A Course on Computer Networks Based on CC2001

Shakil Akhtar and Alaaeldin A. Aly
College of Information Technology
UAE University
{s.akhtar, aly}@uaeu.ac.ae

Abstract

This paper presents the laboratory contents of an updated computer networks course offered at the undergraduate junior or senior level. The design is based upon the recommended computing curriculum by IEEE Computer Society/ACM Task Force, also referred to as CC2001. A set of lab activity experiments have been presented that can be adopted very easily in a traditional fifteen week semester offering.

I. Introduction

The importance of offering an undergraduate networks course that includes cryptography and network security is becoming obvious as we see the rising rate of computer crime and its effect on the society [1]. Security in networks is an important topic. The foundation of security is in cryptology, which is a mathematical hard core of information security, since many of the information security problems (e.g. confidentiality, integrity, authenticity of information) can be solved by means of cryptographical tools/algorithms. Due to this reason the related courses are usually taught at the graduate level [2].

Despite the difficulties of including security related topics at the undergraduate level, the recent trends suggest that undergraduate programs in computing include security related topics. The CS volume of the Year 2001 Model Curricula for Computing (CC-2001 [3]) contains several modules with area descriptions. Some of these are identified as core; others are identified as elective. The coverage in net-centric module includes security related topics. Other modules also contain security related topics in addition to the other recommended material. The recommended topics from security are network security, security and protection, cryptographic algorithms, and computer crime.

Undergraduate IT students at UAE University seeking specialization in either network engineering program or information security program are required to take a two course sequence, first in fundamentals of networking and communications and the second on the cryptographic algorithms and security protocols. It is noted that because of the difficulty of both cryptographic algorithms and security protocols and also the need for special mathematics background, most IT/computer science departments in major universities offer the course for graduate students. However, we have designed the course to be offered for junior/senior level undergraduate IT students [4].

Unlike the IT program at UAE University, most CS programs require only one course in networks, and there are already numerous topics to be covered in that course. It has always been a challenge to offer a single course considering the new trends in computing [5]. The current trends suggest inclusion of additional topics on security with hands-on activities. In this paper, we propose a course on networks based upon the implementation of two separate courses at College of Information Technology at UAE University. We feel that the contents of two courses may be combined carefully to offer a single course in networking that conforms to the CC-2001 suggestions and meets the current demands.

The paper presents the curricular outline for a networks course following a laboratory based approach to support an active learning environment. The suggested methodologies for delivering the course are engaged learning, project-based learning, cooperative learning, and problem-based learning. However, in this paper we only emphasize on the developed labs. The specific tools/technologies used for this course delivery are Java applets, animation, and Blackboard as a web delivery and class management tool. We noted that the students at sophomore/junior level are able to grasp complex mathematical concepts and algorithmic details by following the active learning methodology as applied to this course.

II. Recommended Course Outline

We propose to effectively integrate content and technology and suggest the course delivery method to change from a traditional lecture format to a studio format that consists of a lecture followed by a collaborative and cooperative learning experience. For instance, a 3 credit hour course on Computer Networks may be offered as two studio lectures per week consisting of two hours each. A session may consist of a lecture followed by a learning experience in which students need to participate. The class ends with a summary presented by the instructor and concluding remarks.

The recommended fifteen week course outline consists of most important topics as recommended by the CS model curricula. Also, we expect that successful students who are able to understand and practice the lab activities may pursue Cisco and Network+ certifications. Our proposed list of topic for a fifteen week semester is:

a. The basic definitions of communications and networks fundamentals. (1 week)
b. The 7-layer architecture of the OSI model and its mapping to the TCP/IP model. (1 week)
c. The data transmission, switching and multiplexing concepts and the different transmission media. (3 weeks)
d. The topologies, transmission media, and protocols that are most commonly used for LANs. (2 weeks)
e. The data link layer with the description of techniques used for framing, flow and error controls. (2 weeks)
f. IP, routing and forwarding concepts. (2 weeks)
g. Network security concepts including fundamentals of cryptography, secret and public key algorithms, authentication protocols, and digital signatures. (2 weeks)
h. Exams, quizzes and miscellaneous topics such as network performance and network management. (2 weeks)

III. The Lab Activities

The designed lab activities are expected to cover all of the above mentioned core net-centric computing areas. This section presents the proposed lab activities. However, due to length restrictions, only outline of experiments are presented here. Complete details (colored figures, additional figures and lab handouts) are available from the author's web site (http://faculty.uaeu.ac.ae/s.akhtar). The labs may be used in combination with the recommended textbook [6] that comes with a CD which includes many additional projects.

Lab/activity 1: A class exercise OSI and TCP/IP models (Areas a and b: weeks 1-2)

This Lab is divided into two parts, OSI and TCP/IP. The first part focuses on students' ability to accomplish the following tasks:

- Name the seven layers of the OSI model in order using a mnemonic
- Describe the characteristic, functions and keywords relating to each layer
- Describe the packaging units used to encapsulate each layer
- Name several protocols and standards that operate at each layer

The second part of the lab focuses on the following tasks:

- Describe the 4 layers of the TCP/IP model
- Relate the seven layers of the OSI model to the 4 layers of the TCP/IP model
- Name the primary TCP/IP protocols that operate at each layer

A set of exercises have been created to provide enough practice on the understanding of these layers. For instance, one exercise asks the students to match the OSI and TCP/IP layer names and another exercise asks for the encapsulation units at different layers.

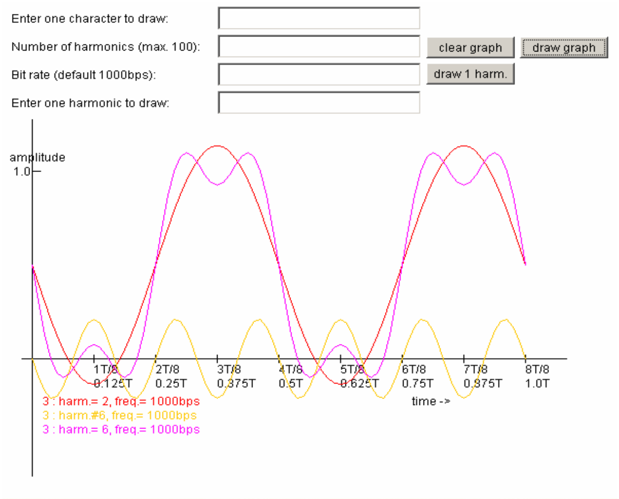

Enter one character to draw:
Number of harmonics (max. 100):
Bit rate (default 1000bps):
Enter one harmonic to draw:
clear graph
draw graph
draw 1 harm.
amplitude
1.0
1T/8
0.125T
2T/8
0.25T
3T/8
0.375T
4T/8
0.5T
5T/8
0.625T
6T/8
0.75T
7T/8
0.875T
8T/8
1.0T
time ->
3 : harm.= 2, freq.= 1000bps
3 : harm.#6, freq.= 1000bps
3 : harm.= 6, freq.= 1000bps

Figure 1: Fourier series decomposition of '3' (00110011) showing the 6th harmonic, sum of first two and first six harmonics

Lab/activity 2: Understanding the data communications using a Fourier series applet (Area c: week 3)

The objective of this lab activity is to explain the Fourier series decomposition for a periodic bit pattern using an applet. The applet accepts an ASCII character as input and draws the Fourier distribution for the periodic decomposition of the character. For example if character ‘A’ is input, the applet will draw the distribution for the periodic bit pattern “01000001”, since ASCII for ‘A’ is Ox41. A sample of output is shown in Figure 1. The applet has four input fields, which are:

1. Enter character to draw - This text field gets the character whose ASCII code will be decomposed into fundamental and harmonic components.
2. Number of harmonics - This field gets the number of harmonics that should to be displayed in the diagram. (1 is the fundamental frequency component).
3. Bit rate - This field gets the bit rate.
4. Enter one harmonic - This field gets the individual harmonic that is to be drawn.

Three button are provided that perform specific functions

1. Clear graph – This clears the graph, the input values and draws the axis and scale.
2. Draw graph – This draws summation of waveforms from the fundamental wave to the harmonic entered in the “Number of harmonic” field.
3. Draw 1 harm – This draws the individual harmonic of the series entered in the “Enter 1 harmonic to draw” field.

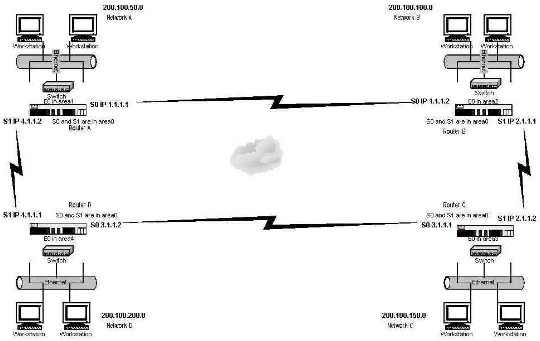


Figure 2: Network topology for Lab/Activity 4

Lab/activity 3: Local Area Network (LAN) cables and testing (Area d: week 6)

This activity involves building and testing various types of cables used in standard LANs. The cables are:

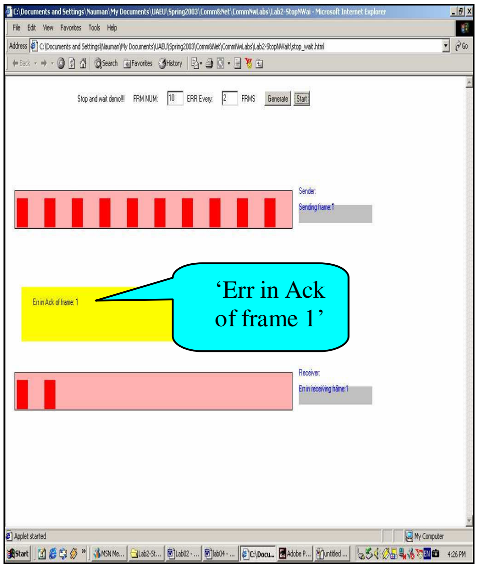
- v Straight-Thru Ethernet patch cable with T568-B (OR T568-A) standards for connection from workstation to hub/switch or patch panel to hub/switch.
- v Rollover Cable for connection from a workstation to the console port on a router or switch.
- v Crossover Cable to communicate between two workstations directly or two switches etc.

Lab/activity 4: A small LAN connection using a Cisco router and a switch (Area d: week 7)

The objectives of this lab are to

- Create a simple LAN with two or more PCs using an
  1. Crossover cable
  2. Ethernet hub/switch and two straight-thru cables
- Use the Control Panel / Network utility to verify and configure the network settings.
- Use the IPCONFIG.EXE utility to verify all IP configuration settings.
- Use the ICMP Ping command to verify the TCP/IP connection between the two workstations.
- Share folders across various workstations.
- Share printers across various workstations.

This lab activity reinforces the understanding of LAN by emphasizing the sharing of information and resources in LANs. A connection with two or more PCs is created as a simple Peer-to-Peer LAN or workgroup in which a folder and a printer are shared on one using Windows 2000. A network diagram is provided to the student as shown in Figure 2. Each group is assigned one of four networks with pre-assigned IP addresses.


C:\Documents and Settings\Nauman\My Documents\UAEU\Spring2003\Comm&Net\CommNwLabs\Lab2-StopNWai - Microsoft Internet Explorer

Address C:\Documents and Settings\Nauman\My Documents\UAEU\Spring2003\Comm&Net\CommNwLabs\Lab2-StopNWait\stop_wait.html

Stop and wait demo!!! FRM NUM: 10 ERR Every: 2 FRMS

Sender:
Sending frame:1

Err in Ack of frame: 1

Receiver:
Err in receiving frame:1

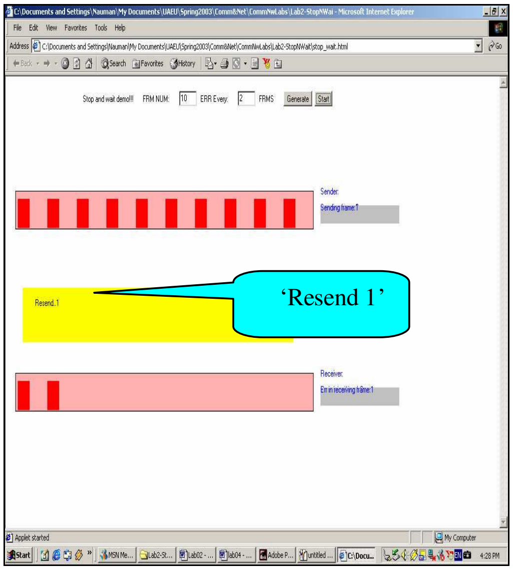
Applet started

‘Err in Ack of frame 1’

Figure 3: Stop and wait with error control implemented with timeout mechanism and acknowledgements (part 1)

Lab/activity 5: Understanding the data link layer protocols such as Stop and wait, and Automatic Repeat Request using an applet (Area e: week 8)

This lab activity demonstrates the use of data link layer protocols and ARQ schemes (Goback N ARQ, Selective Repeat ARQ, Stop & Wait). A series of applets show how the errors in frame and acknowledgements slow down the data transmission. For instance, in stop and wait, it is shown that the sender sends a frame and waits for an ACK or NAK (negative acknowledgement); then sends new packet or resends the old packet. Also, the use of time-outs for lost packets and sequence numbers to distinguish the re-transmitted packet have been illustrated (Figures 3 and 4). Similarly, the use of sliding window control with Goback N and Selective Repeat ARQ may be illustrated.


C:\Documents and Settings\Nauman\My Documents\UAEU\Spring2003\Comm&Net\CommNwLabs\Lab2-StopNWai - Microsoft Internet Explorer

Address C:\Documents and Settings\Nauman\My Documents\UAEU\Spring2003\Comm&Net\CommNwLabs\Lab2-StopNWait\stop_wait.html

Stop and wait demo!!! FRM NUM: 10 ERR Every: 2 FRMS

Sender:
Sending frame:1

Resend..1

‘Resend 1’

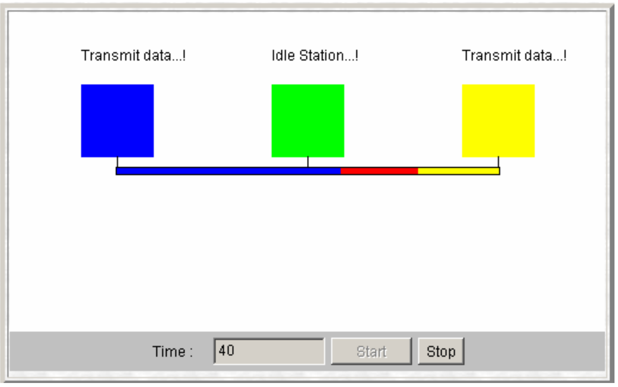
Receiver:
Err in receiving frame:1

Applet started

Figure 4: Stop and wait with error control implemented with timeout mechanism and acknowledgements (part 2)

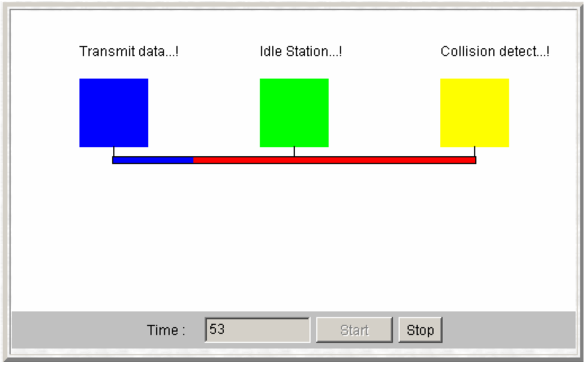
Lab/activity 6: Understanding a CSMA/CD LAN protocol using an applet (Area d: week 9)

The operation of the Carrier Sense Multiple Access/Collision detection (CSMA/CD) protocol has been illustrated using an applet. Different phases of transmission, such as idle condition, transmission, collision, backing off, jamming etc. have been shown as different colors with appropriate display of messages as a function of time (Figures 5-9).


Transmit data...! Idle Station...! Transmit data...!

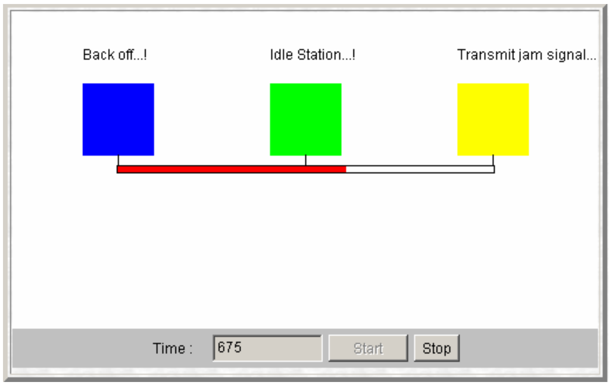
Time : 40

Figure 5: Two stations transmitting simultaneously leading to collision


Transmit data...! Idle Station...! Collision detect...!

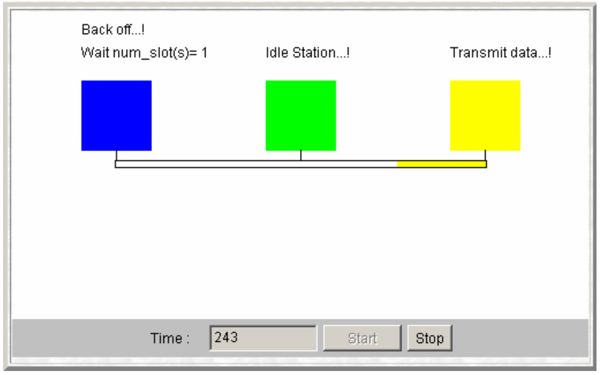
Time : 53

Figure 6: Collision detection by a station after the collision


Back off...! Idle Station...! Transmit jam signal...

Time : 675

Figure 7: transmission of jam signal


Back off...!
Wait num_slot(s)= 1 Idle Station...! Transmit data...!

Time : 243

Figure 8: Binary exponential backoff

Lab/activity 7: Fundamentals of IP addressing including subnets and supernets (Area f: week 10)

This lab focuses on the fundamentals of IP addressing via several hands-on calculation provided as exercises. It is divided into two parts. The first part includes the following activities/tasks:

- Name the five different classes of IP addresses
- Describe the characteristics and use of the different IP address classes
- Identify the class of an IP address based on the network number
- Determine which part (octets) of an IP address is the network ID and which part is the host ID
- Identify valid and invalid IP host addresses based on the rules of IP addressing

The second part focuses on subnet calculations and the ability to accomplish the following tasks:

- Distinguish between a Default Subnet Mask and a Custom Subnet Mask
- Use the "ANDing" process to determine if a destination IP address is Local or Remote
- Use a Class C network and three subnets using a Default Subnet Mask.
- Use a Class C network and three subnets using a Custom Subnet Mask.
- Use a Class B network and three subnets to demonstrate the use of masking.

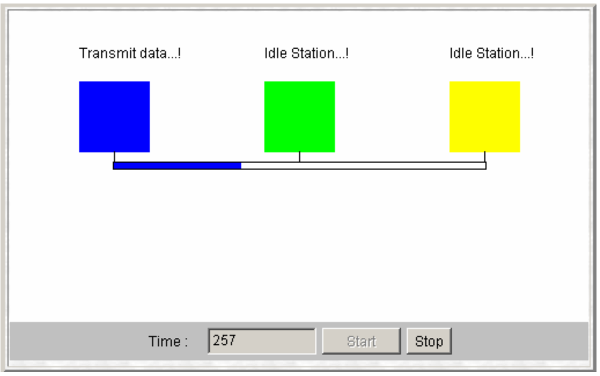


Figure 9: Successful transmission after backoff

Lab/activity 8: Understanding routing using a shortest path routing applet (Area f: week 11)

This lab provides an understanding of the operation of the shortest path algorithm via several applets. The screen snapshots are shown in Figures 10-12.

This applet provides the flexibility to customize a small network. The "Enter Nodes" button is used to enter the nodes of the network. The "Enter Edges" button allows specifying the link between two nodes. The "Change Cost" button is used to change the cost of a specific link. The "Select nodes" button is used to select the source and the destination node. The "Shortest path" button calculates the shortest path and the "Clear" button clears the screen and the user can enter a new network.

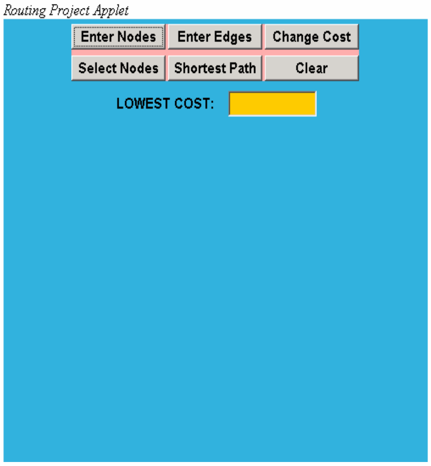


Figure 10: Initial screen for lab/activity 8

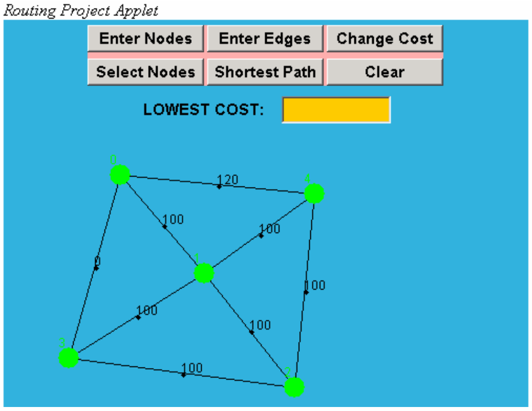


Figure 11: A small network setup for shortest path calculation

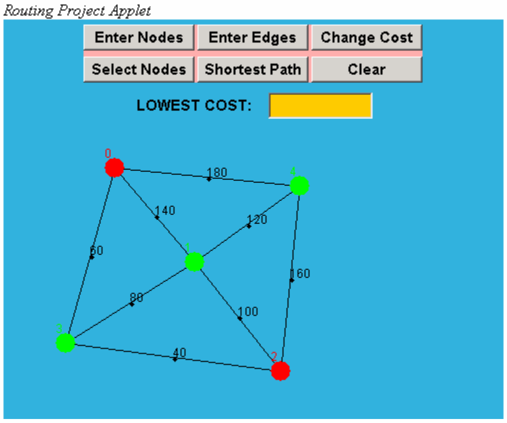
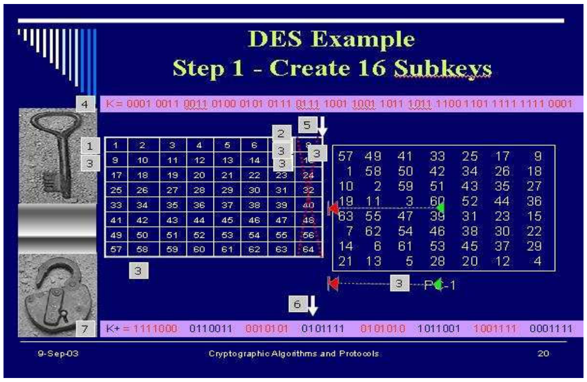


Figure 12: Shortest path algorithm applied between two nodes



DES Example
Step 1 - Create 16 Subkeys

K = 0001 0011 0011 0100 0101 0111 0111 1001 1001 1011 1011 1100 1101 1111 1111 0001

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

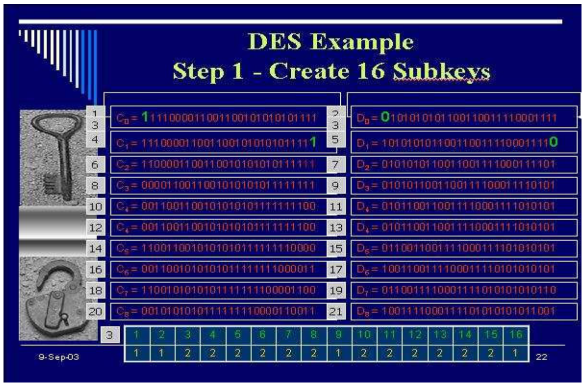
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC-1

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

9-Sep-03 Cryptographic Algorithms and Protocols 20

Figure 13: Sample of DES Animated Slides (1 of 10)



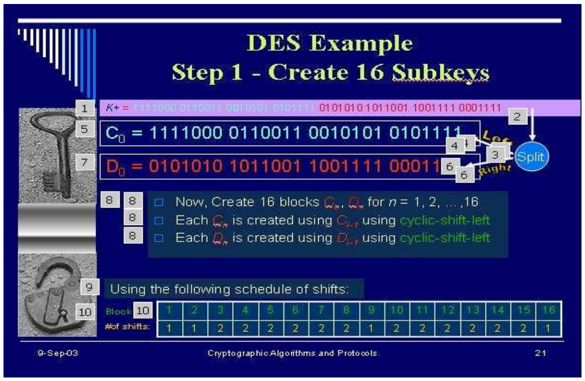
DES Example
Step 1 - Create 16 Subkeys

C_0 = 1111000011001100101010101111 | D_0 = 0101010101100110011110001111
C_1 = 1110000110011001010101011111 | D_1 = 1010101011001100111100011110
C_2 = 1100001100110010101010111111 | D_2 = 0101010110011001111000111101
C_3 = 0000110011001010101011111111 | D_3 = 0101011001100111100011110101
C_4 = 0011001100101010101111111100 | D_4 = 0101100110011110001111010101
C_4 = 0011001100101010101111111100 | D_4 = 0101100110011110001111010101
C_5 = 1100110010101010111111110000 | D_5 = 0110011001111000111101010101
C_6 = 0011001010101011111111000011 | D_6 = 1001100111100011110101010101
C_7 = 1100101010101111111100001100 | D_7 = 0110011110001111010101010110
C_8 = 0010101010111111110000110011 | D_8 = 1001111000111101010101011001

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

9-Sep-03 22

Figure 14: Sample of DES Animated Slides (2 of 10)



DES Example
Step 1 - Create 16 Subkeys

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

C_0 = 1111000 0110011 0010101 0101111

D_0 = 0101010 1011001 1001111 00011

- □ Now, Create 16 blocks C_n, D_n for n = 1, 2, ... ,16
- □ Each C_n is created using C_{i-1} using cyclic-shift-left
- □ Each D_n is created using D_{i-1} using cyclic-shift-left

Using the following schedule of shifts:

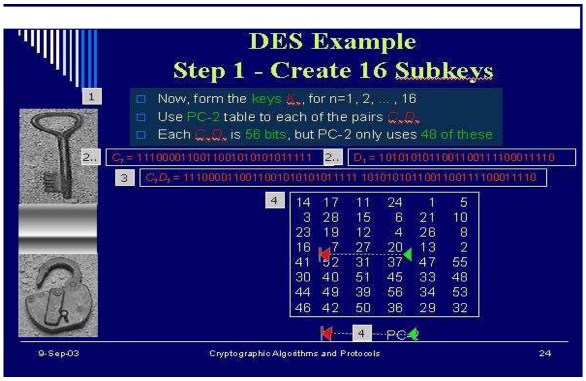
Block	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
#of shifts:	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

9-Sep-03 Cryptographic Algorithms and Protocols 21

Figure 15: Sample of DES Animated Slides (3 of 10)

Lab/activity 9: Practicing private and public keys encryption using both the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) techniques (Area g: week 12)

A lab activity consisting of practice on DES and AES techniques have been created. This is the most widely used encryption technique that takes two inputs: a 64-bit plaintext and a 56-bit key length. There are two major steps to encrypt a 64-bit input plaintext. The first step is to use the 64-bit key and generate 16 subkeys where each subkey is 48 bits in length. The second major step is to perform the encryption, which comprises of 16 rounds. The two steps are long and confusing, which makes it difficult for undergraduate students to follow. However, thru a series of animated slides the concept is taught at the level of students as shown in Figures 13-22.



DES Example
Step 1 - Create 16 Subkeys

- □ Now, form the keys K_n, for n=1, 2, ... , 16
- □ Use PC-2 table to each of the pairs C_nD_n
- □ Each C_nD_n is 56 bits, but PC-2 only uses 48 of these

C_1 = 1110000110011001010101011111 | D_1 = 1010101011001100111100011110

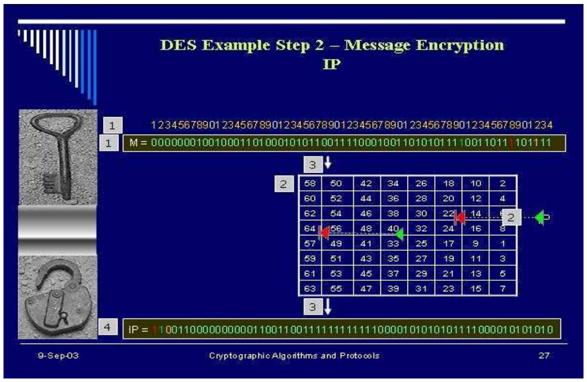
C_1D_1 = 1110000110011001010101011111 1010101011001100111100011110

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

PC-2

9-Sep-03 Cryptographic Algorithms and Protocols 24

Figure 16: Sample of DES Animated Slides (4 of 10)



DES Example Step 2 – Message Encryption
IP

1234567890123456789012345678901234567890123456789012345678901234

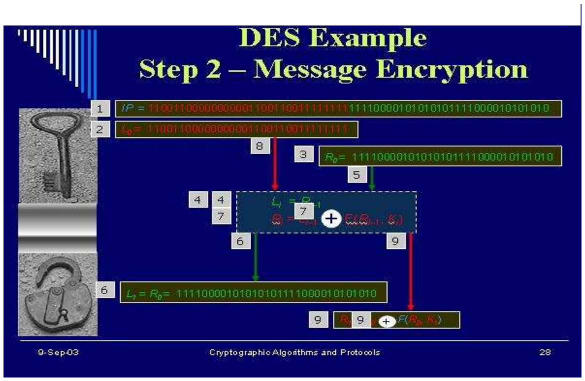
M = 0000000100100011010001010110011110001001101010111100110111101111

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP = 1100110000000000110011001111111111110000101010101111000010101010

9-Sep-03 Cryptographic Algorithms and Protocols 27

Figure 17: Sample of DES Animated Slides (5 of 10)



DES Example
Step 2 – Message Encryption

IP = 1100110000000000110011001111111111110000101010101111000010101010

L_0 = 11001100000000001100110011111111

R_0 = 11110000101010101111000010101010

$L_n = R_{n-1}$

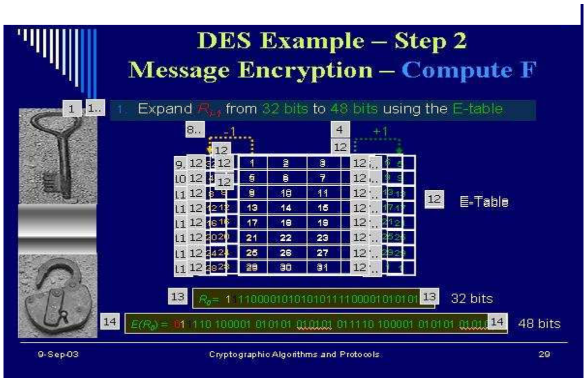
$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$

$L_1 = R_0$ = 11110000101010101111000010101010

$R_1 = L_0 \oplus f(R_0, K_1)$

9-Sep-03 Cryptographic Algorithms and Protocols 28

Figure 18: Sample of DES Animated Slides (6 of 10)



DES Example – Step 2
Message Encryption – Compute F

1. Expand R_{i-1} from 32 bits to 48 bits using the E-table

	1	2	3		
	5	6	7		
	9	10	11		
12	13	14	15		17
16	17	18	19		21
20	21	22	23		25
24	25	26	27		29
28	29	30	31		1

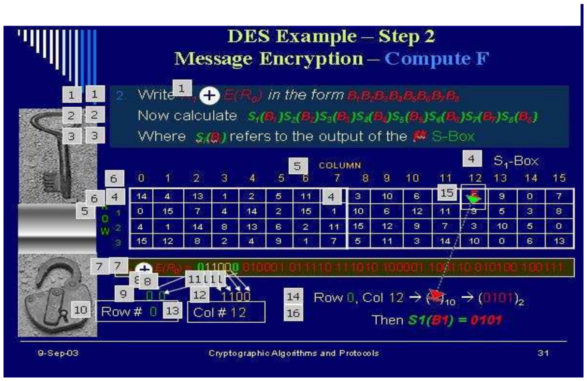
E-Table

R_0 = 1 1110000101010101111000010101 32 bits

$E(R_0)$ = 011110 100001 010101 010101 011110 100001 010101 01010 48 bits

9-Sep-03 Cryptographic Algorithms and Protocols 29

Figure 19: Sample of DES Animated Slides (7 of 10)



DES Example – Step 2
Message Encryption – Compute F

2. Write R_1 ⊕ $E(R_0)$ in the form $B_1B_2B_3B_4B_5B_6B_7B_8$
Now calculate $S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$
Where $S_i(B_i)$ refers to the output of the i^{th} S-Box

S$_1$-Box

ROW \ COLUMN	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	5	11	4	3	10	6	15	5	9	0	7
1	0	15	7	4	14	2	15	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

⊕ $E(R_0)$ = 011000 010001 011110 111010 100001 100110 010100 100111

0 0 1100

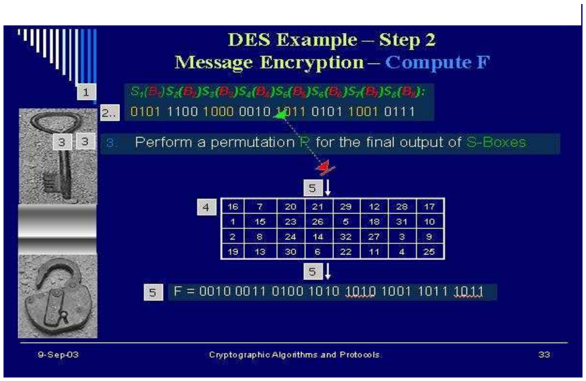
Row # 0 Col # 12

Row 0, Col 12 → $(5)_{10}$ → $(0101)_2$

Then S1(B1) = 0101

9-Sep-03 Cryptographic Algorithms and Protocols 31

Figure 20: Sample of DES Animated Slides (8 of 10)



DES Example – Step 2
Message Encryption – Compute F

$S_1(B_1)S_2(B_2)S_3(B_3)S_4(B_4)S_5(B_5)S_6(B_6)S_7(B_7)S_8(B_8)$:
0101 1100 1000 0010 1011 0101 1001 0111

3. Perform a permutation P for the final output of S-Boxes

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

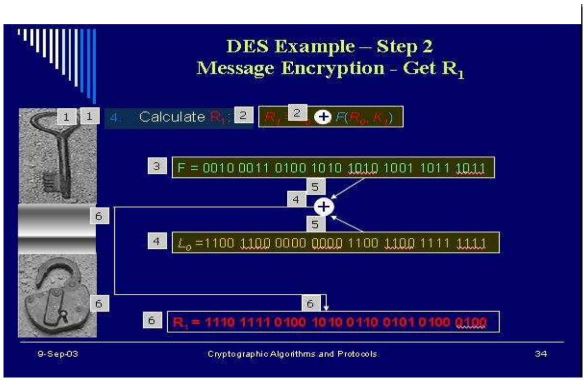
F = 0010 0011 0100 1010 1010 1001 1011 1011

9-Sep-03 Cryptographic Algorithms and Protocols 33

Figure 21: Sample of DES Animated Slides (9 of 10)

Lab/activity 10: Practicing the Mutual Authentication and Digital Signatures Standards (DSS) techniques (Area g: week 13)

In this lab, students are exposed to different authentication and digital signatures techniques with a focus on both the mutual and one-way authentications and the DSS technique. For authentication, two famous approaches are explained using animation and simple applet interface, which are Needham and Schroeder technique and Denning Authentication Server (AS) technique [7]. Figures 21 and 22 show two screen snapshots of the applet interfaces. In the same manner, two approaches for digital signatures are explained using animation and applets techniques. The two approaches are RSA and DSS (Figure 23).



DES Example – Step 2
Message Encryption - Get R_1

4. Calculate R_1: $R_1 = L_0$ ⊕ $F(R_0, K_1)$

F = 0010 0011 0100 1010 1010 1001 1011 1011

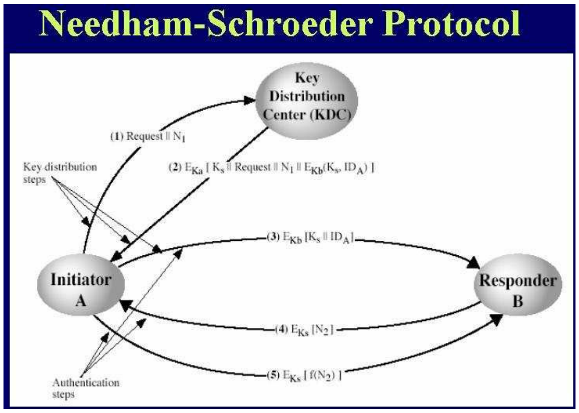
L_0 =1100 1100 0000 0000 1100 1100 1111 1111

R_1 = 1110 1111 0100 1010 0110 0101 0100 0100

9-Sep-03 Cryptographic Algorithms and Protocols 34

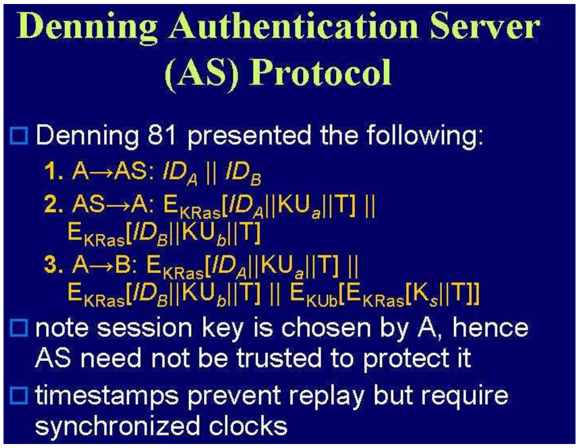
Figure 20: Sample of DES Animated Slides (10 of 10)

Needham-Schroeder Protocol



Key Distribution Center (KDC)
Initiator A
Responder B
(1) Request ‖ N_1
(2) E_{Ka} [K_s ‖ Request ‖ N_1 ‖ $E_{Kb}(K_s, ID_A)$]
(3) E_{Kb} [K_s ‖ ID_A]
(4) E_{Ks} [N_2]
(5) E_{Ks} [$f(N_2)$]
Key distribution steps
Authentication steps

Figure 21: A screen snapshot of Needham-Schroeder protocol applet



Denning Authentication Server (AS) Protocol

□ Denning 81 presented the following:
  1. A→AS: ID_A ‖ ID_B
  2. AS→A: $E_{KRas}[ID_A||KU_a||T]$ ‖ $E_{KRas}[ID_B||KU_b||T]$
  3. A→B: $E_{KRas}[ID_A||KU_a||T]$ ‖ $E_{KRas}[ID_B||KU_b||T]$ ‖ $E_{KUb}[E_{KRas}[K_s||T]]$
□ note session key is chosen by A, hence AS need not be trusted to protect it
□ timestamps prevent replay but require synchronized clocks

Figure 22: A screen snapshot of Denning AS protocol applet

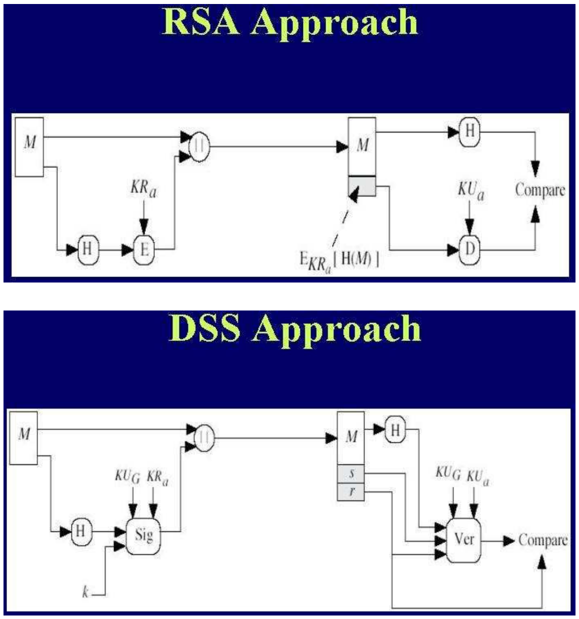


Figure 23: Digital Signature Approaches

Lab/activity 11: Running network utilities on PC such as ftp, telnet, ping, winipcfg etc. (Area h: week 14)

Use of several network utilities on PC is illustrated. This lab may be give either separately as shown here or could be integrated with other previous labs on the need basis. (For instance with lab 4)

```
C:\WINDOWS>arp -a

Interface: 141.209.141.30
  Internet Address      Physical Address      Type
  141.209.131.2         08-00-20-85-95-77     dynamic

C:\WINDOWS>
```

Figure 24: Use of Arp command for address resolution

The commands included in this practice are ARP, netstat, ping, route, tracert, and winipcfg. Screen snapshots are provided to the students as guidelines. For instance, the following instruction is provided for the arp command:

ARP

This command displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP). The IP address is the Internet address of the form abc.cps.cmich.edu, and the physical address is the associated 48 bits (12 hex digits) NIC (network Interface Card) address uniquely assigned to each adapter. Figure ? shows an example run of ARP command.

IV. Conclusions

The lab activities to cover core net-centric computing areas of CC2001 are presented. There are eleven labs deigned to cover different areas (a thru h). Each activity is expected to cover one lab session consisting of two hours or less.

V. References

[1] Computer Emergency Response Team (CERT) Statistics at Carnegie Mellon University, http://www.cert.org/stats/cert_stats.html

[2] Olejar, D., and Stanek, M., "Some Aspects of Cryptology Teaching," IFIP WG 11.8 1st World Conference on Information Security Education WISE1, 17-19 June 1999.

[3] IEEE Computer Society/ACM Task Force on the "Model Curricula for Computing,"

http://www.computer.org/education/cc2001/

[4] A.A. Aly, and S. Akhtar, "A Course on Cryptography and Security Protocols for Undergraduate IT Students," submitted to SIGCSE Bulletin.

[5] Akhtar, S., et. al.: The Networks Course: Old Problems, New Solutions. The Proceedings of the Thirtieth SIGSCE Technical Symposium on Computer Science Education", New Orleans, Louisiana, 1999.

[6] Y. Zheng, and S. Akhtar, “Networks for Computer Scientists and Engineers,” Oxford University Press, 2003.

[7] Stinson, D., Cryptography: Theory and Practice, Boca Raton, FL, CRC Press, 2002