the given propositions. 1+4  
Given, KB= (Mike comes to the party;  
If Cathy comes to the party then Becky comes;  
If Cathy doesn't come then Mike won't come to the party)
- (b) What is MYCIN System? Compare the semantic networks and frames knowledge representation. 2+3
- 3(a) Define Natural Language Processing. Explain the steps of natural language processing. 1+4
- (b) Describe the concept of learning in Neural Networks. Differentiate between pragmatic and discourse integration. 3+2
4. What are constrain satisfaction problem? Solve the following crypto-arithmetic Problem where different letters denote different integer and identical letter denote same integer. 2+8

**SEVEN+EIGHT= TWELVE**

**Contd.**

(2)

5(a) What is machine learning? Compare the analogy based and explanation based learning. 2+2

(b) Define Perceptron. Describe the concept Network Architecture in Multilayer feed forward N/Ws. 2+4

6. Write short notes on any THREE:  $3 \times 4 = 12$

- (i) Genetic Algorithm
- (ii) Boltzmann Machine
- (iii) Bayesian networks
- (iv) Expert system

7(a) What do you mean by Heuristic search. Explain in short any heuristic search. 2+2

(b) Define inference rule. Differentiate between forward and backward chaining in Production rules system. 2+4

8. Convert the following premises into FOPL: 8

- (i) There is an X and Y that is sister of Spot and they are not the same individual.
- (ii) Every pair of objects with property p is equal.
- (iii) There is a king and for all kings that are similar.
- (iv) Parents of horse are horse.
- (v) Everyone does nothing.
- (vi) Brothers are siblings.
- (vii) Anyone who is not sloppy is smart.
- (viii) Not everyone is both smart and boring.



**PURBANCHAL UNIVERSITY**

**2014**

B.E. (Computer) / Seventh Semester / Final  
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

1. Solve the following cryptarithmetic puzzle where different letters denote different integers. Also show all the steps how you advance through constraint satisfaction and state all the assumptions that you make. 10

$$\begin{array}{r} \text{ONE} \\ + \text{TWO} \\ \hline \text{FOUR} \end{array}$$

*(Handwritten notes: X^2, C1=10, X^2 = 10, C1 = 1, Y = 0)*

2. What is an intelligent agent? Explain the types of agent programs with suitable examples. 10

- 3(a) Differentiate between propositional logic and predicate logic. 4

- (b) Convert the following sentences into FOPL: 3×2=6

(i) All framers either like monsoon or they don't cultivate.

(ii) Rotten apples do not taste good.

(iii) Nobody likes corruption.

- 4(a) What is a neural net? Explain its basic structure. 5

- (b) Relate Boltzmann machines with Hopfield networks. 5

- 5(a) What is an expert system? Discuss its applications. 5

- (b) What are the categories of knowledge? Explain. 5

- 6(a) What are production rules? Explain the types of production rules with examples. 6

(2)

- (b) How does semantic network represent knowledge? Explain with suitable example.
8. What do you mean by Case-based Reasoning? Explain forward and backward chaining with example.
9. Write short notes on any TWO:
- (a) Genetic Algorithm
  - (b) Propositional Logic
  - (c) Reasoning
  - (d) Frame System

# PURBANCHAL UNIVERSITY

2011

B.B. (Computer) / Seventh Semester / Choice  
Time: 03.00 hrs.

Full Marks: 80 / Pass Marks: 32

BEQ471CO: Artificial Intelligence

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

- 1(a) Discuss various definitions of artificial intelligence (AI). Explain why AI programs try to model human performance. 5
- (b) In the context of user identification system, based on voice, what would be the consideration of an AI systems in terms of Agent, Environment, Actuators and Sensor? 5
- 2(a) What is the best first search technique? Explain the various operating steps of the  $\Lambda^*$  ( $\Lambda$  star) algorithm by searching a directed graph in which each node represents a point in the problem space. 2+4
- (b) Compare depth first search and breadth first search methods. 4
- 3(a) What is predicate logic? Differentiate it with propositional logic. 1+3
- (b) Explain principal of resolution. Explain the formal steps in Resolution with example. 6
- 4(a) Differentiate between forward and backward chaining with example. 5
- (b) Discuss with suitable example how problem is solved using goal stack planning. 5
- 5(a) What is Rote Learning? 2
- (b) Discuss genetic algorithm with example. 8
- 6(a) Draw a schematic diagram showing the various functional elements of an expert system. Explain the function of each of them. 6

Contd...

(b) Give an example of expert system and give basic characteristics (2)

7. Discuss major advantage of artificial neural networks, and give basic characteristics

briefly back propagation training algorithm. Describe possible application of neural networks. 4

8(a) What do you mean by natural language processing? Discuss in detail the components involved in the natural language understanding process. 5

(b) Briefly explain the edge detection methods 5

9. Write short notes on any TWO: 5+5

- (a) Bayesian Network
- (b) Inductive bias learning
- (c) Frames

**PURBANCIAL UNIVERSITY**

**2011**

Bachelor in Information Technology (B.I.T.)/Seventh Semester/Choice  
Full Marks: 30 /Pass Marks: 32

Time: 03:00 hrs.

BIT415CS: Artificial Intelligence  
Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

**Group A:**

$$2 \times 12 = 24$$

**Answer TWO questions.** Where different letters denote same

1. Solve the following crypto-arithmetic problem, where different letters denote different integers and identical letters denote same

integer: SEND + MORE = MONEY  
Show all steps how you advance through constraint satisfaction.

$$2+10$$

2. Define problem solving agent. Explain with suitable examples,

Show all steps how you advance through constraint satisfaction.

$$5$$

3(a) Explain the architecture of an expert system.  
3(b) Differentiate between artificial intelligence and natural

intelligence.

**Group B:**

$$7 \times 8 = 56$$

**Answer SEVEN questions.** Explain learning by analogy and and.

4. What is Winston's learning? Explain learning by analogy and explanation based learning.

5(a) State the inference theorems with examples.

$$3$$

(b) Write the importance of game playing in AI.

$$3+5$$

6. What is heuristic search? Explain any one of the heuristic search with example.

7. Define Means End Analysis (MEA). Explain how a household robot problem is solved using MEA.

(2)

8. Convert the following sentences into FOPL. 2x4

- (a) Saroj likes to read all kinds of courses.
- (b) If you are idle, you will feel lonely.
- (c) Every child loves his mother.

(d) Sun rises in the east and sets down in the west.

9. What is a neural network? Explain its components. 2+6

10. Explain the importance of genetic algorithm in AI with a suitable demonstration.

11(a) What is "natural language processing"? What are its various steps? 4

11(b) What is "natural language processing"? What are its various steps? 4

11(c) Construct a parse tree for the given sentence:  
"I have enough money to buy a laptop".

$2 \times 4 = 8$

12. Write short notes on any TWO:

- (a) Back propagation
- (b) Machine vision
- (c) Semantic nets and frames

$2 \times 4 = 8$

## **BURBANGLA UNIVERSITY**

2019

— Page No. 10 — / Seventh Semester / Final

B.E. (Computer)

**Full Marks: 80 / Pass Marks: 32**

Time 03.00 hrs Page No. \_\_\_\_\_  
EBC472CO: Software Engineering (New Course)

**SEG472CO: Software Engineering**  
Candidates are required to give their answers in their own words as far as practicable.

*Figures in the margin indicate full marks.*

$$8 \times 10 = 80$$

**Answer EIGHT questions.**



**PURBANCHAL UNIVERSITY**  
**2018**

B.E. (Computer) / Seventh Semester / Final  
Full Marks: 80 / Pass Marks: 32  
Time: 03.00 hrs.

**BEG472CO: Software Engineering (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

$$8 \times 10 = 80$$

**Answer EIGHT questions.**

- 1(a) What is Software and software Engineering? Differentiate between Software Engineering and System Engineering. 2+3
- (b) "Software does not wear out but it does deteriorate" Explain the Statement. 5
2. What are the Characteristics of good Software? Explain phototyping and RAD model for Software Development Process 3+7
- 3(a) Explain 4P's in Software Project Management. Explain the RISK management system in software development. 2+3
- (b) Is UML a programming language? Justify. 5
- 4(a) Explain the principles of Risk Management. 4
- (b) Define Software Configuration management with its components. 6
- 5(a) Differentiate Between Functional and non-Functional Requirement in Software Engineering. 5
- (b) Write down the Use Case Diagram of ATM System. 5
6. Define coupling with its importance in software component. Explain different types of coupling in detail. 4+6
7. Define the term "Quality" in context of Software Engineering. Describe the set of activities carried out in Software Quality Assurance. Give a very brief idea about verifying software quality as one of the best practices in Software Development Industries. 2+4+4

(2)

- 8(a) Explain principle of testing and verification in software. 5
- (b) Explain Black Box Testing and White Box Testing methodologies. 5
9. What is modular decomposition in Software? Explain Top Down  
and Bottom Up software design principle with an example. 3+7



**PURBANCHAL UNIVERSITY  
2017**

B.F. (Computer) Seventh Semester / Final

Time 03.00 hrs.

Full Marks. 80 / Pass Marks 40

**BEG472CO: Software Engineering (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

Answer EIGHT questions.

$8 \times 10 = 80$

1. How the project staffing pattern affects project management Activities? Explain the software project planning in detail. 3+7
2. Discuss the various aspects of conducting feasibility studies. Explain functional and non functional requirements with suitable examples? 4+6
3. Why Waterfall model of software process can not reflect all the software development activities? Explain different phases of Spiral model with suitable diagram. 3+7
4. Define Software Engineering? What are the main causes of software failure? Suggest your important vision to minimize the failure rate of the software? 3+7
5. Why the software reliability being difficult to measure? Explain the outline structure of Software Quality Assurance (SQA) plan. 5+5
6. Define COCOMO. A project size of 83200 lines of code is to be developed and the team has average experience. Calculate the effort, development time, average staff size and productivity of the project. 3+7
7. Why software Architecture is important? Explain in brief about the interface design, architectural design and detail design process. 2.8
8. What are the benefits of ISO-9000 certification? Explain SEI CMM Model in brief. 5+5

(2)

9. Define path coverage and statement coverage. Prepare any graph (G) of your choice and explain how many ways the cyclomatic complexity of G can be computed. 4+6
10. Write short notes on any TWO: 5+5
- (a) Black hole and Miracle in DFD
  - (b) UML
  - (c) SCM

\*\*\*

**PURBANCHAL UNIVERSITY**

**2017**

B.E. (Computer) / Seventh Semester / Final  
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**SEG472CO: Software Engineering (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

$$8 \times 10 = 80$$

**Answer EIGHT questions.**

1. What is software products and explain about its types. Why software engineering is important? 5+5
2. Compare between Waterfall model and Spiral model of software development process. 10
3. Explain about COCOMO. Explain how it is used to estimate the development time and effort. 4+6
4. Explain the importance of Requirement Engineering? What are the steps of requirement engineering? 4+6
5. What is meant by Coupling in the context of software design? Explain the software design principle. 5+5
6. Explain how black box approach of software testing differs from white box approach. Explain the term cyclomatic complexity with example. 5+5
7. Explain Software Requirement specification. What are the good characteristics of a good software requirement specification document? 4+6
8. What do you mean by project scheduling? Differentiate between GANTT chart and PERT chart. 4+6
9. Explain your views regarding Extreme Programming, Cloud Computing and Grid Computing. 10
10. Write short notes on any TWO:  
(a) Software Quality Assurance      (b) Boundary Value Analysis  
(c) Version and Release Management 5+5



**PURBANCHAL UNIVERSITY**  
**2016**

B.E (Computer) / Seventh Semester / Final

Time 03:00 hrs

Full Marks: 80 / Pass Marks: 32

**BEG472CO: Software Engineering (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*Figure in the margin indicate full marks.*

**Answer EIGHT questions.**

**$8 \times 10 = 80$**

1(a) Giving reasons for your answer based on the type of system being developed, suggest the most appropriate generic software process model which might be used as a basis for managing the development of the following systems: 5

- (i) A university accounting system that replaces an existing system.  
(ii) A new software product that would connect computers through satellite communication. Assume that your team has no previous experience in developing satellite communication software.

(b) Define software engineering. Explain software engineering as a Layered Technology. 2+3

2(a) Define software architecture. List different types of it and explain them. 1+1+3

(b) What qualities should be considered while designing software? Briefly discuss the design principles. 2+3

3. How can you differentiate between Black-box and White-box testing strategies? Explain Boundary Value Analysis technique with an example. 5+5

4. What is Requirement Engineering? Explain. 10

5. What do you mean by project planning and project scheduling? Explain the different activities which are performed during project planning. 3+7

6. Discuss the objectives of modular software design. What are the effects of module coupling and cohesion? 5+5

**(2)**

7. Using a suitable example, describe how data flow diagrams (DFD) may be used to document a system design? 10
8. Define software quality assurance. Explain the ISO 9000 quality standard. 4+6
9. What is cyclomatic complexity? Explain with the help of an example. 3+7
10. Write short note on any TWO:
  - (a) Verification vs. validation
  - (b) Software Configuration Management
  - (c) Cloud Computing5+5



**PURBANCHAL UNIVERSITY**

**2016**

B.E. (Computer)/Seventh Semester/Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG472CO: Software Engineering (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*Figure in the margin indicate full marks.*

**Answer EIGHT questions.**

- 1(a) Giving reasons for your answer based on the type of system being developed, suggest the most appropriate generic software process model which might be used as a basis for managing the development of the following systems:  $8 \times 10 = 80$
- (i) A university accounting system that replaces an existing system. 5
- (ii) A new software product that would connect computers through satellite communication. Assume that your team has no previous experience in developing satellite communication software. 5
- (b) Define software engineering. Explain software engineering as a Layered Technology. 2+3
- 2(a) Define software architecture. List different types of it and explain them. 2+3
- (b) What qualities should be considered while designing software? Briefly discuss the design principles. 1+1+3
3. How can you differentiate between Black-box and White-box testing strategies? Explain Boundary Value Analysis technique with an example. 5+5
4. What is Requirement Engineering? Explain. 10
5. What do you mean by project planning and project scheduling? Explain the different activities which are performed during project planning. 3+7
6. Discuss the objectives of modular software design. What are the effects of module coupling and cohesion? 5+5

(2)

- Using a suitable example, describe how data flow diagrams (DFD) may be used to document a system design? 10
- Define software quality assurance. Explain the ISO 9000 quality standard. 4+6
- What is cyclomatic complexity? Explain with the help of an example. 3+7
- Write short note on any TWO: 5+5
- (a) Verification vs. validation
  - (b) Software Configuration Management
  - (c) Cloud Computing



**PURBANCHAL UNIVERSITY  
2015**

B.E. (Computer)/Seventh Semester/Back  
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG472CO: Software Engineering (Old Course)**

Candidates are required to give their answers in their own words as far as practicable.  
Figure in the margin indicate full marks.

**Group A**

**Answer EIGHT questions.**

- 1(a) Explain the activities and Objectives of feasibility study and preliminary investigation on system analysis and design.  $8 \times 10 = 80$
- (b) Discuss in detail waterfall and Boehm's spiral model. 5
- 2(a) Discuss briefly on the system procurement process. 5
- (b) Differentiate between an object and an object class. 5
3. What is system analysis and design? Discuss the objectives of architectural design. 10
4. Why do we need software testing? Justify it. Explain overall software testing mechanism. 10
- 5(a) What factors should be considered for making software with good quality? 5
- (b) What do you understand by availability and software reliability? 5
- 6(a) What are possible software failure and fault? Explain briefly prevention mechanism. 5
- (b) What do you mean by integration testing? 5
7. Draw a context diagram and a Level-0 Data Flow Diagram for the advance booking system of Company and state any assumptions made. 10

Contd. ...

**(2)**

- 8(a) What do you mean by process of modular decomposition? 5
- (b) Explain cohesion & coupling with example. 5
- 9(a) What is software Engineering? Discuss professional responsibilities. 5
- (b) Explain various software design strategies. 5
10. Write short notes on any TWO: 5+5
- (a) Software Maintenance
  - (b) Documentation
  - (c) Regression testing

**PURBANCHAL UNIVERSITY  
2015**

B.E. (Computer)/Seventh Semester/Back

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**SEG472CO: Software Engineering (Old Course)**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

**Group A**

**Answer EIGHT questions.**

$$8 \times 10 = 80$$

- 1.(a) Explain the activities and Objectives of feasibility study and preliminary investigation on system analysis and design. 5
- (b) Discuss in detail waterfall and Boehm's spiral model. 5
- 2.(a) Discuss briefly on the system procurement process. 5
- (b) Differentiate between an object and an object class. 5
3. What is system analysis and design? Discuss the objectives of architectural design. 10
4. Why do we need software testing? Justify it. Explain overall software testing mechanism. 10
- 5.(a) What factors should be considered for making software with good quality? 5
- (b) What do you understand by availability and software reliability? 5
- 6.(a) What are possible software failure and fault? Explain briefly prevention mechanism. 5
- (b) What do you mean by integration testing? 5
7. Draw a context diagram and a Level-0 Data Flow Diagram for the advance booking system of Company and state any assumptions made. 10

**Contd. ...**

**(2)**

- 8(a) What do you mean by process of modular decomposition? 5
- (b) Explain cohesion & coupling with example. 5
- 9(a) What is software Engineering? Discuss professional responsibilities. 5
- (b) Explain various software design strategies. 5
10. Write short notes on any TWO: 5+5
- (a) Software Maintenance
  - (b) Documentation
  - (c) Regression testing

**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer)/Seventh Semester/Chance  
Time: 03.00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG472CO: Software Engineering (Old Course)**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

**Answer EIGHT questions.**

$$8 \times 10 = 80$$

- 1(a) What are the attributes of Software? "Software doesn't wear out but it does deteriorate". Explain the Statement. 2+4
- (b) Differentiate between Software Engineering and System Engineering. 4

2. Differentiate between Spiral Model and Prototype Model? Explain. 10
3. Explain the software configuration management with major components. 10

- 4(a) What are the difference between Software quality and reliability? 5
- (b) Can a program be correct and still not exhibit good quality? Explain. 5

5. Explain Black box Testing and White Box Testing methodologies. What do you understand by regression testing? Explain. 6+4
6. Explain the USE CASE with its components. Draw the USE CASE diagram of ATM machines. Also draw its sequence diagram. 4+3+3

- 7(a) Differentiate between Functional and Non-Functional Requirement. 5
- (b) Explain types of software risk in short and also discuss the risk mitigation, monitoring and management. 5

**(2)**

8. Explain the Main Essence of Object Oriented Software Engineering. How does Structured Analysis differ from Object Oriented Analysis?

5+5

9. Write short notes on any TWO:

$2 \times 5 = 10$

(a) COCOMO Model

(b) Software Crisis

(c) Validation and Verification



## **PURBANCHAL UNIVERSITY**

2018

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

**Full Marks: 80 / Pass Marks: 32**

BEG472CO: Software Engineering (New Course)

*Candidates are required to give their answers in their own words as far as practicable.*

*Figure in the margin indicate full marks.*

## **Group A**

**Answer TWO questions.**

$$2 \times 12 = 24$$

1. Compare Spiral Model and Prototype Model with their important feature.
  2. What is Software Project Management? What are the different project estimation techniques? What is risk management?
  3. What is Software testing? Differentiate between Black-box & white box testing strategies. Explain Boundary Value Analysis technique with suitable example.

### **Group B**

**Answer SEVEN questions.**

$$7 \times 8 = 56$$



**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer)/Seventh Semester /Chance  
Time: 03:00 hrs.

Full Marks: 80 /Pass Marks: 32

**BEG472CO: Software Engineering (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

**Answer TEN questions.**

- 1.(a) What is Software Engineering? Explain the Advantages of Software Engineering. 2+2  
(b) "Software is developed or engineered, it is not manufactured in the classical sense", explain the Statement. 4  
2. What are the attributes of good Software? Explain the "Waterfall model" for Software development Process. 2+6

**Or**

If you are selected as a System Administrator of an Airline System, what kind of team structure, Software model would you suggest. And why Explain. 8

3. Describe different Relationship used in UML with their notations. Design a Data flow diagram of "Banking Information System". 3+5

**Or**

Explain that UML is a language for visualizing, Specifying, Constructing and documenting. What are building blocks of UML? 4+4

4. Define Software Configuration management. What are the major components of SCM Explain? 3+5  
5. Define the term "Quality" in-context of Software Engineering. Describe the set of activities carried out in Software Quality Assurance. Give a very brief idea about verifying software quality as one of the best practices in Software development Industries. 8

(2)

6. What is software testing? Explain Black box Testing and White Box Testing methodologies. 2+6
7. What is modular decomposition in Software? Explain Top Down and Bottom Up software design principle with an example. 2+6
- 8(a) Explain Functional and Non-Functional Requirement of Software. 4
- (b) Explain types of software risk in short and also discuss the risk mitigation, monitoring and management. 4
9. What is meant by Coupling in the context of Software design? Is it true that in a good design, the modules should have low Coupling? Why? 4
- 10(a) Describe how Object oriented design differs from function oriented design? 4+4
- (b) Differentiate between Validation and Verification. 4
11. Write short notes on:  
(a) Quality Vs Reliability  
(b) Software failure and Software crisis  
(c) ISO 9000 Certification for Software 4+4
- ~

**PURBANCHAL UNIVERSITY**

**2014**

B.E. (Computer) / Seventh Semester / Final  
Time: 03.00 hrs.

Full Marks: 80 / Pass Marks: 32

**SEG472CO: Software Engineering**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

**Group A**

**Answer TWO questions.**

**$2 \times 12 = 24$**

1. What is software engineering? What are the various skills that a software engineer should posses? Explain.
2. What is the significance of prototyping in software development? Explain how prototyping can help in requirement specification. What are the demerits of prototyping?
3. Explain Boehm's spiral model in detail and also discuss process variability.

**Group B**

**Answer SEVEN questions.**

**$7 \times 8 = 56$**

4. Explain requirement engineering process.
5. What is modular decomposition? Explain its significance in software design.
6. Explain COCOMO model. Differentiate between Empirical estimation technique and analytical estimation technique.
7. What is project scheduling? Explain GANTT chart and PERT chart used in project scheduling.
8. What are system development methodologies? Explain structured analysis and object-oriented analysis.  
What is a software fault? Explain fault tolerance technique.

**Contd. ...**

(2)

10. Differentiate between functional and non-functional requirement of a software. Explain few software quality measures.
11. Explain various steps of program development. What is program debugging?
12. Write short notes on any TWO:
  - (a) Object oriented design
  - (b) Verification and validation
  - (c) Black box and White box testing



# PURBANCHAL UNIVERSITY

2013

B.E. (Computer) / Seventh Semester / Choice

Time: 03.00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG472CO: Software Engineering**

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

## Group A

**Answer TWO questions.**

$2 \times 12 = 24$

1. What are software products? Explain Boehm's Spiral model of software development in detail.
2. What do you mean by software design? What are the various design principles? Explain modularity in context of software design.
3. What do you mean by software project management? Explain various activities that are carried out during project planning.

## Group B

**Answer SEVEN questions.**

$7 \times 8 = 56$

4. What are object oriented designs? Explain object classes and inheritance.
5. What do you mean by system engineering? What are the things to be engineered while developing a computer based information system?
6. What is Preliminary Investigation? Explain various activities involved in this process.
7. Explain program coding debugging and testing. Why program documentation is important?
8. What is Software Quality assurance? Explain few software quality attributes.

**Contd. ...**

(2)

9. What is software reliability? Explain how reliability can be assessed during quality assurance.
10. Differentiate between verification and validation. Explain few testing strategies.
11. Explain object oriented analysis technique.
12. Write short notes on any TWO:
  - (a) Software faults
  - (b) Domain Specific architecture
  - (c) SDLC



# PURBANCHAL UNIVERSITY

2019

B.E. (Computer) / Seventh Semester / Final

Time: 03.00 hrs

Full Marks: 80 / Pass Marks: 32

REG4900MS: Entrepreneurship (New Course)

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

Answer EIGHT questions.

$8 \times 10 = 80$

1. Who is an entrepreneur? Explain the potential drawbacks and the cultural diversity of Entrepreneurship. 10
2. Differentiate between innovation and creativity. What are the factors that causes mental blocks? 10
3. What are the steps that are involved in making strategic management process? Explain. 10
4. How can a powerful marketing plan be built? Explain. 10
5. Explain different pricing strategies and methods applied for service firms. 10
6. What are the different forms of business ownership? Explain any two of them. 10
7. How can Ratio analysis Tool be effectively used to judge the financial position of a firm? 10
8. Describe the effective pricing techniques for introducing new products or services in the market. 10
9. Write short notes on any TWO:  
(a) Elements of business plan  
(b) Layout and its importance  
(c) Intellectual property  $2 \times 5 = 10$



# PURBANCHAL UNIVERSITY

2018

B.E. (Computer)/Seventh Semester/Final

Time: 03.00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG490MS: Entrepreneurship (New Course)**

*Candidates are required to give their answers in their own words as far as practicable*

*The figures in the margin indicate full marks.*

**$8 \times 10 = 80$**

**Answer EIGHT questions.**

1. Explain the foundation of entrepreneurship in brief using your own logical reasoning.
2. What do you mean by Creativity and Innovation? Suppose you have innovated one IT solution that can be used for welfare of the society. Among Patent, Trademarks and Copyrights, which one would you register under the intellectual property right for preserving your innovative idea.
3. You are going to establish an IT company with your friends after your graduation. What may be (SWOT) strengths, weakness, opportunities and threats that your team will be facing? Describe in brief.
4. What are the elements of Business Plan? Explain five force model of industry and market feasibility.
5. How do you ensure your marketing plan using world wide web?
6. What are the pricing factors? Explain the pricing strategies and tactics for introducing a new product in the market.
7. Explain 'Big Three' of cash management. How do you avoid cash crunch in the business organization.
8. Explain different sources of equity financing.

**Contd. ...**

(2)

9. What are the sources of information for choosing the right location and layout? Explain the factors to be considered in manufacturing layout.
10. Write short notes on any TWO:
- (a) Partnership business
  - (b) The impact of credit on pricing
  - (c) Strategic management process

PURBANCHAL UNIVERSITY

2017

B.E. (Computer) Seventh Semester /Final

Time: 03:00 hrs

Full Marks: 80 /Pass Marks: 32

**BEG490MS: Entrepreneurship (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

**Answer EIGHT questions.**

$8 \times 10 = 80$

- 1(a) Describe ten deadly mistakes of entrepreneurship. 5
- 1(b) Differentiate between creativity and Innovation. Identify various barriers to creativity. 5
- 2(a) Describe the elements of Business Plan and its importance. What are the reasons that a badly Business Plan fail? 5
- 2(b) What do lenders and investors look for in a Business Plan? 5
- 3(a) Explain a Guerilla marketing plan and its objective. Discuss the role of market research in building a guerilla marketing plan. 5
- 3(b) Discuss the 4P'S of marketing and their role in building a successful marketing strategy. 5
- 4(a) Describe the effective pricing techniques for introducing new products for services and existing ones. 5
- 4(b) Explain the pricing strategies for retailers, manufacturers and service organizations. 5
- 5(a) Explain the technique for avoiding a cash crunch in a small company. 5
- 5(b) Differentiate between cash and profit. 5
- 6(a) Describe factors in deciding a location, importance of location, explain layout and discuss any four types of manufacturing layouts. 5
- (b) Describe the fundamental principles involved in managing the "Big three" of cash management. 5

Contd. ...

(2)

- 7(a) Explain the term 'Capital'. Describe equity capital and debt capital and discuss various sources of equity capital. 5
- ✓ (b) Describe Intellectual Property right. Explain Patent, Copyright and Trademark in detail. 5
8. Why does a successful entrepreneur need to analyze financial plan? Explain the example. 10
- 9/ Write short notes on any TWO: 5+5
- (a) Maximizing revenues
  - (b) Equity Financing
  - (c) Liquidity position
- \*\*\*

**PURBANCHAL UNIVERSITY**

**2017**

B.E. (Computer)/Seventh Semester/Final

Time: 03:00 hrs.

Full Marks: 80 /Pass Marks: 32

**BEG490MS: Entrepreneurship (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

**Answer EIGHT questions.**

**$8 \times 10 = 80$**

- 1(a) Define an entrepreneur and explain the benefits of entrepreneurship. 5
- (b) How do you explain the cultural diversity of entrepreneurship? 5
- 2(a) Define creative thinking and explain different ways of enhancing creativity. 5
- (b) Explain different aspects of Intellectual Property. ↗ trade mark  
copy right  
design 5
- 3(a) How can a competitive business model be built? Explain. 5
- (b) Explain any three forms of business ownership. 5
- 4(a) Explain the concept of Marketing Mix in brief. 5
- (b) Explain the impact of credit on pricing. 5
- 5(a) What is Break-Even Analysis? Why is it important for any entrepreneur to consider this analysis seriously? 5
- (b) What is cash budget? Why is it important to prepare a cash budget for any organization? 5
- 6(a) Differentiate between Equity Financing and Debt financing. 5
- (b) Why is layout necessary for an entrepreneur? 5
- 7(a) Describe the sources of equity financing. 5
- (b) Explain in brief the strategic management process. 5
- 8(a) Prepare a business plan of your own area of interest. 10
9. Write short notes on any TWO: 5+5
- (a) Ratio Analysis
- (b) Mistakes of Entrepreneurship
- (c) Financial plan



# PURBANCHAL UNIVERSITY

**2016**

B.B. (Computer) / Seventh Semester / Final

Time: 03.00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG490MS: Entrepreneurship (New Course)

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

Answer EIGHT questions.

$8 \times 10 = 80$

- ✓ Describe the ten deadly mistakes of entrepreneurship and discuss how these mistakes can be avoided?
- ✓ Define creativity and its process. Explain how to enhance the creativity.
- ✓ Why should an entrepreneur develop the business plan? What are the elements of business plan?
- ✓ Explain the advantages and disadvantages of the sole proprietorship and the corporation.
- ✓ Explain Guerrilla marketing plan and pin point the target market.
- ✓ Explain the pricing approach and methods for business organization.
- ✓ Describe the fundamental principles involved in managing the "big three" of cash management.
- ✓ What do you mean by location and layouts? Why is layout necessary for an entrepreneur?
- From the following data forecasts, prepare cash budget for the months of April, May and June 2010:

| Months   | Credit Sales (Rs.) | Credit Purchases (Rs.) | Wages (Rs.) | Office Expenses (Rs.) |
|----------|--------------------|------------------------|-------------|-----------------------|
| February | 60000              | 35000                  | 9000        | 6000                  |
| March    | 6000               | 35000                  | 8000        | 7500                  |
| April    | 70000              | 35000                  | 10000       | 7000                  |
| May      | 68000              | 35000                  | 7500        | 5300                  |
| June     | 56000              | 38000                  | 8500        | 5600                  |

Contd. ....

(2)

Other information:

- (a) Cash Balance on 1<sup>st</sup> April 2010 Rs. 10000.
- (b) Advance tax of Rs. 7500 is payable in February.
- (c) Period of credit allowed to customers is one month and suppliers two months.
- (d) Lay in payments office expenses and wages is one month.

From the following data calculate:

- (a) Gross Profit Ratio
- (b) Net Profit Ratio
- (c) Current Ratio
- (d) Inventory Turnover Ratio
- (e) Liquid Ratio

|                     |             |
|---------------------|-------------|
| Average Inventory   | Rs. 400000  |
| Cost of goods sold  | Rs. 96000   |
| Current Liabilities | Rs. 300000  |
| Fixed Assets        | Rs. 720000  |
| Liquid Assets       | Rs. 380000  |
| Lay term debts      | Rs. 450000  |
| Net Profit          | Rs. 180000  |
| Sales               | Rs. 1260000 |

# PURBANCHAL UNIVERSITY

2015

B.B. (Computer) / Seventh Semester / Final

Full Marks: 80 / Pass Marks: 32

Time: 03.00 hrs.

BEG4900MS: Entrepreneurship (New Course)

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

## Group A

2x12=24

Answer TWO questions.

1. What is an Entrepreneur? Describe in detail characteristics exhibited by entrepreneurs.

2. What is layout? Describe in detail the various types of manufacturing layouts.

3. Estimate the cash requirements of BIRAT FRUIT Co. Ltd for June 2005 on the basis of data given below:

(a) Sales:

February 2005 25000 Rs

March 2005 20000 Rs.

April to June 2005 30000 Rs per month

Roughly half the sales are for cash. 90% of credit sales are collected in the month following the month of sales and the balance one month later.

(b) Fruits are always bought for cash to avail of the cash discount of 5%. The purchase budget for the second quarter (April-June) was Rs 15000 baskets per month at Re 1 per basket.

(c) Wages and salaries for second quarter were budgeted at Rs 500 per month.

(d) Manufacturing and other expenses budget for the quarter:

Cash expenses = Rs. 4500

Depreciation = Rs. 7500

Selling Expenses = Rs. 3000

Administrative Expenses = Rs 2000 (in April and May only)

\* Prepare a cash budget for second quarter of 2005.

Contd. ....

(2)

Group B

Answer SEVEN questions.

$7 \times 8 = 56$

4. What do you mean by (SWOT) strengths, weakness, opportunities and threats facing a business? Discuss.

5. Explain Guerilla marketing plan, its objective and discuss the role of market research in building a Guerilla marketing plan and describes the steps in market research process.

6. Explain the technique for avoiding a cash crunch in a small company.

7. Describe the differences between Equity capital and Debt capital and explain the various sources of equity capital available to entrepreneurs.

8. Explain the pricing methods and strategies for retailers, manufacturers or service firms.

X 9. Describe Ratio Analysis, using formula how you will calculate Current Ratio, Acid Test Ratio/Quick Ratio, Average collection period, Inventory Turnover.

|                    | Year I |             | Year II |             |
|--------------------|--------|-------------|---------|-------------|
|                    | Assets | Liabilities | Assets  | Liabilities |
| Stock              | 10000  |             | 20000   |             |
| Debtors            | 30000  |             | 30000   |             |
| Payment in Advance | 2000   |             | -       |             |
| Cash in hand       | 20000  |             | 15000   |             |
| Sundry Creditors   |        | 25000       |         | 30000       |
| Acceptances        |        | 15000       |         | 12000       |
| Bank over drafts   |        |             |         | 5000        |
|                    | 62000  | 40000       | 65000   | 47000       |

Sales amounted to Rs 350000 in the first year and Rs 30000 in the second year.

10. Describe the effective pricing techniques for introducing new products or services and for existing ones.

11. Describe the fundamental principles involved in managing the 'Big Tree' of Cash management.

12. Write short notes on any TWO.

(a) Intellectual property

(c) Financial Statement

(b) Business Plan Format

(d) Various Form of Ownership

**PURBANCHAL UNIVERSITY**  
**2015**

B.E. (Computer) / Seventh Semester / Choice

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG490MS: Entrepreneurship (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

The figures in the margin indicate full marks.

$$8 \times 10 = 80$$

**Answer EIGHT questions.**

1. Who is an entrepreneur? Briefly describe the ten deadly mistake of the entrepreneurship.
2. How would you describe the relationship of creativity, innovation and entrepreneurship? Is there any way to enhance creativity?
3. Why an entrepreneur requires business plan? Mention the elements of the successful business plan.
4. Which form of business ownership is good for entrepreneurs? Mention the advantages of the limited liability companies.
5. What do understand by Guerilla marketing plan? How competitive edge could be built with the help of Guerilla marketing plan?
6. How do you incorporate value in pricing? Briefly describe the methods of pricing for retailers.
7. What do you understand the 'Big three' of cash management. Briefly explain the ways to avoid cash crunch.
8. List down the important business ratios and give the brief interpretations of them.
9. What are the different sources of financing? Under what conditions entrepreneur prefer equity over debt.
10. Write short notes on any TWO:
  - (a) Marketing on World Wide Web
  - (b) Intellectual Property
  - (c) Layout: Increasing Efficiency

# **E-commerce**

## **BCA VI Semester**

### **Introduction to Ecommerce**

- Electronic Commerce is the process of buying, selling, or exchanging products, services, and information via computer networks.
- Electronic commerce (eCommerce) is a modern business methodology that addresses the needs of organizations, merchants, and consumers to cut costs while improving the quality of goods and services and increasing the speed of service delivery.

#### **Definitions from different perspectives:**

- From a communication perspective, electronic commerce is the delivery of information, products/services, or payments via telephone lines, computer networks, or any other means.
- From a business process perspective, electronic commerce is the application of technology towards the automation of business transactions and workflows.
- From a service perspective, electronic commerce is a tool that addresses the desire of firms, consumers, and management to cut service costs while improving the quality of goods and increasing the speed of service delivery.
- From an online perspective, eCommerce provides the capability of buying and selling products and information on the Internet and other online services.

#### **Characteristic of Ecommerce**

- **It Is About the Exchange of Digitized Information Between Parties.** This information exchange can represent communications between two parties, coordination of the flows of goods and services, or transmission of electronic orders. These exchanges can be between organizations or individuals.
- **It Is Technology-Enabled.** E-commerce is about technology-enabled transactions. The use of Internet browsers in the World Wide Web is perhaps the best known of these technology-enabled customer interfaces. However, other interfaces—including ATMs, electronic data interchange (EDI) between business-to-business, partners, and electronic banking by phone—also fall in the general category of e-commerce. Businesses once managed transactions with customers and markets strictly through human interaction; in e-commerce, such transactions can be managed using technology.
- **It Is Technology-Mediated.** Furthermore, the focus is moving away from the simply technology-enabled transaction to a technology-mediated relationship. Purchases in the marketplace at Wal-Mart are technology-enabled in that we have human contact along with a cash register that does PC-based order processing. What is different now is that the transaction is mediated not so much through human contact but largely by technology—and, in that sense, so is the relationship with the customer. The place where buyers and sellers meet to transact is moving from the physical-world “marketplace” to the virtual-world “market-space.” Hence, the success of the business rests on screens and machines in managing

customers and their expectations. Coming from a past of transactions with human-human contact, that is a big difference.

- **It Includes Intra- and Inter-organizational Activities that Support the Exchange.** The scope of electronic commerce includes *all electronically based* intra- and inter-organizational activities that directly or indirectly support marketplace exchanges. In this sense, we are talking about a phenomenon that affects both how business organizations relate to external parties—customers, suppliers, partners, competitors, and markets—and how they operate internally in managing activities, processes, and systems.

## **The Benefits of ECommerce**

### **◆ Benefits to Organizations**

- ✓ Expands the marketplace to national and international markets
- ✓ Decreases the cost of creating, processing, distributing, storing and retrieving paper-based information
- ✓ Allows reduced inventories and overhead by facilitating pull-type supply chain management
- ✓ The pull-type processing allows for customization of products and services which provides competitive advantage to its implementers
- ✓ Reduces the time between the outlay of capital and the receipt of products and services
- ✓ Supports business processes reengineering (BPR) efforts.
- ✓ Lowers telecommunications cost - the Internet is much cheaper than value added networks (VANs)

### **◆ Benefits to consumers**

- ✓ Enables consumers to shop or do other transactions 24 hours a day, all year round from almost any location
- ✓ Provides consumers with more choices
- ✓ Provides consumers with less expensive products and services by allowing them to shop in many places and conduct quick comparisons
- ✓ Allows quick delivery of products and services (in some cases) especially with digitized products
- ✓ Consumers can receive relevant and detailed information in seconds, rather than in days or weeks
- ✓ Makes it possible to participate in virtual auctions
- ✓ Allows consumers to interact with other consumers in electronic communities and exchange ideas as well as compare experiences
- ✓ Facilitates competition, which results in substantial discounts

### **◆ Benefits to society**

- ✓ Enables more individuals to work at home, and to do less traveling for shopping, resulting in less traffic on the roads, and lower air pollution
- ✓ Allows some merchandise to be sold at lower prices, benefiting less affluent people
- ✓ Enables people in Third World countries and rural areas to enjoy products and services which otherwise are not available to them
- ✓ Facilitates delivery of public services at a reduced cost, increases effectiveness, and/or improves quality

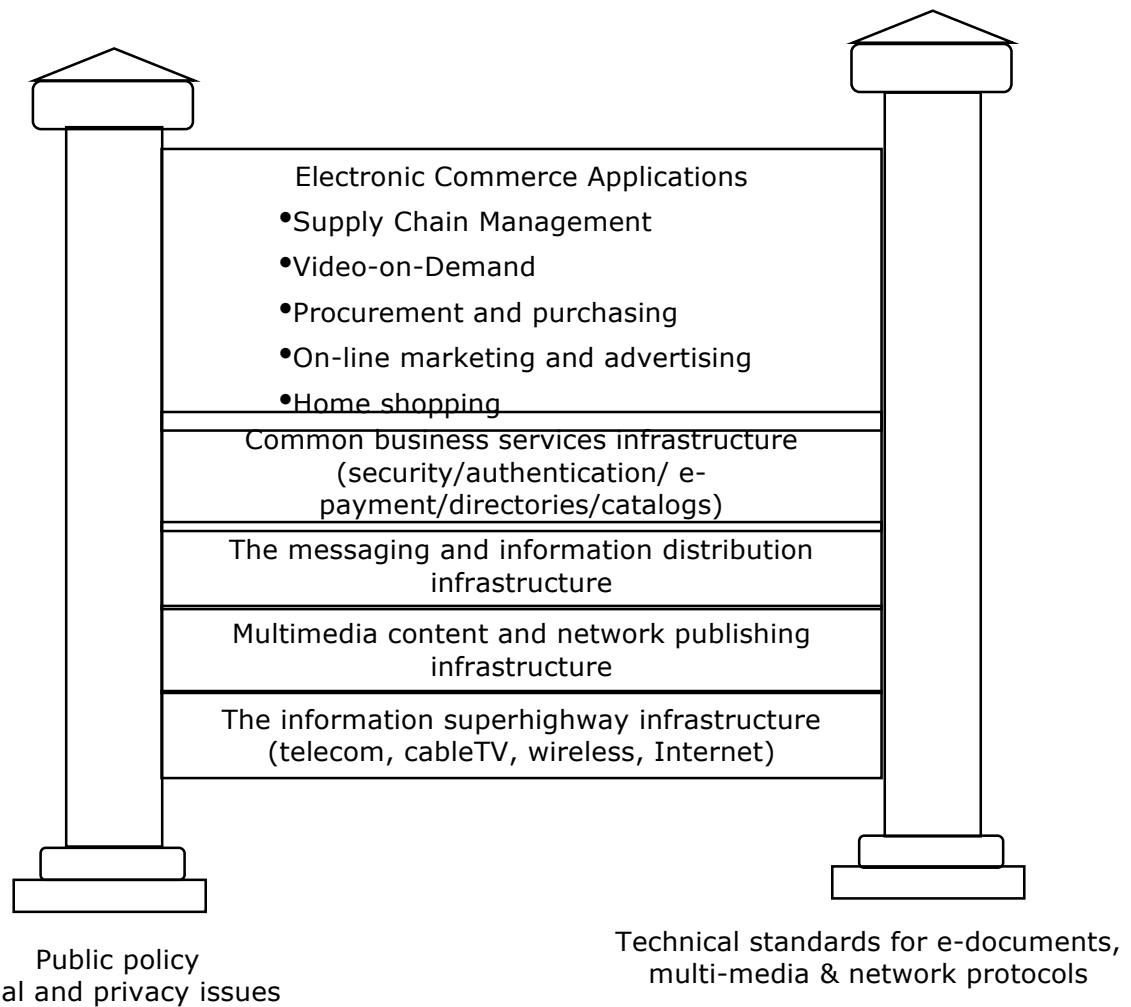
### **Disadvantage of Ecommerce**

Most of the disadvantages of electronic commerce stem from the newness and the rapidly developing pace of the underlying technologies. These disadvantages will disappear as electronic commerce matures and becomes more available to and accepted by the general population. Disadvantages may be:

- Businesses often calculate return on investment numbers before committing to any new technology. Costs, which are a function of technology, can change dramatically during even short-lived electronic commerce implementation projects.
- Many companies have had trouble recruiting and retaining employees with the technological, design, and business process skills needed to create an effective electronic commerce presence. The difficulty of integrating existing databases and transaction-processing software designed for traditional commerce into the software that enables electronic commerce.
- Many businesses face cultural and legal impediments to electronic commerce.
- Some consumers are still fearful of sending their credit card numbers over the Internet.
- Consumers are simply resistant to change and are uncomfortable viewing merchandise on a computer screen rather than in person.

### **E-commerce Framework**

E-Commerce applications will be built on the existing technology infrastructure - a myriad of computers, communication networks, and communication software forming the nascent Information Superhighway. The **technology infrastructure** of the Internet is both an enabler and a driver of change. An infrastructure is defined as "*the foundation of a system.*" In this case, the technological foundation of the Internet, simply put, enables the running of the e-commerce enterprises. The hardware backbone of computers, routers, servers, fiber optics, cables, modems, and other network technologies provides half of the technology equation. The other half includes the soft-ware and communications standards that run on top of the hardware, including the core protocols for the Web. Understanding technology infrastructure—and there-fore understanding what is and is not achievable—is essential to formulating a company's vision and strategy.



The framework for e-Commerce consists of three parts as shown in figure above.

1. The first part consists of a *variety of electronic commerce applications* including both inter- and intra-organizational and electronic market examples such as Supply Chain Management, Video-on-Demand, Procurement and purchasing, On-line marketing and advertising, Home shopping etc.
2. The second part of the building blocks of the infrastructure consists of:
  - **Common business services**, for facilitating the buying and selling process.
  - **Messaging and information distribution**, as a means of sending and retrieving information ( ex-EDI, e-mail, P2P file transfer)
  - **Multi-media content and network publishing**, for creating a product and a means to communicate about it.

- **Information Superhighway infrastructure** consisting of telecommunication, cable operator, ISPs , Wireless technologies and Internet.
3. The third part consists of the *public policy* and *technical standards* necessary to support the applications and the infrastructure.

**Public policies** govern issues like universal access, privacy, and information pricing. The public policy infrastructure affects not only the specific business but also direct and indirect competitors. It should take into consideration of:

- Cost of accessing information
  - Regulation to protect consumers from fraud and protect their right to privacy.
- Policies of global information traffic to detect information pirating and obscene sites.

### **Media Convergence**

- Convergence is the melding of consumer electronics, television, publishing, telecommunications, and computers for the purpose of facilitating new forms of information-based commerce.
- Multimedia convergence is the conversion of text, voice, data, image, graphics, and full-motion video into digital content.
- Cross-media convergence is the integration of various industries – entertainment, publication, and communication media – based on multimedia content.

### **Convergence driven by Technology**

- Convergence of content translates all types of information content – books, business documents, videos, movies, music – into digital information.
- Convergence of transmission compresses and stores digitized information so it can travel through existing phone and cable wiring.
- Convergence of information access devices have the sophistication to function as both computers and televisions.
- Convergence of content such as books, business documents, videos, movies, music into digital format so that information can be processed, searched, sorted, enhanced, converted, compressed, encrypted, replicated, transmitted.
- Convergence of transmission to transmit digitized voice, data, image and video.
- Convergence of information access devices
  - Computers with televisions
  - Telephone with internal fax machine, modem, video monitor.

### **Convergence driven by Market conditions**

- The widespread availability of increasingly low-cost, high-performance enabling component technologies, including semiconductors, storage and display devices, communication systems, and operating systems among others.

- Entrepreneurs who are feeding on anticipated end-user demand for new applications – both products and services – that rely on the aforementioned enabling technologies.
- Aggressive regulatory actions that are introducing competition in monopoly markets.
- Availability of low-cost, high-performance enabling component technologies.
- Meeting an end user demand for new applications-both products and services.
- Aggressive regulatory actions to introduce competition in monopoly markets.

### **Just-In-Time**

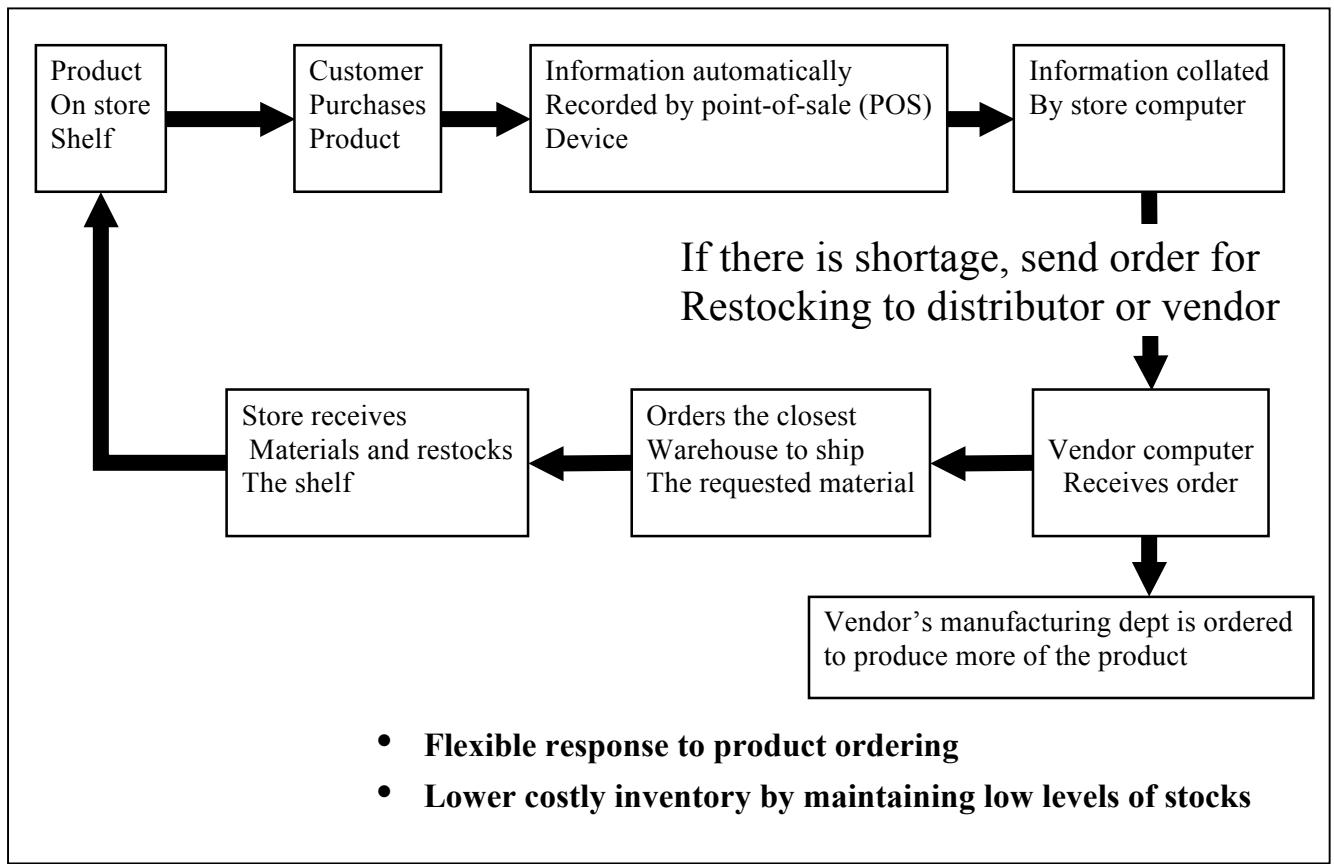
- Just-in-time (JIT) is viewed as an integrated management system consisting of a number of different management practices dependent on the characteristics of specific plants.
- JIT is an evolution of the Japanese approach to manufacturing and initially introduced for the Toyota production system.
- JIT is based on two principles:
  - ✓ Elimination of all waste (time, materials, labor, and equipment) in the production cycle.
  - ✓ Empowering workers
- JIT purchasing allows a manufacturer to incorporate its suppliers' efforts toward eliminating waste in the upstream portion of the manufacturing cycle.
- JIT purchasing focuses on the reduction of inventories throughout the logistical systems of the manufacturing firms involved and provides a careful audit of the production process.
- In a production plant the needed materials are to be supplied just in time, no earlier or later than is demanded for processing. Production costs will decrease as the required level of stock is reduced.
- It enhances quality control of production, as all stages of production are closely monitored, enabling an adequate assessment of imperfections.
- To achieve JIT savings, many large corporations have installed private communications networks.
- The I-way makes JIT practice more affordable and easily available to a number of small firms.

### **Quick Response Retailing**

- Quick Response (QR) is a version of JIT purchasing tailored for retailing.
- To reduce the risk of being out of stock, retailers are implementing QR systems.
- QR provides for a flexible response to product ordering and lowers costly inventory levels.
- QR retailing focuses on market responsiveness while maintaining low levels of stocks.
- It creates a closed loop encompassing the retailer, vendor, and consumer chain, and as consumers make purchases the vendor automatically orders new deliveries from the retailer through its computer network.

- The bar-coded articles are logged by the cash registers at the point of sale, the inventory system of the store then determines the needed supply, and the system transmits an order message to the retailer.
- The availability of accurate information with respect to the current sales enables sophisticated marketing capable of responding to consumers' preferences.

### The Quick Response Chain



### What is the Supply Chain?

- Supply chain is the business process that links manufacturers, retailers, customers, and suppliers in the form of a “chain” to develop and deliver products as one “virtual” organization of pooled skills and resources.
- Supply chain is the flow of materials, information, money, and services from raw material suppliers through factories and warehouses to the end customers
- It includes *organizations* and *processes* that create and deliver the following to the end customers:
  - Products
  - Information
  - Services

## Supply Chain Components

- Upstream supply chain—includes the activities of suppliers (manufacturers and/or assemblers) and their suppliers
- Internal supply chain—includes all in-house processes used in transforming the inputs received from the suppliers into the organization's outputs
- Downstream supply chain—includes all the activities involved in delivering the product to the final customers

## Types of Supply Chains

- Integrated build-to-stock (push-based or supply-driven model)
- Continuous replenishment
- Build-to-order (pull-based or demand-driven) —model in which a manufacturer begins assembly of the customer's order almost immediately upon receipt of the order
- Channel assembly—model in which product is assembled as it moves through the distribution channel

## What is supply chain management?

- SCM is a generic term that encompasses the coordination of order generation, order taking, and order fulfillment / distribution of products, services, or information.
- SCM is about integrating the internal and external partners on the supply and process chains to get raw materials to the manufacturers and finished products to the consumer.
- A supply chain management is a network of supplier, **manufacturing, assembly, distribution, and logistics facilities** that perform the functions of **procurement** of materials, **transformation** of these materials into intermediate and finished products, and **distribution** of these products to customers.
- Supply chains exist in both service and manufacturing organizations.
- SCM is a systems approach to managing the entire flow of information, materials, and services from raw materials suppliers through factories and warehouses to the end customer.
- SCM is a major application area of Internet Technologies and Electronic Commerce. (ITEC)

## Functions of Supply Chain Management

| SCM Functions       | Goals                                                                                                    | Benefits                                                                                               |
|---------------------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------|
| Supplier management | To reduce the number of suppliers and get them to become partners in business in a win/win relationship. | - reduce purchase order (PO) processing costs<br>- increase number of POS processed by fewer employees |

|                          |                                                                                                                  |                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Inventory management     | Shorten the order-ship-bill cycle.                                                                               | - improve auditing capabilities<br>- reduce inventory level<br>- improve inventory turns<br>- eliminate out-of-stock occurrences           |
| Distribution management  | move documents related to shipping (Bill of lading, purchase orders, advanced ship notices, and manifest claims) | - data accuracy<br>- improve resource planning                                                                                             |
| Channel management       | Quick dissemination of information about changing operational conditions to trading partners.                    | instant access to technical, product and pricing information                                                                               |
| Payment management       | link companies, suppliers and distributors for e-payment                                                         | - increase the speed of computing the invoices.<br>- reduce clerical errors.<br>- increase the number of invoices processed (productivity) |
| Financial management     | Enable global companies to manage foreign trade exchange account.                                                | -access risk and exposure in global financial markets.<br>- deal with global information as opposed to local market information.           |
| Sales force productivity | Improve the communication and flow of information among the sales, customer and production.                      | - Greater access to market intelligence and competitors' information.<br>- Better customer relationship management (CRM)                   |

## **Business Model**

### **Introduction**

- In the most basic sense, a business model is the method of doing business by which a company can sustain itself -- that is, generate revenue.
- The business model spells-out how a company makes money by specifying where it is positioned in the value chain.
- Some models are quite simple:
  - A company produces a good or service and sells it to customers. If all goes well, the revenues from sales exceed the cost of operation and the company realizes a profit.
- Other models can be more intricately woven:
  - Broadcasting is a good example. Radio, and later television, programming has been broadcast over the airwaves free to anyone with a receiver for much of the past century. The broadcaster is part of a complex network of distributors, content creators, advertisers (and their agencies), and listeners or viewers. Who makes money and how much is not always clear at the outset.
- Internet commerce will give rise to new kinds of business models.

### **Electronic markets**

Electronic markets have three functions such as: (i) matching buyers and sellers, (ii) facilitating commercial transactions, and (iii) providing legal infrastructure. Information technology performs and also helps to increase market efficiency and reduce transaction costs. The interaction between participants is supported by electronic trade processes that are basically search, valuation, payment and settlement, logistics and authentication.

### **Desirable Characteristics of an Electronic Marketplace**

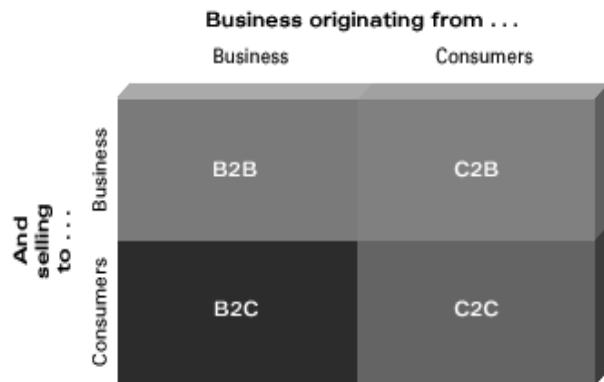
- Critical mass of buyers and sellers
- Opportunity for independent evaluations and for customer dialogue and discussions.
- Negotiation and bargaining
- New product and services offering
- Seamless interface of information, standardization and compatible EDI software and network services
- Provision for resolving dispute or disagreement

### **Categories of Business Models**

1. E-business model based on the relationship of transaction parties
2. E-business model based on the relationship of transaction types.

**1. Electronic business model based on the transaction parties**

- Business-to-Consumer (B2C)
- Business-to-Business (B2B)
- Business-to-Government (B2G)
- Consumer-to-Consumer (C2C)
- Consumer-to-Business (C2B)



### Summary of e-business transaction model

| Model | Description                                                                                                            |
|-------|------------------------------------------------------------------------------------------------------------------------|
| B2C   | Sells products or services directly to consumers                                                                       |
| B2B   | Sells products or services to other businesses or bring multiple buyers and sellers together in a central marketplace. |
| B2G   | Business selling to local, state agencies                                                                              |
| C2C   | Consumer sells directly to other consumers.                                                                            |
| C2B   | Consumer fixes price on their own, which businesses accept or decline.                                                 |

### Business-to-Commerce (B2C) Model

It refers to exchange between businesses and consumers. These are the e-commerce sites that sell products and services, or provide information services directly to consumers. They include such well-known companies as Yahoo!, Amazon.com, and LandsEnd.com. Some B2C e-businesses provide high-value content to consumers for a subscription fee. Examples are Wall Street journal (financial news and articles), Consumer Reports (product reviews and evaluation), and eDiets.com (nutritional counseling).

B2C e-business models include virtual malls, which are web sites that host many online merchants. Virtual malls typically charge online merchants setup, listing, or transaction fees and many include transaction handling services and marketing options. Example of virtual malls includes *excite.com*, *women.com*, *amazon.com* and *yahoo.com*.

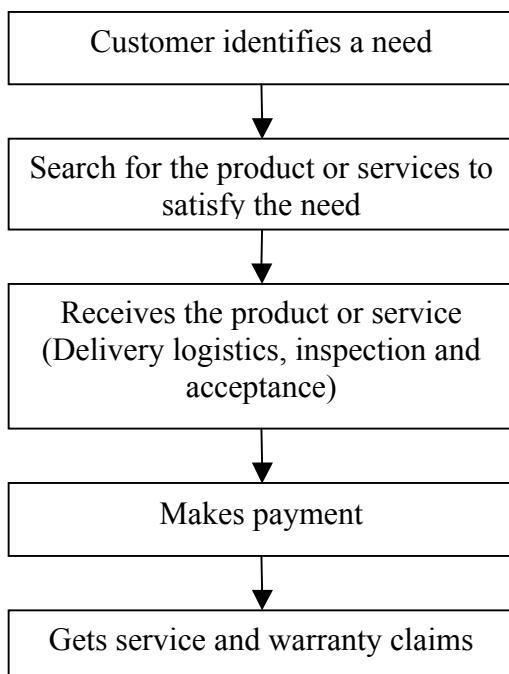
## Why B2C??

- Inexpensive costs, big opportunities
- Globalization
- Reduced operational costs
- Customer-convenience
- Knowledge Management

## How does B2C Work?

B2C e-commerce is more than just an online store. It really is managing the entire process, but just using technology as a tool for order processing and customer support. The following details explain the processes in B2C marketplace.

1. Visiting the virtual Mall
2. Customer registration
3. Customer buys products
4. Merchant processes the order
5. Credit card or e-payment processes
6. Operations Management
7. Shipment and delivery (Logistics) system
8. Customer reception of goods or services
9. After sales services



## **Consumer-to-Business (C2B) Model**

In this model, Consumers can band together to present themselves as a buyer group to buy the same or similar products and obtain volume discounts from a business. This process is known as demand aggregation.

*Demand aggregation* combines purchase requests from multiple buyers into a single large order, which justifies a discount from the business. Example: [www.sugarloaf.net](http://www.sugarloaf.net). Demand aggregation is also possible and much more widespread, of course, in the B2B sector.

This C2B model, also called a *reverse auction* or *demand collection model*, enables buyers to name their own price, often binding, for a specific good or service generating demand. The web site collects the "demand bids" and then offers the bids to participating sellers. Example: ReverseAuction.com (travel, autos, consumer electronics) and priceline.com (travel, telephone, hotels).

## **Business-to-business (B2B) Model**

B2B e-commerce defines e-commerce that takes place between organizations. Trade is global; companies do business with other companies in countries all over the world. *B2B marketplaces* are Internet-based services that bring together buyers and sellers. They have the potential to bring together large numbers of buyers and sellers, thereby giving buyers more choices and aggregating demand for the sellers. Transaction costs can be reduced, resulting in potential savings for both buyers and sellers. One commonly used technique is to have the marketplace conduct a reverse auction.

**Reverse auction** is the process in which a buyer posts its interest in buying a certain quantity of items, and sellers compete for the business by submitting successively lower bids until there is only one seller left. Marketplaces usually make their money by charging a transaction fee for their services. For example, FreeMarkets is a company that holds auctions so corporations can buy industrial parts, materials, and services from suppliers via the Internet.

## **Advantages of B2B**

- Direct interaction with customers
- Focused sales promotion
- Building customer loyalty
- Scalability
- Savings in distribution costs

## **Consumer-to-Consumer (C2C) Model**

It involves transactions between and among consumers. These exchanges can include third-party involvement, as in the case of the auction website eBay. Other activities include classified ads, games, jobs, Web-based communications and personal services. C2C is also often referred to as peer-to-peer (P2P).

## **2. Electronic business models based on transaction types**

- Brokerage
- Advertising
- Infomediary
- Merchant
- Manufacturer (Direct)
- Affiliate
- Community
- Subscription
- Utility

The models are implemented in a variety of ways. A firm may combine several different models as part of its overall Internet business strategy. For example, it is not uncommon for content driven businesses to blend advertising with a subscription model.

### **1. Brokerage Model**

- Brokers are market-makers: they bring buyers and sellers together and facilitate transactions.
- Brokers play a frequent role in business-to-business (B2B), business-to-consumer (B2C), or consumer-to-consumer (C2C) markets.
- Usually a broker charges a fee or commission for each transaction it enables. The formula for fees can vary.

#### **Characteristics of brokerage Model**

- Price discovery mechanism is its key-principle
- It is a meeting point for sellers and buyers.
- Auction and exchanges are the modes of transactions
- It is a "Free Market"
- It consists of Global Network of buyers and Sellers
- It is virtual Marketplace enabled by the Internet
- It encompasses all types of organization now.

#### **Advantages of Brokerage Model**

- C2C trading, which
  - allows buyers and sellers to trade directly bypassing intermediaries, and
  - reduce cost for both parties
- Global reach
- Trading convenience, which
  - allows trading at all hours, and
  - provides continually updated information
- Sense of community through direct buyer and seller communication
- Efficient access to information

- Alleviation of risks of anonymous trading

### **Brokerage models include:**

#### **Marketplace Exchange**

- Provides a full range of services covering the transaction process, from market assessment to negotiation and fulfillment, for a particular industry.
- The exchange can operate independently of the industry, or it can be backed by an industry consortium. The broker typically charges the seller a transaction fee based on the value of the sale. There also may be membership fees.

**Buy/Sell Fulfillment** Customer specifies buy or sell orders for a product or service, including price, delivery, etc. The broker charges the buyer and/or seller a transaction fee.

#### **Demand Collection System**

- The patented "name-your-price" model pioneered by Price line.
- Prospective buyer makes a final bid for a specified good or service, and the broker arranges fulfillment.

#### **Auction Broker**

- Conducts auctions for sellers (individuals or merchants).
- Broker charges the seller a listing fee and commission scaled with the value of the transaction.
- Auctions vary in terms of the offering and bidding rules. Reverse auctions are a common variant.
- Provides a third-party payment mechanism for buyers and sellers to settle a transaction.
- Is a catalog operation that connects a large number of product manufacturers with volume and retail buyers.
- Broker facilitates business transactions between franchised distributors and their trading partners.

**Transaction Broker** It provides a third-party payment mechanism for buyer and sellers to settle a transaction.

**Distributor** It is a catalog operation that connects a large number of product manufacturers with volume and retail buyers. Broker facilitates business transactions between franchised distributors and their trading partners.

**Search Agent** It is an agent (i.e., a software agent or "robot") used to search-out the price and availability for a good or service specified by the buyer, or to locate hard to find information.

#### **Virtual Mall**

- Hosts online merchants
- The Mall typically charges setup, monthly listing, and/or per transaction fees.

- More sophisticated malls provide automated transaction services and relationship marketing opportunities.

## **2. Advertising Model**

- The web advertising model is an extension of the traditional media broadcast model.
- The broadcaster, in this case, a web site, provides content (usually, but not necessarily, for free) and services (like e-mail, chat, forums) mixed with advertising messages in the form of banner ads.
- The banner ads may be the major or sole source of revenue for the broadcaster.
- The broadcaster may be a content creator or a distributor of content created elsewhere.
- The advertising model only works when the volume of viewer traffic is large or highly specialized.

### **Portal**

- Portal is a point of entry to the web, usually a search engine that includes diversified content or services.
- The high volume makes advertising profitable and permits further diversification of site services
- Personalized portal allows customization of the interface and content. This increases loyalty as a result of the user's own time invested in personalizing the site.

**Niche Portal** Niche portal cultivates a well-defined user demographic. For example, a site that attracts home buyers, young women, or new parents, can be highly sought after as a venue for certain advertisers who are willing to pay a premium to reach that particular audience.

**Classifieds** List items for sale or wanted for purchase. Listing fees are common, but there also may be a membership fee.

### **Registered Users**

- Content-based sites that are free to access but require users to register.
- Registration allows inter-session tracking of users' site usage patterns and thereby generates data of greater potential value in targeted advertising campaigns.

**Query-based Paid Placement** Sell favorable link positioning (i.e., sponsored links) or advertising keyed to particular search terms in a user query, such as Overture's trademark "pay-for-performance" model.

### **Contextual Advertising**

- Freeware developers who bundle ads with their product.
- For example, a browser extension that automates authentication and form fill-ins, also delivers advertising links or pop-ups as the user surfs the web.

- Contextual advertisers can sell targeted advertising based on an individual user's surfing behavior.

### **Content-Targeted Advertising**

- As defined by Google, content-targeted advertising extends the precision of search advertising to the rest of the web.
- Google identifies the meaning of a web page and then automatically delivers relevant ads when a user visits that page.
- Content-targeted advertising provides an opportunity for advertisers to reach users based on specific content keywords and enables website publishers to generate new revenue from content pages.

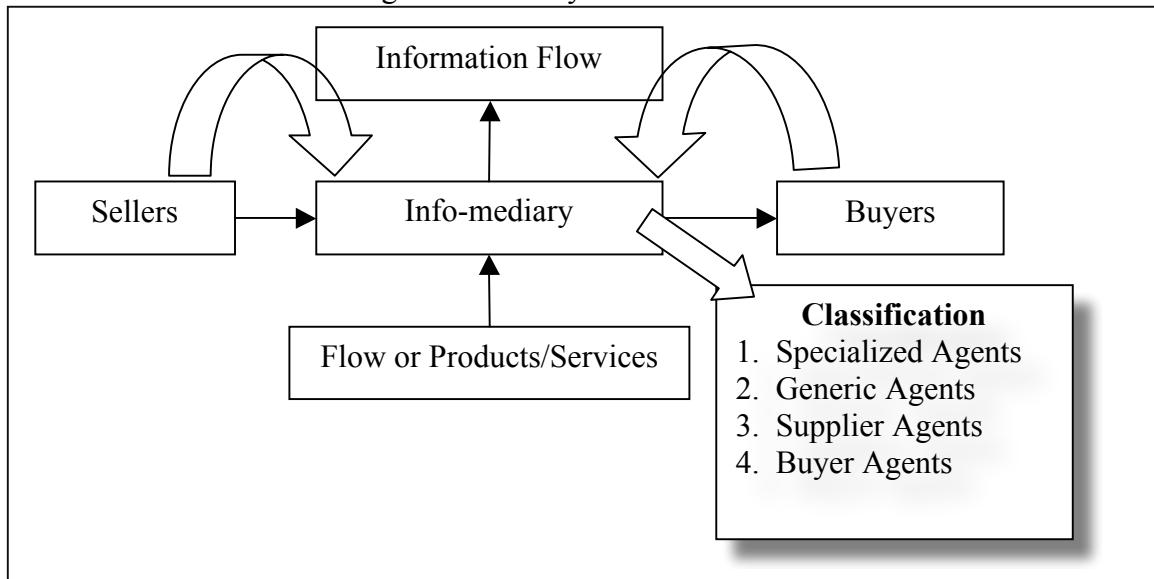
### **Ultramercials**

- Interactive online advertisements that require the user to respond intermittently in order to wade through the message before reaching the intended content.
- Ultramercials can be used as a gateway to what would otherwise be subscriber-only premium content.

### **3. Infomediary Model**

- An organizer of virtual community is called an information intermediary or infomediary, who helps customer to collect, manage and maximize the value of information about consumers.
- Data about consumers and their buying/consumption habits are valuable, especially when that information is carefully analyzed and used to target marketing campaigns.
- Independently collected data about producers and their products are useful to consumers when considering a purchase.
- Some firms function as infomediaries (information intermediaries) assisting buyers and/or sellers understand a given market.

Fig: Info-mediator Model



**Types of Info-mediary Model include:**

**Advertising Networks**

- Service that feeds banner ads to a network of sites, thereby enabling advertisers to deploy large marketing campaigns.
- By using cookies, the Ad Network operator collects data on web users that can be used to analyze marketing effectiveness.

**Audience Measurement Services** Online audience market research agencies

**Incentive Marketing**

- The customer loyalty program model.
- Provides incentives to customers such as redeemable points or coupons for making purchases from associated retailers.
- Data collected about users is sold for the purpose of targeted advertising.

**Meta-mediary** Facilitates transactions between buyer and sellers by providing comprehensive information and ancillary services, but does not get involved in the actual exchange of goods or services between the parties.

**4. Merchant Model**

Wholesalers and retailers of goods and services. Sales may be made based on list prices or through auction.

**Virtual Merchant or e-tailer** A merchant that operates over the web.

**Catalog Merchant** Mail-order business with a web-based catalog. Combines mail, telephone and web ordering.

**Click and Mortar** Traditional brick-and-mortar retail establishment with web storefront.

**Bit Vendor** A merchant that deals strictly in digital products and services and in its purest form conducts both sales and distribution over the web.

**5. Manufacturer (Direct) Model**

The manufacturer or "direct model", it is predicated on the power of the web to allow a manufacturer (i.e., a company that creates a product or service) to reach buyers directly and thereby compress the distribution channel. The manufacturer model can be based on efficiency, improved customer service, and a better understanding of customer preferences.

### **Brand Integrated Content**

Traditionally, manufacturers rely on advertising to build customer awareness. Commercials via broadcasters like radio, television and mass market publishers (newspapers and magazines), or through product placement in TV and motion pictures, have been a mainstay of modern business. The Web enables a manufacturer to integrate their brand more intimately with the content.

### **6. Affiliate Model**

In contrast to the generalized portal, which seeks to drive a high volume of traffic to one site, the affiliate model provides purchase opportunities wherever people may be surfing. It does this by offering financial incentives (in the form of a percentage of revenue) to affiliated partner sites. The affiliates provide purchase-point click-through to the merchant. It is a *pay-for-performance* model -- if an affiliate does not generate sales, it represents no cost to the merchant. The affiliate model is inherently well-suited to the web, which explains its popularity. Variations include banner exchange, pay-per-click, and revenue sharing programs.

### **7. Community Model**

"Community", an Internet buzz word is defined as

- A unified body of individuals.
- The people with common interests living in a particular area, broadly, the area itself.
- An interacting population of various kinds of individuals in a common location.

E-Communities are formed when groups of people meet online to fulfill certain needs, which include personal interests, relationships, entertainment and transactions. E-Communities cater to groups of people who come online to serve their common interests and needs, exchange information, share interests, trade goods and services, entertain and seek help. The viability of the community model is based on user loyalty (as opposed to high traffic) volume. Consumer loyalty can be achieved by building e-communities. First, visitors come and look for information. Then, they start to contribute to the web site by, for instance, suggesting ways to improve the site or its services. Finally, they work inside the web site, for instance, volunteering as editors for a message board or by serving on a customer advisory board. Users have a high investment in both time and emotion. Revenue can be based on the sale of ancillary products and services or voluntary contributions or on a subscription fee for premium services.

**Open Source Model** -- best known in the example of Linux, where software is developed voluntarily by a global community of interested programmers. The businesses that emerge around open source products rely on revenue generated from related services like systems integration, product support, tutorials and user documentation. In the field of software operating systems, the Open Source is viewed as a threat to the "commercial software development" (CSD) model advocated by Microsoft. [[Red Hat](#)]

**Public Broadcasting Model** -- similar to the traditional public broadcasting model -- the listener or viewer contributor method used in not-for-profit radio and television broadcasting. The model is predicated on the creation of a community of users who support the site through voluntary donations. Not-for-profit organizations may also seek funding from charitable foundations and corporate sponsors that support the organizational mission. The web holds great potential as a contributor based model because the user base is more readily apparent.

**Knowledge Networks** -- or expert sites, that provide a source of information based on professional expertise or the experience of other users. Sites are typically run like a forum where persons seeking information can pose questions and receive answers from (presumably) someone knowledgeable about the subject. The experts may be employed staff, a regular cadre of volunteers, or in some cases, simply anyone on the web who wishes to respond.

## **8. Subscription Model**

Users are charged a periodic -- daily, monthly or annual -- fee to subscribe to a service. It is not uncommon for sites to combine free content with "premium" (i.e., subscriber- or member-only) content. Subscription fees are incurred irrespective of actual usage rates. Subscription and advertising models are frequently combined.

**Content Services** -- beyond newspapers and magazines, the Web has encouraged the use of the subscriber model for music and video, as well.

**Person-to-Person Networking Services** -- are conduits for the distribution of user-submitted information, such as individuals searching for former school mates.

**Trust Services** -- an independent third party that engenders trust between unfamiliar parties entering into a transaction. The need of trust increases with the value and complexity of the product or service that is sold. Trust services typically come in the form of membership associations that abide by an explicit code of conduct, and in which members pay a subscription fee.

**Internet Services Providers** -- offer Internet connectivity and related services on a monthly subscription.

## **9. Utility Model**

The utility or "on-demand" model is based on metering usage, or a "*pay as you go*" approach. Unlike subscriber services, metered services are based on actual usage rates. Traditionally, metering has been used for essential services (e.g., electricity water, long-distance telephone services). Internet service providers (ISPs) in some parts of the world operate as utilities, charging customers for connection minutes, as opposed to the subscriber model common in the U.S.

**Metered Subscription:** in this case subscribers purchase access to content in metered portions (e.g., numbers of pages viewed)

### Exercise

1. Explain the required features of a B2B platform for e-commerce.
2. What sort of details could a hotel chain provide to assist potential clients in booking a hotel that matches their travel plans?
3. Select a product that a computer retailer might sell, such as printers, scanners, and zip drives. What sort of details about this product could an online computer provide to their clients?

## Security and Encryption

### What is Cryptography/Encryption

- Encryption is the method of using a mathematical algorithm to transfer information into a format that can not be read which is called *cipher text*.
- Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data.
- Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.
- Decryption is the method of using algorithm transform encrypted information back into a readable format and it is called *plain text*.
- Encryption and decryption require the use of some secret information, usually referred to as a *key*. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different.
- In cryptography the original message is usually called the *plaintext* while the encrypted message is called the *cipher text*.

### Cryptography Goal

Cryptology provides methods that enable a communicating party to develop trust that his communications have the desired properties, in spite of the best efforts of an entrusted party (or adversary). A fundamental goal of cryptography is to adequately address these four areas in both theory and practice. Cryptography is about the prevention and detection of cheating and other malicious activities.

**1. Confidentiality** is a service used to keep the content of information from all but those authorized to have it. Secrecy is a term synonymous with confidentiality and privacy.

**Confidentiality is the evidence that the contents of the message have not been disclosed to a third party or unauthorized entity.**

**2. Data integrity** is a service which addresses the unauthorized alteration of data. To assure data integrity, one must have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion, deletion, and substitution.

**Data integrity is the proof that the message content has not been altered deliberately or accidentally during transmission.**

**3. Authentication** is a service related to identification or process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based). This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information

delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons this aspect of cryptography is usually subdivided into two major classes: *entity authentication* and *data origin authentication*. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).

**Authentication means establishing the identities of the person one is transacting with.**

**4. Non-repudiation** is a service which prevents an entity from denying previous commitments or actions. When disputes arise due to an entity denying that certain actions were taken, a means to resolve the situation is necessary. For example, one entity may authorize the purchase of property by another entity and later deny such authorization was granted. A procedure involving a trusted third party is needed to resolve the dispute.

**Non-repudiation is the certainty of knowing that the sender of the message cannot later deny having sent it.**

### **Terminology defined**

**Cryptanalysis** is the study of mathematical techniques for attempting to defeat cryptographic techniques, and, more generally, information security services.

A **cryptanalyst** is someone who engages in cryptanalysis.

A **Cryptology** is the discipline or study of cryptography and cryptanalysis.

A **cryptosystem** is a general term referring to a set of cryptographic primitives used to provide information security services. Most often the term is used in conjunction with primitives providing confidentiality, i.e., encryption.

### **Types of Cryptography**

There are several ways of classifying cryptography based on the number of keys that are employed for encryption and decryption, and by their application and use. The three types of cryptography are( as shown in Figure):

- **Secret Key Cryptography:** Uses a single key for both encryption and decryption.
- **Public Key Cryptography:** Uses one key for encryption and another for decryption.
- **Hash Functions:** Uses a mathematical transformation to irreversibly "encrypt" information.



**A) Secret key (symmetric) cryptography.** SKC uses a single key for both encryption and decryption.



**B) Public key (asymmetric) cryptography.** PKC uses two keys, one for encryption and the other for decryption.



**C) Hash function (one-way cryptography).** Hash functions have no key since the plaintext is not recoverable from the ciphertext.

## 1. Secret/Symmetric Key cryptography

Secret cryptography is based on the sender and receiver of a message knowing and using the same secret key: the sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message as shown in figure below. This method is known as *secret-key*. Because a single key is used for both functions, secret key cryptography is also called *symmetric encryption*.

Using symmetric cryptography, it is safe to send encrypted messages without fear of interception (because an interceptor is unlikely to be able to decipher the message); however, there always remains the difficult problem of how to securely transfer/distribute the key to the recipients of a message so that they forgery cannot decrypt the message.

The main problem with symmetric key is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, or a phone system, or some other transmission medium to prevent the disclosure of the secret key being communicated. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. The generation, transmission and storage of keys is called key management; all cryptosystems must deal with key management issues. Because all keys in a secret-key cryptosystem must remain secret, secret-key cryptography often has difficulty providing secure key management, especially in open systems with a large number of users.



Symmetric algorithms can be divided into two categories. Some operate on the plaintext a single bit (or sometimes byte) at a time; these are called **stream algorithms** or **stream ciphers**. Others operate on the plaintext in groups of bits. The groups of bits are called **blocks** and the algorithms are called **block ciphers**. For modern computer algorithms, a typical block size is 64 bits.

### Data Encryption Standard (DES)

The most common secret-key cryptography scheme used today is the *Data Encryption Standard (DES)*, designed by IBM in the 1970s and adopted by the National Bureau of Standards (NBS) [now the National Institute for Standards and Technology (NIST)] in 1977 for commercial and unclassified government applications.

DES is a *symmetric cryptosystem*. When used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single-user encryption, such as to store files on a hard disk in encrypted form. In a multi-user environment, secure key distribution may be difficult; public-key cryptography provides an ideal solution to this problem. DES is an *encryption block-cipher* employing a 56-bit key that operates on 64-bit blocks. DES has a complex set of rules and transformations that were designed specifically to yield fast hardware implementations and slow software implementations. Instead of defining just one encryption algorithm, DES defines a whole family of them. Several variants of DES are currently in use, including Triple-DES

### Advantages of symmetric-key cryptography

- Symmetric-key ciphers can be designed to have high rates of data throughput. Some hardware implementations achieve encrypt rates of hundreds of megabytes per second, while software implementations may attain throughput rates in the megabytes per second range.
- Keys for symmetric-key ciphers are relatively short.
- Symmetric-key ciphers can be employed as primitives to construct various cryptographic mechanisms such as hash functions and computationally efficient digital signature schemes.
- Symmetric-key ciphers can be composed to produce stronger ciphers.

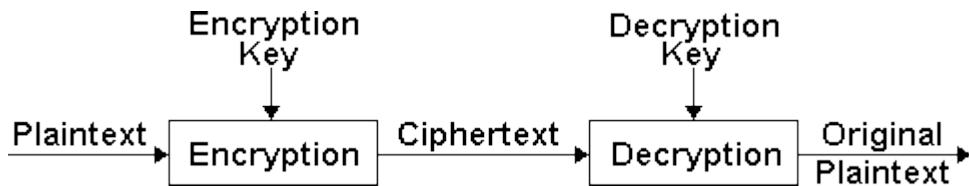
### Disadvantages of symmetric-key cryptography

- In a two-party communication, the key must remain secret at both ends.
- In a large network, there are many key pairs to be managed. Consequently, effective key management is required.

- In a two-party communication between entities A and B, sound cryptographic practice dictates that the key be changed frequently, and perhaps for each communication session.
- Digital signature mechanisms arising from symmetric-key encryption typically require large keys for the public verification function.

## **2. Public Key Cryptography**

The concept of *public-key cryptography* was introduced in 1976 by Whitfield Diffie and Martin Hellman in order to solve the key management problem. In their concept, each person gets a pair of keys, one called the *public key* and the other called the *private key*. Each person's public key is published while the private key is kept secret. All communications involve only public keys, and no private key is ever transmitted or shared. No longer is it necessary to trust some communications channel to be secure against eavesdropping or betrayal. The only requirement is that public keys are associated with their users in a trusted (authenticated) manner (for instance, in a trusted directory). Anyone can send a confidential message by just using public information, but the message can only be decrypted with a private key, which is in the sole possession of the intended recipient. Furthermore, public-key cryptography can be used not only for privacy (*encryption*), but also for authentication (*digital signatures*).



### **Public key**

It is available to others for use when the information will be sent to an individual. People can use the user's public key to decrypt information sent by that person.

### **Private key**

It is only accessible to the individual and they can use it to decrypt any messages encrypted with the public key. In addition, they can use the private key to encrypt messages, so these messages can only be decrypted with the matching public key.

In practice, the public key is placed in a public database known as a *key server*. Whenever somebody wants to find out what public key is, they send a request to the key server.

## **Advantages of public-key cryptography**

- Only the private key must be kept secret (authenticity of public keys must, however, be guaranteed).
- Depending on the mode of usage, a private key/public key pair may remain unchanged for considerable periods of time, e.g., many sessions (even several years).
- Many public-key schemes yield relatively efficient digital signature mechanisms.
- The key used to describe the public verification function is typically much smaller than for the symmetric-key counterpart. In a large network, the number of keys necessary may be considerably smaller than in the symmetric-key scenario.

## **Disadvantages of public-key encryption**

- Throughput rates for the most popular public-key encryption methods are several orders of magnitude slower than the best known symmetric-key schemes.
- Key sizes are typically much larger than those required for symmetric-key encryption, and the size of public-key signatures is larger than that of tags providing data origin authentication from symmetric-key techniques.
- No public-key scheme has been proven to be secure.

## **Advantages and Disadvantages of Public-Key Cryptography Compared with Secret-Key Cryptography**

The primary advantage of public-key cryptography is increased security and convenience. Private keys never need to be transmitted or revealed to anyone. In a secret-key system, by contrast, the secret keys must be transmitted (either manually or through a communication channel), and there may be a chance that an enemy can discover the secret keys during their transmission.

Another major advantage of public-key systems is that they can provide a method for digital signatures. Authentication via secret-key systems requires the sharing of some secret and sometimes requires trust of a third party as well. As a result, a sender can repudiate a previously authenticated message by claiming that the shared secret was somehow compromised by one of the parties sharing the secret.

A disadvantage of using public-key cryptography for encryption is speed; there are popular secret-key encryption methods that are significantly faster than any currently available public-key encryption method.

Nevertheless, public-key cryptography can be used with secret-key cryptography to get the best of both worlds. For encryption, the best solution is to combine public- and secret-key systems in order to get both the security advantages of public-key systems and the speed advantages of secret-key systems. The public-key system can be used to encrypt a secret key which is used to encrypt the bulk of a file or message. Such a protocol is called a *digital envelope*.

In some situations, public-key cryptography is not necessary and secret-key cryptography alone is sufficient. This includes environments where secure secret-key agreement can take place, for example by users meeting in private. It also includes environments where a single authority knows and manages all the keys (e.g., a closed banking system). Since the authority knows everyone's keys already, there is not much advantage for some to be "public" and others "private."

Public-key cryptography is usually not necessary in a single-user environment. In general, public-key cryptography is best suited for an open multi-user environment.

## **Public-Key Cryptography Infrastructures**

Public-key cryptography is a wonderfully useful gem of mathematics and computer science – a publicly published set of numbers that can be used to encrypt a private message so that it is undecipherable to a snooper.

A public key is a series of 310 digits used to encrypt information sent to the key's owner, let's call him Joe. To decrypt these messages so he can read them, Joe uses his private key, which only he knows. Both the public and the private keys are derived from a pair of large prime numbers according to a relatively simple mathematical formula. In theory, it might be possible to derive the private key from the public key by working the formula backwards. In practice, no one has ever done it and it doesn't look like anyone ever will. Factoring large numbers is so hard that even the most powerful supercomputers in the world can't break an ordinary public key.

In an ideal world, everyone would have a public key that could be used to buy and sell things over the Internet, and engage in secure email communication with friends and strangers alike. There would be a directory on the Internet that would list everyone's public key, like numbers in a telephone book. But in the 25 years since public key cryptography was invented, no such infrastructure has been built. Why?

The problem is not technical – even the cheapest computers now have the power to handle 1024-bit encryption – it's economic and sociological. When it became clear that untold riches could be had if only people would entrust their credit card numbers to the Internet, the infrastructure for one-sided public key cryptography – using the vendor's public key – sprang up almost overnight.

If everyone had a public key, it could function as a credit card that would be much less prone to fraud, and allow people to send each other email no one else could read. The reason they don't turns on the question of trust, say Microsoft Research cryptographers Josh Benaloh and Dan Simon.

Let's say Joe is the vice president of the First National Bank. He's at home one night, when he gets an email from Frank the bank president. It says "I left my car keys in the vault, but I forgot the combination. Please send it to me. Here is a public key that you can use to encrypt the combination so that only I will get it. Key =

X3AFK94KSD39SSAJ349SKFM232..." The key may safely encrypt the combination, but unless Joe is absolutely sure that the message and the key really came from Frank, he would be ill advised to send the vault combination.

Now, if there were a central directory, or a series of them, maintained by institutions in which everyone had absolute trust, then Joe could be sure that it was the real Frank he was dealing with, that his data would be safe as it traveled over the wires and no one but Frank could read it.

Some people use public key cryptography to exchange secure messages, but mostly they're people who already know and trust each other. Most people have never had their email intercepted or exchanged sensitive information over the Internet. "Until there's a strong public demand for the infrastructure, no one will build it," says Benaloh. "Until the system is so easy to use that you don't even know it's there, no one will use it," says Simon.

Preventing public key fraud and abuse turns out to be a tough problem, and a big reason there is no public key infrastructure today. Any directory would have to keep an up-to-date list of the deadbeats who didn't pay their bills and had their keys revoked. Should public keys have an expiration date? How often should they expire? What if someone gets hold of Joe's private key? What if someone calls and says he's Joe and someone has stolen his private key and gets Joe's key cancelled so that Joe, vacationing in Bali, suddenly finds his credit cut off? "The list of problem scenarios goes on and on until the public key system begins to look more exploitable than today's credit card system," says Benaloh.

Perhaps unforeseen developments will motivate entrepreneurs to solve these problems and build a public key infrastructure. "We'd like to make it happen," says Benaloh. "Idea-wise, we're leaders. Implementation-wise, the need has to come first."

## RSA Algorithm

RSA is a *public-key cryptosystem* for both *encryption* and *authentication*; it was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. It may be used to provide both *secrecy* and *digital signatures*. [Adoption of RSA seems to be proceeding more quickly for Authentication (digital signatures) than for privacy (encryption)]. Encryption and authentication take place without any sharing of private keys: each person uses only other people's public keys and his or her own private key. Anyone can send an encrypted message or verify a signed message, using only public keys, but only someone in possession of the correct private key can decrypt or sign a message.

### Example: How RSA provide digital signature?

This example shows how a digital signature works for an e-document to be sent from the sender X to the receiver Y.

X runs a program that uses a hash algorithm to generate a *digital fingerprint* ( bits pattern that uniquely identifies a much larger bits pattern) for the document and encrypts the digital fingerprint with his private key.

This X's generated digital signature is transmitted along with the data. Y decrypts the signature with X's public key and runs the same hash program on the document. If the digital fingerprint output by the hash program match the fingerprint send by X (after that has been decrypted), then the signature is authentic otherwise it's invalid. If the documents were altered by intruder, the fingerprint will not matched (i.e. the output from the hash programs will be different), then the receiver will know that data tampering occurred. If the senders signature has been forget (encrypted with wrong private key), the fingerprint won't match. Hence, digital signature verifies both the identity of the sender and the authenticity of the data in the documents.

### **3. Hash Functions**

A hash function  $H$  is a transformation that takes a variable-size input  $m$  and returns a fixed-size string, which is called the hash value  $h$  (that is,  $h = H(m)$ ). Hash functions with just this property have a variety of general computational uses, but when employed in cryptography the hash functions are usually chosen to have some additional properties.

The basic requirements for a cryptographic hash function are:

- the input can be of any length,
- the output has a fixed length,
- $H(x)$  is relatively easy to compute for any given  $x$ ,
- $H(x)$  is one-way,
- $H(x)$  is collision-free.

A hash function  $H$  is said to be *one-way* if it is hard to invert, where “hard to invert” means that given a hash value  $h$ , it is computationally infeasible to find some input  $x$  such that  $H(x) = h$ .

If, given a message  $x$ , it is computationally infeasible to find a message  $y \neq x$  such that  $H(x) = H(y)$  then  $H$  is said to be a *weakly collision-free* hash function.

A *strongly collision-free* hash function  $H$  is one for which it is computationally infeasible to find any two messages  $x$  and  $y$  such that  $H(x) = H(y)$ .

The hash value represents concisely the longer message or document from which it was computed; one can think of a message digest as a “digital fingerprint” of the larger document. Examples of well-known hash functions are MD2, MD5 and SHA.

Perhaps the main role of a cryptographic hash function is in the provision of digital signatures. Since hash functions are generally faster than digital signature algorithms, it is typical to compute the digital signature to some document by computing the signature on

the document's hash value, which is small compared to the document itself. Additionally, a digest can be made public without revealing the contents of the document from which it is derived. This is important in digital timestamping where, using hash functions, one can get a document timestamped without revealing its contents to the timestamping service.

### **Digital signature**

Authentication builds a trustworthy relationship and maintains confidentiality. Just like physical signatures, digital signatures (an electronic substitute for manual signature) are a method of guaranteeing somebody's identity.

It is an identifier composed of a certain sequence of bits, which is created through *hash function* and the result is encrypted with the sender's private key.

As long as you don't let anybody know what your private key is, it will take impossibly large amounts of computing power to "forge" your digital signature. It is an extremely good idea to "sign" electronic documents by using your private key to encrypt the "message digest" of the document. A message digest is a relatively short block of numbers that prevents anybody from altering your document. Changing even a single letter would cause the message digest to become completely different.

*A digital signature* of a message is a number dependent on some secret known only to the signer, and, additionally, on the content of the message being signed. Signatures must be verifiable; if a dispute arises as to whether a party signed a document. Digital signature forms the basis for formally legally binding contracts in the course of e-commerce, hence creating a framework for secure online transactions.

Digital signatures have many applications in information security, including *authentication*, *data integrity*, and *non-repudiation*. One of the most significant applications of digital signatures is the certification of public keys in large networks. Certification is a means for a trusted third party (TTP) to bind the identity of a user to a public key, so that at some later time, other entities can authenticate a public key without assistance from a trusted third party.

The concept and utility of a digital signature was recognized several years before any practical realization was available. The first method discovered was the *RSA signature scheme* (explained above), which remains today one of the most practical and versatile techniques available.

### **Definition**

**Digital certificates** are your digital password "an internet ID". They are confirmation of who you are and the reliability of your data. Digital certificates are based on public/private key technology. Each key is like a unique encryption device. No two keys are ever identical, which is why a key can be used to identify its owner.

## Basic definitions

1. A ***digital signature*** is a data string which associates a message (in digital form) with some originating entity.
2. A ***digital signature generation algorithm*** (or ***signature generation algorithm***) is a method for producing a digital signature.
3. A ***digital signature verification algorithm*** (or ***verification algorithm***) is a method for verifying that a digital signature is authentic (i.e., was indeed created by the specified entity).
4. A ***digital signature scheme*** (or ***mechanism***) consists of a signature generation algorithm and an associated verification algorithm.
5. A ***digital signature signing process*** (or ***procedure***) consists of a (mathematical) digital signature generation algorithm, along with a method for formatting data into messages which can be signed.
6. A ***digital signature verification process*** (or ***procedure***) consists of a verification algorithm, along with a method for recovering data from the message.

## What are DSA and DSS?

Digital Signature Standard (DSS) specifies a Digital Signature Algorithm (DSA) as part of the U.S. government's Capstone project. DSS was selected to be the digital authentication standard of the U.S. government.

DSA is based on the discrete logarithm problem and derives from cryptosystems proposed by *Schnorr* and *ElGamal*. It is used for authentication only.

In DSA, signature *generation is faster than signature verification*, whereas in RSA, signature *verification is faster than signature*. NIST claims that it is an advantage of DSA that signing is faster, but many people in cryptography think that it is better for verification to be the faster operation.

## Criticism on DSA

- It lacks key exchange capability
- The underlying cryptosystem is too recent and has been subject to too little scrutiny for users to be confident of its strength
- Verification of signatures with DSA is too slow
- The existence of a second authentication standard will cause hardship to computer hardware and software vendors, who have already standardized on RSA and

- The process by which NIST chose DSA was too secretive and arbitrary

## **Challenge-Response Systems**

As the business transactions on the network are taking the form of a client-server interaction, user authentication has become increasingly important issues in the client-server access. Two most commonly used challenge-response authentication methods are:

- Token or Smart card Authentication
- Third party Authentication

### **Token or Smart card Authentication**

A *smart card* computes a *password* or *encryption keys* and furnish it directly to the host computer for logging-in.

#### **Procedure**

- User log on with a stagnant password
- Host computer issue 8 character password, which the user type into the card.
- Card provide a one-time password that's acceptable.
- Users required to provide a personal identification number (PIN) to defeat against loss or theft.

These card or handheld password generators (HPGs) generate a random password for each access attempt. HPG's algorithm is initialized with "seed" data unique to the user and is synchronized with the host algorithm. HPGs typically work on a challenge-response basis, where, on an access attempt, the host presents the remote user with *some numeric code*. The user then enters that code into the HPG, which responds with the password to be used. Access is granted by the host if the password returned by the user is what would have been calculated by the HPG's algorithm.

### **Third-Party Authentication**

- The password or encryption key is not transmitted over the public network.
- "Authentication server" maintains a file each registered users.
- At log-on time, server prompt for the randomly chosen facts.
- Upon receiving the facts from the user, server generate a token.
- Server transmits an encrypted message containing the token, which can be decoded with the user's key.
- Users are allowed to log on to network services with authenticated token only.

## **Kerberos**

Kerberos is a commonly used third party authentication protocol. Developed by MIT's Project Athena, Kerberos is named for the three-headed dog who, according to Greek mythology, guards the entrance of Hades (rather than the exit, for some reason!).

Kerberos is a secret-key encryption-based system that authenticate users and network connections.

Assumption :

- *Distributed environment is made up of unsecured workstations, moderately secure servers and highly secure key-management machines or server.*
- *IP packets on the network can be read, modified, and inserted by intruder.*

Kerberos employs a client/server architecture and provides user-to-server authentication rather than host-to-host authentication. In this model, security and authentication will be based on secret key technology where every host on the network has its own secret key.

**Kerberos Goal** is to accomplish security

- without relying on authentication by the host computer
- without basing trust on the IP addresses
- without requiring physical security of all the hosts on the network

The Kerberos Server/KDC has two main functions, known as the **Authentication Server (AS)** and **Ticket-Granting Server (TGS)**. The steps in establishing an authenticated session between an application client and the application server are:

1. The Kerberos client software establishes a connection with the Kerberos server's AS function. The AS first authenticates that the client is who it purports to be. The AS then provides the client with a secret key for this login session (the *TGS session key*) and a ticket-granting ticket (TGT), which gives the client permission to talk to the TGS. The ticket has a finite lifetime so that the authentication process is repeated periodically.
2. The client now communicates with the TGS to obtain the Application Server's key so that it (the client) can establish a connection to the service it wants. The client supplies the TGS with the TGS session key and TGT; the TGS responds with an application session key (ASK) and an encrypted form of the Application Server's secret key; this secret key is *never* sent on the network in any other form.
3. The client has now authenticated itself *and* can prove its identity to the Application Server by supplying the Kerberos ticket, application session key, and encrypted Application Server secret key. The Application Server responds with similarly encrypted information to authenticate itself to the client. At this point, the client can

initiate the intended service requests (e.g., Telnet, FTP, HTTP, or e-commerce transaction session establishment).

### **Points to remember**

1. Kerberos does not produce digital signature.
2. Kerberos authenticate requests for network resources rather than to authenticate authorship of documents.
3. Kerberos provide real-time authentication in a distributed environment.

### **Application of Kerberos**

Third party payment servers that grant tickets to clients for usage of some server resources.

Implementation of **NetCash** and **NetCheque**.

**NetCash:** A framework that supports real-time electronic payments with provision of anonymity over an unsecured public network.

**NetCheque** can be used to deposits which authorizes the transfer of account balances from the account against which the check was drawn to the account to which the check was deposited.

### **Encrypting documents and electronic mail**

Encrypting email provide confidentiality and sender authentication. Some of the methods being used are:

- Privacy Enhanced Mail (PEM)
- Pretty Good Privacy (PGP)

### **Privacy Enhanced Mail (PEM)**

- **PEM** includes *encryption*, *authentication*, and *key management*, and allows use of both *private-key* and *secret-key* cryptosystems.
- Supports multiple cryptographic tools: encryption algorithm, digital signature algorithm, hash functions etc.
- Uses *DES algorithm* for encryption and the *RSA algorithm* for sender authentication and key management.
- Supports *non-repudiation*.
- Commercially available PEM: RIPEM (developed by Mark Riordan), but it does not support certificates.

## Pretty Good Privacy (PGP)

- Pretty Good Privacy [developed by Philip Zimmermann] is a widely used private e-mail scheme based on RSA public key cryptosystem.
- Public key (as large as 1024 bits) cryptosystems tend to be very slow. To speed things up, the public key algorithm is used to send a secret key for a symmetric key algorithm.
- In PGP, RSA public-key encryption scheme is used for authentication.
- PGP employs IDEA [International Data Encryption Algorithm], a very popular symmetric key algorithm; to provide confidentiality by encrypting messages.

Key management is one of the bottlenecks for PGP.

## Certification Authority, Certification Policies and Practices

The role of certification authority is important in making secure e-commerce possible. However, the effectiveness of a **certification authority (CA)** depends on its services being recognized as practical, trustworthy, and legally enforceable. Such recognition depends on the certification authority's practices being well-documented and such documentation being made available to the applicable community of interest. This documentation typically takes the form of a **certificate policy (CP)**, a **certification practice statement (CPS)**, and user agreements.

### CP/CPS concepts

The precise relationship between a CP and CPS varies. Typically, CPs state requirements at a high level and CPSs state in detail how such requirements are satisfied. Multiple CPSs may be written that satisfy a particular CP. Certificates issued under any of these CPSs can assert the same CP in an X.509 certificate. CPs are sometimes used as the basis of a decision to use a particular certificate, but recourse to a more detailed CPS is often also necessary. Certificate classes typically distinguish between distinct levels of service and map to a CP or CPS in various ways. One possibility is to have different CPs represent different certificate classes.

Before a commercial certification authority can commence providing service, it should establish its business and legal practices and describe the controls that it will use to ensure trustworthy operations. A CP or CPS typically identifies the service levels available in terms of certificate classes or similar concepts. Certificate formats may be described, usually with reference to a recognized standard such as X.509. Any particular structure that applies to the relationships between certification authorities, such as a hierarchical structure, may be identified. If a certification authority provides a name registration service, the CP or CPS may describe the policies associated with that service, including dispute resolution procedures. The use of a repository should also be described.

## **Certification Authorities and CP/CPS**

Certification authorities must use technologies and procedures that provide a reasonable degree of security and reliability, consistent with the attendant risks and suitable for the applications supported by its services. A CP or CPS, or other document referenced by the CP or CPS, typically describes the information, physical, and personnel security measures. Certification authorities must also have sufficient financial resources to maintain their operations and perform their duties, and they must be reasonably able to bear the applicable risk of liability to subscribers and relying parties.

A CP or CPS typically describes the manner in which certification authorities warrant their services and apportion their liability. This may include general warranties, disclaimers of warranty, and limitations of liability. Enhanced warranty protection or insurance programs may also be described.

A CP or CPS may describe procedures for and implications of certificate suspension, revocation, and expiration.

## **Review Questions**

### **1. What is Certification Practice Statement, or CPS?**

CPS is a public statement of the practices and procedures for issuing and validating Certificates and for supporting reliance on Certificates. May satisfy one or more Certificate Policy and may be established, or accompanied, by a contract which describes the legal responsibility all the concerned parties. Basically document state services supported and practices used throughout the certificate life cycle.

### **2. What are the various levels of a certificate hierarchy?**

**Rudimentary:** The applicant may apply for a certificate through an open net-work such as the Internet and need only provide an e-mail address. The private signature key may exist in software or hardware.

**Basic:** The applicant may apply in person or through a network (via comparison with trusted information in a database or through other trusted means).

**Medium:** The applicant must appear in person before a registration authority, trusted agent, or an entity certified by a state or Federal agency as being authorized to confirm identities. The applicant must present one Federal-government-issued picture ID, or at least two forms of non-Federal- government-issued identification (at least one of which must be a picture ID).

**High:** The applicant must appear in person before a registration authority or trusted agent. The applicant identity validation requirements are consistent with Medium. The private signature key must exist in hardware.

### **3. What are the roles of a Certificate Authority?**

- Enables the generation of key pairs by the end entities

- After the end entity has made itself known to the CA, the CA has authenticated that, the CA:
  - Issues a certificate for that end entity's published key
  - Returns that certificate to the end entity and/or post that certificate in a public repository
- Updates key pairs regularly for the end entity and updates the corresponding certificate
- Refreshes or renews certificates as they expire if nothing relevant in the environment has changed.
- Issues cross certificates to other CAs
- Suspends or revokes certificates
- Issues certificate practice statements to show how its system is trustworthy and conforms to any applicable certificate policy

#### **4. What factors must be considered while choosing a CA?**

- Demonstrated reliable operation
- Implemented trustworthy hardware/software systems
- Personnel checks
- Adequate financial resources
- Has issued an acceptable certificate policy/certificate practice statement
- Reasonable restrictions on liability
- Properly accredited
- Properly cross-recognized

#### **5. What are the various agreements that CA has to make?**

- Certificate Policy
- Certificate Practice Statement
- Registration Authority Agreements
- Subscription Agreements with Customers
- Cross certification Agreements
- Outsourcing Agreements
  - Key escrow agencies (for Key Recovery, in case of Key Lost)
  - Key issuance and management software
  - Time Stamping software
  - Record storage and management entities

#### **6. Why is Key Recovery an issue in PKI?**

Cryptography is so secure that a user cannot recover the private key even when he is given the encryption algorithm, the public key and the cipher text. However, private keys can be lost due to:

- Individual forgetting passwords
- Individual losing physical item storing passwords
- Malicious interference by an employee, former employee, or outsider
- Individual, being fired, become disabled or dying

In such a situation, attacking the cryptographic algorithm to retrieve the private key may be a futile (worthless) attempt. Rather, the key management policies must be properly laid out.

**7. What should be the functions of a CA in case it decides to stop business?**

- Notify other certification authorities in the PKI of its intention to cease acting as a certification authority at least 90 days before cessation.
- Provide to the subscriber of each unrevoked or unexpired certificate it has issued at least 90 day notice of its intention to cease acting as a certification authority.
- Revoke all certificates that remain unrevoked or unexpired at the end of the 90-day notice period, whether or not revocation has been requested by the subscribers.
- Give notice of revocation to each affected subscriber.
- Make a reasonable effort to minimize disruption from cessation of certification services to its subscribers and to persons duly needing to verify digital signatures by reference to the public keys contained in outstanding certificates.
- Make reasonable arrangements for preserving its records.

In the case of a commercial certification authority, pay reasonable restitution (not to exceed the certificate purchase price) to subscribers for premature revocation of their certificates.

## **Electronic payment system**

- The World Wide Web has potential to become a highly efficient electronic marketplace for goods and services, and there is a need for a cash payment system that is scaleable, anonymous and secure.
- When payments are effected electronically, there is always a risk that organizations may resort to gathering information relating individuals with the amounts that they have spent, locations involved and types of good purchased.
- Misuse of such information can give rise to serious breaches of personal privacy.
- If a payment system for the WWW is to receive widespread support, it must offer its users some form of protection against the gathering of such information.
- The most effective method of achieving this is to implement a form of electronic cash, where the coins' being spent cannot be linked with their owner.
- This gives rise to a secondary problem in that since the coin is an electronic quality that is easily duplicated, such a payment system must guard against the coin being spent more than once ( double spending).
- Furthermore, it should not be possible for an attacker to bypass the system or to falsely obtain monetary value from it.
- Therefore new methods of payment are needed to meet the emerging demands of e-commerce. These neo-payment instruments must be secure, have a low processing costs, and be accepted widely as global currency tender. The various issues need to be addressed for such wide acceptance is summarized below:
  - Form and Characteristics of Payment Instruments such as
    - eCash
    - eChecks
    - Credit/debit Card.
  - Financial Risk Management
    - Privacy
    - Fraud
    - Mistakes
    - Bank Failures
  - Security Features
    - Authentication
    - Privacy
    - Anonymity
  - Electronic payment Business Process linking consumers and organizations.

## **Digital/Electronic payment requirement**

For any digital payment system to succeed, the following criteria ought to be satisfied:

| Criteria      | Need for the criteria                              |
|---------------|----------------------------------------------------|
| Acceptability | Payment infrastructure needs to be widely accepted |
| Anonymity     | Identity of the customers should be protected      |

|                |                                                                          |
|----------------|--------------------------------------------------------------------------|
| Convertibility | Digital money should be able to be converted to any type of fund.        |
| Efficiency     | Cost per transaction should be near zero.                                |
| Flexibility    | Several methods of payment should be supported.                          |
| Integration    | Interfaces should be created to support the existing system.             |
| Scalability    | Infrastructure should not breakdown if new customers and merchants join. |
| Security       | Should allow financial transactions over open networks.                  |
| Reliability    | Should avoid single points of failure.                                   |
| Usability      | Payment should be as easy as in the real world.                          |

### **Types of electronic Payment Systems**

Online payments can be broadly divided into three main categories as shown:

1. Banking and Financial Payment –B2B marketplace
  - » Large-scale or wholesale payment
  - » Small scale or retail payment ( ATM )
  - » Home-banking ( Bill payment)
2. Retailing Payment
  - » Credit cards (VISA / Mastercard)
  - » Private label credit/debit card)
  - » Charge card ( American Express)
3. On-line e-Commerce Payment
  - Token-based payment
    - » eCash (Digicash)
    - » eCheque (NetCheques)
    - » Smart Card or debit Cards (Mondex electronic currency card)
  - Credit Card-based payment systems
    - » Encrypted credit-cards ( www form-based encryption)
    - » Third-Party authorization numbers ( eg First-virtual)

### **Electronic Fund Transfer (EFT)**

Research into e-payment systems for consumers can be traced back to the 1940s, and the first applications, credit cards, appeared soon after. In the early 1970s, the emerging electronic payment technology was labeled electronic funds transfer (EFT). EFT is defined as:

*Any Transfer of Fund initiated through an electronic terminal, telephonic instruments or computer or magnetic tape so as to order, instruct or authorize a financial institution to debit/credit an account.*

EFT utilizes computer and telecommunication components both to supply and to transfer money or financial assets. Transfer is information based and intangible.

### **Properties of Paper Money**

- **Negotiable:** Can be traded
- **Act as Legal tender:** payee is obliged to take it.
- **Bearer Instrument:** Possession is a *prima-facie* proof of ownership.
- Can be held without bank account.
- **No risk** on the part of the Acceptor

### **Electronic Cash (or eCash)**

Electronic cash is the electronic equivalent of real paper cash, backed by bank and can be implemented using *RSA public-key cryptography, digital signatures, and blind signatures*.

In electronic cash system there is usually a bank, responsible for issuing currency, customers who have accounts at the bank and can withdraw and deposit currency, and merchants who will accept currency in exchange for goods or a service. Every customer, merchant, and bank has its own public/private key pair. The keys are used to encrypt, for security, and to digitally sign, for authentication, blocks of data that represent coins. A bank digitally signs coins using its private key. Customers and merchants verify the coins using the bank's widely-available public key. Customers sign bank deposits and withdrawals with their private key, and the bank uses the customer's public key to verify the signature. Special client and merchant software is required to use the Ecash system. The client software is called a "cyberwallet" and is responsible for withdrawing and depositing coins from a bank, and paying or receiving coins from a merchant.

The eCash system consists of three main entities:

- **Banks** that mint coins, validate existing coins and exchange real money for eCash.
- **Buyers** who have accounts with a bank, from which they can withdraw and deposit eCcash coins.
- **Merchants** who can accept eCash coins in payment for information, or hard goods. It is also possible for merchants to run a pay-out service where they can pay a client eCash coins.

The **purchase of e-cash** from an online currency (or bank) involves two steps: (i) establishment of an account and (ii) maintaining enough money in the account to back the purchase. Some customers might prefer to purchase e-cash with paper currency, either to maintain anonymity or because they do not have bank account.

Once the tokens are purchased, two types of transactions are possible: ***Bilateral*** and ***Trilateral***. Typically, transactions involving cash are bilateral or two-party (buyer and seller) transactions, whereby the merchant checks the digital signature by using the bank's public key. If satisfied with the payment, the merchant stores the digital currency on his machine and deposits it later in the bank to redeem the face value of the note. Transactions involving financial instruments other than cash are usually trilateral or three-party ( buyer, seller, and bank) transactions, whereby the "notes" are sent to the merchant, who immediately sends them directly to the digital bank to verify the validity of these notes and they have not spent before. The account of the merchant is credited.

## Properties of Electronic Cash

### ■ Monetary Value

- » It must be backed by either by bank, bank-authorized credit, or bank-certified cashier's checks.
- » When e-cash created by one bank is accepted by others, reconciliation must occur without any problems. Stated another way, e-cash without proper bank certification carries the risk that when deposited, it might be returned for insufficient funds.

### ■ Interoperability

- » Exchangeable as payment for other ecash, paper cash, goods or services, line of credit, deposits in banking accounts, bank notes or obligations, electronic benefits transfer.
- » Need of multiple banks with an international clearing house that handles the exchange ability issues because all customers are not going to use the same bank or even in the same country.

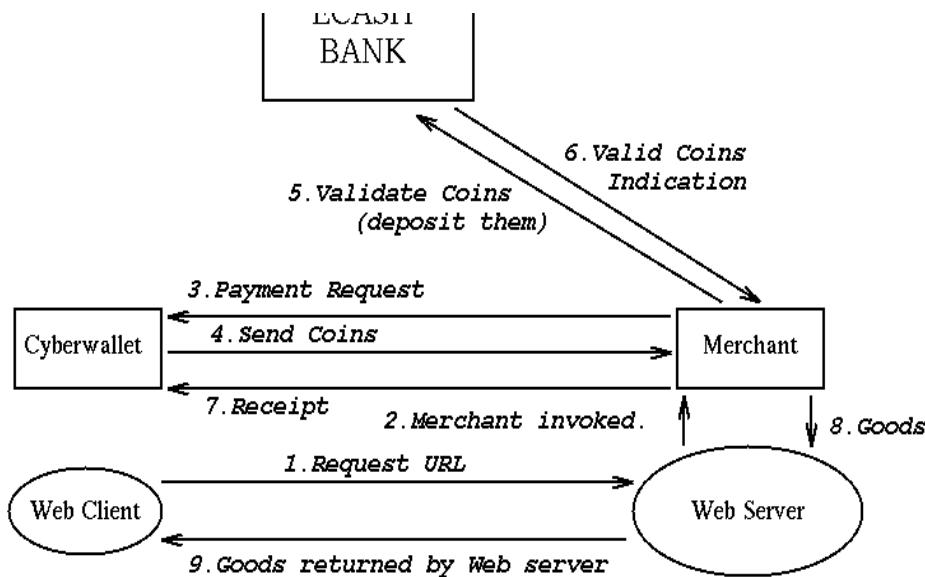
### ■ Retrievability

- » Remote storage and retrieval for exchange e-cash.
- » Use of Mondex card (a pocket size electronic wallet) for storing ecash.

### ■ Security

- » Preventing or detecting duplication and double-spending. Detection is essential in order to audit whether prevention is working or not.

## How Electronic Cash Work?



1. The user's Web client sends a HTTP message requesting the URL to the Merchant's normal Web server. This URL will invoke a Common Gateway Interface (CGI) program.

2. The CGI program invoked will be the merchant Ecash software, and it will be passed details of the item selected encoded in the URL. The location of the buyer's host machine will also be passed in an environment variable from the server to the merchant Ecash software.

3. The merchant software, now contacts the buyer's wallet using a TCP/IP connection, asking it for payment.

4. When the cyberwallet receives this request, it will prompt the user, asking them if they wish to make the payment. If they agree, the cyberwallet will gather together the exact amount of coins and send this as payment to the merchant. The coins will be encrypted with the merchant's public key so that only the merchant can decrypt them:

$\{\text{Coins}\}K[\text{public}, \text{Merchant}]$

If they disagree or do not have the exact denominations necessary to make a correct payment, the merchant is sent a payment refusal message.

5. When the merchant receives the coins in payment, he must verify that they are valid coins, and have not been double spent. To do this he must contact the bank, as only the minting bank can tell whether coins have been spent before or not. Thus the merchant packages the coins, signs the message with his private key, encrypts the message with the bank's public key, and sends it to the bank.

$\{\{\text{Coins}\}K[\text{private}, \text{Merchant}]\}K[\text{public}, \text{Bank}]$

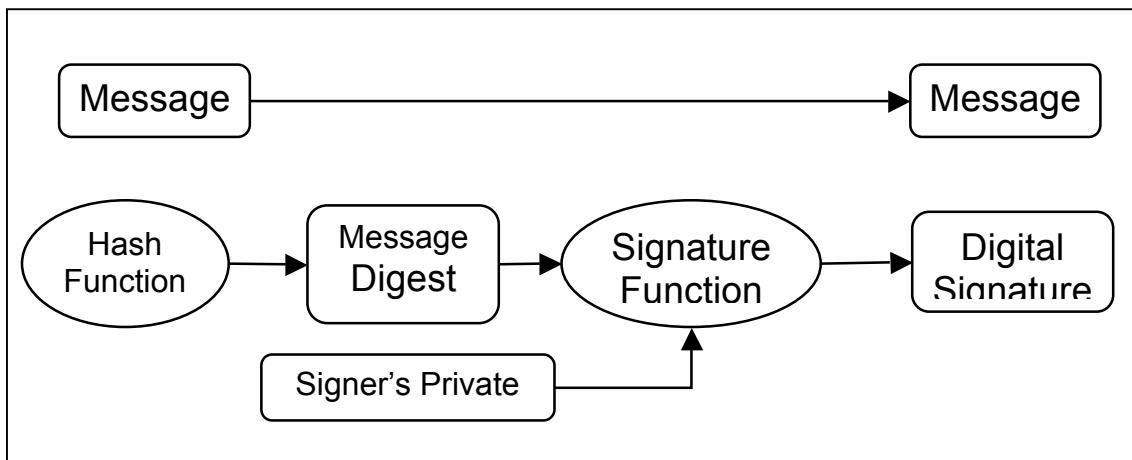
6. The bank validates the coins by checking the serial numbers with the large on-line database of all the serial numbers ever spent and returned to the bank. If the numbers

appear in the database then they are not valid, since they have been spent before. If the serial numbers don't appear in the database, and have the bank's signature on them, then they are valid. The value of the coins are credited to the merchant's account. The coins are destroyed, and the serial numbers added to the database of spent coins. Thus coins are good for one transaction only. The bank notifies the merchant of the successful deposit.

7. Since the deposit was successful, the merchant was paid, and a signed receipt is returned to the buyer's cyberwallet.
8. The purchased item, or an indication of successful purchase of hard goods, is then sent from the merchant Ecash software to the Web Server.
9. The Web server forwards this information to the buyer's Web client.

### **Creation of Digital Signature**

Figure illustrates how digital signature is created by a payer (buyer) with his private key to ensure Authenticity, and no repudiation of the eCash where as Data-integrity and Confidentiality is maintained by encrypting the message and the Digital signature by the payee public key.



### **How to avoid Double Spending?**

When the consumer is issued a bank note, it is issued to that person's license. When he or she gives it to somebody else, it is transferred specifically to that other person's license. Each time the money changes hands, the old owner adds a tiny bit of information to the bank note based on the bank note's serial number and his or her license. If somebody attempts to spend money twice, the bank will now be able to use the two bank notes to determine who the cheater is. Even if the bank notes pass through many different people's hands, whoever cheated will get caught, and none of the other people will ever have to know about the cheat.

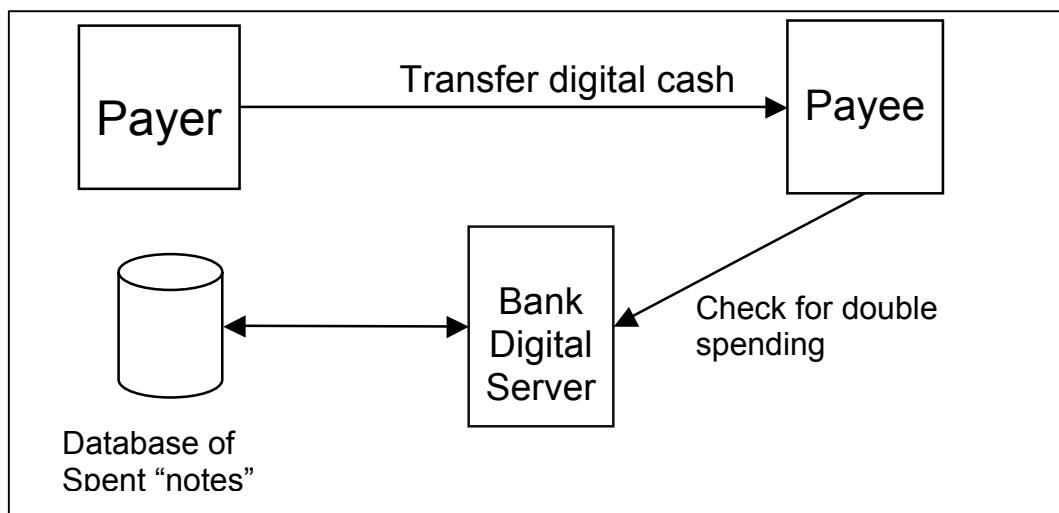


Fig: Detection of double spending

### Advantage of eCash

#### ■ Anonymity

- The electronic cash used is untraceable, due to the blind signatures used when generating coins.

#### ■ Security

- Employ secure protocols using RSA public key cryptography, the Ecash system is safe from eavesdropping, and message tampering . Coins cannot be stolen while they are in transit. However, the protection of coins on the local machine could be strengthened by password protection and encryption.

### Operational risk of eCash

Operational risk associated wit eCash can be mitigated by imposing constraints, such as limits on:

- The time over which a given electronic money is valid,
- The amount than can be stored on and transferred by electronic money,
- The number of exchanges that can take place before money needs to be redeposit with a bank or a financial institution, and
- The number of such transactions that can be made during a given period of time.

### Disadvantage of eCash

One drawback of eCash is its inability to be easily divided into smaller amounts. A number of variations have been developed for dealing with the "change" problem. Customers are issued a single number called "open check" that contains multiple denomination values sufficient for transactions up to prescribed limit.

## **Electronic Checks (eChecks)**

An eCheck is the electronic version or representation of a paper check.

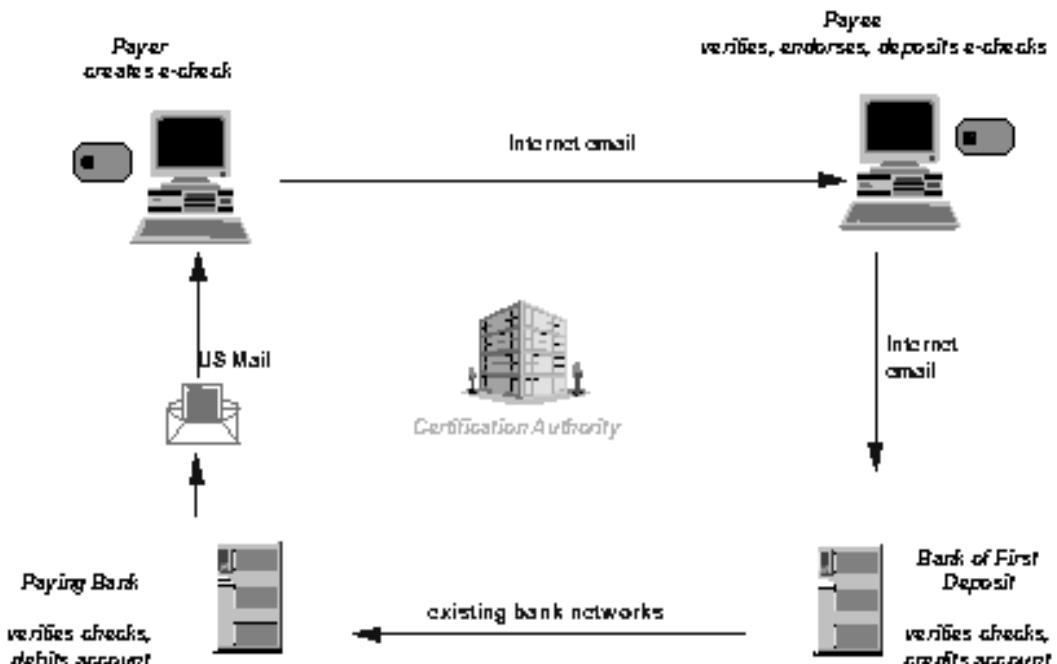
- contains the same information as paper checks such as:
  - » Name of the payer
  - » Name of the financial institute
  - » Payer's account number
  - » Name of the payee
  - » Amount of the check.
- Are based on the same rich legal framework as paper checks.
- Can be linked with unlimited information and exchanged directly between parties.
- Can be used in any and all remote transactions where paper checks are used today.
- Enhance the functions and features provided by bank checking accounts.
- Expand on the usefulness of paper checks by providing value-added information.
- Two core components of technology include:
  - » FSML (Financial Service Markup Language )
  - » Digital Signature (also include endorsement signature by payee)

## **Why use eChecks?**

- eChecks have important new features. They offer:
  - The ability to conduct bank transactions, yet are safe enough to use on the Internet
  - Unlimited, but controlled, information carrying capability
  - Reduces fraud losses for all parties - automatic verification of content and validity
  - Traditional checking features such as stop payments and easy reconciliation
  - Enhanced capabilities such as effective dating
- The eCheck:
  - can be used by all account holders, large and small, even where other electronic payment solutions are too risky, or not appropriate
  - is the most secure payment instrument available today
  - provides rapid and secure settlement of financial obligations
  - can be used with existing checking accounts
  - can be initiated from a variety of hardware platforms and software applications

## **How eChecks Function ?**

## E-check system flow



### At the buyer's side:

- Buyer register with a third-party accounting server ( also acts as a billing server) before he/she is able to able to write electronic checks.
- The registration process may require a credit card or bank account to back the checks.
- Once registered, buyers can contact sellers for goods and/or services and payment can be done in the form of echecks with total amount of purchased items. These checks may be send through email or any other media.

### At the receiving side:

- Forward check to Accounting server ( Billing server) for Authentication and payment.
- Accounting server verifies the Digital signature on the check using the kerberos Authentication scheme.

- eCheck is a special kind of a “token”.
- User’s Digital signature is used to create one ticket - a check – which the seller’s digital “endorsement” transforms into another- An order to bank for EFT.
- When deposited, the check authorizes the transfer of account balances from the account against which the check was drawn to the account to which the check was deposited.

### **Advantages of eChecks**

- Ease of use as it works in the same as the traditional checks.
- Well suited for clearing micro-payments.
- Use of conventional cryptography makes it faster.
- Create float by charging the buyer or seller a transaction fee.
- Financial risk is assumed by the accounting server resulting in easier acceptance.
- Reliability and scalability by multiple accounting server.
- Interaccount server protocol to allow buyer and seller to belong to different domains, regions or countries.

### **Smart Cards**

Smart Cards are credit/debit cards and other card products enhanced with microchip capable of holding more information than the traditional magnetic strip. (Estimate to be 80 times more than a magnetic strip).

The money on the card is saved in an encrypted form and is protected by a password to ensure the security of the smart card solution.

Smart Cards are basically of two types:

- Relationship-based smart credit cards
- Electronic purses (or debit card or electronic money)

### **Relationship-based smart card**

It is an enhancement of existing card services and/or the addition of new services that a financial institute delivers to its customers via a chip-based card or other device.

The new services may include:

- access to multiple financial accounts
- Value-added marketing programs
- Other information as per the card holder may want to store such as name, birth date, personal shopping preferences, and actual purchase records.

These information will enable merchants to accurately track consumer behavior and develop promotional programs designed to increase shopper loyalty.

The following offers are expected to provide by relationship-based products:

- Access to multiple accounts, such as debit, credit, investments or stored value for e-cash, on one card or an electronic device.
- A variety of functions - such as cash access, bill payment, balance inquiry, or fund transfer for selected accounts.
- Multiple access options at multiple locations using multiple device types, such as ATM ( automated teller machine), a screen phone, a PC, A PDA ( Personal digital assistant), or Interactive TVs

### **Electronic Purses and Debit cards**

These are wallet-sized smart cards embedded with programmable microchips that store sums of money for people to use instead of cash.

#### **How electronic purse works?**

- Purse is loaded with money, at an ATM or from any authorized entity/bank.
- While payment, card reader verify authentication of the payer and availability of sufficient funds.
- If valid, the value of purchase is deducted from the balance on the card and added to an e-cash account of the payee and the remaining balance is displayed.
- When the balance on the electronic purse is depleted, the purse can be recharged with more money

#### **Advantages of Smart Cards**

- Direct Exchange of money without the need for intermediaries.
- Ease of use
- Secured
- Both online-and-offline operations possible.
- Low transaction costs from the merchant side.
- Guarantee Anonymity

#### **Credit Card based electronic payment system**

Credit card payments are nowadays the most common and preferred post-payment method on the Internet. Credit cards have proved popular for a number of reasons as follows:

- The system is familiar to users and was widely used before the advent of e-commerce, this bolstering the users' confidence.

- Transaction costs are hidden from users (i.e. basically met by the sellers, and passed on to all customers, not just credit card users.)
- Payment is simple anywhere and in any currency, thus matching the global reach of the Internet.
- The credit issuing company shares the transaction risk; helping overcome consumers' fear and reluctance to buy goods they have not actually seen, from the sellers they do not know.

The disadvantages of Credit Cards for e-Commerce include the fact that they cannot be used directly for small value payments or peer-to-peer transactions.

### **Disadvantages**

- Relatively high transaction cost for small-value payments.
- Does not support peer-to-peer transaction
- Protecting the security of transaction is vital, especially in the virtual world where there is no payment guarantee to the merchant by a bank.

### **A Classification of Credit Cards-Based Payment**

Credit card payment on online networks can be classified into the following three basic categories:

**1. Payment using plain credit card information.** The easiest method of payment is the exchange of (unencrypted) credit cards over a public network such as telephone lines or the Internet. The low level of security inherent in the design of the Internet makes this method problematic. Authentication is also a problem as the merchant is usually responsible to ensure that the person using the credit card is its owner.

**2. Payment using encrypted credit card information.** Encrypting credit card information is a solution to the problems inherent in above category. However, one concern here is the cost of the transaction itself, which could prohibit low-value payments (micro-payments).

**3. Payment using third-party verification.** One solution to security and verification problems is the introduction of a third-party, such as **First Virtual**, which is a company that collects and approves payments from one client to another. After a certain period of time for processing, one credit card transaction for the total accumulated amount is completed.

### **Benefits of Credit Card**

There are various benefits of accepting credit cards, both from the business's perspective and from the consumer's perspective, and we evaluate each of these.

## **The Business Perspective**

- A "Cashless" Society
- Improvement In Sales
- Impulse Sales : Turn Browsers Into Buyers
- Increased Profits
- Reduced Expenses
- Security
- Cheque Problems
- Pre-Approvals of funds
- Efficient than checks
- Working Capital
- Competition

## **The Consumer Perspective**

- Convenience
- No Benefit Of Doubt
- Credibility
- Cheque/Cash Problems
- Security Deposits
- Limitations Of Credit Cards-Based Payment

Despite of numerous advantages of using credit cards mentioned above, there are certain limitations. One disadvantage to credit cards, from the consumer's viewpoint, is that their transactions are ***not anonymous***. Credit card companies do use this to their advantage by compiling data based on spending habits. Another limitation is the ***potential bottleneck*** due to the complexity of ***verification phase*** in a credit card processing. Encryption and transaction speed need to be balanced to avoid long waits at the customer's end. There are also questions of ***reliability*** of the infrastructure under component failures and ***system overload conditions***.

## **Getting a Merchant Account**

In order to accept credit cards, you must apply for a ***merchant account***. Historically, merchant account status was granted only to a bank's preferred customers who had been in business longer than two years and had a storefront. Financial statements, copies of tax returns, and, in some cases, a substantial credit reserve, were required. Due to growing credit card fraud, banks have become more selective, and many business owners have been denied merchant account status regardless of the quality or term of their existing bank relationship.

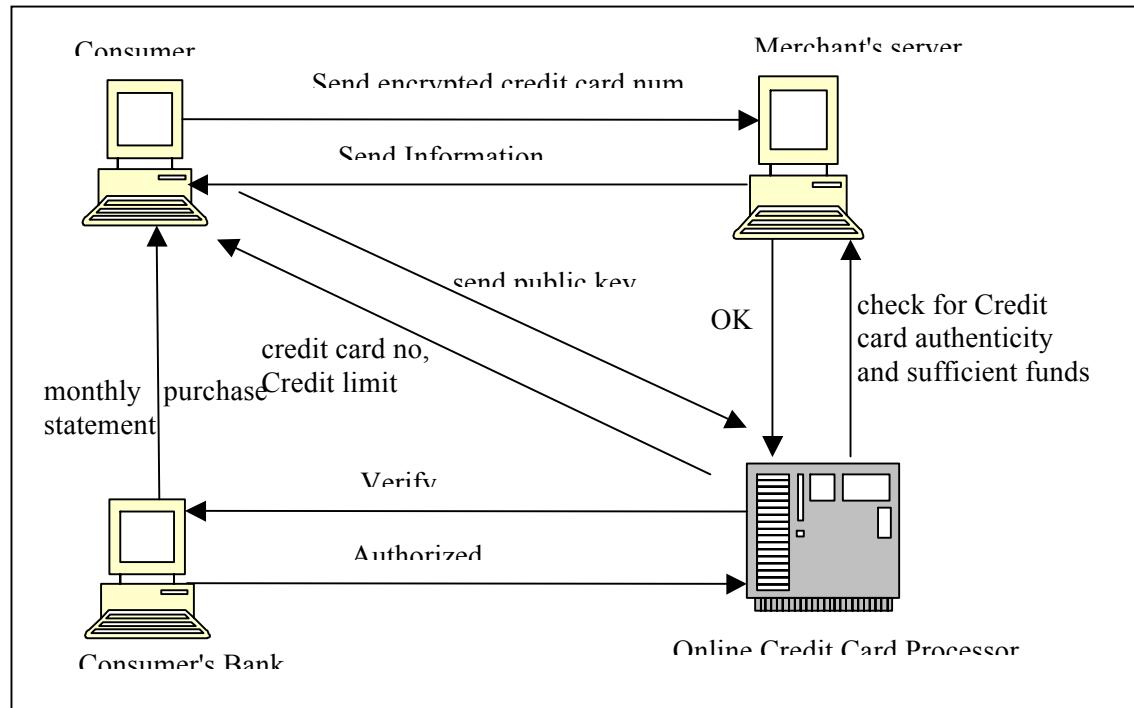
## **Security Issues and Encryption of Credit Cards**

While it is possible to take and transmit credit card information on non-secure WWW pages or via e-mail, this is not very safe. Encryption is initiated when credit card

information is entered into a browser or other e-commerce device and sent securely over the network from buyer to seller as an encrypted message. This practice however, does not meet the important requirements of an adequate financial system, such as non-refutability, speed, safety, privacy and security. To make a credit card transaction truly secure and nonrefutable, the following sequence of steps must occur before actual goods, services, or fund flow:

1. A customer presents his or her credit card information ( along with an authenticity signature or other information) securely to the merchant.
2. The merchant validates the customer's identity as the owner of the card account.
3. The merchant relays the credit card charge information and signature to its bank or online credit card processors.
4. The bank or processing party relays the information to the customer's bank for authorization approval.
5. The customer's bank returns the credit card data, charge authentication, and authorization to the merchant.

In this scheme, each consumer and vendor generates a public key and a secret key. The public key is sent to the credit card company and put on its public key server. The secret key is encrypted with a password, and an unencrypted version is erased. The credit card company sends the consumer a credit card number and a credit limit.



## **The secure e-payment Process Method**

Secure payment transaction system is critical to e-commerce. Without a secured payment transaction system, does not matter robust is the technology and business model being adopted, e-commerce will be a castle built on the sand.

There are two common standards used for secure e-payments such as:

- Secure Socket Layer (SSL)
- Secure Electronic Transaction (SET)

### **Secure Socket Layer (SSL)**

Netscape developed a protocol in 1994 known as Secure Sockets Layer (SSL), which is built into Netscape and Internet Explorer. Most people use this security protocol without even knowing it; when you see that little padlock or key icon in your browser window, SSL is running.

SSL is a secure socket layer between HTTP and TCP on the web server and provides a transport layer security protocol. It establishes a secure encrypted communication channel between two computers. Communicating parties use that channel to exchange data in a confidential manner. SSL also enables both parties to check the integrity of that data and optionally, to authenticate each other. SSL was designed to be a generic secure communication protocol - not a payment protocol.

#### **Why is SSL so widely used? Why is it not good enough for e-payments?**

SSL is the foundation of most secure e-commerce transactions today. From encrypting sensitive payment details to verifying the authenticity of a web site, SSL provides sufficient security for e-commerce. In the context of electronic payments, SSL allows the cardholder to transmit their payment details to the merchant's server in a secure manner. SSL is widely used by e-commerce sites; it provides a private, reliable connection between client and server computers. At the heart of SSL is a form of electronic identification called a *digital certificate*. These certificates rely on *public key cryptography* to *authenticate* users or devices, and to securely exchange the cryptographic information necessary to ensure privacy on the communication channel. While SSL is designed to allow both ends of a connection to authenticate the other with certificates, usually the client does not authenticate itself; only the server sends its certificate. While SSL is the protocol of choice today to secure Web transactions, most implementations do not authenticate the client (i.e., the user). Thus, there is a major gap in the security it provides.

SSL-based e-payments suffer because:

- No mechanism to provide strong authentication of the cardholder or merchant
- No controls over what that merchant does with the cardholder's payment details.
- Lack of policy and legal frameworks to allow a customer to trust a merchant.

Despite these issues, SSL is now a de facto standard in the payments industry.

## Secure Electronic Transaction (SET)

In 1996 Visa and MasterCard developed the SET protocol. It was designed to provide trusted electronic transactions. This would provide security to all parties involved in the transaction and address many of the limitations associated with an SSL-only transaction such as client Authentication.

SET is an open standard, now managed by SETCo LLC . SET defines four components – a Certificate Authority, Cardholder Wallet, Merchant SET Modules and Payment Gateways - any of which a technology vendor may implement.

The SET specifications include the following:

**Highly Secure** - The transmission of credit card information can be transmitted over public networks using strong encryption technologies.

**Low visibility** - Only the information a partner needs to see is displayed. The merchant does not need to see the credit card information and the bank does not need to see which orders have been placed.

**Recognized standards** - Transaction flows, the message formats, integrity, authentication, confidentiality and encryption algorithms are all defined in the SET standards.

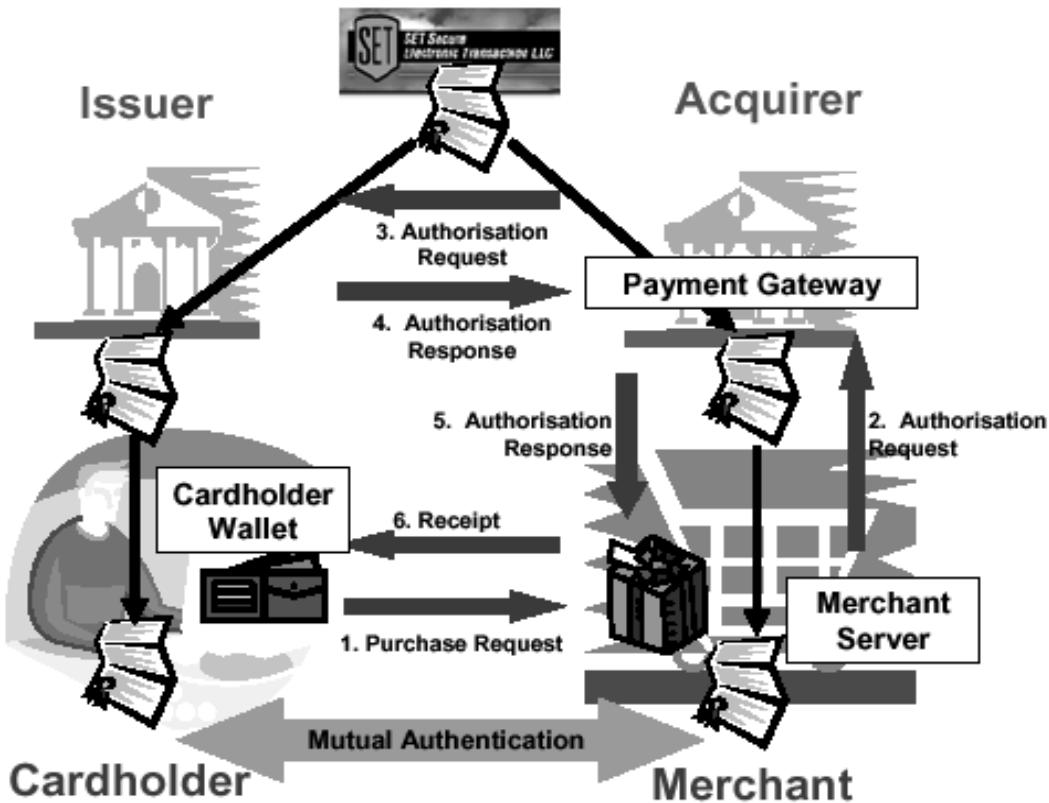
**Non-repudiation** - The SET standards defines a public key infrastructure, which is used for verification of the participants and to encrypt/decrypt the messages sent between the partners. A digital signature is used to identify the participants.

Just as with SSL, digital certificates form the foundation of SET security. In contrast to SSL, however, SET requires customers to possess certificates so merchants and banks can verify their identities as legitimate cardholders. Thus the protocol adds another layer of trust to an e-commerce transaction.

To use SET for payment, users must obtain a certificate. An organization known as a certificate authority (CA) issues digital certificates to customers. In the case of SET, the bank issuing a credit card might act as the CA.

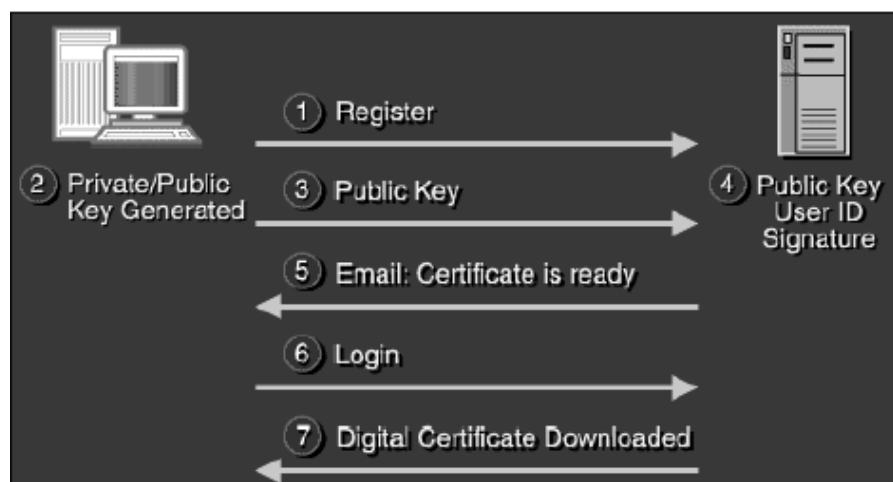
SET requires cardholder, merchant and acquirer software, and some components of a Public Key Infrastructure (PKI) to support the trust architecture. SET allows the cardholder and merchant to authenticate each other with digital certificates before a transaction. The cardholder is sure they are dealing with a legitimate merchant, and the merchant has proof that the cardholder is authorized to use the selected card. Once this trust is established, both parties can exchange transaction information. SET uses a ‘fat

wallet': a large application installed on the cardholder's PC to hold payment details and perform the SET transaction for the cardholder.



### Using SET and Certification Authority (CA)

To use SET for payment, users must obtain a certificate. An organization which is known as a certificate authority (CA) issues digital certificates to customers. In the case of SET, the bank issuing a credit card might act as the CA. The following visual generically illustrates how a customer might obtain a certificate from a CA. The following visual generically illustrates how a customer might obtain a certificate from a CA.



The steps in the visual are described below.

1. The customer registers at the certificate authority's (CA) website.
  - The CA could be a recognized authority such as VeriSign or the customer's bank.
  - User information includes a social security, driver's license, or passport number to uniquely identify the user.
  - A username (likely an email address) and password are selected for future interactions with the site.
  - Credit card information is submitted for payment (if required).
  - Other details such as key strength (e.g., 2048 bit key length) and certificate extensions can also be selected.
2. The customer's browser software (e.g., Netscape) generates a public and private key pair.
  - The RSA public key algorithm is most commonly used to generate the key pairs.
  - The public key is a publicly distributed value that other people/sites use to authenticate the user and send encrypted information to the user.
  - The private key decrypts messages sent to the user.
3. The browser sends the public key to the CA server.
  - The private key should always be kept secured on the user machine and never transmitted over the Internet.
4. The CA generates the user's certificate. The certificate includes the items below.
  - The user's public key (submitted in Step 3)
  - ID information (submitted in Step 1)
  - The CA's digital signature, binding the key to the user's identity.
5. When the certificate has been created, the CA notifies the user.
  - The process usually takes less than one hour.
  - An email is sent to the address provided during registration.
  - A URL to the certificate is generally provided in the notification message.
6. The customer logs onto the CA website.
  - Clicking on the link in the email takes the user directly to the certificate download area.
  - The customer supplies his/her username and password (chosen in Step 1).
  - After reviewing the certificate information, the user clicks on a download button to retrieve the certificate.
7. The certificate is downloaded and installed.
  - This is generally an automated process within browser programs.
  - The browser usually stores certificates on the local hard drive in a certificate database, which should be password protected.

- Information about the user's certificates (as well as those belonging to other people and websites) is available to the user via the browser interface.

In the steps above, the only unencrypted information sent across the Internet is the notification email. As long as the customer has chosen a good password, this should not compromise the certificate retrieval process. All the connections to the CA's website will most likely be secured using Secure Sockets Layer.

## **Marketing and Advertising**

### **Internet Marketing- an Introduction**

At its core, the mission of marketing is to attract and retain customers. To accomplish this goal, a traditional bricks-and-mortar marketer uses a variety of marketing variables—including pricing, advertising, and channel choice—to satisfy current and new customers. In this context, the standard marketing-mix toolkit includes such mass-marketing levers as television advertising, direct mail, and public relations, as well as customer-specific marketing techniques such as the use of sales reps.

With the emergence of the Internet and its associated technology-enabled, *screen-to-face* interfaces (e.g., mobile phones, interactive television), a new era of marketing has emerged. In short, these are new, exciting changes that have a profound impact on the practice of marketing. At the same time, some of the fundamentals of business strategy—seeking competitive advantage based on superior value, building unique resources, and positioning in the minds of customers—have remained the same.

Frameworks such as the 4Ps of marketing or the five forces of competitive analysis are important because they provide easy-to-remember, simplifying structures for complex problems. They also serve as guides to managerial action. Thus, understanding the five forces enables firms to comprehensively map their competitive environment while simultaneously identifying specific actions for their managers.

### **Marketing Strategies for the Web**

|                  |                                                                                            |
|------------------|--------------------------------------------------------------------------------------------|
| ▪ Brands         | Web site becomes most important brand                                                      |
| ▪ Change         | The rules on the Internet are changing                                                     |
| ▪ Conciseness    | Keep page short and spread information on several pages                                    |
| ▪ Content        | Content is king, don't bore customer.                                                      |
| ▪ Dynamic Sites  | Create dynamic sites that use new technologies to adapt information based on user profiles |
| ▪ Finances       | Try new market with low advertising pricing schemes.                                       |
| ▪ Free Give-away | Create freebee offerings for loyal customers                                               |
| ▪ Global Village | Think global, but localize                                                                 |
| ▪ Live Events    | Online events create awareness fast                                                        |
| ▪ Niche Markets  | The Internet is a series of niche markets and mass markets                                 |
| ▪ Promotion      | Promote site everywhere                                                                    |
| ▪ Syndication    | Co-brand services and products                                                             |
| ▪ Technology     | Use Internet technology to maximize marketing objectives                                   |

### **DEFINITION AND SCOPE OF INTERNET MARKETING**

Marketing is a way of managing a business so that each important business decision is made with full knowledge of the impact it will have to the customer. It deals with all the steps between determining customer needs and supplying them at a profit. It entails

drawing a management plan that views all marketing components as a part of a total system that requires effective strategic planning, organization, leadership and control.

Marketing has two underlying assumptions: (1) all company policies and activities should be aimed at satisfying customer needs and (2) profitable sales volume is a better company goal than maximum sale volume.

It is perhaps best to begin with the basic American Marketing Association definition of marketing:

*Marketing is the process of planning and executing the conception, pricing, promotion, and distribution of ideas, goods, and services to create exchanges that satisfy individual and organizational goals.*

*Selling* is often used as an equivalent term for marketing, although this is not the case. The sales approach almost always focuses on *volume*, while the marketing approach focus on *profit*. In short, under the sales approach, the *customer exists for the business*, while under the marketing approach, the *business exists for the customer*.

### **The Basics: What Is Marketing?**

The definition summarized above has four critical features. These are:

**Marketing Is a Process.** A process is a particular method of doing an activity, generally involving a series of steps or operations. The classical marketing approach involves four broad steps: *market analysis, market planning, implementation, and control*. Market analysis involves searching for opportunities in the marketplace, upon which a particular firm—with unique skills—can capitalize. Market planning requires segmentation, target market choice, positioning, and the design of the marketing mix (also termed the 4Ps, or marketing program). Market implementation includes the systems and processes to go to market with the marketing program. Finally, marketing control refers to the informal and formal mechanisms that marketing managers can use to keep the marketing program on course. Analysis, planning, implementation, and control collectively provide a process for marketing managers to follow in the design and execution of marketing programs.

**It Involves a Mix of Product, Pricing, Promotion, and Distribution.** Strong marketing programs do not involve one action, such as the design of a great product. Rather, the most successful marketing programs involve *mixing* the ingredients of marketing to deliver value to customers. This mixing entails blending the right amounts of the 4P ingredients, at the right time, and in the right sequence. Too often, marketing programs fail because they allocate too many (or too few) resources in an uncoordinated way.

**It Is About Exchange.** Marketing is not successful unless two parties exchange something of value. The *buyer* may exchange time, money, or services, while the *seller* must exchange something of value to the buyer. The traditional retail context provides the simplest illustration of this principle. A given consumer exchanges money for a particular good or service. However, exchange also occurs in a wide variety of contexts, many of

which are non-monetary. These include bartering, volunteering services, and political donations. It Is Intended to Satisfy Individual and Organizational Needs. The aim of marketing is to provide a satisfactory outcome for both the firm and the customer. Firms can have highly satisfied customers if they provide services for free. However, those organizations are not likely to have a long life. The key to modern marketing is simultaneously satisfying the customer, the firm, and its shareholders. In the long run, the firm must have a positive cash flow or show a clear path to profitability for investors to maintain confidence.

## **What is Internet Marketing?**

If traditional marketing is about creating exchanges that simultaneously satisfy the firm and customers, what is Internet marketing?

*Internet marketing is the process of building and maintaining customer relationships through online activities to facilitate the exchange of ideas, products, and services that satisfy the goals of both parties.*

This definition can be divided into five components:

**Process:** Like a traditional-marketing program, an Internet-marketing program involves a process. The seven stages of the Internet-marketing program process are setting corporate and business-unit strategy, framing the market opportunity, formulating the marketing strategy, designing the customer experience, designing the marketing program, crafting the customer interface, and evaluating the results of the marketing program. These seven stages must be coordinated and internally consistent. While the process can be described in a simple linear fashion, the marketing strategist often has to loop back and forth during the seven stages.

**Building and Maintaining Customer Relationships:** The goal of marketing is to build and create lasting customer relationships. Hence, the focal point shifts from *finding* customers to *nurturing* a sufficient number of committed, loyal customers. Successful marketing programs move target customers through three stages of relationship building: *awareness, exploration, and commitment*. It is important to stress that the goal of Internet marketing is not simply building relationships with online customers. Rather, the goal is to build offline (as relevant) as well as online relationships. The Internet marketing program may well be part of a broader campaign to satisfy customers who use both online and offline services.

**Online:** By definition, Internet marketing deals with levers that are available in the world of the Internet. However, as noted above, the success of an Internet marketing program may rest with traditional, offline marketing vehicles. Consider, for example, the recruiting and job-seeking service Monster.com. Monster's success can be tied directly to the effectiveness of its television advertising and, in particular, its widely successful Super Bowl ads of the past two years.

**Exchange:** At the core of both online and offline marketing programs is the concept of exchange. In both the online and offline worlds, exchange is still the heart of marketing. In the new economy, firms must be very sensitive to cross-channel exchanges. That is, an online marketing program must be evaluated according to its overall exchange impact—not just the online exchange impact. Hence, online marketing may produce exchanges in retail stores. Firms must be increasingly sensitive to these cross-channel effects if they are to measure the independent effects of online and offline marketing programs.

**Satisfaction of Goals of Both Parties:** One of the authors of this book is a loyal user of the website weather.com. Each day he arises and checks the weather in his city as well as the weather in cities he will be traveling to during the week. He is clearly satisfied with and loyal to the site. To the extent that weather.com can monetize this loyalty—most likely, in the form of advertising revenue—both parties will be satisfied.

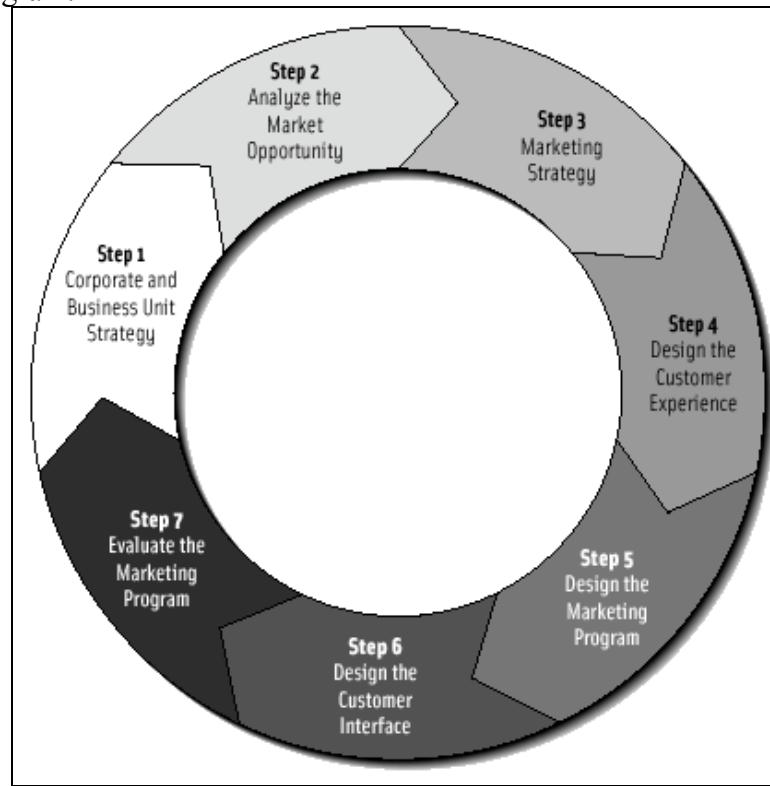
However, if the firm is unable to meet its financial obligations to employees, suppliers, or shareholders, then the exchange is unbalanced. Customers are still happy, but the firm is unable to sustain its revenue model. Both parties must be satisfied for exchange to continue.

### Nature of Marketing in the Electronic Commerce Environment

|                                                 | Mass marketing                                             | Direct marketing                                            | Interactive marketing                                                             |
|-------------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------|-----------------------------------------------------------------------------------|
| Distribution Channel                            | Broadcast and print media (consumer is passive)            | Postal service using mailing lists (consumer is passive)    | The internet (consumer is active and is the catalyst for what is shown on screen) |
| Market Strategy (sample products)               | High Volume (food, autos, personal and home-care products) | Targeted Goods (Credit cards, travel, autos, subscriptions) | Targeted audience (services and all types of product information)                 |
| Enabling technology                             | Storyboard, DTP                                            | Databases and statistical tools                             | Information servers, client browsers, bulletin boards, and software agent.        |
| Authors of marketing material                   | Ad agencies                                                | Ad Agencies and companies                                   | Companies and consumers                                                           |
| Expected outcome from successful Implementation | Volume sales                                               | Bounded sales, data for analysis.                           | Data for analysis, customer relationships, new product ideas, volume sales)       |

### THE SEVEN STAGES OF INTERNET MARKETING

Fig shows an overview of the seven stages of Internet marketing. The seven stages are these: setting corporate and business-unit strategy, framing the market opportunity, formulating the marketing strategy, designing the customer experience, designing the marketing program, crafting the customer interface, and evaluating the results of the marketing program.



### **Stage One: Setting Corporate and Business-Unit Strategy**

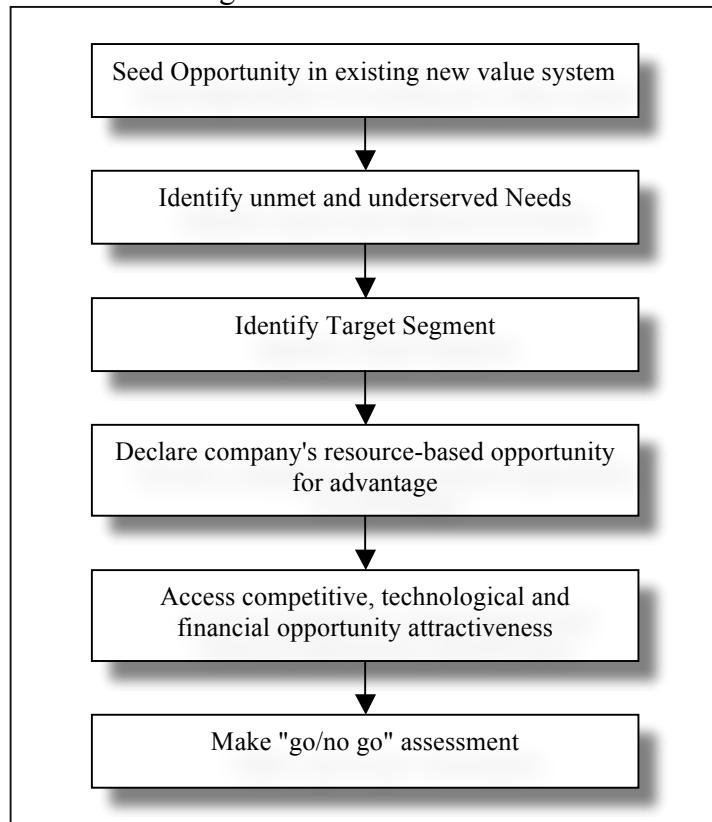
Corporate strategy addresses the interrelationship between the various business units in a firm, including decisions about which units should be kept, sold, or augmented. Business-unit strategy focuses on how a particular unit in the company attacks a market to gain competitive advantage.

Consider, for example, Amazon.com. Corporate-strategy issues relate to the choice, mix, and number of business units such as kitchen, music, electronics, books, and tools/hardware. Once these business units are established and incubated in Amazon's corporate head-quarters, the senior leadership team of each unit sets the strategic direction and steers the business unit toward its goals.

### **Stage Two: Framing the Market Opportunity**

Stage two entails the analysis of market opportunities and an initial first pass of the business concept—that is, collecting sufficient online and offline data to establish the burden of proof of opportunity assessment. Let's say, for example, that you are running a major dot-com business such as Amazon. The senior management team is continually

confronted with go/no-go decisions about whether to add a new business unit or develop a new product line within an existing business unit. What mechanism do they put in place to evaluate these opportunities? In this second part of the Internet-marketing process, a simple six-step methodology helps evaluate the attractiveness of the opportunity as shown in the diagram.



The six steps include: seeding the opportunity, specifying unmet or underserved customer needs, identifying the target segment, declaring the company's resource-based opportunity for advantage, assessing opportunity attractiveness, and making the final go/no-go decision. The final go/no-go choice is often a corporate or business-unit decision.

However, it is very important to stress that marketing plays a critical role in this market-opportunity assessment phase. In order for the firm to make an informed choice about the opportunity, the management team needs to obtain a sufficient picture of the marketplace and a clear articulation of the customer experience that is at the core of the opportunity. Thus, during the market-opportunity assessment phase, the firm also needs to collect sufficient market research data.

### **Stage Three: Formulating the Marketing Strategy**

Internet marketing strategy is based upon corporate, business-unit, and overall marketing strategies of the firm. This set of linkages is shown in diagram below. The marketing strategy goals, resources, and sequencing of actions must be tightly aligned with the business-unit strategy. Finally, the overall marketing strategy comprises both offline and online marketing activities.

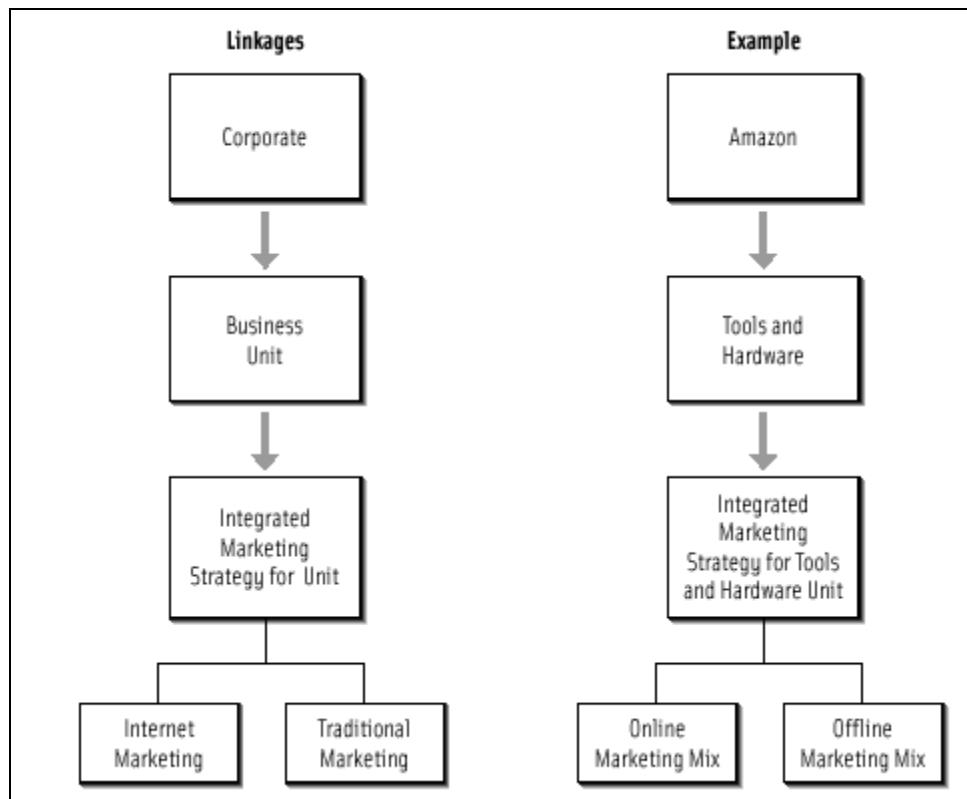


Fig: Corporate, business-unit, and marketing strategy

#### **Stage Four: Designing the Customer Experience**

Firms must understand the type of customer experience that needs to be delivered to meet the market opportunity. The experience should correlate with the firm's positioning and marketing strategy. Thus, the design of the customer experience constitutes a bridge between the high-level marketing strategy (step three) and the marketing program tactics (step five).

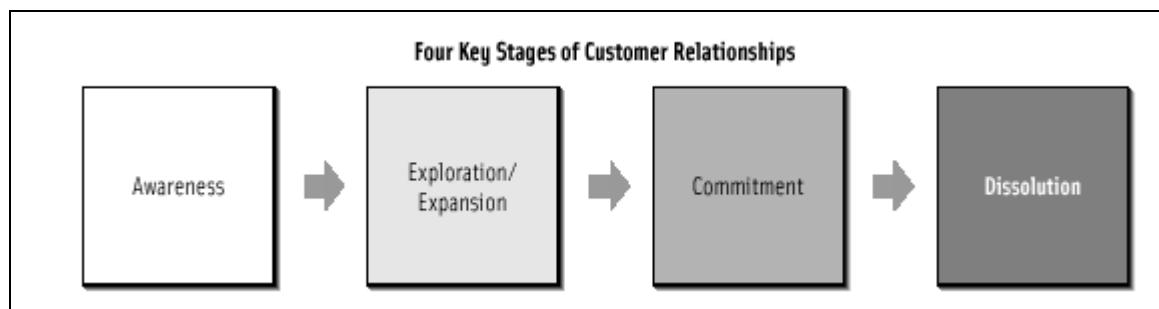
#### **Stage Five: Designing the Marketing Program**

The completion of stages one through four results in clear strategic direction for the firm. The firm has made a go/no-go decision on a particular option. Moreover, it has decided upon the target segment and the specific position that it wishes to own in the minds of the target customer. Stage five entails designing a particular combination of marketing actions (termed levers) to move target customers from awareness to commitment. The framework used to accomplish this task is the Marketspace Matrix. Simply put, the Internet marketer has six classes of levers (e.g., pricing, community) that can be used to create target customer awareness, exploration, and, it is hoped, commitment to the firm's offering. However, prior to discussion of the Marketspace Matrix, the stages of the

customer relationship and the associated classes of levers that can be employed must be defined.

**Building and Nurturing Customer Relationships:** A relationship can be defined as a bond or connection between the firm and its customers. This bond can originate from cognitive or emotional sources. The connection may manifest itself in a deep, intense commitment to the brand or a simple, functional-based commitment (e.g., regular use of weather.com). Whether defined as a function or an organization-wide culture, marketing is responsible for acquiring and retaining target customers. In this process, successful marketers manage to move desirable customers from awareness through exploration and, finally, commitment. Once customers reach commitment, the firm is in a position to observe their behavior patterns and determine which customers to nurture and which customers to terminate (or serve at a lower level of cost).

Managing this building and pruning process is one of marketing's key tasks. The four stages of customer relationships are briefly outlined below.



**Awareness:** When customers have some basic information, knowledge, or attitudes about a firm or its offerings but have not initiated any communications with the firm, they are in the awareness stage. Consumers become aware of firms through a variety of sources, including word-of-mouth, traditional marketing such as television advertising, and online marketing programs such as banner ads. Awareness is the first step in a potentially deeper relationship with the firm. However, as one can imagine, awareness without action is not in the best interests of the firm.

**Exploration:** In the exploration stage, the customers (and firm) begin to initiate communications and actions that enable an evaluation of whether or not to pursue a deeper connection. This stage is also likely to include some trial on the part of the customer. Exploration is analogous to sampling songs, going on a first date, or test-driving a car. In the online world, exploration may take the form of frequent site visits, some e-commerce retail exchanges, and possibly even the return of merchandise. It may include phone call follow-ups on delivery times or e-mails about product inventory. The exploration stage may take only a few visits or perhaps years to unfold.

**Commitment:** In this context, commitment involves feeling a sense of obligation or responsibility for a product or firm. When customers commit to a website, their repeated, enduring attitudes and behaviors reflect loyalty. Commitment is a state of mind (e.g., I strongly prefer Amazon.com over Barnes & Noble.com) as well as a pattern of behavior (e.g., 9 out of 10 of my book purchases are made through Amazon). One direct measure

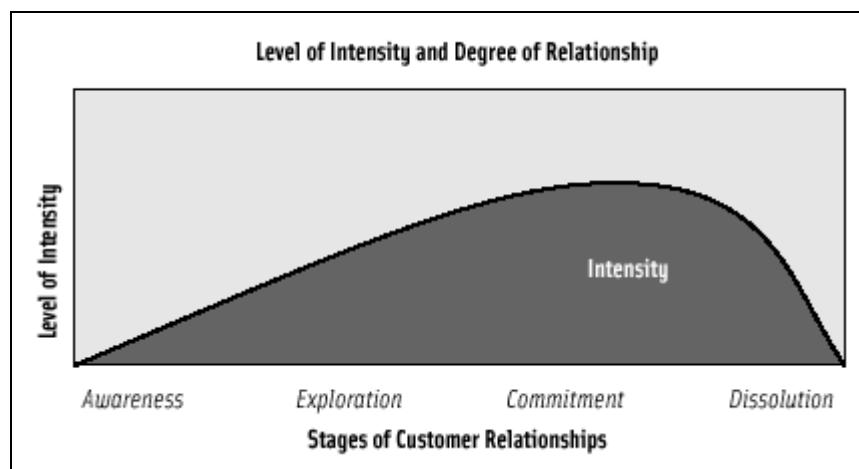
of commitment to a particular site is the extent to which the individual has invested in *customizing the site* (e.g., creating a Myweather page on weather.com).

**Dissolution:** Not all customers are equally valuable to the firm. In an industrial-marketing context, managers often refer to the 80/20 rule of profitability. That is, 20 percent of customers provide 80 percent of the profit. By implication, therefore, a large number of customers are unprofitable or have high cost to serve. Firms should segment their most valuable and less valuable customers. The most valuable customers may be identified based on profit, revenue, and/or strategic significance (e.g., a large well-regarded customer may not be profitable but opens the door to new accounts). The firm does not want this set of customers to terminate the relationship. Unprofitable, non-strategic customers are a different matter. Often it is in the best interests of the firm to terminate the relationship or encourage this set of customers to disengage with the firm.

The four stages vary by the intensity of the connection between the firm and the customer (see figure below). Intensity of connection may be defined as the degree or amount of connection that unfolds between the firm and its target customers.

Three dimensions capture intensity:

1. The frequency of the connection. (How often does the customer visit the site?)
2. The scope of the connection. (How many different points of contact does the customer have with the firm?)
3. The depth of contact. (How thoroughly is the customer using the site?)



A customer might visit a website such as Amazon on a regular basis, but only to purchase books. This visitor would have a high level of frequent contact but a low level of scope. Another customer might visit Amazon frequently but not stay on the site for a long duration or engage in deeper connections such as writing reviews, commenting on products, or communicating with other Amazon users. This customer would have high frequency but low depth. In all cases, relationship intensity is correlated with the stage of the relationship.

**The Internet Marketing Mix:** The traditional 4Ps of marketing are *product, price, promotion, and place/distribution*. All four of these choices are part of the Internet marketing mix, plus two new elements: *community and branding*.

Community is the level of interaction that unfolds between users. Certainly, the firm can encourage community formation and nurture community development. However, community is about user-to-user connections. Branding is a critical component of building long-term relationships on the Web. Thus, rather than view branding as a subcomponent of the product, it is developed here as a moderating variable upon the levers—product, pricing, communication, community, and distribution.

**Product:** The product is the service or physical good that a firm offers for ex-change. A wide range of product forms are being offered on the Internet, including physical goods (e.g., clothing), information-intensive products (e.g., *The Wall Street Journal* online), and services (e.g., online grocers). Frequently, the offerings are a combination of all three forms. In the course of building customer relationships, the firm can use a variety of product levers to build enduring customer relationships. Product packaging is often used to build customer awareness, upgrades and complementary services enable customers to explore a deeper connection, and customized offerings strengthen commitment. The key point is that specific product levers can be used to encourage a stronger connection.

**Pricing:** Price is the amount the firm charges customers for a particular market transaction. This would include the price of the product, shipping, handling, warranty, and other financial costs incurred by the customer. Price is critical because it influences the perceived customer value (the complete product offering minus cost is often termed customer value). While a casual observer might view the pricing levers quite narrowly (there is only one choice: the price to charge for the good), there is a wide variety of traditional and new-to-the-world levers that emerge on the Internet. Traditional levers include such potential choices as tiered loyalty programs, volume discounts, subscription models, and targeted price promotions. The Internet has created an entirely new category of pricing tools for new-economy firms to use, including dynamic pricing strategies.

**Communication:** It defines marketing communication as activities that inform one or more groups of target customers about the firm and its products. This text takes a broad view of market communication to include all types of firm-level communications, including public relations, the use of sales representatives, and online advertising. Everyone knows how advertising and other forms of communication such as *television and direct mail* can make target customers aware of the offerings of the firm. However, marketing communication can also encourage *exploration, commitment, and dissolution*. For example, **viral marketing** (where one user informs another user about a site through e-mails) often leads to exploration of a firm's offerings by new customers. Also, **permission marketing** (where customers opt to receive communications from the firm) is intended to encourage commitment to the firm. Both offline and online communication levers can encourage customers to build a stronger bond with the firm and should be integrated in any marketing program.

**Community:** Community is defined as a set of interwoven relationships built upon shared interests, which satisfy members' needs otherwise unattainable individually. One of the unique aspects of the Internet is the speed with which communities can be formed. Equally important is the impact that these communities can have on the firm. A critical question confronting Internet marketers is how communities should be leveraged to build deep customer relationships. Communities can be leveraged to build awareness (e.g., user-to-user communication to make others aware of a product promotion), encourage exploration (e.g., user groups discussing which automotive options to purchase—or not purchase), and commitment (e.g., bonds between users lead to deepening involvement with the site)..

**Distribution:** The Internet is simultaneously a completely new form of commerce—a revolution in how customers and firms interact—and a distribution channel for the firm's products. With respect to the role as a distribution channel, the Internet has the power to shift customers to a new channel—or to use this channel in combination with other channels (e.g., search the Internet and then purchase at the retail store). Distribution levers include the number of intermediaries (both online and offline), the breadth of channel coverage, and the messaging from the channels. Broad levels of distribution impact both customer awareness and the potential for more customer exploration of the firm and its offerings.

**Branding:** Branding plays two roles in marketing strategy. First, branding is an outcome or result of the firm's marketing activities. Marketing programs affect how consumers perceive the brand, and hence its value. Second, branding is a part of *every* marketing strategy. That is, each marketing activity is enhanced if the brand is strong, or suppressed if the brand is weak. Thus, a strong advertising program for Travelocity.com is likely to produce better results than a strong advertising program for a site with a weaker brand, such as Travel.com. Branding levers work in concert with other marketing levers to produce positive financial and/or customer results for the firm. In sum, the Internet marketing mix comprises six classes of levers. Figure uses a cloud metaphor to show how branding mixes with each of these elements to produce an interactive effect. This interactive, or multiplier, effect of the brand can be positive or negative. Importantly, this does not mean that the other mix elements do not interact, because they do. However, branding is unique insofar as it is both a lever and an outcome of marketing actions.

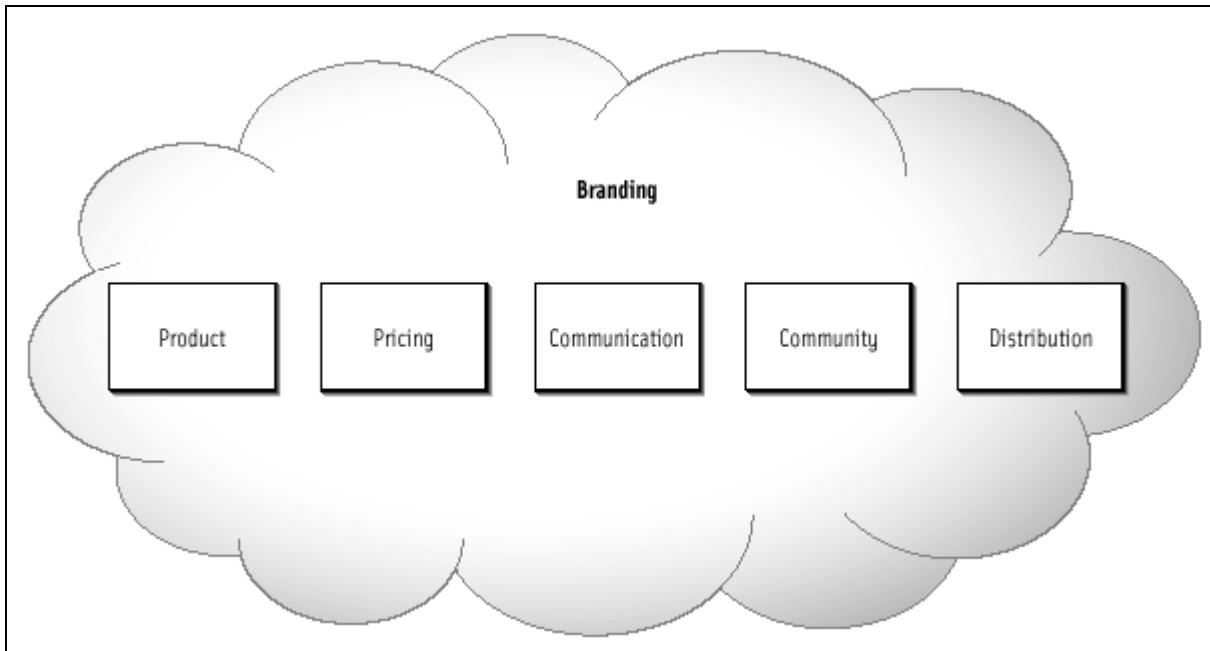


Fig: Internet Marketing Mix

**Individualization and Interactivity:** The previous section provided an overview of the six variables in the Internet marketing mix. However, simply specifying that the firm is able to manage these six classes of variables in an online environment does not do full justice to the uniqueness of the Internet environment. Two very important concepts need to be introduced to fully understand the profound implications that the Internet brings to business. These two concepts are *individualization (or customization)* and *interactivity*. The first concept is individual-level marketing exchange. In addition to high levels of interactivity, customers expect to have a personal experience with the firm.

**Broadcast** approaches send the same messages to all members of the target audience. The Internet enables the firm to engage in customer-specific actions—a broadcast to an audience of one. Equally important, the customer can control the *degree of customization* by taking action to set the level of customization he or she desires. Hence, the amount of individualization can be controlled either by the firm or by the customer.

**Interactivity** is defined as the extent to which a two-way communication flow occurs between the firm and customers. The Internet enables a level of customer dialogue that has not previously been experienced in the history of business.

Certainly customers could have conversations with retail-store clerks, sales reps, or managers; however, it was not possible at the scale that the Internet affords. Hence, the fundamental shift is one from broadcast media such as television, radio, and newspapers to one that encourages debate, exchange, and conversation.

Figure below shows how the 2Is (interactivity and individualization) impact the design of all of the levers of the Internet marketing mix. Pricing can be both inter-active and individualized—indeed, that is the essence of dynamic pricing. And market communications can be both interactive and individualized—that is the purpose of real-time customer service on the Web. Furthermore, products and services can be designed in real time by the customer, maximizing both interactivity and customization. This level of custom dialogue has revolutionized the impact of the Internet on marketing.

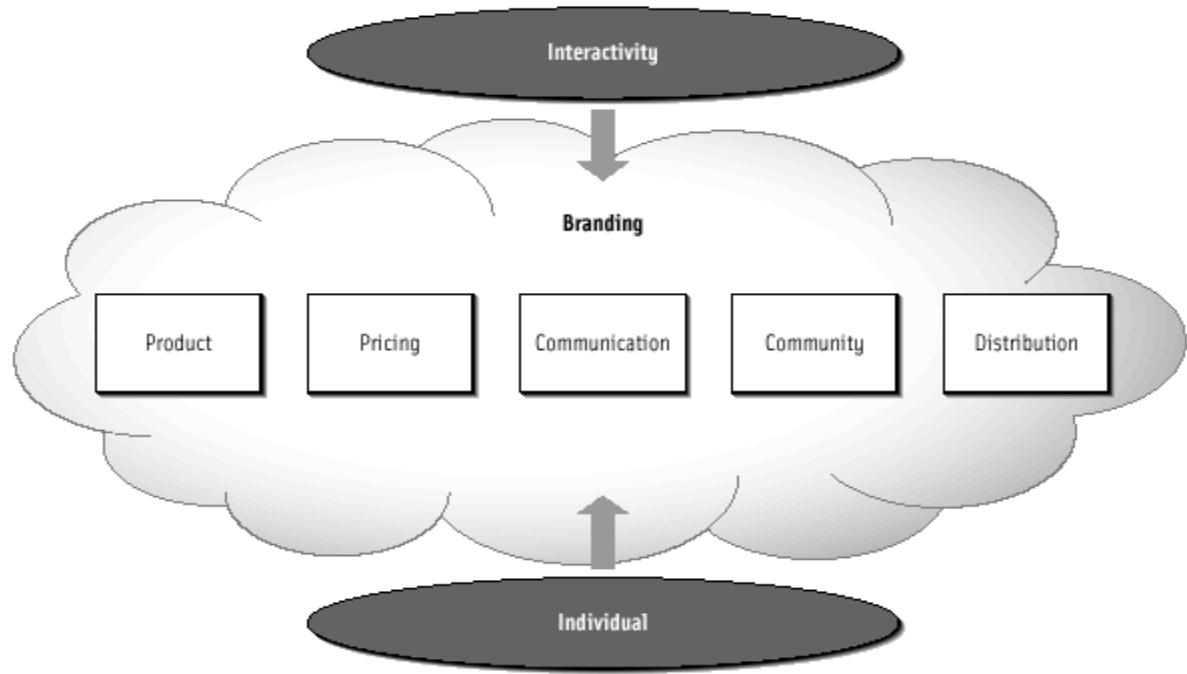


Fig: Impact of 2Is in the Internet Marketing Mix

**The Marketspace Matrix.** Having touched upon customer relationships, the Internet marketing mix, and the 2Is, attention now turns to the Marketspace Matrix. Exhibit 1-9 illustrates the key cross-tabulation that needs to be managed by the Internet marketing team. The design of the marketing program—or, to put it differently, the process of filling in the relationship-levers matrix—must be guided by a series of principles..

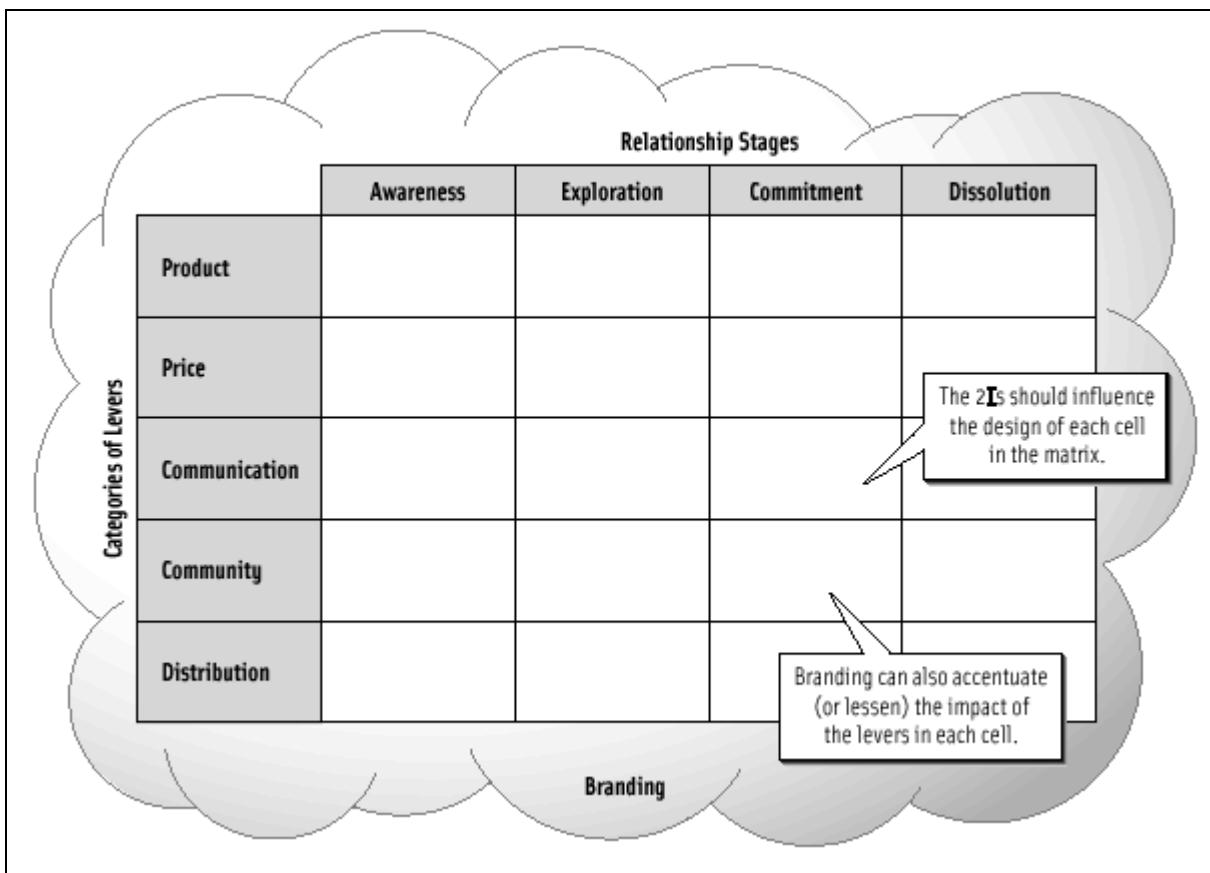


Fig: The marketspace matrix

### Stage Six: Crafting the Customer Interface

The Internet has shifted the locus of the exchange from the marketplace (i.e., face-to-face interaction) to the marketspace (i.e., screen-to-face interaction). The key difference is that the nature of the exchange relationship is now mediated by a technology interface. This interface can be a desktop PC, subnotebook, personal digital assistant, mobile phone, wireless applications protocol (WAP) device, or other Internet-enabled appliance. As this shift from people-mediated to technology-mediated interfaces unfolds, it is important to consider the types of interface design considerations that confront the senior management team. What is the look-and-feel, or context, of the site? Should the site include commerce activities? How important are communities in the business model?

### Stage Seven: Evaluating the Marketing Program

This last stage involves the evaluation of the overall Internet marketing program. This includes a balanced focus on both customer and financial metrics.

### Personalization in e-commerce

Electronic commerce is the process of managing business occurring over networks, which use non-proprietary protocols such as Internet. Business includes buying and selling of information, services and goods and maintaining a network of relationships between organizations and individuals.

Recommender systems are e-commerce applications that provide advice to users about products or services they might be interested in. Web based recommender systems are the most notable application of the web personalization, i.e., the process of tailoring a web site to individual users' characteristics or preferences. Recommender systems are exploiting a vast range of AI technologies and are defining new scenarios for human to human and human to machine interaction. The ultimate goal is to offer an enhanced one-to-one solution for each single user and meet his needs more effectively and efficiently.

Adding information to the site that generates the interest of the user group without having a direct relationship to the company. Data mining technologies are being used to offer an effective marketing program to particular target markets. Understanding the needs of the customers can be beneficial to create better products, content and services. Privacy of the personal information about the customers are ensured.

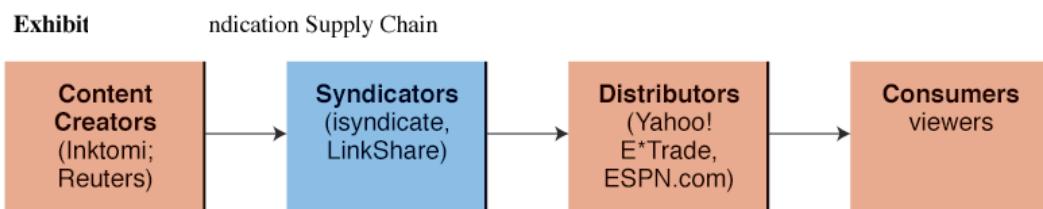
### **Virtual Societies**

Virtual societies refers to the creation of the community of customers and the sellers ( e-tailers or service provider) in the market-space. The most commonly known virtual societies are

- A. Affiliate networks
- B. Internet Communities
- C. Interactive users group

### **A. AFFILIATE NETWORKS**

Syndication is the sale of the same good (e.g., digital content) to many customers, who then integrate it with other offerings and resell it or give it away free



Syndication of the content and technologies to other sites or even to other media is the most common method of marketing online products. For example Portals, that offer content, products or even services.

Affiliate networks are a special form of customizing online products to resellers that extend their offerings by adding products, services or information from various suppliers or providers. The resellers should be able to reconfigure the offerings on their own to customers.

*Affiliate programs* are marketing programs designed to enable merchants to mobilize other websites, or affiliates, to help them sell products, procure traffic, or build brand. *Affiliate programs* are arrangements made between e-commerce sites that direct users from one site to the other. These affiliates, in essence, serve as new distribution channels for merchants. If a sale is made as a result, the originating site receives a commission. Usually this is done using an online ad in combination with click-throughs or some other measure of effectiveness. **Click-throughs** are a count of the number of people who visit one site, click on an ad, and are taken to the site of the advertiser. For example, Amazon.com's affiliate network is probably the most known which has more than 500,000 associates, Web sites with ads directing customer traffic to the Amazon.com site. Every time a customer clicking on the Amazon.com ad on an associate's Web site buys something at Amazon.com, the associate receives a commission of up to 15 percent of the amount of the sale.

## B. Internet Communities

Target groups are mapped with Internet communities. Building up such communities will not only enhance one-to-one marketing strategy, but will also allow one-to-many and many-to-many communication within the user groups. It is also easier to customize products for certain communities.

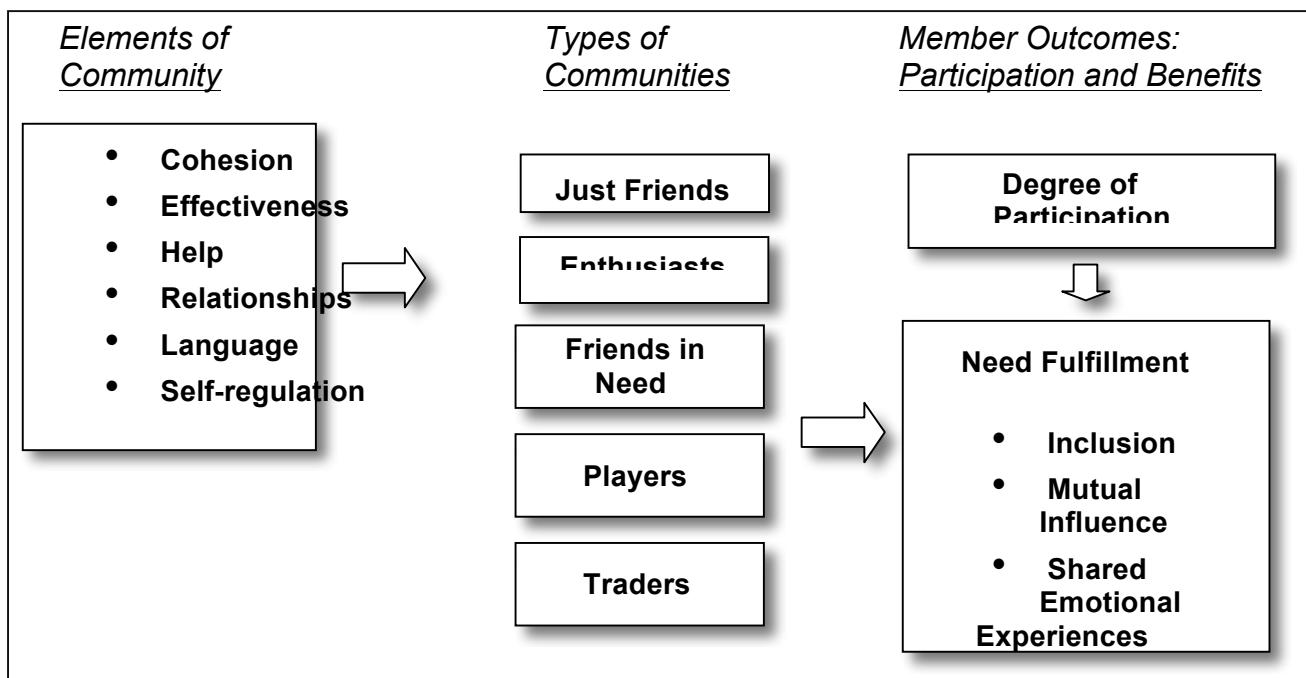


Fig: Communities — Elements, Types, and Benefits

## C. Interactive User Groups

It is necessary to build an Interactive user group through dialogue exchange or discussion group such as bulletin board to focus on the target group and serve them better and to

achieve customer loyalty. Interactivity can be improved by providing a different email address for every type of request. For example separate email address for providing advertisement price and posting comments about the web in general.

Other simple measures to increase the interactivity of web site include offering contests or sweepstakes on the web pages. Providing additional free information, products or services upon registration, offering demo or free trial for limited duration, feedback forms and providing search engines can increase the interaction between the consumers and the company in the electronic business.

### **Localization**

*The process of converting media products developed in one country to a form culturally and linguistically acceptable in countries outside the original target market.* In order to make a product more attractive, it is necessary to localize a product or service to compete with local market. For this, e-business should support the "Act global, think local" philosophy. For this, web sites should support the local language, format of dates being used, currency , government law and culture or religions of that particular region. Another issue may be the form where customers need to fill in their postal address. Postal codes have different formats in different countries and the field "state", that is used in US is not needed ion other countries.

### **Online Measurement**

#### **User Tracking**

The Internet combines the tracking capabilities of direct mail and the instancy of TV and radio broadcast with the addition of interactivity. The most commonly used methods of user tracking on the web are *counting, auditing and rating*.

*Counting* is the process, which is normally done by the web site owners. It consists of monitoring and reporting user activity. The measurement is done on the basis of the web server log files. The measurement units used for online advertising are called *page views and visits*. Page views are all pages that were viewed by the online consumers and a visit consists of all page views by a single customer.

Auditing is the process of verifying the counting; i.e. checking the log files. Auditing is done by an impartial third party organization, which is trusted both by the advertiser as well as the web site owner.

#### **Log file Analyzer**

Every web server is able to keep track of the users accessing its web pages by saving the action into a log file. Automatic log file analyzer tools provides a graphical output of the data to analyze log files on highly-frequented sites.

In order to analyze log files, it is necessary to import the data into the proprietary database of the analyzer. Filters can be used in most products to analyze traffic for a certain period of time or certain user groups or areas on the web server. Once the data has been imported, the filters have been chosen; the data is processed and the analyzer creates graphical reports such as tables and charts.

### **Measurement Units**

**Page View:** An HTML page that has been successfully downloaded, including all embedded elements (such as graphics)

**Hits:** Every access to the web server, including HTML pages, graphics, sounds, frames.

**Visits:** A sequence of page views performed by a single visitor. If the user does not view a page for fifteen minutes then the visit is over.

**Ad Impression:** Number of banner views on a certain web page.

**Ad Click:** Number of clicks on a banner for a certain web page.

## **Advertising on the Net**

Advertising is the process of reaching the customer using a broadcast or direct mail campaign orchestrated to influence purchasing behavior. Advertising plans are conceived within the confines of parameters set by a marketing plan. With the advent of electronic commerce, a new type of interactive advertising is emerging whereby customers can choose the information they wish to access.

Offline and e-commerce merchants can advertise in many of the same ways that offline merchants advertise. In addition, e-commerce merchants can utilize a variety of Web-based marketing efforts, including *search engine and directory listings, classified listings, banner ads, and viral and affiliate programs*.

## **Banner Ads**

It is a graphic advertising display linked to the advertiser's Web page. **Banner Ads** represent the most common advertising product on the Web. Banner ads can be found on virtually every commercial webpage in existence, along with many non-commercial webpages. Banner ads, like paid placements on search engines and Web directories, can also be highly targeted. For example, when browsing the automobiles section of *The New York Times* on the Web, a banner ad advertising automobiles appears on the page. When browsing the travel section, a travel advertisement appears. Two types of Banners are

- ◆ Keyword banners
- ◆ Random banners
- ◆ Benefits of banner ads

- ◆ Customized to the target audience or one-to-one ads
- ◆ Utilize “force advertising” marketing strategy
- ◆ Direct link to advertiser
- ◆ Multi media capabilities
  
- ◆ Limitations of banner ads
  - ◆ High cost
  - ◆ Click ratio—the ratio between the number of clicks on a banner ad and the number of times it is seen by viewers; measures the success of a banner in attracting visitors to click on the ad
  - ◆ Declining click ratio—viewers have become immune to banners
  
- ◆ ***Banner swapping***—an agreement between two companies to each display the other’s banner ad on its Web site
  - ◆ Direct link between one site to the other site
  - ◆ Ad space bartering

***Banner exchanges***—markets in which companies can trade or exchange placement of banner ads on each other’s Web sites (bcentral.com). It is still the largest Internet advertising medium

### **Types of Advertising**

Two different advertising paradigms are emerging in the online world according to the activity on the company's side, that are:

- Active or push-based advertising
  - Broadcast model
  - spamming (unsolicited advertising)
- Passive or pull-based advertising
  - Billboards or World wide web
  - Catalogs or yellow page directories
  - Endorsements

#### **Active or push-based advertising**

Push advertising refers to all efforts to get the word out to an entire group of potential customers in order to hit the few that many be currently interested in your product or service. Most traditional offline advertising efforts (magazine, billboard, newspaper, TV, classifieds, etc) as well as online banners ads and email broadcasts are considered push marketing.

#### **The Broadcast Model**

Broadcasting messages provides a means for reaching a great number of people in a short period of time. It typically use direct mail, spot television, or cable television. A spot

television ad runs on one station in one market. The number of viewers who see, the ad depends on how many viewers are tuned into the television station at a specific time. The number of people reached by advertising depends on the penetration and channel/program viewer ship in a given market. Beyond television's reach, an additional advantages is its ability to convey the message with sight, sound and motion. The disadvantages of television advertising are relatively high cost of production; limited exposure time; short air time; and the clutter of many other ads. Television ads may require multiple exposures to achieve message retention and consumer action.

In general, broadcast model is intrusive and resource intensive when implemented in on-line environments. Its principal drawback is that it requires active choice on the part of the customer to watch the program or read the message.

### **The junk Mail model (spamming)**

The most popular forms of direct marketing on the Internet are direct e-mail and newsgroup postings. These often unsolicited messages are referred to as *spam*.

Direct mail advertisers use targeted mailing lists to reach highly specialized audiences. In addition to low waste in ad waste in ad exposure, direct mail provides an advertiser with great flexibility in the message presentation. Disadvantages of direct mail include relatively high cost per contact, the need to obtain updated and accurate mailing lists, the difficulty in getting the audience's attention, and the possible cost to customers who pay for e-mail, plus of targeted direct mail. Direct mail is the most intrusive of all forms of Internet advertisement, because it is easily implemented using email.

The electronic equivalent of direct mail is "*junk-mail*". These junk mail creates an unwanted expense as well as an annoyance. As a result, spam is typically not well received in the Internet community. Many organizations have even developed applications designed to filter out and delete spam.

### **Spam**

The term Spam refers to unsolicited, unwanted, inappropriate bulk email, Usenet postings. Spam is often referred to as Unsolicited Bulk Mail (UBM), Excessive Multi-Posting (EMP), Unsolicited Commercial email (UCE), spam mail, bulk email or just junk mail.

An electronic message is "spam" IF: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender.

Spam is the electronic equivalent of junk mail. People send Spam in order to sell products and services or to promote an email scam. Some Spam is purely ideological, sent by

purveyors of thought. The bulk of Spam is intended, however, to draw traffic to web sites and money making schemes.

### **Passive or Pull-based Advertising**

Pull based advertising provides a feedback loop, connecting company and customer. It is more discourse oriented and content driven and as such promotes interactively between customers and firms. It includes:

**Billboards:** setting up the Web pages by many different commercial ventures.

**Catalogs or yellow pages:** directories that are searchable and browse able databases of advertising.

**Endorsements:** Specific posting made to subject-oriented Internet discussion forums and Recommendations from users for product-oriented or service-oriented Internet discussion forums.

### **The Billboard or WWW Model**

It refers to information placed where it will come to the attention of customers in the course of other activities and does not require active search. Billboard advertising is often used to reinforce or remind the consumer of the advertising messages communicated through other media.

Advantage:

- Complete coverage of the market
- maintain high level of viewing frequency
- No cost to customers
- Readily implemented in the WWW, Gopher and similar mechanisms.

The disadvantages of billboard advertising are related to viewing time. Because target customers are typically surfing or moving, billboard advertisement must communicate with a minimum of words. Message must be simple, direct and easily understood.

### **Catalog and Yellow Pages Directory Model**

The catalog model is the least intrusive model but requires active search on the part of the customer. The term *directory service refers* not only to the types of services provided by the telephone companies' White Pages but to electronic resource location and services, yellow pages services, mail address lookup etc.

### ***Search Engine and Directory Listings***

Search engine and directory listings are the most popular method people employ when searching for information or stores on the Web. What the yellow pages does offline, search engines and directories do online, serving as the default source for finding information about stores and products. As a result, Web merchants have to take the

appropriate steps necessary to get their websites listed in search results and directory listings, mainly through the use of meta tags or by paying for placement.

**Meta tags:** Meta tags are HTML tags that most search engines read when indexing the Web. These tags allow website developers to get their websites listed or indexed properly within a search engine. There are a variety of meta tags, but two of them stand out in importance for search engine indexing: *keyword* and *description tags*. Keyword tags provide keywords for search engines to associate with a developer's website, and description tags allow the website developer to substitute his or her own description for the website in place of the description that the search engine would normally generate. Meta tags are useful tools for getting a website noticed, but they certainly are not an end-all solution. With the rapid growth of the Web, search engines are having a hard time keeping up.

**Paid placements:** To differentiate their websites from the hoards of websites out there, many e-commerce merchants turn to paid placements in addition to meta tags. In the yellow pages, the bigger and more noticeable the placement, the more that particular placement costs. With directories and search engines, the same applies. By paying for placement, Web merchants can gain increased visibility with potential customers. Web merchants might pay to have their websites listed as more relevant or higher on the list of results, or they can buy highly-targeted keywords that serve up their listing when a potential customer performs a search on a particular keyword. As you might have guessed, the pricing and evaluation criteria for these types of advertisements mirror those of the offline world. The more targeted the advertisement and the greater its reach, the more expensive and effective it is.

## Customer Endorsements

Endorsements, where people tell of their experiences with products and services- both positive and negative, represent one unique aspect of advertising on the Internet. It could be in the form of question and answer forum or an experience shared. It is the most effective advertisements on the Internet as it offers publicly in an interactive medium. Anyone who disagrees can post his or her opinions, and such debates often form the best-and most unbiased-analyses of products and services. Advertisers whose products and services are discussed positively by others gain customer and loyalty.

### Some guidelines for Internet Advertising

- Don't send intrusive messages. People should not receive a commercial message they either hasn't asked to receive or do not want to receive.
- Don't sell consumer data without the express permission of the user.
- Advertising should appear only in designated news groups and list servers.

- |                                                                                                       |
|-------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Conduct promotions and direct selling only under full disclosure. |
| <input checked="" type="checkbox"/> Conduct research only with the consumer's informed consent.       |
| <input checked="" type="checkbox"/> Never use Internet communications software to conceal activities. |

## Interactive Marketing Process on the Internet

- 
- |         |                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1. | Segment and identify potential customers<br>( Initial market research done reaching relevant groups such as WWW servers, listservs, news groups)                                                                                         |
| Step 2. | Create promotional, advertising, and educational material<br>( WWW page with multimedia effects-audio and video)<br>( Product information and complementary products, order forms, and questionnaires)                                   |
| Step 3. | Put the material on customers' computer screens<br>Push-based marketing- direct marketing using news groups, listservs and e-mail.)<br>Pull-based marketing-indirect ( static) marketing-WWW pages                                       |
| Step 4. | Interacting with customers<br>Dialogue with the customer; interactive discussion among customers about various features offering endorsements, testimonials, questions/answers.                                                          |
| Step 5. | Learning from customers ( repeat customers are 80 per cent of the customer base).<br>Incorporating feedback from customer in advertising, marketing strategy.<br>Identifying new markets, using experience in a new product development. |
| Step 6. | On-line customer service and support.                                                                                                                                                                                                    |
- 

## Issues in Marketing and Advertising

|                                   |                                                                                                                                                          |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product and price-related topics  | Nature of consumer product interface<br>Information based products-creation and bundling.                                                                |
| Promotion related topics          | Electronic market segmentation and product positioning<br>Cultivating brand loyalty<br>Broadcast vs. narrowcast advertising<br>New product Introduction. |
| Market research methods and tools | Market research using WWW access-logs<br>Market research using source databases                                                                          |
| Managing the search space.        | Interactive catalogs and directories<br>Electronic institutions or brokerages<br>Software agents                                                         |

## **Summary**

The integration of E-Commerce and marketing should bring with it a renaissance of advertising, sales, and marketing functions as it presents is a new way of conducting, managing, and executing business transactions using computer and telecommunications networks. Electronic commerce improve the productivity and competitiveness of participating businesses by providing unprecedented access to an on-line global marketplace with millions of customers and thousands of products and services. It provides companies with new, more cost- and time-efficient means for working with customers, suppliers, and development partners. E-Commerce enables companies with

- (1) Shorten procurement cycles through on-line catalogs, ordering, and payment;
- (2) Cut costs on both stocks and manufacturing parts through efficient JIT and QR system that reduce inventory and facilitate automatic replenishment; and
- (3) Shrink product development cycle and accelerate time-to-market through collaborative engineering and product customization.

The use of network based infrastructure reduces the cost by adding values information services in the whole gamut of supply chain management bringing both buyers and sellers into a common e-hub where buyers can browse multi-media catalogs, solicit bids, place an order and sellers will respond to bids, schedule production, and coordinate deliveries.

## **Auction**

- ◆ Auction—a market mechanism by which a seller places an offer to sell a product and buyers make bids sequentially and competitively until a final price is reached
- ◆ Auctions deal with products and services for which conventional marketing channels are ineffective or inefficient

**Electronic auctions (e-auctions)**—auctions conducted online

- Host sites on the Internet serve as brokers offering:
- Services for sellers to post their goods for sale**
- Allowing buyers to bid on those items**
- Many sites have certain etiquette rules that must be adhered to in order to conduct fair business

**Major online auctions offer:**

- Consumer products
- Electronic parts
- Artwork
- Vacation packages

- Airline tickets
- Collectibles
- Excess supplies and inventories being auctioned off by B2B marketers

## **Dynamic pricing**

Prices that change based on supply and demand relationships at any given time. The four major categories of dynamic pricing are based on the number of buyers and sellers involved:

- One buyer, one seller
- One seller, many potential buyers
- One buyer, many potential sellers
- Many sellers, many buyers

**Exhibit 2.8** Types of Dynamic Pricing

|               |     |                                          |                                           |
|---------------|-----|------------------------------------------|-------------------------------------------|
|               |     | Negotiation,<br>Bartering,<br>Bargaining | Reverse<br>auctions,<br>RFQ,<br>Tendering |
| <b>Buyers</b> | One |                                          |                                           |
| Many          | One | Forward<br>(regular)<br>auctions         | Dynamic<br>exchanges                      |

### **Sellers**

#### ◆ ***One buyer, one seller uses***

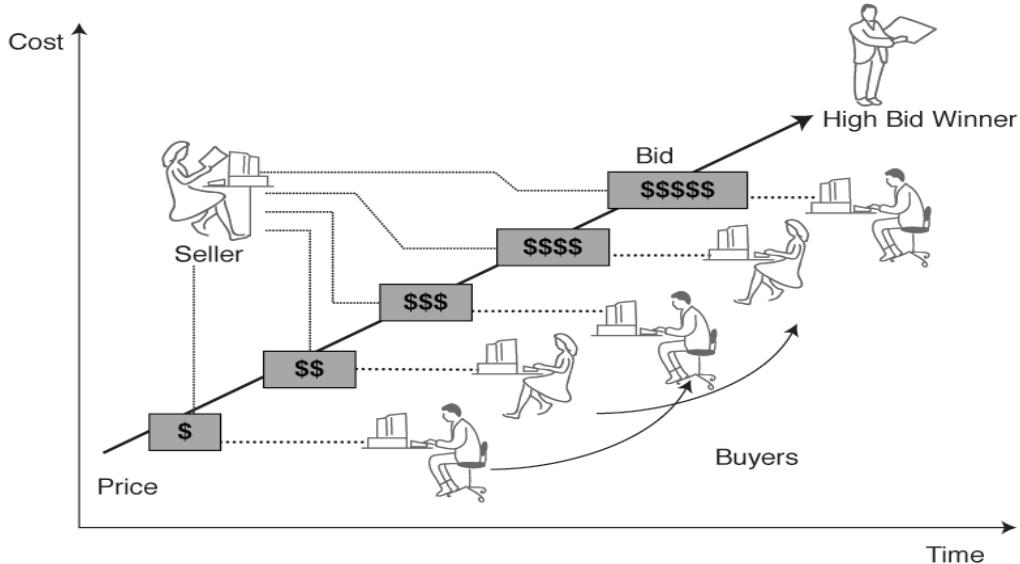
- Negotiation
- Bargaining
- Bartering
- Price will be determined by:
  - Each party's bargaining power
  - Supply and demand in the item's market
  - Possibly business environment factors

#### ◆ ***One seller, many potential buyers***

- Forward auction—an auction in which a seller entertains bids from buyers
- English auction—an auction in which buyers bid on an item in sequence and the price increases with time
- Yankee auction—auction of multiple identical items in which bidders can bid for any number of the items offered, and the highest bid wins
- Dutch auction—an auction of multiple identical items, with prices starting at a very high level and declining as the auction time passes

- Free-fall (declining price) auction—a variation of the Dutch auction in which only one item is auctioned at a time; the price starts at a very high level and declines at fixed time intervals, the winning bid is the lowest one when the time expires

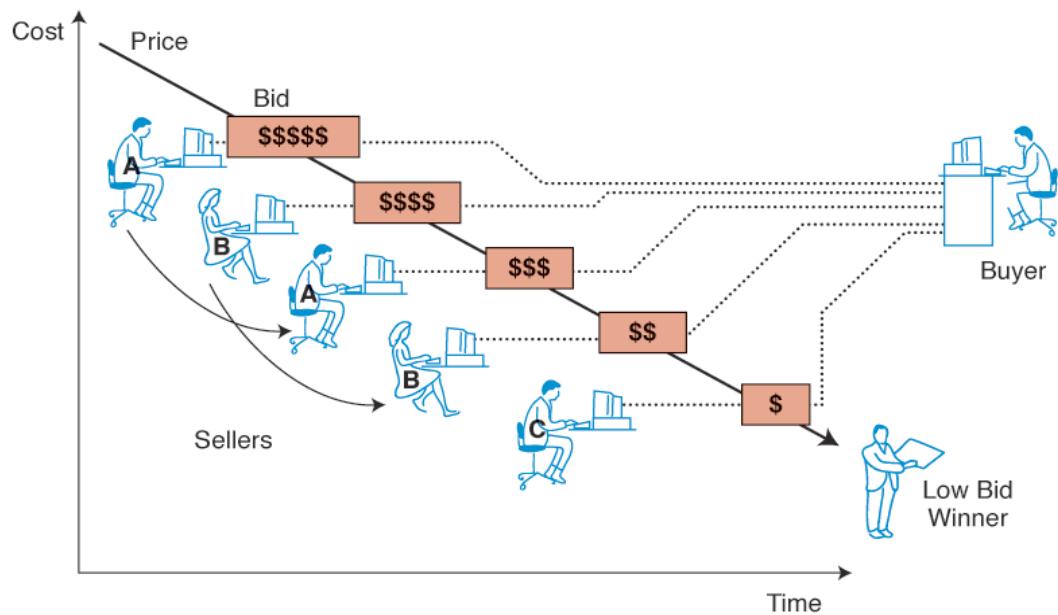
**Exhibit 2.9** English Auction, Ascending Price



♦ ***One buyer, many potential sellers***

- Reverse auction (bidding, or tendering system)—auction in which the buyer places an item for bid (tender) on a request for quote (RFQ) system, potential suppliers bid on the job, with price reducing sequentially, and the lowest bid wins; primarily a B2B or G2B mechanism
- “Name-your-own-price” model
- Consumer-to-business (C2B) model

**Exhibit 2.10** The Reverse Auction Process



- ◆ **Many sellers, many buyers**
  - Double Auction—buyers and their bidding prices and sellers and their asking prices are matched, considering the quantities on both sides

### Limitation of e-Auction

- ◆ Possibility of fraud—defective goods or receive goods/services without paying
- ◆ Limited participation—invitation only or Open to dealers only
- ◆ Lack of security—C2C auctions sometimes not done in an unencrypted environment
- ◆ Limited software—only a few “complete” or “off-the-shelf” market-enabling solutions
- ◆ Localization—the process of converting media products developed in one country to a form culturally and linguistically acceptable in countries outside the original target market
- ◆ Using internet radio for localization: Internet radio—a Web site that provides music, talk, and other entertainment, both live and stored, from a variety of radio stations

## Other issues in Ecommerce

### INTERNET GOVERNANCE

The Internet has garnered a reputation as a largely unregulated realm, a modern lawless "wild west" frontier where an anything goes mentality has taken hold. Certainly, it can seem that way at times. But before you saddle-up and grab your cowboy hat, you may want to stop and familiarize yourself with the more than 75 sections of the United States Code that may (apparently) be applied to illegal activity on the Internet.

That is not to say new laws to govern Internet activity will not be required in the future. But do not mistake this need for a lack of law currently on the books governing web activity.

There are two broad governance issues raised by the Internet. One issue deals with how the Internet itself, a technologically complex global communication network, can be managed so it can continue to grow. There are several organizations, many of which are gathered under the umbrella of the Internet Society, which oversee the complicated task of balancing competing interests in the evolution of **new technical standards** (see Table below).

The second major issue is how to legally govern activity conducted on the Web. This task remains the responsibility of the government in every nation around the world that is connected to the Internet. The regulatory agenda covers a wide range of activities:

- the regulation of business transactions and securities trading;
- consumer protection (including the protection of minors);
- fairness in advertising;
- the protection of intellectual property;
- various forms of taxation on the sale of goods and services;
- prohibitions on gambling, the trafficking of alcohol and other controlled substances across borders;
- regulations on the safety of food and prescription drugs;
- the protection of free speech and controls on the distribution of indecent materials.

These are just some of the areas in which the government has had a historical role.

The global nature of the web greatly complicates effective governance. Transactions on the Internet can crisscross state and national borders without easy detection. Any legal regime that may be desired to govern web activity must deal with issues of compliance and enforcement in order to be implemented effectively. That also means there is a greater need for cooperation between various branches of government and law enforcement in and between countries.

### FEDERAL LAWS APPLICABLE TO CYBERCRIME

***Types of Unlawful Conduct and Examples of Potentially Applicable Federal Laws***

**Internet Fraud**

- unfair or deceptive acts or practices; false advertisements
- credit card fraud
- fraud in connection with identification documents and information; fraud in connection with access devices; and fraud in connection with computers
- mail, wire, and bank fraud
- money laundering

**Online Child Pornography, Child Luring, and Related Activities**

- sexual exploitation and other abuse of children
- transportation for illegal sexual activity

**Internet Sale of Prescription Drugs and Controlled Substances**

- unfair or deceptive acts or practices; false advertisements
- smuggling goods into the United States
- mail, wire, and bank fraud; injunctions against fraud
- Federal Food, Drug, and Cosmetic Act
- Drug Abuse Prevention and Control

**Internet Sale of Firearms**

- firearms

**Internet Gambling**

- Interstate Horseracing Act
- transmission of wagering information
- lotteries
- interstate and foreign travel or transportation in aid of racketeering enterprises
- interstate transportation of wagering paraphernalia
- prohibition of illegal gambling businesses
- professional and amateur sports protection

**Internet Sale of Alcohol**

- liquor traffic
- shipments into states for possession or sale in violation of state law

**Online Securities Fraud**

- securities fraud

**Software Piracy and Intellectual Property Theft**

- criminal copyright infringement
- copyright protection and management systems
- smuggling goods into the United States
- frauds and swindles
- protection of trade secrets
- trafficking in counterfeit labels for phonorecords, copies of computer programs or computer program documentation or packaging, and copies of motion pictures or other audio visual works

**INTELLECTUAL PROPERTY**

Everything in cyberspace is composed of bits, the binary code that is the foundation of computing. It makes digital works -- images, music, video, software, and written compositions -- perfectly reproducible by the creator of the work and anybody else who possesses it. Not just once, but an infinite number of times. There is no degradation factor that limits the value of derivative copies. On the web, *a copy is the original*.

The binary reality of the web poses interesting questions regarding the nature of intellectual property and how to protect it. One of the virtues of the web is its reach: the ability to widely distribute digital works less expensively and faster than ever before. There is great value in being able to communicate to millions of people. So much so, the web is bursting with content that is given away freely. The downside is the lack of physical control creators are able to exert on the subsequent dissemination and use of their work. When everything we create is reducible to ones and zeroes, technically there is no impediment to making copies.

Traditionally, there are three means of legal protection for intellectual property: patent, trademark and copyright. With each mechanism, the web presents its own unique challenge, not the least of which is the fact that nations differ in their approach to intellectual property law.

Mistaking the free distribution of content with the placement of intellectual property in the public domain is common among web users. A web page is not public domain material. Property holders can distribute their works freely while retaining their right of control over that work -- that is, their copyright.

To make matters worse, what is allowed under copyright law with respect to digital works is not always clear. Although there are provisions for the "fair use" of copyrighted materials, the law has evolved under a technological regime that rests on the physical reproduction of the work (i.e., print publishing, photocopying, audio tape and vinyl disc recordings, videos, and film). But the web opens many new questions of what is legal, appropriate, and fair to copyright owners and consumers. The same can be said with respect to trademark and patent law.

Here are a few of the areas where e-commerce businesses are struggling to understand how intellectual property rights will be handled under international law:

- When is a hyperlink from one site to web pages within another site illegal?
- When is a business method patentable?
- When is a domain name a trademark infringement?
- When is a web crawler trespassing?
- When is a metatag a trademark infringement?
- When is your reputation someone else's property?
- When is sharing information a crime?

With each of these questions, it is not entirely clear what's fair under the law and what's not. Ultimately, it will be up to the judicial system to sort it out.

As the Internet continues its remarkable expansion, its capacity to disseminate information, knowledge and content has thrust the intellectual property system to the center of the debate over the future shape of the online world. In this new and rapidly changing environment, information and knowledge are increasingly the source of value; hence the intellectual property system - the body of law protecting creations of the mind - is crucial in maintaining a stable and equitable foundation for the development of the digital society.

**Intellectual Property rights (IPR)** refers to the *legal rights* which results from the intellectual Activity (creations of the mind) in the industrial, scientific, literary and artistic fields.

Rights relating to:

- literary, artistic and scientific works,
- performances of performing artists, phonograms, and broadcasts
- inventions in all fields of human endeavor,
- scientific discoveries
- industrial designs
- trademarks, service marks, and commercial names and designations
- protection against unfair competition
- and all other rights resulting from intellectual activity in the industrial, scientific, literary or artistic fields.”

### **Aim of Intellectual Property Rights**

*“Safeguarding creators and other producers of intellectual goods and services by granting them certain time-limited rights to control the use made of those productions.”*

### **Categories of Intellectual Property Rights**

- Industrial Property
  - Inventions (patents)
  - Trademarks
  - Industrial designs
  - Geographic indications of source
- Copyrights
  - literary and artistic works
    - Novels
    - poems
    - Plays
    - Films
    - musical works
    - Drawings
    - Paintings
    - photographs and sculptures architectural designs

## **PATENT, TRADEMARK, AND COPYRIGHT**

### **Patent**

A patent for an invention is the *grant of a property right to the inventor*, issued by the Patent and Trademark Office. The term of a new patent is time bound (20 years from the date on which the application for the patent was filed in the United States) and it has to be renewed after expiry.

The right conferred by the patent grant is "*the right to exclude others from making, using, offering for sale, or selling*" the invention or "*importing*" the invention. What is granted is not the right to make, use, offer for sale, sell or import, but the right to exclude others from making, using, offering for sale, selling or importing the invention.

### **Trademark**

A trademark is a distinctive sign (word, name, symbol or device) which is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others. A servicemark is the same as a trademark except that it identifies and distinguishes the source of a service rather than a product. The terms "trademark" and "mark" are commonly used to refer to both trademarks and servicemarks.

Trademark rights may be used to prevent others from using a confusingly similar mark, but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark.

Its origin dates back to ancient times, when craftsmen reproduced their signatures, or "marks" on their artistic or utilitarian products. Over the years these marks evolved into today's system of trademark registration and protection. The system helps consumers identify and purchase a product or service because its nature and quality, indicated by its **unique** trademark, meets their needs.

### **What does a trademark do?**

A trademark provides protection to the owner of the mark by ensuring the exclusive right to use it to identify goods or services, or to authorize another to use it in return for payment. The period of protection varies, but a trademark can be renewed indefinitely beyond the time limit on payment of additional fees. Trademark protection is enforced by the courts, which in most systems have the authority to block trademark infringement. In a larger sense, trademarks promote initiative and enterprise worldwide by rewarding the owners of trademarks with recognition and financial profit. Trademark protection also hinders the efforts of unfair competitors, such as counterfeiters, to use similar distinctive signs to market inferior or different products or services. The system enables people with skill and enterprise to produce and market goods and services in the fairest possible conditions, thereby facilitating international trade.

## **Copyright**

Copyright is a *legal term* describing *rights given to creators for their literary and artistic works* or it is a form of protection provided to the authors of "*original works of authorship*" including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished.

The 1976 Copyright Act generally gives the owner of copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly.

The copyright protects the form of expression rather than the subject matter of the writing. For example, a description of a machine could be copyrighted, but this would only prevent others from copying the description; it would not prevent others from writing a description of their own or from making and using the machine. Copyrights are registered by the Copyright Office.

### **What is covered by copyright?**

The kinds of works covered by copyright include:

- Literary works: novels, poems, plays, reference works, newspapers and computer programs; databases; films, musical compositions, and choreography;
- Artistic works: paintings, drawings, photographs and sculpture; architecture; and advertisements, maps and technical drawings.

### **What rights does copyright provide?**

The original creators of works protected by copyright, and their heirs, have certain basic rights. They hold the exclusive right to use or authorize others to use the work on agreed terms. The creator of a work can prohibit or authorize:

- its **reproduction** in various forms, such as printed publication or sound recording;
- its **public performance**, as in a play or musical work;
- **recordings** of it, for example, in the form of compact discs, cassettes or videotapes;
- its **broadcasting**, by radio, cable or satellite;
- its **translation** into other languages, or its adaptation, such as a novel into a screenplay.

Many creative works protected by copyright require mass distribution, communication and financial investment for their dissemination (for example, publications, sound recordings and films); hence, creators often sell the rights to their works to individuals or

companies best able to market the works in return for payment. These payments are often made dependent on the actual use of the work, and are then referred to as *royalties*.

These economic rights have a time limit, according to the relevant WIPO treaties, of 50 years after the creator's death. This limit enables both creators and their heirs to benefit financially for a reasonable period of time. Copyright protection also includes moral rights, which involve the right to claim authorship of a work, and the right to oppose changes to it that could harm the creator's reputation.

The creator - or the owner of the copyright in a work - can enforce rights administratively and in the courts, by inspection of premises for evidence of production or possession of illegally made - "pirated" - goods related to protected works. The owner may obtain court orders to stop such activities, as well as seek damages for loss of financial rewards and recognition.

### **Are ideas, methods or concepts protected by copyright?**

Copyright protection extends only to expressions and not to ideas, procedures, and methods of operation or mathematical concepts as such. This principle has been confirmed by the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) of the World Trade Organization (WTO) as well as the WIPO Copyright Treaty.

### **Why protect copyright?**

Copyright and its related rights are essential to human creativity, by giving creators incentives in the form of recognition and fair economic rewards. Under this system of rights, creators are assured that their works can be disseminated without fear of unauthorized copying or piracy. This in turn helps increase access to and enhances the enjoyment of culture, knowledge, and entertainment all over the world.

### **Enforcing digital copyright using technology**

- Aim=>> Use technology to help protect copyrighted works against unauthorized access, reproduction, manipulation, distribution, performance, or display.
- Controlling Access to Copyrighted works
  - Controlling server access
  - Controlling document access
  - Encryption
- Controlling the use of work
- Authenticating the work
- Implementing electronic contracts

Software-based systems are used to implement licensing of rights and metering of use. A combination of access control, encryption technologies, and digital

signatures can be used by copyright owners to protect, license, and authenticate information.

## Internetworking and Ecommerce

### Security threats and attacks

The Internet has made large amounts of information available to the average computer user at home, in business and in education. For many people, having access to this information is no longer just an advantage, it is essential. Yet connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. Users who connect their computers to the Internet must be aware of these dangers, their implications and how to protect their data and their critical systems. Firewalls can protect both individual computers and corporate networks from hostile intrusion from the Internet.

Confidence, reliability and protection of information against *security threat* are a crucial pre-requisite for the functioning of the electronic commerce.

A **security threat** is defined as a circumstance, condition or event with the potential to cause *economic hardship* to data or network resources in the form of destruction, disclosure, Modification of data, denial of service, and/or fraud, waste and abuse.

Example of threats to server

- Unauthorized modification of server data
- Unauthorized eavesdropping or modification of incoming data packets
- Compromise of a server system by exploiting bugs in the server software

### Types of Attacks

|                                          |                                                                                                                                                                                                                                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. Spoofing (masquerade) attacks         | Spoofing attacks happen when a hacker appears to have a trusted network and the victim is convinced in transacting with him.                                                                                                                                                             |
| 2. Man-in-the-middle (hijacking) attacks | These attacks happen when a hacker captures packets being sent from a host to another.                                                                                                                                                                                                   |
| 3. Denial-of-service-attacks             | It's the most common type of attacks. It happens when the host or system cannot work properly because another program is using all its resources. These attacks might crash the entire system due to the rapid flood of information generated by the hacker when he is trying to log in. |
| 4. Insider attacks                       | These attacks happen internally to gain unauthorized access. It can do by spying messages between applications and having the existing control systems.                                                                                                                                  |

|  |  |
|--|--|
|  |  |
|--|--|

Mobile code (Software agent) and malicious code are the two major security threats that are emerging in the electronic commerce nowadays.

**Mobile code** is an executable program that has the ability to move from machine to machine and invoke itself without external influence. Firewalls can circumvent such threat by filtering incoming data packets.

**Malicious code** refers to viruses, worms, Trojan horses, logic bombs and other deviant software programs

### Example of Malicious Code

---

**Virus:** A code segment that replicates by attaching copies of itself to existing executables (.EXE files). The new copy of the virus is executed when a user executes the host program. The virus may include additional "payload" that triggers when specific conditions are met. Ex- some viruses display a text string or delete all files on the Hard disk on a particular date.

**Trojan horse:** These attacks happen by hiding an unauthorized command within the function of a program or files. It is also a program that performs a desired task but also includes unexpected (and undesirable) functions. Ex-Editing program that could be modified to randomly delete one of the user's files each time they perform a useful function (editing).

**Worm:** A self-replicating program that is self-contained and does not require a host program. It creates a copy of itself and causes it to execute with the intervention of user. It commonly utilizes network services to propagate to other host systems.

---

### Types of Security

- a. client-server network security
- b. Data and transaction security

#### A. Client-server network security:

Network security on the Internet is a major concern for commercial organizations, especially top management as Internet connectivity effectively breaches the physical security perimeter of the corporate network and opens itself to access from other networks comprising the public Internet.

#### **Client-server network security problems**

Various *Client-server network security problems* are mentioned below:

1. Physical security holes
2. Software security holes
3. Inconsistency usage holes

**Physical security holes** causes unauthorized physical access to a computer or access to network system by hacking the password. The possible remedy for this problem is preventing access to the unauthorized personnel.

**Software security holes** result from badly written programs or "privileged" software are "compromised" into doing things that should not. Ex- "rlogin" hole in the IBM-RS6000 work stations enabling crackers ( a malicious hacker) to create a "root" shell or super user access mode which could be used to delete the entire file system, or create a new account or password file.

**Inconsistency usage holes** result from the incompatible assembling of hardware and software. Such problems are difficult to isolate once a system is set up and running. Hence care must be taken while building a system with unconnected hardware and software.

## **Protection of Client-Server Network**

To reduce these security threats, various protection methods are used which are:

1. Access Control Mechanism
2. Trust based Security
3. Security through Obscurity (STO)
4. Password Schemes
5. Biometric System

### **1. Access Control Mechanism**

At the file level, operating system typically uses mechanisms such as *access control lists* that specify the resources various users and groups are entitled to access. It uses various *authentication methods* to make sure that only valid users and programs have access to information resources ( such as databases). *Access control mechanism* ensures that authenticated users are allowed access only to those resources that they are entitled to use. Such mechanisms include:

- Password protection
- encrypted smart cards

### **2. Trust based security**

The philosophy behind this protection methodology is to TRUST everyone and do nothing extra as a precautionary effort. There is no restriction to access the information in the Private network as long as the users are trust-worthy and all privileges are granted to them. This approach worked in the past, when the system administrator had to worry

about a limited threat but such is no longer the case in the current scenario where nobody wants to take risk and make company at its stake by exposing the valuable information to the unsecured domain.

### **3. Security through Obscurity (STO)**

Network can be secured as long as nobody from outside its management group is allowed to find out anything about its operational details and users are provided information on a *need-to-know basis*. Methodology being used is information hiding (such as password) in a binary files or scripts with the presumption that "nobody will ever find them." It provides a false sense of security in computing systems.

### **4. Password Schemes**

It creates a first-level barrier to accidental intrusion. Various approaches being used in these schemes are creation of one-time passwords, including smart cards, randomized tokens, and challenge-response schemes.

### **5. Biometric Systems**

It is the most secure level of authorization, involve some unique aspect of a person's body such as comparison of fingerprints, palm prints, retinal patterns, or on signature verification or voice recognition. Recent biometric system include recognition of keyboard typing patterns and reading infrared facial patterns using simple video camera for image capturing.

## **B. Data and transaction security:**

It ensures the *privacy* and confidentiality in electronic messages and data packets, including the authentication of remote users in network transactions for activities such as on-line payments. The goal is to defeat any attempt to assume another identity in data communication. *Encryptions* using various cryptographic methods are being used as a preventive measure.

Major threat to data security is unauthorized network monitoring, called "*packet sniffing*".

### **Threats to Message security**

- Message Confidentiality
- Message and System integrity
- Message Sender Authentication/Identification

**Confidentiality** means maintaining the privacy of the sensitive data (such as credit card numbers, employee records, government files, and social security numbers) being

traversing through the network. Confidentiality precludes access to, or release of, such information to unauthorized users.

**Message and System Integrity** causes the contents remain unmodified during transport. In other words, information received must have the same content as in information content being sent. It must be clear that no one has added, deleted, or modified any part of the message. Unauthorized combination of messages either by intermixing or concatenating during submission, validation, processing, or delivery should not be allowed.

While confidentiality protects against the passive monitoring of data, mechanisms for integrity must prevent active attacks involving the modification of data.

The various techniques being used for message integrity are:

- Error detection codes or checksums
  - Sequence numbers
  - Encryption
- ✓ Error detection codes operate on the entire message or selected fields within a message.
- ✓ Sequence numbers prevent reordering, loss or replaying of messages by attackers.
- ✓ Encryption techniques such as digital signatures can detect modifications of a message.

**Message Sender Authentication/Identification** is a mechanism whereby the receiver of a transaction or message can be confident of the identity of the sender and/or the integrity of the message. In other words, authen...

### The Internet Protocol (IP) suite

TCP/TP is a family of protocols. Samples of these protocols are UDP, IP Multicast, and Mobile IP. The most accurate name for this set of protocols is the “Internet Protocol Suite” as these protocols define how certain applications are to be accomplished on the Internet: electronic messaging, online connections, and the transfer of files.

The TCP/IP suite of protocols was initially used to interconnect hosts on ARPNET, PRNET (packet radio), SATNET (packet satellite). The design of the Internet protocols explicitly accounted for the fact that the networks being tied together were heterogeneous in nature. They each supported different speeds, error characteristics, data unit sizes, and information formats.

The TCP/IP protocols stack has five layers:

1. Application or process layer is an application protocol such as e-mail
2. Transport layer is a protocol such as TCP that provides services needed by many applications

3. Internetwork layer provides the basic service of getting datagram to their final destination
4. Network layer takes care of IP addressing and domain name services (DNS)
5. Physical layer includes the protocols needed to manage a specific medium, such as Ethernet or a point-to-point line. At the lowest level of the physical layer is the actual physical infrastructure, for example, the telephone network, dedicated links, and satellite circuits.

The layering is called TCP/IP because TCP and IP are seldom seen apart. They are separate layers that address discrete functions. IP handles functions of routing and addressing, essentially making sure that each data packet put on the network is sent to the right destination node. TCP handles end-to-end transport layer connectivity between communicating processes. It ensures that all data associated with the connection are sent in the right sequence and that its corresponding TCP segment has correctly received and passed the data to the appropriate process or entity.

While TCP can not exist without an underlying IP entity, IP can live without TCP. In this case, there is a simple, non connection-oriented protocol called the UDP that takes the place of TCP.

Data packets sent without high-level session controls are called datagram. This can result in faster throughput; there is no way to be certain the datagram were actually delivered.

Most often TCP and IP operate inseparably, example of the TCP/IP stack sending and receiving electronic mail. At the application layer is an application protocol for e-mail. Email, like other application protocols, simply defines a standard set of commands and messages to be sent that one e-mail application sends to another. However, this application protocol assumes reliable communication between the two computer services provided by lower-level layers of TCP and IP. TCP is responsible for making sure that the e-mail messages get through to the other end. It keeps track of what is sent and retransmits anything that did not get through. If any message is too large for one datagram, TCP will split it up to several datagram and make sure that they all arrive correctly. The network is made up of several computers; datagram must be routed from the source to the destination. Routing requires several services that have been collectively put together into IP. These functions are common to many applications, they are put together into a separate protocol rather than being part of the specifications for sending mail. IP can be thought of as forming a library of procedures that applications draw upon for reliable delivery.

TCP/IP does include the fundamental concept of independent layers, thus allowing the flexibility for computers operating with similar protocol stacks to communicate with one another. The name of a unit of data flowing through the layers depends on where it exists in the protocol stack. If it is in an application, it is called message; if it is between the IP and the TCP layers, it is called a TCP segment (more generally, a transport message); if it is between the IP and UDP layers, it is called a UDP datagram; if it is between the packet driver and the IP layer, it is called an IP packet; if it is on a packet driver (e.g. Ethernet), it is called a frame.

## **User Datagram Protocol (UDP)**

UDP an alternative of TCP is a connectionless datagram delivery service that does not guarantee delivery. UDP does not maintain an end-to-end connection with the remote UDP module; it merely pushed the datagram out on the net and accepts incoming datagram off the net.

What TCP and UDP have in common is their responsibility for dividing outbound data from the application layer into packets of appropriate sizes, transferring them to the IP layer to be stamped and shipped; unpacking inbound packets from the IP layer; and passing data to the application layers. UDP adds two, values to what is provided by IP. One is the multiplexing of information between applications based on port number. The other is a checksum to check the integrity of data. Network applications that use UDP are MBONE broadcast video on the Internet, Network File System (NFS) and Simple Network Management Protocol (SNMP).

## **Internet Protocol**

IP represents the heart of the Internet protocol suite. The IP layer provides services that permit data to travel hosts residing on multiple networks. In addition to inter-network routing, IP provides error reporting and fragmentation and reassembly of information units.

In addition to IP, the inter-network layer also incorporates two other protocols: The Internet Control Message Protocol (ICMP) and the Internet Group Management Protocol (IGMP). ICMP provides diagnostic, error messaging, and demand-reply functions, such as replies to packet Internet groper (ping) request- IGMP is responsible for User Datagram Protocol (UDP) broadcasting or multicasting, such as sending UDP packets to all IP machines or to multiple machines on the same inter-network.

At the inter-network layer, IP provides both packet addressing and best-effort forwarding services. It addresses and transfers data packets from the transport layer to the physical link layer; passes back incoming packets that have destination addresses (sockets) within the machine from the physical link layer to the transport layer, and forwards to a router.

The sending host provides the network with the network address of the receiving host to ensure that the network routes the data properly. The Internet routing protocol runs not only on local hosts, but also on gateway that connect two networks. A gateway's primary responsibility is to relay data from one network to the other, making sure it gets to the appropriate destination host.

## **Firewall and Network Security**

A firewall is a software program or hardware appliance that protects the resources of a network or workstation as of users from other networks. This means that it will authorize

or prohibit traffic from entering the workstation based on the settings configured. A user can then control from where they are willing to accept packets. It also hides internal systems and information from the public.

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a *hardware device* or a *software program* running on a secure host computer. In either case, it must have at least two network interfaces, one for the network it is intended to protect (private network), and one for the network it is exposed to (public network). A firewall sits at the junction point or gateway between the two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers. The term firewall comes from the fact that by segmenting a network into different physical subnetworks, they limited the damage that could spread from one subnet to another just like firedoors or firewalls.

## Firewalls Techniques

There are several types of firewall techniques:

- **Packet filter:** Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Application gateway:** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.
- **Circuit-level gateway:** Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Proxy server:** Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques.

A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

Firewall work closely with a router program; verifying each network packet to resolve whether to forward it in the direction of its destination. It includes or works with a proxy

server that makes network requests on behalf of workstation users. A firewall is often installed in a specifically chosen computer separate from the rest of the network so that no incoming request can get directly at private network resources.

### Note

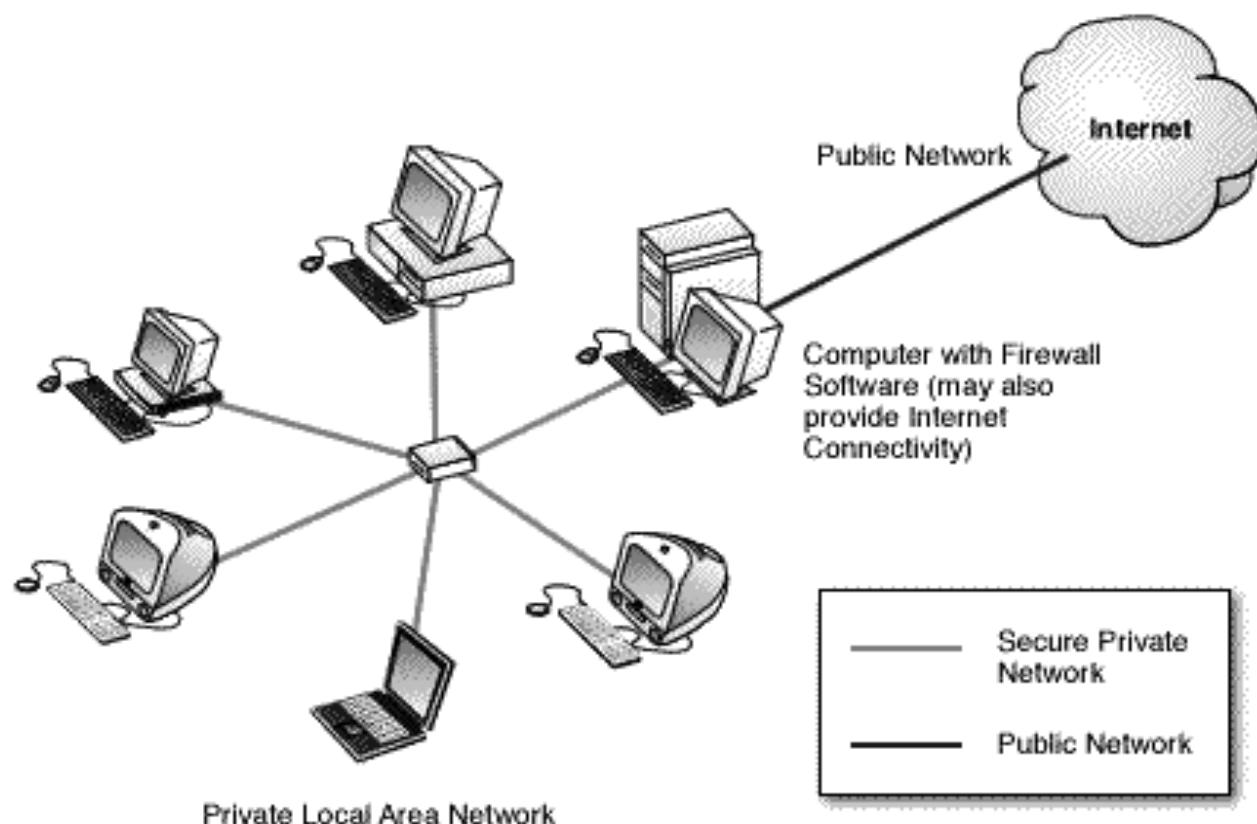
People often think that having a firewall between your internal network and the ``Big Bad Internet'' will solve all your security problems. It may help, but a poorly setup firewall system is more of a security risk than not having one at all. A firewall can add another layer of security to your systems, but it cannot stop a really determined cracker from penetrating your internal network. If you let internal security lapse because you believe your firewall to be impenetrable, you have just made the crackers job that much easier.

### Forms of firewalls

There are two types of firewalls, *software* and *hardware*.

#### 1. Software Firewall

Computer running firewall software to provide protection



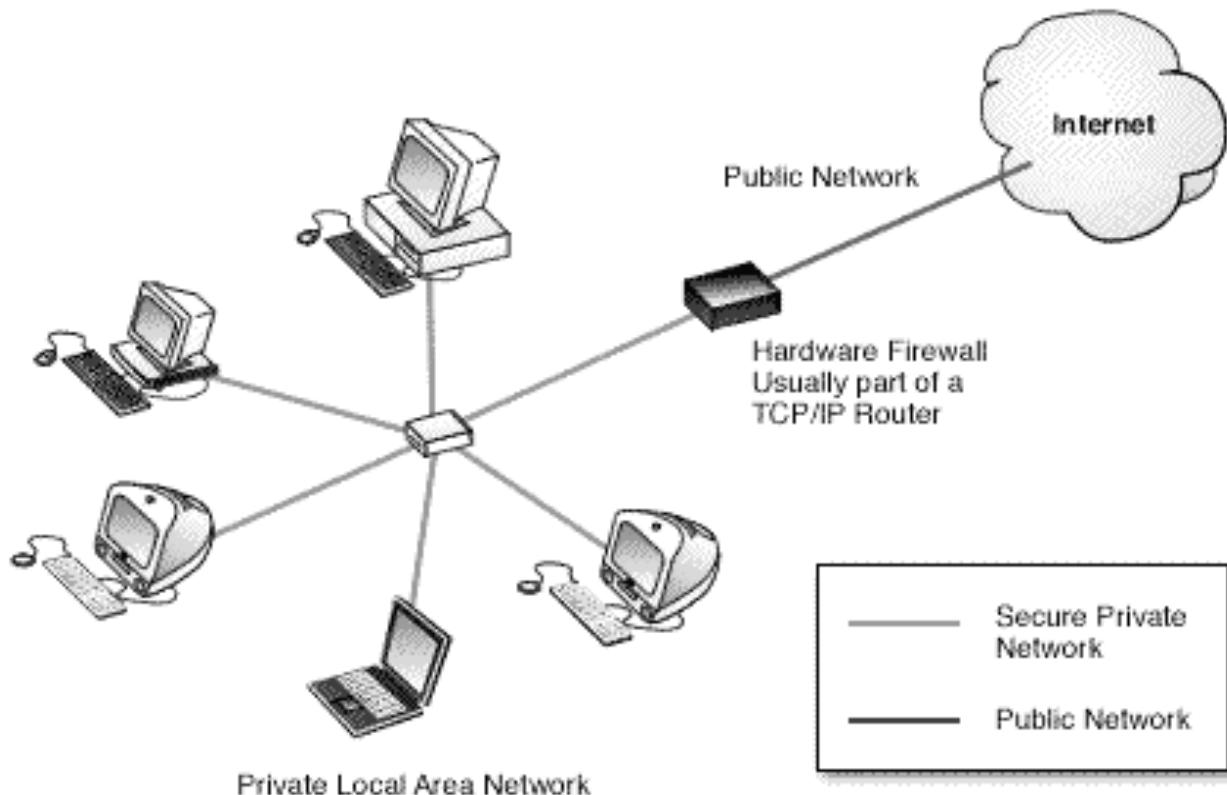
Recommended software firewalls:

- BlackICE Defender
- Norton Internet Security 2001

- Tiny Personal Firewall
- ZoneAlarm
- DoorStop Personal (Macintosh)
- NetBarrier (Macintosh)

## 2. Hardware Firewall

Hardware firewall providing protection to a Local Network



Recommended Hardware firewalls:

- Linksys Etherfast Cable & DSL Router
- Netgear RT311 Gateway Router
- Macsense MIH-120 XRouter

### Firewall functions

The fundamental principle of firewall models and configurations is to allow users from a protected network to access public network while at the same time protecting the company's product and services for the public.

A firewall may permit all traffic from beginning to end unless it meets certain criteria, or it may reject all traffic unless it meets certain criteria. Firewalls may be alarmed with the nature of traffic, or with basis or destination addresses and ports. They may also make

use of multipart rule basis that evaluate the application data to determine if the traffic should be allowable. A firewall determinant depends on which network layer it operates at. The network layers definition follows under the “OSI and TCP/IP Network models”.

Useful functions of firewall include:

- Filtering Packets.
- Serving as a circuit-level or application-level gateway.
- Detecting annoyances.
- Providing enhanced password verifications.
- Taking tricky actions.
- Allowing encrypted access.

## Notes

### What does a firewall do?

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, ftp or telnet. Firewalls can also filter traffic by packet attribute or state.

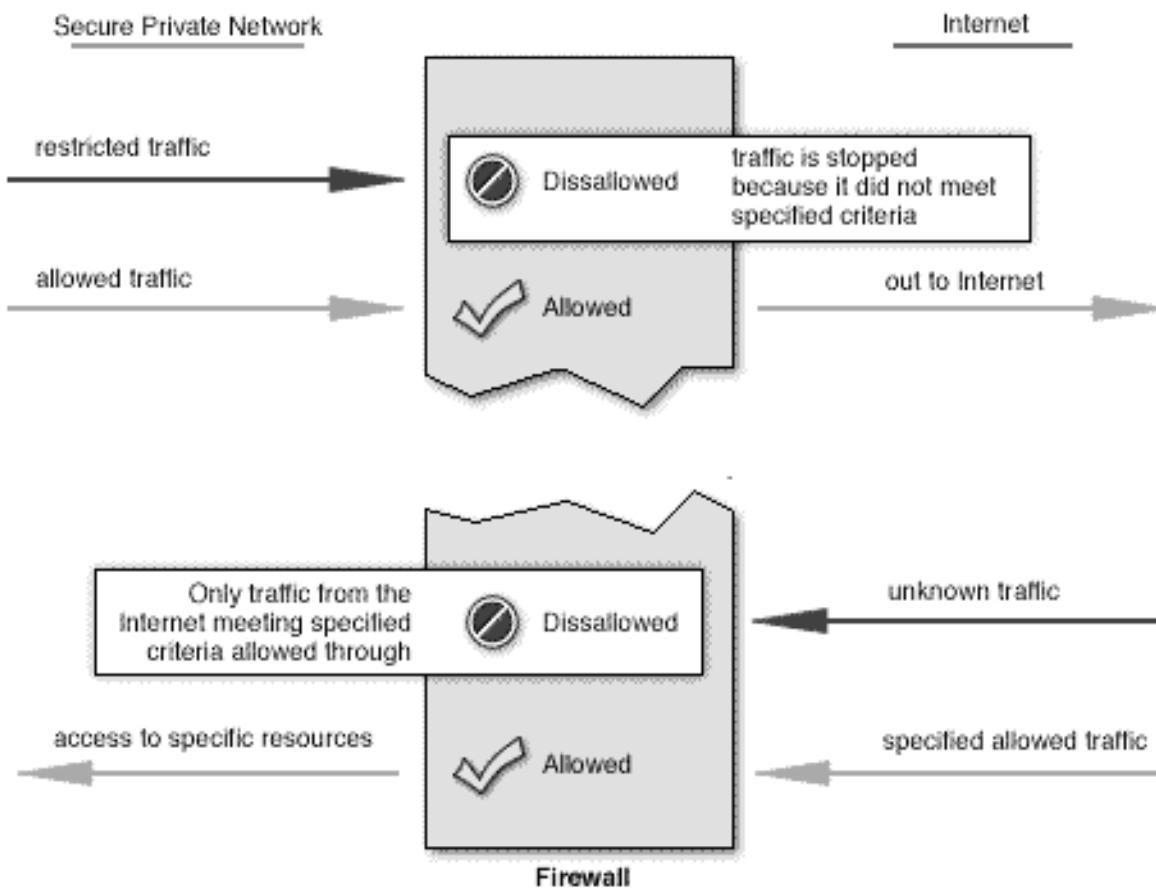
### What can't a firewall do?

A firewall cannot prevent individual users with modems from dialling into or out of the network, bypassing the firewall altogether. Employee misconduct or carelessness cannot be controlled by firewalls. Policies involving the use and misuse of passwords and user accounts must be strictly enforced. These are management issues that should be raised during the planning of any security policy but that cannot be solved with firewalls alone. Firewalls are poor protection against threats such as viruses. A firewall cannot protect replace user security-consciousness. In general, a firewall cannot protect against data-driven attacks-attacks in which something is mailed or copied to an internal host and then executed.

### How does a Firewall work?

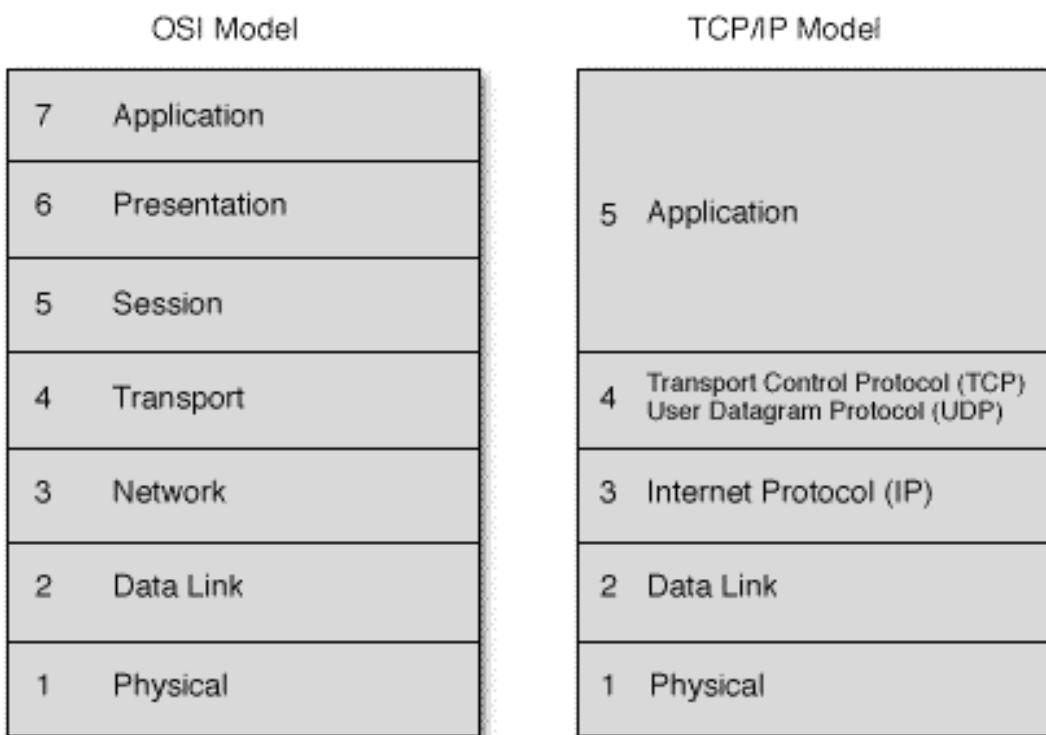
There are two access denial methodologies used by firewalls. A firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria. The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another. Firewalls may be concerned with the type of *traffic*, or with *source* or *destination addresses* and *ports*. They may also use

complex rule bases that analyse the application data to determine if the traffic should be allowed through. How a firewall determines what traffic to let through depends on which network layer it operates at.



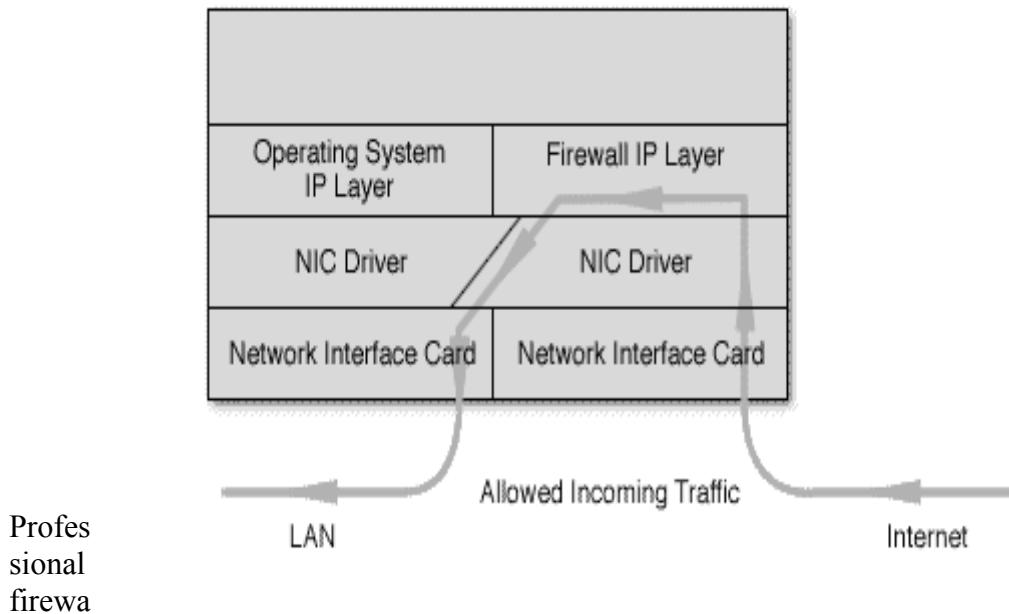
### **open Systems Interconnection (OSI) and Transmission Control Protocol/ Internet Protocol (TCP/IP) Network models**

Network structural design is planned around a seven layer model. Each layer has its own set of duties. This enables networks to counterpart network protocols and physical chains. The TCP/IP model is older than the OSI industry standard model which is dissimilar in every respect.



Firewalls function at different layers to use different criteria to limit traffic. The lowest layer where a firewall can work is layer three. In the OSI form this is the network layer. In TCP/IP it is the Internet Protocol layer. This layer is disturbed with routing packets to their target. At this layer firewall can determine whether a packet is from trusted basis,

but it cannot alarm what it contains. At the transport layer (layer 4) firewalls know supplementary about the packet and it allows or denies transportation access. At application layer firewall have great information of what is going on and to be decided to access or not.

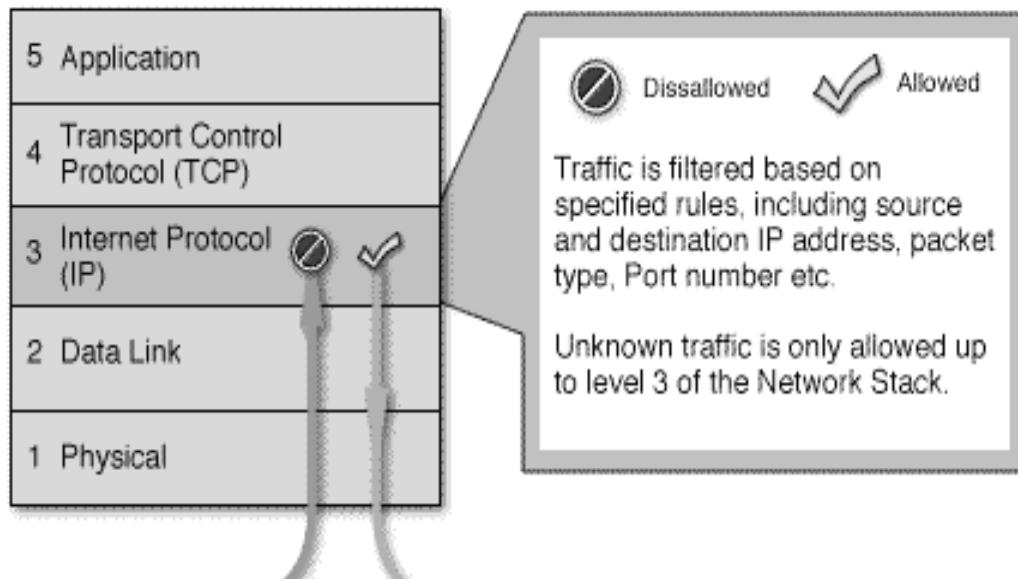


Professional  
firewa

ll products seize each network packet before the operating system does; therefore, there is no straight path from the Internet to the operating system's TCP/IP stack. As a result it is very tricky for strangers to gain control of the firewall host computer then "open the doors" from the inside.

## Types of firewalls

### 1. IP packet filters/screening routers



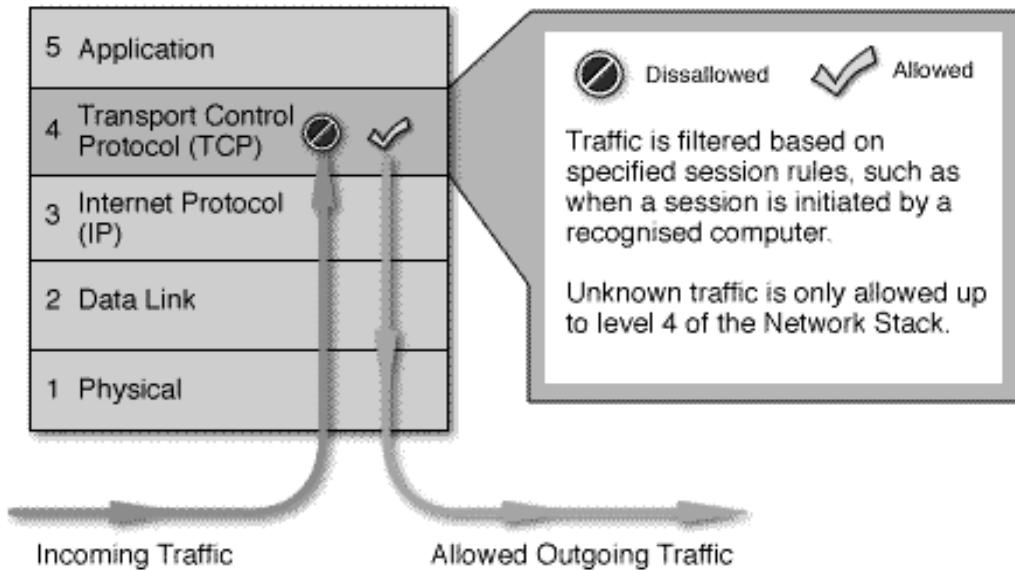
Packet filtering firewall functions at the network level of the OSI model or the IP layer of TCP/IP. They are usually part of a router. A **router** is a device that receives packets from one network and forwards them to another network. The benefit of packet filtering firewalls is their low cost and low impact on network presentation. Most routers support packet filtering. This type of firewall only works at the network layer. Network Address Translation (NAT) routers offer the reward of packet filtering firewalls but can also conceal the IP addresses of computers behind the firewall, and offer a point of circuit-based filtering.

### IP spoofing

Many firewalls examine the source IP addresses of packets to determine if they are legitimate. A firewall may be instructed to allow traffic through if it comes from a specific trusted host. A malicious cracker would then try to gain entry by "spoofing" the source IP address of packets sent to the firewall. If the firewall thought that the packets originated from a trusted host, it may let them through unless other criteria failed to be met. Of course the cracker would need to know a good deal about the firewall's rule base to exploit this kind of weakness.

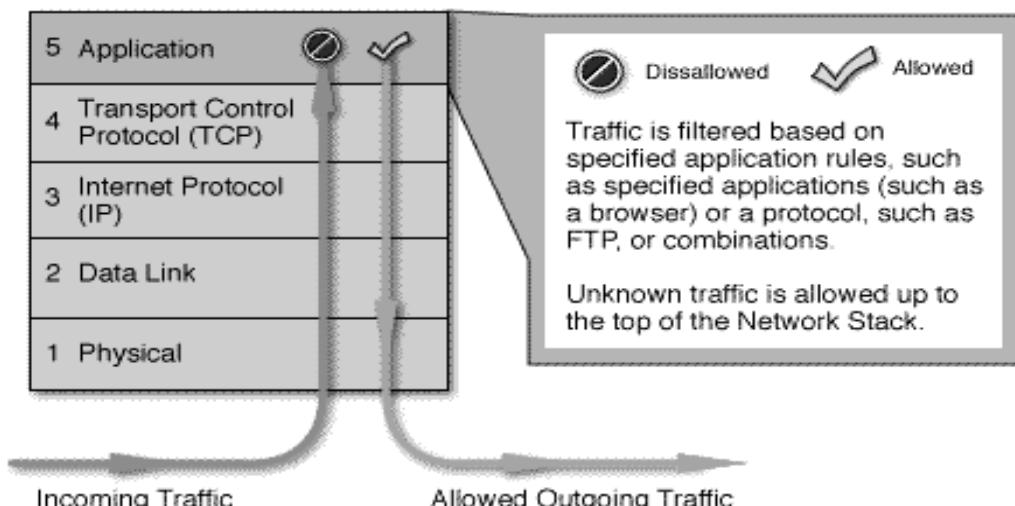
An effective measure against IP spoofing is the use of a *Virtual Private Network (VPN)* protocol such as **IPSec**. This methodology involves encryption of the data in the packet as well as the source address. The VPN software or firmware decrypts the packet and the source address and performs a checksum. If either the data or the source address have been tampered with, the packet will be dropped. Without access to the encryption keys, a potential intruder would be unable to penetrate the firewall.

## 2. Circuit level gateways



Circuit level gateways work at the session layer of the OSI model, or the TCP layer of TCP/IP. “They monitor TCP handshaking between packets to determine whether a requested session is legitimate”. Circuit level gateways are comparatively cheap and have the advantage of hiding information regarding the private network they protect.

### 3. Application level gateways



Application level gateways, also called proxies and are comparable to circuit-level gateways except that they are application specific. This means that they can filter packets at the application layer of the OSI model. Incoming or outgoing packets cannot contact services for which there is no proxy. Application level gateways can also be used to log user

activity and logins. They offer an elevated level of security, but have a significant impact on network performance.

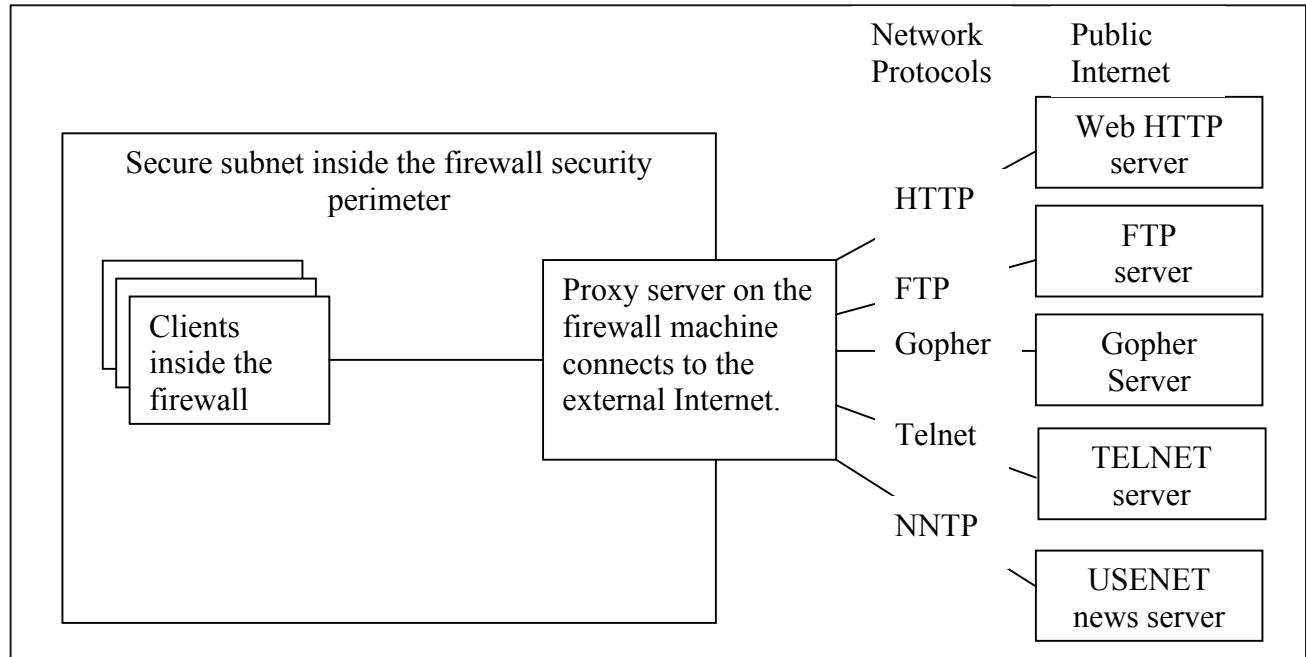
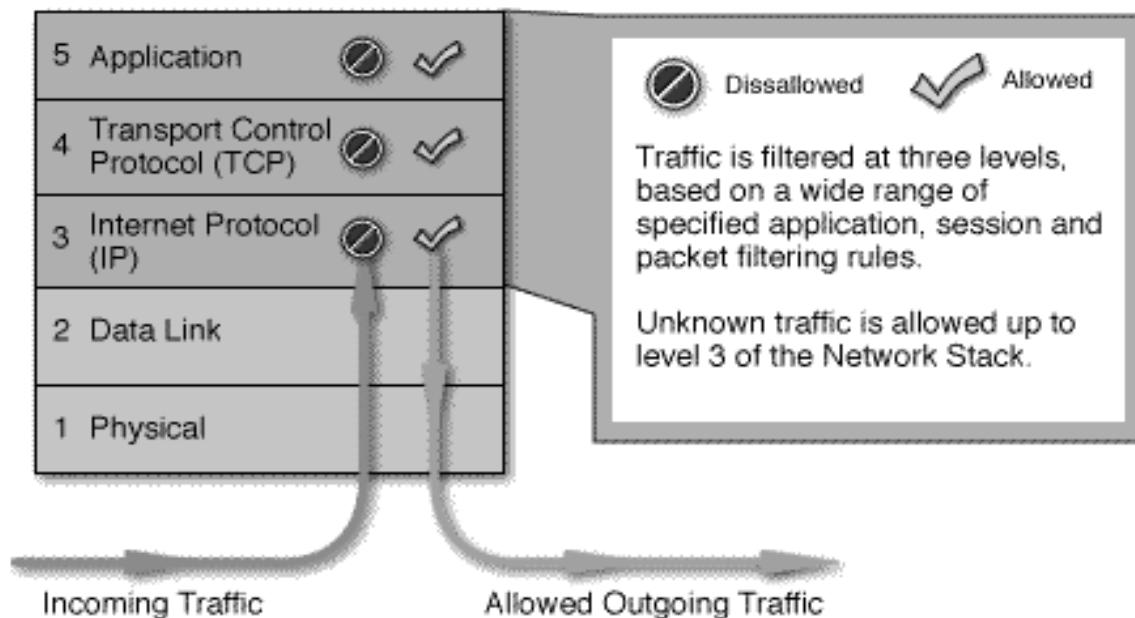


Fig: Proxy Server on the WWW

Proxy server is running either on a firewall host or other internal host, which has full internet access, making connections to the public Internet through SOCKS or other firewall software.

#### 4. Stateful multilayer inspection firewalls

Stateful Multilayer inspection firewalls merge the aspects of the other three types of firewalls. They filter packets at the network layer, determine whether session packets are legal and estimate contents of packets at the application layer. They allow direct connection between client and host and determine the problem caused by the lack of transparency of application level gateways. Stateful multilayer inspection firewalls present a high level of security, good performance and transparency to end users and they are costly.



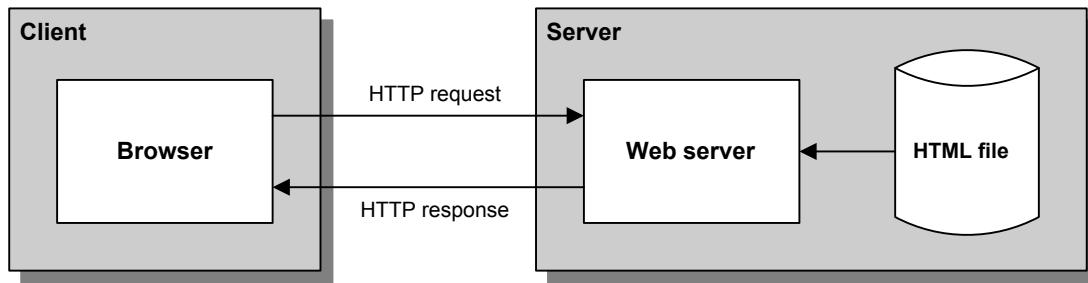
### Benefits of a firewall

Firewalls protect private local area networks from hostile intrusion from the Internet. Consequently, many LANs are now connected to the Internet where Internet connectivity would otherwise have been too great a risk.

Firewalls allow network administrators to offer access to specific types of Internet services to selected LAN users. This selectivity is an essential part of any information management program, and involves not only protecting private information assets, but also knowing who has access to what. Privileges can be granted according to job description and need rather than on an all-or-nothing basis.

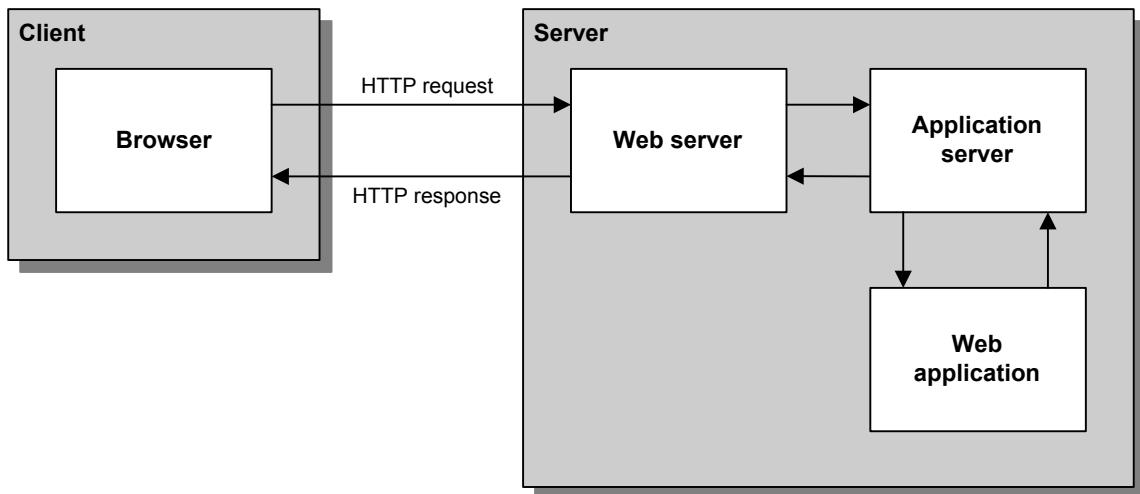
## Web Technologies

### Static web page



- ◆ A *static web page* is an HTML document that is the same each time it's viewed. It doesn't change in response to user input.
- ◆ Static web pages are usually simple HTML files that are stored on the web server with a file extension of .htm or .html. When a browser requests a static web page, the web server retrieves the file from disk and sends it back to the browser.
- ◆ A web browser requests a page from a web server by sending the server an HTTP message known as an *HTTP request*.
- ◆ The HTTP request includes, among other things, the name of the HTML file being requested and the Internet address of both the browser and the web server.
- ◆ A user working with a browser can initiate an HTTP request in several ways. One way is to type the address of a web page, called a *URL*, or *Uniform Resource Locator*, into the browser's address area and press Enter. Another way is to click a link that refers to a web page.
- ◆ A web server replies to an HTTP request by sending a message known as an *HTTP response* back to the browser.
- ◆ The HTTP response contains the addresses of the browser and the server as well as the HTML document that's being returned.

## Dynamic web page



- ◆ A *dynamic web page* is an HTML document that's generated by a web application. Often, the web page changes according to information that's sent to the web application by the browser.
- ◆ When a web server receives a request for a dynamic web page, the server passes the request to an *application server*.
- ◆ The application server executes the web application, which generates an HTML document. This document is returned to the application server, which passes it back to the web server. The web server, in turn, sends the document back to the browser.
- ◆ After the page is displayed, the user can interact with it using its controls. Some of those controls let the user *post* the page back to the server, so it's processed again using the data the user entered.
- ◆ To determine what application server is used to process a request, the web server looks up the extension of the requested file in a list of *application mappings*.
- ◆ Each application mapping specifies which application should be run to process files with that extension.
- ◆ If the file extension is aspx, the request is passed to ASP.NET.
- ◆ If the file extension isn't in the list of application mappings, the requested file is returned to the browser without any processing.
- ◆ The process that begins with the user requesting a web page and ends with the server sending a response back to the client is called a *round trip*.
- ◆ After a web application generates an HTML document, it ends. Then, unless the data the application contains is specifically saved, that data is lost.

## **HTTP Overview**

- HTTP is the standard Web transfer protocol.
- The HTTP is the language that Web clients and Web servers use to communicate with each other.
- It is essentially the backbone of the web.
- The common protocol used by HTTP at transport layer is TCP which is not formally required by the standard.
- It is a constantly evolving protocol with several versions in use and others are still under development.
- This protocol has two items: the set of requests from browsers to servers and the set of responses going back the other way.
- It is a stateless protocol and does not maintain any information from one transaction to the next, so the next transaction needs to start all over again
- The advantage is that an HTTP server can serve a lot more clients in a given period of time, since there's no additional overhead for tracking sessions from one connection to the next.

## **HTTP Transaction**

All HTTP transactions follow the same general format. Each client request and server response has three parts: the request or response line, a header section, and the entity body. The client initiates a transaction as follows:

1. The client contacts the server at a designated port number (by default, 80). Then it sends a document request by specifying an HTTP command called a *method*, followed by a document address, and an HTTP version number. For example:

```
GET /index.html HTTP/1.0
```

Uses the GET method to request the document *index.html* using version 1.0 of HTTP.

2. Next, the client sends optional header information to inform the server of its configuration and the document formats it will accept. All header information is given line by line, each with a header name and value. For example, this header information sent by the client indicates its name and version number and specifies several document preferences:

```
User-Agent: Mozilla/2.02Gold (WinNT; I)
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg, */*
```

The client sends a blank line to end the header.

3. After sending the request and headers, the client may send additional data. This data is mostly used by CGI programs using the POST method. It may also be used

by clients like Netscape Navigator-Gold, to publish an edited page back onto the Web server.

The server responds in the following way to the client's request:

1. The server replies with a status line containing three fields: HTTP version, status code, and description. The HTTP version indicates the version of HTTP that the server is using to respond. The status code is a three digit number that indicates the server's result of the client's request. The description following the status code is just human-readable text that describes the status code. For example, this status line:

HTTP/1.0 200 OK

indicates that the server uses version 1.0 of HTTP in its response. A status code of 200 means that the client's request was successful and the requested data will be supplied after the headers.

2. After the status line, the server sends header information to the client about itself and the requested document. For example:

```
Date: Fri, 20 Sep 1996 08:17:58 GMT  
Server: NCSA/1.5.2  
Last-modified: Mon, 17 Jun 1996 21:53:08 GMT  
Content-type: text/html  
Content-length: 2482
```

A blank line ends the header.

3. If the client's request is successful, the requested data is sent. This data may be a copy of a file, or the response from a CGI program. If the client's request could not be fulfilled, additional data may be a human-readable explanation of why the server could not fulfill the request.

In HTTP 1.0, after the server has finished sending the requested data, it disconnects from the client and the transaction is over unless a *Connection: Key Admin* header is sent. In HTTP 1.1, however, the default is for the server to maintain the connection and allow the client to make additional requests.

Being a stateless protocol, HTTP does not maintain any information from one transaction to the next, so the next transaction needs to start all over again. The advantage is that an HTTP server can serve a lot more clients in a given period of time, since there's no additional overhead for tracking sessions from one connection to the next.

## File Transfer Protocol (FTP)

- File Transfer Protocol (FTP) is a method of transferring files from a client to a server or vice versa.
- Files are transferred over the Internet using TCP/IP protocol.
- FTP (RFC 959) is old-time protocol that maintains two simultaneous connections.
- The first connection uses the telnet remote login protocol to log the client into an account and process commands via the *protocol interpreter*.
- The second connection is used for the *data transfer process*.
- Whereas the first connection is maintained throughout the FTP session, the second connection is opened and closed for each file transfer.
- The FTP protocol also enables an FTP client to establish connections with two servers and to act as the third-party agent in transferring files between the two servers.
- FTP servers rarely change, but new FTP clients appear on a regular basis.
- These clients vary widely in the number of FTP commands they implement.
- Very few clients implement the third-party transfer feature, and most of the PC clients implement only a small subset of the FTP commands.
- Although FTP is a command-line oriented protocol, the new generation of FTP clients hides this orientation under a GUI environment.
- FTP uses TCP port 21.

\* \* \* \* \* THE END \* \* \* \*

**PURBANCHAL UNIVERSITY**  
**2019**

B.E. (Computer) / Seventh Semester / Final  
 Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG473CO: Simulation & Modeling (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

- 1(a) Explain the concept of System. Differentiate between Continuous and discrete, Deterministic and Stochastic system with example. 5
- (b) Explain the phases and steps in simulation study. 5
2. A vegetable shopkeeper is trying to determine how much green vegetable he has to purchase for selling. The probability distribution of no. of customer is as follow.

|                     |      |      |      |      |
|---------------------|------|------|------|------|
| No. of customer/Day | 8    | 10   | 12   | 14   |
| Probability         | 0.35 | 0.30 | 0.25 | 0.10 |

Customer order 1,2,3 or 4 kg of vegetable as per the following probability distribution.

|                     |     |     |     |     |
|---------------------|-----|-----|-----|-----|
| Kg ordered/Customer | 1   | 2   | 3   | 4   |
| Probability         | 0.4 | 0.3 | 0.2 | 0.1 |

Vegetable sells for Rs. 50 per kg. All vegetable not sold for the day are sold at half price. Based on 5 days of simulation how much vegetable the shopkeeper should purchase each day. 10

- 3(a) Discuss the basic philosophy of Monte-Carlo simulation. 5
- (b) Explain the concept of continuous system simulation. 5
- 4(a) Explain mid square random number generator. 5
- (b) Enumerate the qualities of good random number generator. Use linear congruential method to generate random numbers with full period with seed value 6 and 7. Take  $a=12$ ,  $c=5$  and  $m=26$ . 5

(2)

5. What do you mean by testing of random numbers, why it is needed? Use Chi-Square test to test the following random numbers with confidence level 95%. 3+7
- 36, 91, 51, 02, 54, 06, 58, 06, 58, 02, 54, 01, 48, 97, 43,  
22, 83, 25, 79, 95, 42, 87, 73, 17, 02, 42, 95, 38, 79, 29,  
65, 09, 55, 97, 39, 83, 31, 77, 17, 62, 03, 49, 90, 37, 13,  
17, 58, 11, 51, 92
6. "Simulation output has to be analyzed", Justify the statement. Explain the process of replication of runs and elimination of internal bias in the analysis of simulation output. 10
7. List out the various simulation tools. Explain GPSS in brief with suitable example. 10
8. Explain the principle of discrete system simulation. Explain feedback system with its application. 4+6
9. Write short notes on any TWO 5+5  
(a) Markov Chain  
(b) Application areas of simulation  
(c) Kendall's notation



**PURBANCHAL UNIVERSITY**  
**2017**

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG473CO: Simulation & Modeling (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer EIGHT questions.**

1. What do you mean by system simulation? Why do we need simulation? Explain a field of life where you would like to use simulation. 2.5+2.5+5
2. Why do you need a model for simulation? Explain the phases and steps to be followed in Simulation. 2+8
3. What are the different types of simulation? Explain each with example. Explain the concept of Monte Carlo Simulation with suitable example to calculate the value of " $\pi$ (pi)" using  $x^2+y^2=9$ . 5+5
4. What is a queuing system? Why is it an important part of Simulation studies? Explain the Kendall's' queuing notation for different types of queues. 3+2+5
5. Explain the LCG and MCG methods of random number generation. Generate a sequence of random numbers with  $X_0=37$ ,  $a=7$ ,  $c=29$  and  $m=100$ . 5+5
6. Develop poker test for the following 1000 4-digit random numbers generated during an experiment to test whether they are independent or not at 5% level of significance. ( $\alpha_{0.05,2}=5.99$ ) 10
 

| combination               | Observed frequency |
|---------------------------|--------------------|
| Three different digits    | 700                |
| Two like digits           | 278                |
| Three exactly same digits | 22                 |
7. What do you mean by analog methods? Explain the analog computer model of automobile suspensions system. 4+6

(2)

8. Discuss Markov chains with their practical areas of application.  
Why are differential equations used in continuous system  
simulation? 6+4
9. Write short notes on any TWO 5+5
- (a) Continuous and Discrete System
  - (b) GPSS
  - (c) Simulation Run Statistics
- \*\*\*

**PURBANCHAL UNIVERSITY**  
**2017**

B.E. (Computer) / Seventh Semester / Final

Full Marks: 80 / Pass Marks: 32

Time: 03.00 hrs.

**BEG473CO: Simulation & Modeling (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

1. What do you mean by system simulation? What is Model?  
 Explain the steps in simulation study with necessary flowchart.  
 2+2+6

✓ 2. Define continuous and discrete systems. Write advantages and limitations of simulation techniques. Write its application areas.  
 2+6+2

3. Discuss Monte Carlo Method. Using Monte Carlo method, calculate the integral  $\int x dx$ . How Monte Carlo Method differs from stochastic simulation?  
 3+5+2

✓ 4. What do you mean by feedback system? What is analog method?  
 Design the analog computer model for the given second order differential equation:  
 $M\ddot{x} + D\dot{x} + Kx = KF(t)$   
 2+3+5

5. Describe Measurement of System Performance of Queuing system with necessary formulae. What is Markov Chain? 7+3

✓ 6. What do you mean by verification and validation of simulation model? Describe the techniques for verification of simulation model.  
 3+7

✓ 7. Why computer generated random numbers are called pseudo random numbers? Describe Linear Congruential Generator with example. Mention the qualities of efficient random number generator.  
 2+5+3

Contd. ...

*S/2015*

(2)

✓ 8. Describe estimation methods for simulation output. Explain GPSS with an example. 5+5

✓ 9. Write short notes on any TWO

- (a) Hybrid Simulation
- (b) Poker Test
- (c) A pure Pursuit Problem

\*\*\*

**PURBANCHAL UNIVERSITY**  
**2017**

B.E. (Computer) / Seventh Semester / Back

Time : 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG473CO: Simulation & Modeling (Old Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

**8×10=80**

1. What do you mean by continuous and discrete systems? Explain with an example of each. Describe real time simulation briefly. What are the limitations of Simulation technique? 2+2+2+4
2. Explain static mathematical model. Describe steps and phases in Simulation study. 4+6
3. State and explain qualities of an efficient random number generator. Generate 5 random numbers using LCM with  $a=11$ ,  $m=16$ ,  $c=1$  and  $X_0=7$ . 5+5
4. A sequence of 1000 four-digit numbers has been generated and an analysis shows the following combinations and frequencies: 10

| <b>Combination, <math>i</math></b> | <b>Observed frequency, <math>O_i</math></b> |
|------------------------------------|---------------------------------------------|
| Four different digits              | 565                                         |
| One pair                           | 392                                         |
| Two pairs                          | 17                                          |
| Three like digits                  | 24                                          |
| Four like digits                   | 2                                           |
| Total                              | 1000                                        |

Based on the poker test, test whether these numbers are independent at  $\alpha=0.05$ . 10

5. Distinguish analog computers with digital computers. Draw and briefly explain analog computer model of liver. 4+6
6. Explain the importance of Markov chain. Find the value of  $\Pi$  using Monte Carlo method. 4+6

**Contd. ...**

(2)

7. A baker is trying to determine how many dozens of cake to bake each day. The probability distribution of the number of cake-customers is as follows:

|                      |      |      |      |      |
|----------------------|------|------|------|------|
| No. of Customers/Day | 8    | 10   | 12   | 14   |
| Probability          | 0.40 | 0.30 | 0.20 | 0.10 |

Customers order 1, 2, or 3 dozen cakes according to the following probability distribution:

|                               |      |      |      |
|-------------------------------|------|------|------|
| No. of dozen ordered/Customer | 1    | 2    | 3    |
| Probability                   | 0.45 | 0.30 | 0.25 |

Cakes sell for 540 per dozen. They cost 380 per dozen to make. All cakes not sold at the end of the day are sold at half price. Based on 6 days of simulation, how many dozen, to the nearest to 10 dozen, cakes should be baked each day? 10

8. Explain GPSS block diagram for a telephone system in detail. 10
9. Why is analysis of simulation output important? Describe estimation methods. 3+7
10. Write short notes on any TWO: 5+5
- (a) Continuous System Modeling Program version III (CSMP III)
  - (b) Pure pursuit problem
  - (c) Normally distributed random number

\*\*\*

**PURBANCHAL UNIVERSITY**  
**2016**

B.E. (Computer) / Seventh Semester / Final  
Time: 09:00 hrs. Full Marks: 80 / Pass Marks: 32  
BEG473CO: Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.  
All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

1. What do you mean by system simulation? Why do we need simulation? Explain a field of life where you would like to use simulation. 2.5+2.5+5

2. Define and explain the concept of system. Why do you need a model for simulation? Explain the limitations and areas of applications of simulation techniques. 3+2+5

3. What are the different types of simulation? Explain each with example. Explain the concept of Monte Carlo simulation with suitable example to calculate the value of " $\pi$ " using  $x^2+y^2=25$ . 5+5

4. What is queuing system? Why is it an important part of simulation studies? Explain different queuing disciplines. 5+5

5. Explain the LCG and MCG methods of random number generation. Generate a sequence of random numbers with  $X_0=37$ ,  $a=7$ ,  $c=29$  and  $m=100$ : 0.8, 0.5, 0.9, 0.7 5+5

6. Why do we have t test Random Numbers? Explain the Chi Square test method of testing random numbers with example. 10

7. What do you mean by analog methods? Explain the analog computer model of automobile suspensions system. 4+6

8. Discuss Markov chains with their practical areas of application. Why are differential equations used in continuous system simulation? 6+4 5+5

9. Write short notes on any TWO

(a) Continuous and Discrete System

(b) Steps and Phases in Simulation Study

(c) Simulation Run statistics

**PURBANCHAL UNIVERSITY**  
**2015**

B.E. (Computer) / Seventh Semester / Choice

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG473CO. Simulation & Modeling (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer EIGHT questions.**

1. Define Simulation. List out its advantages and disadvantages. Also deal with when the use of simulation is appropriate and when it is inappropriate. 10
2. What is discrete event simulation? Draw and explain the flowchart for the organization of discrete event simulation. 3+7
- 3(a) Differentiate between Monte Carlo Simulation with Stochastic Simulation. 4  
(b) Illustrate the case of random process. Consider a game in which an unbiased coin is repeatedly flipped. For each flip you have to pay Re 1 and when the difference between heads and tails tossed becomes 3, you get Rs 8. If the required difference obtained is less than 8 flips, you win some money and if it is more than 8 flips you lose. Illustrate the simulation to decide whether to play this game or not. 6
- 4(a) What are the properties of random numbers? Why the random numbers generated by a computer are called Pseudo-random numbers? Explain. 5  
(b) Write an algorithm for generating random numbers for two or more generators. Also determine its maximum period.
- 5(a) What are the methods used for testing of random numbers? Explain Poker test. 5

Contd. ...

**(2)**

- (b) Test whether the 2<sup>nd</sup>, 7<sup>th</sup>, 12<sup>th</sup> and so on, numbers in the sequence in the given table is auto correlated. (Use  $\alpha=0.05$ ). 5

|      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|
| 0.12 | 0.01 | 0.23 | 0.68 | 0.86 | 0.96 | 0.21 | 0.88 | 0.92 |
| 0.81 | 0.11 | 0.05 | 0.24 | 0.89 | 0.48 | 0.51 | 0.81 | 0.23 |
| 0.33 | 0.29 | 0.68 | 0.58 | 0.91 | 0.60 | 0.35 | 0.46 | 0.55 |
| 0.43 | 0.56 | 0.99 |      |      |      |      |      |      |

6. What is feedback system? Using analog method of simulation, explain the working procedure of human liver with appropriate block diagram, 3+7

- 7(a) Explain point of estimation and confidence level estimation technique during analysis of simulation output. 5

- (b) Explain initial bias in simulation. How can it be eliminated? 5

8. Explain the different blocks used in GPSS. Draw the GPSS block diagram for the following scenario: A machine tool in a manufacturing shop is turning out parts at the rate of 1 every 7 minutes. As they are finished, the parts go to an inspector, who take  $5\pm2$  minutes to examine one and rejects about 15% of the parts. 4+6

9. Write short notes on any TWO: 5+5

- (a) Static Vs Dynamic simulation
- (b) SIPOSRIPT
- (c) Validation and Verification



**PURBANCHAL UNIVERSITY**  
**2015**

B.E. (Computer) / Seventh Semester / Final  
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BEG473CO, Simulation & Modeling (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

1. What do you mean by simulation and modeling? Explain the steps in the simulation study? 3+7

2(a) Explain the analogy method of system study with suitable example. 5

(b) Explain how continuous model can be solved numerically with an example. 5

3(a) Explain the arrival and departure routine queuing model for a banking system. 5

(b) Calculate the following using Monte Carlo simulation. (Use your own random numbers): 5

$$I = \int_{-3}^{5} (x^2 - 1) dx$$

4(a) What are the properties of random numbers? Why the random numbers generated by a computer are called Pseudo-random numbers? 2+2

(b) Write the algorithm for linear congruential method. Using the multiplicative congruential method, find the period of the generators for  $a=13$ ,  $m=2^6$ , and  $X_0=2$  and 4. 3+3

Contd...

(2)

5(a) Explain the Mid square method for generating random numbers with an example.

(b) Consider the given sequence:

0.41 0.68 0.89 0.94 0.74 0.41 0.55 0.62 0.36 0.27  
0.19 0.72 0.75 0.08 0.54 0.02 0.01 0.36 0.16 0.28  
0.18 0.01 0.95 0.61 0.18 0.47 0.23 0.32 0.82 0.53  
0.31 0.12 0.73 0.04 0.83 0.45 0.13 0.57 0.63 0.29

Based on run test check whether given sequence is random or not. [Given  $Z_{\alpha/2} = 1.96$ ]

6(a) Explain feedback system with suitable example.

(b) Explain the mathematical modeling of replication of runs.

7(a) Why simulation output is analyzed? Explain estimation method for analysis of simulation output. 2+3

(b) What is initial bias in simulation output? Mention the idea of elimination of initial bias. 3+2

8(a) Draw different types of GPSS block-diagram symbols and explain with the help of GPSS block-diagram of manufacturing shop. 5

(b) State some types of Simulation languages. Illustrate the possible event interactions in Hybrid Simulation. 5

9. Write short notes on any TWO 5+5

(a) Differential equation

(b) Simulation Run statistics

(c) Markov Chain

**PURBANCHAL UNIVERSITY**  
**2014**

B.E. (Computer) / Seventh Semester / Final  
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG473CO: Simulation & Modeling**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

1. Explain the ways to study a system. What are the criteria of classifying Simulation models? Brief it with suitable example. 3+7
2. What do you mean by discrete event simulation? Explain the principal approaches for advancing the simulation clock in discrete event simulation. 4+6
- 3(a) Explain the concept of Monte-Carlo simulation over stochastic simulation. 5  
(b) Find the value of pi ( $\pi$ ) by using Monte Carlo simulation using the equation  $x^2+y^2= 16$ ? Also Calculate error when compared with its analytical value. 5
4. The computing facility of Purbanchal University has large no. of personal computers. On 50% of working days no computer fails, on 30% of the days 1 machine fails & on 20% of days 2 machines fails. There is a repairing facility, which has one-service personnel. He can fix the problem on the average 40% of the machine in 1 day, 35% in 2 days & 25% in 3 days. The service person says he is overloaded and computer waits a long time for service. He reminds that next should go for second service person. Consider the 30 days slot and verify if the service person claims is correct by computing his efficiency, the number of computers waiting for service and average waiting time for computers. 10

(2)

5. Why are differential equations so important in simulation?  
Explain continuous system simulation with suitable example. 5+5
- 6(a) What are the qualities of good random number generators?  
What are the methods used for testing of random numbers? 5
- (b) Test whether the 2<sup>nd</sup>, 7<sup>th</sup>, 12<sup>th</sup> and so on, numbers in the sequence in the given table are auto correlated. (use  $\alpha=0.05$ ) 5

|      |      |      |      |      |      |      |      |      |      |
|------|------|------|------|------|------|------|------|------|------|
| 0.12 | 0.01 | 0.23 | 0.25 | 0.58 | 0.87 | 0.55 | 0.96 | 0.22 | 0.88 |
| 0.11 | 0.22 | 0.85 | 0.36 | 0.69 | 0.87 | 0.19 | 0.92 | 0.75 | 0.43 |
| 0.68 | 0.58 | 0.91 | 0.60 | 0.35 | 0.33 | 0.15 | 0.49 | 0.27 | 0.99 |

7. Why the output of simulation has to be analyzed? Explain  
Replication of Runs method to any simulation output. 4+6

- 8(a) Why is simulation tool required? What is GPSS language & its  
application? 3+3
- (b) Explain in details of GPSS block diagram symbols. 4

9. Write short notes on any TWO:  
(a) Poker test  
(b) Feedback system  
(c) Elimination of internal bias  $2 \times 5 = 10$

~

# PURBANCHAL UNIVERSITY

2013

B.E. (Computer) / Seventh Semester / Choice

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

## BEG473CO: Simulation & Modeling

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

### Answer EIGHT questions.

1. Explain the ways to study a system. What are the criteria of classifying Simulation models? Brief it with suitable example. 3+7
2. What do you mean by discrete event simulation? Explain the principal approaches for advancing the simulation clock in discrete event simulation. 4+6
- 3(a) List the entities, attributes, activities and state variables in the working of your college workshop. 5  
(b) Find the value of pi ( $\pi$ ) by using Monte Carlo simulation using the equation  $x^2+y^2=25$ ? Also Calculate error when compared with its analytical value. 5
- 4(a) Explain Normally distributed random numbers. 3  
(b) In the random walk problem the drunkard can take steps in four directions, forward, backward, to left and to right. The probabilities associated with these are 40%, 10%, 25%, and 25%. The distances covered in the forward, backward, to left and to right steps are 75 cm, 45 cm, 60 cm, and 60 cm respectively. Simulate the walk for 20 steps, and find the location at the end of 20 steps, while the starting point is (0,0) on the x-y scales. 7
- 5(a) What do you mean by a continuous system, explain pure pursuit problem to represent the continuous system. 5  
(b) Represent the following equation in terms of analog computer block diagram:  $Ax''+Bx'+Cx+D=0$  5
- 6(a) What are the qualities of good random number generators? Explain any two methods of generation of random numbers. 2+3

Contd. ...

(2)

- (b) A random sequence of 10 numbers has been generated as  
 $R(i)=\{0.24, 0.89, 0.11, 0.61, 0.23, 0.86, 0.41, 0.64, 0.50, 0.65\}$ .  
Use Kolmogorov-Smirnov test with  $\alpha=0.05$  to test whether the  
numbers are uniformly distributed. 5
7. Why the output of simulation has to be analyzed? Explain  
Replication of Runs method to any simulation output. 4+6
8. Explain Discrete Simulation Language in brief. Explain the  
system concepts of Simscript. How a program is organized in a  
Simscript. 3+3+4
9. Write short notes on any TWO: 5+5  
(a) Feedback system  
(b) Real time simulation  
(c) GPSS



**PURBANCHAL UNIVERSITY**

**2019**

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

**$8 \times 10 = 80$**

1(a) What is an artificial intelligence? Explain about PEAS any artificial intelligence agent. 2+4

(b) Compare Blind search and Heuristic search. 4

2. What is an expert system and what are its applications? Briefly describe the various steps involved in the development of an expert system. 4+6

3. Describe the various levels of analysis used in natural language processing. 10

4. Express the following sentences into FOPL. 5×2=10

(a) Steve only likes easy course.

(b) Science courses are hard.

(c) All apples in the basket are rotten

(d) Bill eats peanuts and is still alive.

(e) Rita eats everything Bill eats.

5. Define constraint satisfaction problem. Stating necessary conditions and assumptions solve the following crypto-arithmetic problem. SEND+MORE=MONEY. 2+8

6(a) What is neural network? How back propagation works for learning in multilayer network? 2+4

(b) What is hill climbing and its problems? 4

7(a) What are the different types of learning. Explain the induction learning with suitable examples. 2+4

**Contd. ...**

- (b) How does semantic network represent knowledge? Explain with suitable example. 4
8. Write the algorithm of depth-first search and explain with suitable example. 5+5
9. Write short notes on any TWO:  
(a) Genetic Algorithm  
(b) Bayesian network  
(c) Reinforcement learning



**PURBANCHAL UNIVERSITY**

**2018**

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

**8×10=80**

1. What is AI? How is it different from natural intelligence? Support with example. 2+8
2. What is heuristic function? Explain Hill climbing problems with examples. 3+7
3. Define knowledge and knowledge representation. Explain semantic networks and frames are used for knowledge representation with example. 2+8
4. What is non-linear planning? Explain MYCIN-Style probabilities and its application. 4+6
5. Explain natural language processing. Discuss different steps in language understanding and generation in brief. 4+6
6. Convert the following sentences into CNF (Conjunctive Normal Form):  
(a) If Virat is a human, he can think.  
(b) Salmon, Shark and Tarpon are fishes.  
(c) All dogs have a tail.  
(d) Everybody is good at something.  
(e) John likes whatever Peter dislikes and dislikes whatever Peter likes. 5×2=10
7. Solve the following crypto-arithmetic problem: 10  
**CROSS + ROADS = DANGER**

Show all the steps that you advance through constraint satisfaction.

**Contd. ...**

**(2)**

Hopfield  
3+7

8. What is neural network? Explain perception and Hopfield network in brief. 5+5
9. Write short notes on any TWO:
- (a) Simulated Annealing
  - (b) Characteristics of expert-system
  - (c) Bayesian networks.



**PURBANCHAL UNIVERSITY**  
**2017**

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer EIGHT questions.**

**$8 \times 10 = 80$**

- 1(a) ✓ Why is machine learning an important in artificial intelligence?  
Explain inductive learning with an example. 2+4
- 1(b) ✓ How does frame system represent knowledge? Explain with suitable example. 4
2. What is constraint satisfaction problem? Stating necessary conditions and assumptions solve the following crypto-arithmetic problem: EAT+THAT=APPLE. 2+8
3. ✓ What is natural language? Describe the various tasks used in natural language processing. 2+8
4. ✓ Express the following sentences into FOPL:
  - (a) Ram only likes easy course.
  - (b) Management courses are easy.
  - (c) All courses in the Computer department are easy.
  - (d) Bill eats peanuts and is still alive.
  - (e) Sita eats everything Ram eats. $5 \times 2 = 10$
5. What is decision support system? Briefly describe the various steps involved in the development of an expert system. 2+8
6. ✓ What is perceptron? How back propagation works for learning in multilayer network. Explain with suitable examples. 2+8
- 7(a). Explain the importance of artificial intelligence and AI agent. 2+3
- 7(b). Briefly explain the heuristic search with example. 5

*...Amritpal*

**Contd. ...**

(2)

8 Explain iterative deepening. Discuss decision tree

9 Write short notes on any TWO:

- (a) Genetic Algorithm
- (b) Forward chaining-and backward changing
- (c) Reasoning with uncertainty
- (d) Semantic Network

\*\*\*

extra

# PURBANCHAL UNIVERSITY

2017

B.E. (Computer) / Seventh Semester / Final

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

SEQ471CO: Artificial Intelligence (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

**8×10=80**

1. Define PEAS and its properties. Explain the challenges of Al. 7+3
2. What is depth-first search? State its algorithm. Explain how depth-limited search and iterative-deepening search solves the problem of depth-first search. 4+6
3. What do you mean by adversial search? Explain MinMax problem with example. Write the importance of game playing in Al. 2+5+3
- (A) State the inference theorems. Define logic and explain propositional calculus with examples. 6+4
5. How is an expert system different from natural intelligence? Explain the role of knowledge base and inference engine in expert system. 4+6
6. State back-propagation algorithm. Explain the working of Hopfield network with suitable example. 4+6
- 7(a) What are natural language understanding and natural language generation? 5
- (b) Explain case-based reasoning with proper flowchart. 5
- 8(a) How is problem formulated? Explain the types of problem with examples. 5
- (b) Solve the following cryptarithmetic puzzle by stating all the necessary assumptions that you make: 5

(2)

9. Write short notes on any TWO:

5+5

- (a) Forward-chaining vs backward-chaining
- (b) Semantic net
- (c) Reinforcement learning

≡≡

943  
265

984  
258

**PURBANCHAL UNIVERSITY**  
**2017**

B.E. (Computer)/Seventh Semester/Final

Time: 03.00 hrs.

Full Marks: 80 /Pass Marks: 32

**BEG471CO: Artificial Intelligence (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer EIGHT questions.**

**$8 \times 10 = 80$**

- 1(a) Why is machine learning an important in artificial intelligence? Explain inductive learning with an example. 2+4
- (b) How does frame system represent knowledge? Explain with suitable example. 4
2. What is constraint satisfaction problem? Stating necessary conditions and assumptions solve the following crypto-arithmetic problem: EAT+THAT=APPLE. 2+8
3. What is natural language? Describe the various tasks used in natural language processing. 2+8
4. Express the following sentences into FOPL:  $5 \times 2 = 10$
- (a) Ram only likes easy course.
  - (b) Management courses are easy.
  - (c) All courses in the Computer department are easy.
  - (d) Bill eats peanuts and is still alive.
  - (e) Sita eats everything Ram eats.
5. What is decision support system? Briefly describe the various steps involved in the development of an expert system. 2+8
6. What is perceptron? How back propagation works for learning in multilayer network. Explain with suitable examples. 2+8
- 7(a) Explain the importance of artificial intelligence and AI agent. 2+3
- (b) Briefly explain the heuristic search with example. 5

**Contd. ...**

(2)

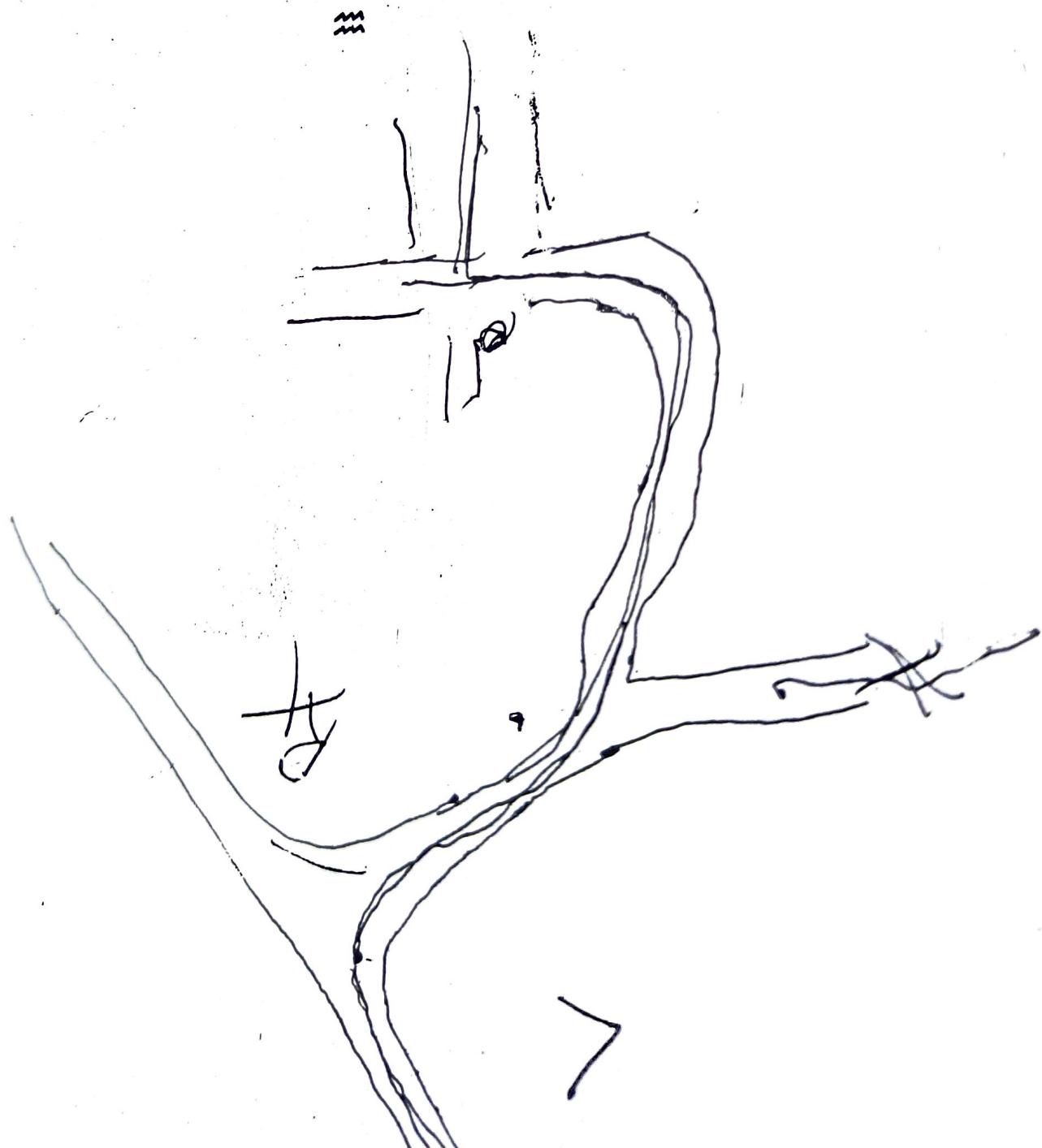
5+5

Explain iterative deepening. Discuss decision tree.

5+5

Write short notes on any TWO:

- (a) Genetic Algorithm
- (b) Forward chaining-and backward changing
- (c) Reasoning with uncertainty
- (d) Semantic Network



**PURBANCHAL UNIVERSITY**  
**2016**

6 (Computer) / Seventh Semester / Final  
Time 03.00 hrs

Full Marks: 80 / Pass Marks: 32

BEG471CO: Artificial Intelligence (New Course)

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

$8 \times 10 = 80$

Answer EIGHT questions.

1(a) What is an artificial intelligence. Explain with suitable example about the importance of artificial intelligence. 2+4

(b) Compare Blind search and Heuristic search. 4

2 Why do you need an expert system? Briefly describe the various steps involved in the development of an expert system. 2+8

3(a) What is natural language? Describe the various levels of analysis used in natural language processing. 2+8

4. Express the following sentences into FOPL: 5×2=10

(a) Steve only likes easy course.

(b) Science courses are hard.

(c) All courses in the basket weaving department are easy.

(d) Bill eats peanuts and is still alive.

(e) Rita eats everything Bill eats.

5. What is constraint satisfaction problem? Stating necessary conditions and assumptions solve the following crypto-arithmetic problem. 2+8

$$\begin{array}{r} \text{CROSS} \\ + \text{ROAD} \\ \hline \text{DANGER} \end{array}$$

6. What is neural network? How does back propagation work for learning in multilayer network? 2+4+4

7(a) Why learning is important in artificial intelligence? Explain he induction learning with suitable examples.

(2)

(b) What is a frame and a frame system? Explain. 4

7(a) Explain the importance of game-playing in AI. 5

(b) Describe explanation-based learning. 5

8(a) State and explain best-first algorithm. 5

(b) Construct a parse tree for the following sentence:  
"The beautiful lady works in central bank of the city".

$$2 \times 5 = 10$$

9. Write short notes on any TWO:

(a) Machine learning

(b) Back propagation

(c) Bayesian Network



**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer) / Seventh Semester / *Chance*

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**SEG471CO: Artificial Intelligence (Old Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer ALL questions.**

1(a) What is AI? Describe expected approaches of AI where system think and Act rationally. 1+3

(b) Define the problem as a state space search. Apply the technique and solve the following water jug Problem: "A farmer was sent to a nearby pond to fetch 2 gallons of water. He was given two pails-one 4, the other 3 gallons. How can he measure requested amount of water? (Hints: define state representation, initial state, operators and goal state as when required.)" 1+5

2(a) What is logic? Illustrate with representation of knowledge in propositional logic in the given knowledge base and draw the conclusion whether Becky comes or not from the given propositions. 1+4

Given, KB= (Mike comes to the party;

If Cathy comes to the party then Becky comes;

If Cathy doesn't come then Mike won't come to the party)

(b) What is MYCIN System? Compare the semantic networks and frames knowledge representation. 2+3

3(a) Define Natural Language Processing. Explain the steps of natural language processing. 1+4

(b) Describe the concept of learning in Neural Networks. Differentiate between pragmatic and discourse integration. 3+2

4. What are constrain satisfaction problem? Solve the following crypto-arithmetic Problem where different letters denote different integer and identical letter denote same integer. 2+8

**SEVEN+EIGHT= TWELVE**

**Contd. ...**

- 5(a) What is machine learning? Compare the analogy based and explanation based learning. (2) 2+2
- (b) Define Perceptron. Describe the concept Network Architecture in Multilayer feed forward N/Ws. 2+2
6. Write short notes on any THREE: 2+4
- (i) Genetic Algorithm
  - (ii) Boltzmann Machine
  - (iii) Bayesian networks
  - (iv) Expert system
- 3×4=12
- 7(a) What do you mean by Heuristic search. Explain in short any heuristic search. 2+2
- (b) Define inference rule. Differentiate between forward and backward chaining in Production rules system. 2+4
8. Convert the following premises into FOPL: 8
- (i) There is an X and Y that is sister of Spot and they are not the same individual.
  - (ii) Every pair of objects with property p is equal.
  - (iii) There is a king and for all kings that are similar.
  - (iv) Parents of horse are horse.
  - (v) Everyone does nothing.
  - (vi) Brothers are siblings.
  - (vii) Anyone who is not sloppy is smart.
  - (viii) Not everyone is both smart and boring.



**PURBANCHAL UNIVERSITY**

**2017**

B.E. (Computer) / Seventh Semester / Back

Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (Old Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**Answer EIGHT questions.**

**$8 \times 10 = 80$**

- 1.(a) Compare A\* algorithm to greedy algorithm to show how it uses heuristic cost to generate optimum solution with an example. 6
- (b) Differentiate between inference and reasoning. Why possibilities reasoning are important in the AI? Explain with suitable example. 4
2. What do you mean by frames and semantic .Net? Express the following sentence into FOPL: 10
- (a) A person is a mammal.  
(b) Shakti Gauchan is a Person.  
(c) Person has nose.  
(d) Shakti Gauchan is in Nepalese team.  
(e) Uniform color of Shakti Gauchan is Red/Blue.
3. Discuss the constraint satisfaction probleim Solve the following crypt-arithmetic problem: 10
- (a) FORTY  
TEN  
+ TEN  
SIXTY
- (b) LOGIC  
+LOGIC  
PROLOG
4. Why conjunctive normal form and Disjunctive normal form is required? Explain all the steps with example. 10
- 5.(a) What is learning system? Explain rote learning and reinforcement learning. 6
- (b) Describe MIN MAX problem with example. 4

(2)

6. Explain the different steps involved in the natural language processing (NLP) and justify that NLP requires artificial intelligence? 10
- 7(a) What is expert system? Explain the difference between Human expert vs expert system with example. 5
- (b) Describe forward chaining and backward chaining in expert system. 5
8. What is multi-layer perception? How learning and validation is done in back propagation algorithm? Explain application of neural networks? 5+5
9. Write short notes on any TWO: 5+5
- (a) Alpha-beta pruning search
  - (b) Decision tree
  - (c) Learning by Induction
  - (d) Hill-climbing search



Date \_\_\_\_\_

**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer) / Seventh Semester / Final

Full Marks. 80 / Pass Marks. 32

Time. 03.00 hrs.

**BED471CO: Artificial Intelligence (New Course)**

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

$$8 \times 10 = 80$$

Answer EIGHT questions.

- 1.(a) Explain with suitable examples intelligence, artificial intelligence and agent. 1+2+3
- 1.(b) Compare DFS and BFS. 4
- 2) Describe the structure of an expert system. Briefly describe the various the steps involved in the development of an expert system. 4+6
- 3.(a) Discuss game tree with an example. 5
- 3.(b) Explain Alpha-Beta pruning algorithm. 5
4. Express the following sentences into FOPL. 5x2=10
- 4.(a) Lipton is a tea. 1
- 4.(b) Lata is a child who drinks tea. 1
- 4.(c) Ruma dislikes children who drink tea. 1
- 4.(d) Ruma disliked Lata. 1
- 4.(e) Anything anyone eats and isn't killed by is food. 1

5. Define constraint satisfaction problem. Stating necessary conditions and assumptions, solve the following cryptarithmic problem. 2+8

CROSS

+ ROADS

DANGER

Contd. ....

(2)

6. Define ANN and its components. Explain back propagation learning mechanism in ANN. 5+5

7(a) What are the different types of learning? Explain rote learning and induction learning with suitable examples. 2+2=2

7(b) How does semantic network represent knowledge? Explain, with suitable example. 4

8. Differentiate between forward chaining and backward chaining. Use truth table approach to reach the goal for the following: 5×2=10

- (a) if it rain, roads are wet
- (b) if roads are wet and driving is careless, vehicles are slippery
- (c) if vehicles are slippery, accident occurs
- (d) It is raining
- (e) Driving is careless.

Prove the goal that accident occurs.

9. Write short notes on any TWO:

- (a) Genetic Algorithm
- (b) Inference Engine
- (c) Components of NLP

**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer)/Seventh Semester/Final

Time: 03:00 hrs.

Full Marks: 80 /Pass Marks: 32

**BEG471CO: Artificial Intelligence (New Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer EIGHT questions.**

**8×10=80**

- 1(a) Explain with suitable examples intelligence, artificial intelligence and agent. 1+2+3
- (b) Compare DFS and BFS. 4
- 2) Describe the structure of an expert system. Briefly describe the various the steps involved in the development of an expert system. 4+6
- 3(a) Discuss game tree with an example. 5
- (b) Explain Alpha-Beta pruning algorithm. 5
4. Express the following sentences into FOPL. 5×2=10
- (a) Lipton is a tea.
- (b) Lata is a child who drinks tea.
- (c) Ruma dislikes children who drink tea.
- (d) Ruma disliked Lata.
- (e) Anything anyone eats and isn't killed by is food.
5. Define constraint satisfaction problem. Stating necessary conditions and assumptions, solve the following cryptarithmic problem. 2+8

CROSS

+ ROADS

DANGER

(2)

6. Define ANN and its components. Explain back propagation learning mechanism in ANN. 5+5

7(a) What are the different types of learning? Explain rote learning and induction learning with suitable examples. 2+2+2

(b) How does semantic network represent knowledge? Explain with suitable example. 4

8. Differentiate between forward chaining and backward chaining. Use truth table approach to reach the goal for the following:  
 $5 \times 2 = 10$

- (a) if it rain, roads are wet
- (b) if roads are wet and driving is careless, vehicles are slippery
- (c) if vehicles are slippery, accident occurs
- (d) It is raining
- (e) Driving is careless

Prove the goal that accident occurs.

9. Write short notes on any TWO: 5+5

- (a) Genetic Algorithm
- (b) Inference Engine
- (c) Components of NLP



**PURBANCHAL UNIVERSITY**  
**2015**

B.E. (Computer) / Seventh Semester / Choice  
 Time 03:00 hrs. Full Marks: 80 / Pass Marks: 32

**SEG471CO: Artificial Intelligence (New Course)**

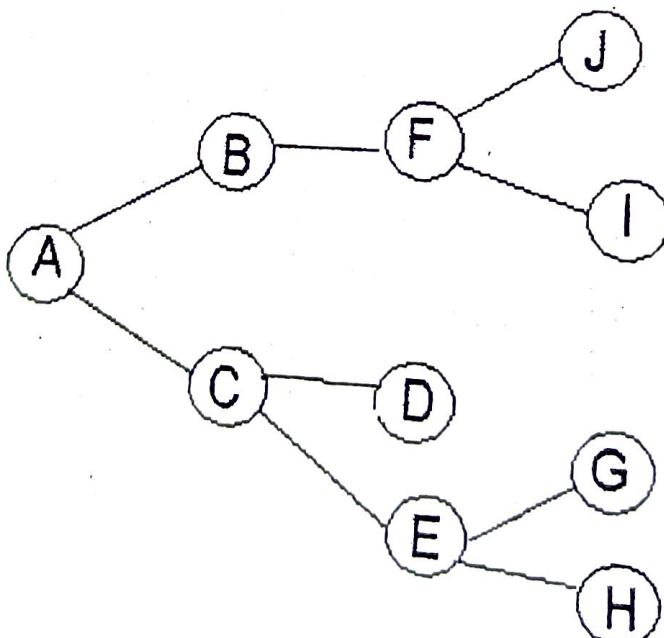
Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

**$8 \times 10 = 80$**

**Answer EIGHT questions.**

- 1(a) Define Artificial intelligence and rationality. Discuss the applications of AI with examples. 5
- (b) Explain the PCAS elements of an agent with any suitable example. 5
- 2(a) Compare the Bidirectional search with depth limited search. Explain the working of iterative deepening search. 4
- (b) Starting from state A, execute BFS and DFS. The goal node is G. Show the sequence in which nodes are expanded. Note that the alphabetically smaller node is expanded first to break ties. 6



3. Explain learning system in AI. Discuss and compare the explanation based learning and reinforced learning and better of the two for different systems.

2+8

(2)

- 4(a) Compare reasoning with inferencing. Explain the Bayesian network as statistical reasoning. 6
- (b) Discuss case based reasoning. 4
5. Explain with a block diagram the expert system. Compare this system with natural intelligence. 7+3
- 6(a) What do you mean by heuristic search. Explain the hill climbing algorithm. 2+4
- (b) Briefly describe the types of agents. 4
- 7(a) Convert the following sentences into FOPL: 4×1.5=6  
(i) Anyone passing his exams and winning the lottery is happy.  
(ii) Anyone who studies or is lucky can pass all his exams.  
(iii) John didn't study well but he is lucky.  
(iv) Anyone who is lucky wins the lottery.
- (b) Use resolution to prove "John is happy".
- 8(a) Compare the natural language processing with natural language generation. Describe in detail the steps of NLP. 6
- (b) Explain with necessary diagram the artificial neural network architecture. 4
9. Write short notes on any FOUR: 4×2.5=10  
(a) Forward chaining Vs backward chaining  
(b) Semantic Nets  
(c) Min Max problem  
(d) Perceptron Network  
(e) CSP problems

1  
&

**PURBANCHAL UNIVERSITY**

**2015**

B.E. (Computer) / Seventh Semester / Choice  
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

**BEG471CO: Artificial Intelligence (Old Course)**

*Candidates are required to give their answers in their own words as far as practicable.*

*All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.*

**Answer ALL questions.**

- 1(a) What is AI? Describe expected approaches of AI where system think and Act rationally. 1+3
- (b) Define the problem as a state space search. Apply the technique and solve the following water jug Problem: "A farmer was sent to a nearby pond to fetch 2 gallons of water. He was given two pails-one 4, the other 3 gallons. How can he measure requested amount of water? (Hints: define state representation, initial state, operators and goal state as when required.)" 1+5
- 2(a) What is logic? Illustrate with representation of knowledge in propositional logic in the given knowledge base and draw the conclusion whether Becky comes or not from the given propositions. 1+4  
Given, KB= (Mike comes to the party;  
If Cathy comes to the party then Becky comes;  
If Cathy doesn't come then Mike won't come to the party)
- (b) What is MYCIN System? Compare the semantic networks and frames knowledge representation. 2+3
- 3(a) Define Natural Language Processing. Explain the steps of natural language processing. 1+4
- (b) Describe the concept of learning in Neural Networks. Differentiate between pragmatic and discourse integration. 3+2
4. What are constrain satisfaction problem? Solve the following crypto-arithmetic Problem where different letters denote different integer and identical letter denote same integer. 2+8

**SEVEN+EIGHT= TWELVE**

Contd.

(2)

5(a) What is machine learning? Compare the analogy based and explanation based learning. 2+2

(b) Define Perceptron. Describe the concept Network Architecture in Multilayer feed forward N/Ws. 2+4

6. Write short notes on any THREE:  $3 \times 4 = 12$

- (i) Genetic Algorithm
- (ii) Boltzmann Machine
- (iii) Bayesian networks
- (iv) Expert system

7(a) What do you mean by Heuristic search. Explain in short any heuristic search. 2+2

(b) Define inference rule. Differentiate between forward and backward chaining in Production rules system. 2+4

8. Convert the following premises into FOPL: 8

- (i) There is an X and Y that is sister of Spot and they are not the same individual.
- (ii) Every pair of objects with property p is equal.
- (iii) There is a king and for all kings that are similar.
- (iv) Parents of horse are horse.
- (v) Everyone does nothing.
- (vi) Brothers are siblings.
- (vii) Anyone who is not sloppy is smart.
- (viii) Not everyone is both smart and boring.



# **PURBANCHAL UNIVERSITY**

2014

**PURBANCHAL UNIVERSITY**  
**2014**  
**B.E. (Computer) / Seventh Semester / Final**  
**Time: 03:00 hrs.**  
**BEGAN**

**Full Marks: 80 / Pass Marks: 32**

## **BEG471CO: Artificial Intelligence**

**Candidates are required to give their answers in their own words as far as practicable.**

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.—

**Answer EIGHT questions.**

1. Solve the following cryptarithmetic puzzle where different letters denote different integers. Also show all the steps how you advance through constraint satisfaction and state all the assumptions that you make. 10

$$\begin{array}{r} \text{at you make.} \\ \text{ONE} \\ + \text{TWO} \\ \hline \text{FOUR} \end{array} \quad \begin{array}{l} T^2 \\ T^1 \\ \hline T = 10^1 - C_1 + C_2 \end{array}$$

2. What is an intelligent agent? Explain the types of agent programs with suitable examples. 10

- 3(a) Differentiate between propositional logic and predicate logic. 4

- (b) Convert the following sentences into FOPL:  $3 \times 2 = 6$

(i) All framers either like monsoon or they don't cultivate.

(ii) Rotten apples do not taste good.

(iii) Nobody likes corruption.

- 4(a) What is a neural net? Explain its basic structure.

- (b) Relate Boltzmann machines with Hopfield networks.

- 5(a) What is an expert system? Discuss its applications.

- g) What are the categories of knowledge? Explain.

- (b) What are the categories of knowledge? Explain.  
Q.5. Define the types of production rules

- 6(a) What are production rules? Explain the types with examples.

(2)

- (b) How does semantic network represent knowledge? Explain with suitable example.
8. What do you mean by Case-based Reasoning? Explain forward and backward chaining with example.
9. Write short notes on any TWO:
- (a) Genetic Algorithm
  - (b) Propositional Logic
  - (c) Reasoning
  - (d) Frame System

4

5+5

# PURBANCHAL UNIVERSITY

2011

B.F. (Computer) / Seventh Semester / Choice  
Time: 03.00 hrs.

Full Marks: 80 / Pass Marks: 32

BEQ471CO: Artificial Intelligence

Candidates are required to give their answers in their own words as far as practicable.

All questions carry equal marks. The marks allotted for each sub-question is specified along its side. Assume suitable data if necessary.

Answer EIGHT questions.

- 1(a) Discuss various definitions of artificial intelligence (AI). Explain why AI programs try to model human performance. 5
- (b) In the context of user identification system, based on voice, what would be the consideration of an AI systems in terms of Agent, Environment, Actuators and Sensor? 5
- 2(a) What is the best first search technique? Explain the various operating steps of the  $\Lambda^*$  ( $\Lambda$  star) algorithm by searching a directed graph in which each node represents a point in the problem space. 2+4
- (b) Compare depth first search and breadth first search methods. 4
- 3(a) What is predicate logic? Differentiate it with propositional logic. 1+3
- (b) Explain principle of resolution. Explain the formal steps in Resolution with example. 6
- 4(a) Differentiate between forward and backward chaining with example. 5
- (b) Discuss with suitable example how problem is solved using goal stack planning. 5
- 5(a) What is Rote Learning? 2
- (b) Discuss genetic algorithm with example. 8
- 6(a) Draw a schematic diagram showing the various functional elements of an expert system. Explain the function of each of them. 6

Contd...

(2)

(b) Give an example of expert system and give basic characteristics of Expert system.

7. Discuss major advantage of artificial neural networks, Describe briefly back propagation training algorithm. Give different possible application of neural networks.

8(a) What do you mean by natural language processing? Discuss in detail the components involved in the natural language understanding process.

(b) Briefly explain the edge detection methods

9. Write short notes on any TWO:

(a) Bayesian Network

(b) Inductive bias learning

(c) Frames

PURBANCHAL UNIVERSITY  
2011

Bachelor in Information Technology (B.I.T.) / Seventh Semester / Choice  
Time: 03:00 hrs.

Full Marks: 80 / Pass Marks: 32

BITM415CS: Artificial Intelligence

Candidates are required to give their answers in their own words as far as practicable.

Figure in the margin indicate full marks.

Group A:

$$2 \times 12 = 24$$

Answer TWO questions.

1. Solve the following crypto-arithmetic problem, where different letters denote different integers and identical letters denote same integer: SEND + MORE = MONEY  
Show all steps how you advance through constraint satisfaction. 2+10
2. Define problem solving agent. Explain with suitable examples, the types of agent programs in AI. 7
- 3(a) Explain the architecture of an expert system. 5
- (b) Differentiate between artificial intelligence and natural intelligence. 5

Group B:

$$7 \times 8 = 56$$

Answer SEVEN questions.

4. What is Winston's learning? Explain learning by analogy and explanation based learning. 2+6
- 5(a) State the inference theorems with examples. 3
- (b) Write the importance of game playing in AI. 3
6. What is heuristic search? Explain any one of the heuristic search with example. 3+5
7. Define Means End Analysis (MEA). Explain how a household robot problem is solved using MEA. 3+

Could

(2)

8. Convert the following sentences into FOPL.

2×4

(a) Saroj likes to read all kinds of courses.

(b) If you are idle, you will feel lonely.

(c) Every child loves his mother.

(d) Sun rises in the east and sets down in the west.

9. What is a neural network? Explain its components.

2+6

10. Explain the importance of genetic algorithm in AI with a suitable demonstration.

11(a) What is natural language processing? What are its various steps?

4

(b) Construct a parse tree for the given sentence:  
"I have enough money to buy a laptop".

4

12. Write short notes on any TWO:

2×4=8

(a) Back propagation

(b) Machine vision

(c) Semantic nets and frames