
	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

COURSE FILE

NAME OF COURSE : B.Tech.
FACULTY : Anuj Yadav/Sandeep Mandal/Chirag Joshi
SESSION : 2017-18
SUBJECT : Cryptography & Network Security
COURSE CODE : DA 7210
NAME OF CLASS COORDINATOR : Anuj Kumar Yadav


PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

CONTENTS

S.NO.	CONTENTS	Page No
1.	Syllabus	
2.	Lesson Plan	
3.	Time Table	
4.	Attendance Register	
5.	Theory Performance Sheet, Teacher's Comments, Teacher's Suggestions	
6.	Scheme of Evaluation (Course Structure) (Practicals Attendance cum Practical Performance Sheet), Teacher's Comments, Teacher's Suggestions	
7.	Lecture Handouts	
8.	List of Assignments	
9.	Mid Term Question Paper, Final End Sem. Question Paper, list of debar students on attendance basis	
10.	Scheme of evaluation Pattern	
11.	Result Analysis (Theory & Practicals (if any)	
12.	Check List	

PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

SYLLABUS

Course Title: CRYPTOGRAPHY & NETWORK SECURITY (DA7210)

Unit I : Introduction to security attacks, services and mechanism, introduction to cryptography.

Conventional Encryption: Conventional encryption model, classical encryption techniques-substitution ciphers and transposition ciphers, cryptanalysis, steganography, stream and block ciphers.

Modern Block Ciphers: Block ciphers principals, Shannon's theory of confusion and diffusion, feistel structure, data encryption standard(DES), strength of DES, differential and linear crypt analysis of DES, block cipher modes of operations, triple DES, confidentiality using conventional encryption, traffic confidentiality, key distribution

Unit II : Introduction to prime and relative prime numbers, finite field of the form $GF(p)$, modular arithmetic, Fermat's and Euler's theorem, primality testing, Euclid's Algorithm, Chinese Remainder theorem, Principals of public key crypto systems, RSA algorithm, security of RSA, key management, Diffie-Hellman key exchange algorithm, introductory idea of Elliptic curve cryptography, Elgamal encryption.

Unit III : Message Authentication and Hash Function: Authentication requirements, authentication functions, message authentication code, hash functions, birthday attacks, security of hash functions and MACS, MD5 message digest algorithm, Secure hash algorithm(SHA). Digital Signatures: Digital Signatures, authentication protocols, digital signature standards (DSS), proof of digital signature algorithm.

Unit IV : Authentication Applications: Kerberos and X.509, directory authentication service, electronic mail security-pretty good privacy (PGP), S/MIME.

Unit V : IP Security: Architecture, Authentication header, Encapsulating security payloads, combining security associations, key management.

Web Security: Secure socket layer and transport layer security, secure electronic transaction (SET).

System Security: Intruders, Viruses and related threads, firewall design principals, trusted systems.

Text Book:

1. William Stallings, "Cryptography and Network Security: Principals and Practice", Prentice Hall, New Jersey.

Reference Book:

1. Johannes A. Buchmann, "Introduction to Cryptography", Springer-Verlag.
2. Bruce Schneier, "Applied Cryptography".

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

LESSON PLAN

Course code: DA7210 Course Name: Cryptography and Network Security

Course Objectives:-

This course deals with both theoretical and practical aspects of cryptography, to give an insight to the problems that arise in cryptography and the techniques used to solve them. It introduces both symmetric key cipher system and public key cryptography, covering methods of obtaining the objectives of CIA (confidentiality, integrity and authenticity). It surveys cryptographic tools used to provide security, such as shared key encryption (DES, 3DES, etc.); public key encryption, key exchange, and digital signature (Diffie-Hellmann, RSA, DSS, etc.). It then reviews how these tools are utilized in the internet protocols and applications such as SSL/TLS, IPSEC, Kerberos, PGP, S/MIME, SET, and others (including wireless). System security issues, such as viruses, intrusion, and firewalls.

Lecture No.	Contents	Text/ Ref. Book	Pages
1-2	Introduction to security attacks, services and mechanism, introduction to cryptography	TB	15-26
3-5	Conventional encryption model, classical encryption techniques-substitution ciphers and transposition ciphers, cryptanalysis, steganography, stream and block ciphers	TB	33-55
6-8	Block ciphers principals, Shannon's theory of confusion and diffusion, fiestal structure, data encryption standard(DES), strength of DES	TB	68-88
9-10	Differential and linear crypt analysis of DES, block cipher modes of operations, triple DES, confidentiality using conventional encryption, traffic confidentiality, key distribution	TB	89-90,190-206
11-12	Introduction to prime and relative prime numbers, finite field of the form GF(p), modular arithmetic	TB	108-122,245-246
13-14	Fermat's and Euler's theorem, primality testing, Euclid's Algorithm, Chinese Remainder theorem	TB	248-257
15-16	Principals of public key crypto systems, RSA algorithm, security of RSA, key management	TB	269-289
17-18	Diffie-Hellman key exchange algorithm, introductory idea of Elliptic curve cryptography, Elgamal encryption	TB	301-308,317-320
19-20	Authentication requirements, authentication functions	TB	329-332
21-22	Message authentication code, hash functions, birthday attacks, security of hash functions and MACS	TB	333-341,372-375

PREPARED BY :

REVIEWED BY :

APPROVED BY :

23-24	MD5 message digest algorithm, Secure hash algorithm(SHA)	RB TB	331-335 342-352
25-26	Digital Signatures: Digital Signatures, authentication protocols, digital signature standards (DSS), proof of digital signature algorithm	TB	396-400,403-406
27-29	Kerberos and X.509, directory authentication service	TB	452-470,429-435
30-31	Electronic mail security-pretty good privacy (PGP), S/MIME	TB	568-578,587-590
32-33	IPSec Architecture, Authentication header	TB	616-622
34-35	Encapsulating security payloads, combining security associations, key management	TB	627-638
36-38	Secure socket layer and transport layer security, secure electronic transaction (SET)	TB	489-505
39-40	Intruders, Viruses and related threads, firewall design principals, trusted systems	LECTURE NOTES	

Learning Outcomes:-At the end of the course

- I. Students will have the basic knowledge about different methods of conventional encryption.
- II. Students will have the knowledge about the concepts of public key encryption.
- III. Students will acquire knowledge about authentication functions, message authentication codes and different hash algorithms.
- IV. Students will acquire knowledge about network security tools and authentication applications.
- V. Students will able to analyze security requirements and apply appropriate security mechanism.

Text Books [TB]:

William Stallings, “Cryptography and Network Security: Principals and Practice”, 5th ed. Pearson Prentice Hall, 2011.


Reference Books [RB]:

- I. Behrouz A. Forouzan , Debdeep Mukhopadhyay, “Cryptography and Network Security”, 2nd ed. Tata McGraw Hill Education Private Limited, 2011.
- II. Atul Kahate , “Cryptography and Network Security”, 3rd ed. Tata McGraw Hill Education Private Limited, 2012.

PREPARED BY :

REVIEWED BY :

APPROVED BY :

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

Instructors' Contact Details:

Mr. Anuj Kumar Yadav (Course Coordinator), Assistant Professor, Room No.320 Vedanta, Contact Tel. No. +919997909115

E-mail: anuj.kumar@dituniversity.edu.in

Mr. Sandip Mandal, Assistant Professor, Room No.314 Vedanta, Contact Tel. No. +918449007365

E-mail: sandip.mandal@dituniversity.edu.in

Mr. Chirag Joshi, Assistant Professor, Room No.413 Vedanta, Contact Tel. No. +919827279630

E-mail: chirag.joshi@dituniversity.edu.in

Teaching Methodology:

- Lectures delivered in interactive mode using whiteboard and power point presentation.
- Questioning, Figures & real life examples related to the topics
- Time to time evaluation using surprise test and assignments.
- Students have to work individually as well as in groups inside as well as outside the class.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

TIME TABLE

NAME OF FACULTY : Anuj Kumar Yadav

BRANCH/SECTION : CSE – A,B,E

SESSION : 2017-18

SEMESTER : VIIth

SUBJECT CODE : DA7210

DIT UNIVERSITY DEHRADUN

2016-17, Odd Semester

W.E.F.: 26-07-2017

Teacher Anuj Kumar Yadav

Department: CSE

Teacher's Abbrev.

LOAD

17

	9-10	10-11	11-12	12-1	1-2	2-3	3-4
Mon	DA7210 CSE-B	DA7210 CSE-A				DA7210-CSE-E-VISH105	
Tue		DA7210 CSE-A	DA7210-CSE-E-VISH105			DA 7210 CSE C2 VE 505 B	
Wed	DA7210 CSE-B	DA7210 CSE-A				DA 7210 CSE E2 VE 505 F	
Thu			DA7210-CSE-E-VISH105			DA 7210 CSE B1 VE 505 E	
Fri	DA7210 CSE-B					DA 7210 CSE A1 VE 505 B	
Sat							

PREPARED BY :

REVIEWED BY :

APPROVED BY :



Cryptography & Network Security Course File

Issue No.: 01

Date:

Rev No.: NIL

Rev. Date: NIL

Clause: NIL

Page:

NAME OF FACULTY : Chirag Joshi

BRANCH/SECTION : CSE – C,D

SESSION : 2017-18

SEMESTER : VIIth

SUBJECT CODE : DA7210

DIT UNIVERSITY DEHRADUN

2017-18, Odd Semester

W.E.F.:

Teacher Mr.Chirag Joshi
Department:

Teacher's Abbrev.
Hour:


CJ

	9-10	10-11	11-12	12-1	1-2	2-3	3-4
Mon	DA7210-CSE-D-VISH509	DA7210-CSE-C-VISH505		DA3010 CSE-CSF, VE-403			
Tue	DA7210-CSE-D-VISH509	DA7210-CSE-C-VISH505				DA7210-CSE-C1-VE-505A	
Wed	DA7210-CSE-D-VISH509	DA7210-CSE-C-VISH505		DA3010-CSE- CSF-T3-VE- 403		DA7210-CSE-E1-VE-505F	
Thu		DA3010 CSE-CSF, VE- 403				DA7210-CSE-D1-VE-323A	
Fri		DA3010-CSE- BDA-T3-VE-402				DA3010 CSE-CSF, VE-403	
Sat							

PREPARED BY :


REVIEWED BY :

APPROVED BY :

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

ATTENDANCE REGISTER

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

THEORY PERFORMANCE SHEET

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

Teacher's Comments:

- Whether syllabus is well framed as per the professional needs
☐ Yes ☐ No ☐ Needs upgradation
- Whether reference books are available in library with latest edition
☐ Yes ☐ No ☐ Needs to be procured (provide list)
- Whether proper text books are available in learning resources with latest edition
☐ Yes ☐ No ☐ Needs to be procured (provide list)
- Whether e- books are available
☐ Yes ☐ No ☐ Need to be added
- Outcome of action taken for the week students in their performance
☐ No improvement ☐ slightly improved ☐ excellent change
☐ Good change ☐ No change
- Whether syllabus can be completed in stipulated time (if No, mention reason)
☐ Yes ☐ No
- Whether you are facing difficulty while handling the subject (if yes, provide details)
☐ Yes ☐ No
- Syllabus need to be revised as per futuristic professional demand
☐ Yes ☐ No ☐ syllabus is well framed
- Overall performance in your subject is
☐ Good ☐ Better ☐ Average ☐ Poor

Teacher's Suggestions:

-
-
-
-
-

- Summary of course files (**to be filled by course coordinator**)
 - a. The contents of course file are properly annexed as per the checklist
☐ Yes ☐ No
 - b. Whether faculty had made any noteable suggestions/ comments (if any mention briefly)

-
-
-

C .Recommendations/ Suggestions from your side if any about the subject & practical

•

•

d. Whether the course was conducted effectively by all faculties

☐ Satisfactory ☐ Not satisfactory

• **Remarks by HOD/ Dean/ Director**

a. Whether the course is conducted uniformly, regularly as per the syllabus & lesson plan


☐ Satisfactory ☐ Not satisfactory

• b. Critical observations and recommendations by **HOD/ Dean/ Director**

PREPARED BY :

REVIEWED BY :

APPROVED BY :


	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

Practicals List Of Cryptography and Network Security (DA7210)

All programs may be write in C or C++ or Java or Python according to knoweledge and choice of student.

1. Write a program for encryption and Decryption of the plaintext and display the cipher text and plaintext using Ceaser Cipher.
2. Write a program for Encryption and Decryption of the plaintext and display the cipher text and plaintext using playfair Cipher.
3. Write a program for Encryption and Decryption of the plaintext and display the cipher text and plaintext using using Hill Cipher.
4. Write a a program for Encryption and Decryption of the plaintext and display the cipher text and plaintextVigenere Cipher.
5. Write a program to perform bitwise XOR, right shift, left shift ,AND, OR on the given bits.
6. To implement Simple DES.
7. Write a program for the modular arthematic and GCD calculation for the given numbers.
8. Implement RSA encryption decryption algorithm
9. Implement Diffi-Hellmen Key exchange Method.
10. Write a program to generate SHA-1 hash algorithm.
11. Implement a digital signature algorithm.
12. Perform various encryption-decryption techniques with cryptool.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

LECTURE HANDOUTS

Cryptography

Human being from ages had two inherent needs: (a) to communicate and share information and (b) to communicate selectively. These two needs gave rise to the art of coding the messages in such a way that only the intended people could have access to the information. Unauthorized people could not extract any information, even if the scrambled messages fell in their hand. *The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.* The word ‘cryptography’ was coined by combining two Greek words, ‘Krypto’ meaning hidden and ‘graphene’ meaning writing.

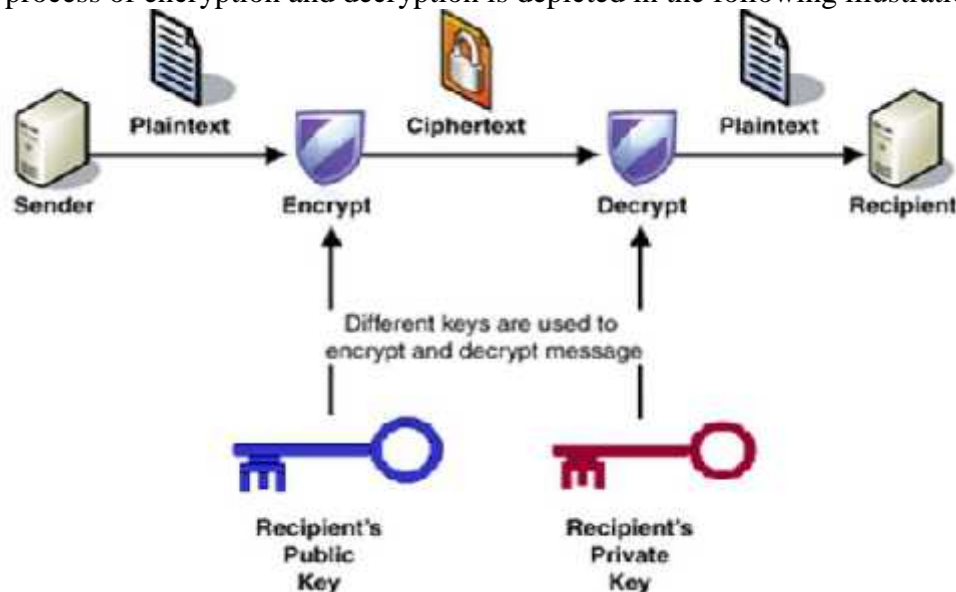
Public Key Cryptography

Unlike symmetric key cryptography, we do not find historical use of public-key cryptography. It is a relatively new concept.

Symmetric cryptography was well suited for organizations such as governments, military, and big financial corporations were involved in the classified communication.

With the spread of more unsecure computer networks in last few decades, a genuine need was felt to use cryptography at larger scale.

The process of encryption and decryption is depicted in the following illustration:



Hash Functions

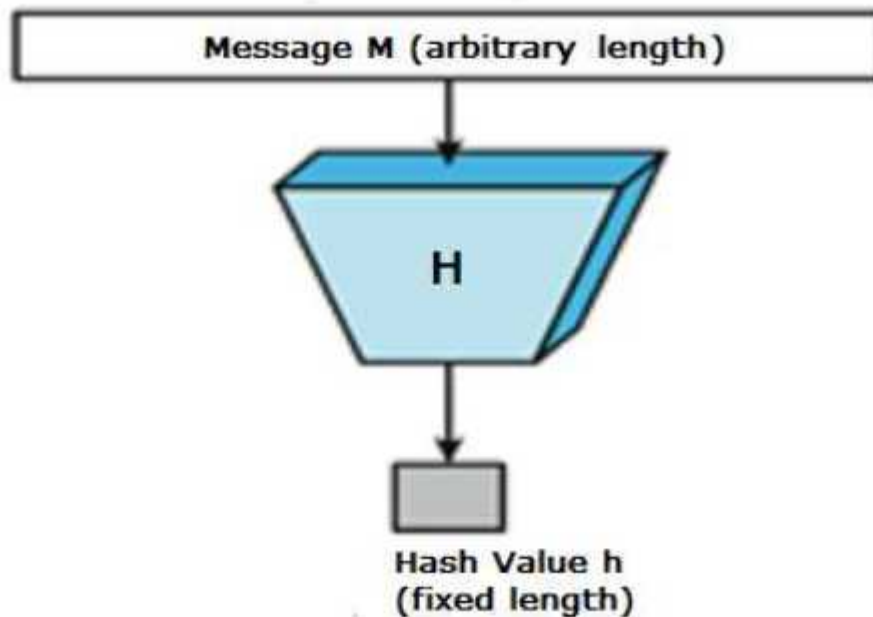
Hash functions are extremely useful and appear in almost all information security applications.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input to the hash function is of arbitrary length but output is always of fixed length.

Values returned by a hash function are called message digest or simply hash values.

The following picture illustrated hash function

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------



Popular Hash Functions

Let us briefly see some popular hash functions:

Message Digest (MD)

MD5 was most popular and widely used hash function for quite some years.

- The MD family comprises of hash functions MD2, MD4, MD5 and MD6. It was adopted as Internet Standard RFC 1321. It is a 128-bit hash function.


- In 2004, collisions were found in MD5. An analytical attack was reported to be successful only in an hour by using computer cluster. This collision attack resulted in compromised MD5 and hence it is no longer recommended for use.

Secure Hash Function (SHA)

Family of SHA comprise of four SHA algorithms; SHA-0, SHA-1, SHA-2, and SHA-3.

Though from same family, there are structurally different.

- The original version is SHA-0, a 160-bit hash function, was published by the National Institute of Standards and Technology (NIST) in 1993. It had few weaknesses and did not become very popular. Later in 1995, SHA-1 was designed to correct alleged weaknesses of SHA-0.
- SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security.
- In 2005, a method was found for uncovering collisions for SHA-1 within practical time frame making long-term employability of SHA-1 doubtful.

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

- SHA-2 family has four further SHA variants, SHA-224, SHA-256, SHA-384, and SHA-512 depending up on number of bits in their hash value. No successful attacks have yet been reported on SHA-2 hash function.
- Though SHA-2 is a strong hash function. Though significantly different, its basic design is still follows design of SHA-1. Hence, NIST called for new competitive hash function designs.
- In October 2012, the NIST chose the Keccak algorithm as the new SHA-3 standard. Keccak offers many benefits, such as efficient performance and good resistance for attacks.

RIPEND

The RIPEND is an acronym for RACE Integrity Primitives Evaluation Message Digest. This set of hash functions was designed by open research community and generally known as a family of European hash functions.

- The set includes RIPEND, RIPEMD-128, and RIPEMD-160. There also exist 256, and 320-bit versions of this algorithm.
- Original RIPEMD (128 bit) is based upon the design principles used in MD4 and found to provide questionable security. RIPEMD 128-bit version came as a quick fix replacement to overcome vulnerabilities on the original RIPEMD.
- RIPEMD-160 is an improved version and the most widely used version in the family. The 256 and 320-bit versions reduce the chance of accidental collision, but do not have higher levels of security as compared to RIPEMD-128 and RIPEMD-160 respectively.

Whirlpool

This is a 512-bit hash function.

- It is derived from the modified version of Advanced Encryption Standard (AES). One of the designer was Vincent Rijmen, a co-creator of the AES.
- Three versions of Whirlpool have been released; namely WHIRLPOOL-0, WHIRLPOOL-T, and WHIRLPOOL.

Digital signatures

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages.

They are used to bind signatory to the message.


Similarly, a digital signature is a technique that binds a person/entity to the digital data.

This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

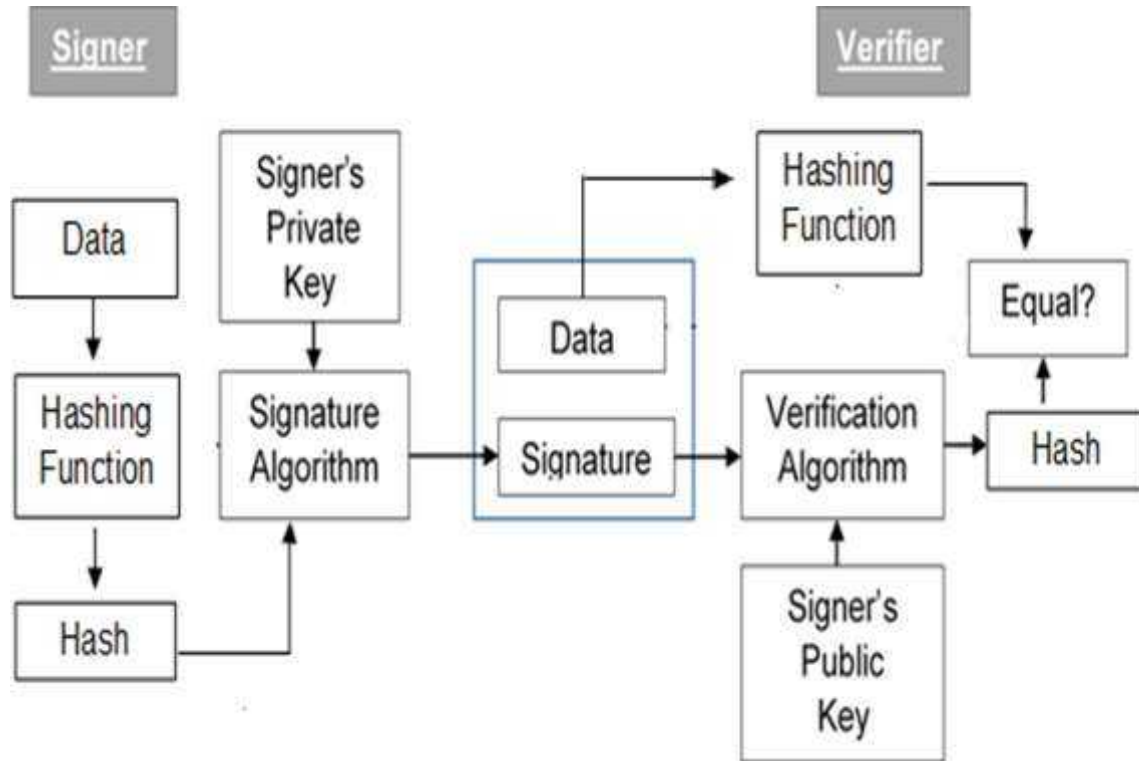
In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration:



Cryptography – Benefits

Cryptography is an essential information security tool. It provides the four most basic services of information security:

- **Confidentiality** – Encryption technique can guard the information and communication from unauthorized revelation and access of information.
- **Authentication** – The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
- **Data Integrity** – The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
- **Non-repudiation** – The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

Cryptography – Drawbacks

Apart from the four fundamental elements of information security, there are other issues that affect the effective use of information:

- A strongly encrypted, authentic, and digitally signed information can be **difficult**

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

to access even for a legitimate user at a crucial time of decision-making. The network or the computer system can be attacked and rendered non-functional by an intruder.

- **High availability**, one of the fundamental aspects of information security, cannot be ensured through the use of cryptography. Other methods are needed to guard **Cryptography**


against the threats such as denial of service or complete breakdown of information system.

- Another fundamental need of information security of **selective access control** also cannot be realized through the use of cryptography. Administrative controls and procedures are required to be exercised for the same.
- Cryptography does not guard against the vulnerabilities and **threats that emerge from the poor design of systems**, protocols, and procedures. These need to be fixed through proper design and setting up of a defensive infrastructure.
- Cryptography comes at cost. The cost is in terms of time and money:
 - o Addition of cryptographic techniques in the information processing leads to delay.
 - o The use of public key cryptography requires setting up and maintenance of public key infrastructure requiring the handsome financial budget.
- The security of cryptographic technique is based on the computational difficulty of mathematical problems. Any breakthrough in solving such mathematical problems or increasing the computing power can render a cryptographic technique vulnerable.

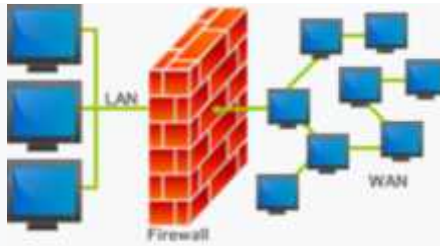
Firewall

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted outside network, such as the Internet. Firewalls are often categorized as either network firewalls or host-based firewalls. Network firewalls filter traffic between two or more networks; they are either software appliances running on general-purpose hardware, or hardware-based firewall computer appliances. Firewall appliances may also offer other functionality to the internal network they protect, such as acting as a DHCP or VPN

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

Types



An illustration of where a firewall would be located in a network

Firewalls are generally categorized as network-based or host-based. Network-based firewalls are positioned on the gateway computers of LANs, WANs and intranets. Host-based firewalls are positioned on the network node itself. The host-based firewall may be a daemon or service as a part of the operating system or an agent application such as endpoint security or protection. Each has advantages and disadvantages. However, each has a role in layered security.

Firewalls also vary in type depending on where communication originates, where it is intercepted, and the state of communication being traced.

Network layer or packet filters

Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. The firewall administrator may define the rules; or default rules may apply. The term "packet filter" originated in the context of BSD operating systems.

Network layer firewalls generally fall into two sub-categories, stateful and stateless.

Stateful firewalls maintain context about active sessions, and use that "state information" to speed packet processing. Any existing network connection can be described by several properties, including source and destination IP address, UDP or TCP ports, and the current stage of the connection's lifetime (including session initiation, handshaking, data transfer, or completion connection). If a packet does not match an existing connection, it will be evaluated according to the ruleset for new connections. If a packet matches an existing connection based on comparison with the firewall's state table, it will be allowed to pass without further processing.


Stateless firewalls require less memory, and can be faster for simple filters that require less time to filter than to look up a session. They may also be necessary for filtering stateless network protocols that have no concept of a session. However, they cannot make more complex decisions based on what stage communications between hosts have reached.

Application-layer

Application-layer firewalls work on the application level of the TCP/IP stack (i.e., all browser traffic, or all telnet or FTP traffic), and may intercept all packets traveling to or from an application. They block other packets (usually dropping them without acknowledgment to the sender).

On inspecting all packets for improper content, firewalls can restrict or prevent outright the spread of networked computer worms and Trojans. The additional inspection criteria can add extra latency to the forwarding of packets to their destination.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

Application firewalls function by determining whether a process should accept any given connection. Application firewalls accomplish their function by hooking into socket calls to filter the connections between the application layer and the lower layers of the OSI model. Application firewalls that hook into socket calls are also referred to as socket filters. Application firewalls work much like a packet filter but application filters apply filtering rules (allow/block) on a per process basis instead of filtering connections on a per port basis. Generally, prompts are used to define rules for processes that have not yet received a connection. It is rare to find application firewalls not combined or used in conjunction with a packet filter.

Also, application firewalls further filter connections by examining the process ID of data packets against a rule set for the local process involved in the data transmission. The extent of the filtering that occurs is defined by the provided rule set. Given the variety of software that exists, application firewalls only have more complex rule sets for the standard services, such as sharing services. These per-process rule sets have limited efficacy in filtering every possible association that may occur with other processes. Also, these per-process rule sets cannot defend against modification of the process via exploitation, such as memory corruption exploits. Because of these limitations, application firewalls are beginning to be supplanted by a new generation of application firewalls that rely on mandatory access control (MAC), also referred to as sandboxing, to protect vulnerable services.

Proxies


A proxy server (running either on dedicated hardware or as software on a general-purpose machine) may act as a firewall by responding to input packets (connection requests, for example) in the manner of an application, while blocking other packets. A proxy server is a gateway from one network to another for a specific network application, in the sense that it functions as a proxy on behalf of the network user.

Proxies make tampering with an internal system from the external network more difficult, so that misuse of one internal system would not necessarily cause a security breach exploitable from outside the firewall (as long as the application proxy remains intact and properly configured). Conversely, intruders may hijack a publicly reachable system and use it as a proxy for their own purposes; the proxy then masquerades as that system to other internal machines. While use of internal address spaces enhances security, crackers may still employ methods such as IP spoofing to attempt to pass packets to a target network.

Network address translation

Firewalls often have network address translation (NAT) functionality, and the hosts protected behind a firewall commonly have addresses in the "private address range", as defined in RFC 1918. Firewalls often have such functionality to hide the true address of computer which is connected to the network. Originally, the NAT function was developed to address the limited number of IPv4 routable addresses that could be used or assigned to companies or individuals as well as reduce both the amount and therefore cost of obtaining enough public addresses for every computer in an organization. Although NAT on its own is not considered a security feature, hiding the addresses of protected devices has become an often used defense against network reconnaissance.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

Computer virus

A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Infected computer programs can include, as well, data files, or the "boot" sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus

Operations and functions

Parts

A viable computer virus must contain a search routine, which locates new files or new disks which are worthwhile targets for infection. Secondly, every computer virus must contain a routine to copy itself into the program which the search routine locates. The three main virus parts are:

Infection mechanism

Infection mechanism (also called 'infection vector'), is how the virus spreads or propagates. A virus typically has a search routine, which locates new files or new disks for infection.

Trigger

The trigger, which is also known as logic bomb, is the compiled version that could be activated any time an executable file with the virus is run that determines the event or condition for the malicious "payload" to be activated or delivered such as a particular date, a particular time, particular presence of another program, capacity of the disk exceeding some limit, or a double-click that opens a particular file.

Payload

The "payload" is the actual body or data that perform the actual malicious purpose of the virus. Payload activity might be noticeable (e.g., because it causes the system to slow down or "freeze"), as most of the time the "payload" itself is the harmful activity, or some times non-destructive but distributive, which is called Virus hoax.


Phases

Virus phases is the life cycle of the computer virus, described by using an analogy to biology. This life cycle can be divided into four phases:

Dormant phase

The virus program is idle during this stage. The virus program has managed to access the target user's computer or software, but during this stage, the virus does not take any action. The virus will eventually be activated by the "trigger" which states which event will execute the virus, such as a date, the presence of another program or file, the capacity of the disk exceeding some limit or the user taking a certain action (e.g., double-clicking on a certain icon, opening an e-mail, etc.). Not all viruses have this stage.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

Propagation phase

The virus starts propagating, that is multiplying and replicating itself. The virus places a copy of itself into other programs or into certain system areas on the disk. The copy may not be identical to the propagating version; viruses often "morph" or change to evade detection by IT professionals and anti-virus software. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.


Triggering phase

A dormant virus moves into this phase when it is activated, and will now perform the function for which it was intended. The triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

Execution phase

This is the actual work of the virus, where the "payload" will be released. It can be destructive such as deleting files on disk, crashing the system, or corrupting files or relatively harmless such as popping up humorous or political messages on screen.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
---------------	---------------	---------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

LIST OF ASSIGNMENTS


Assignment-1

1. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?
2. Differentiate between
 - I. confusion and diffusion
 - II. Steganography and Cryptography
3. Explain the role of firewall in system security.
4. Discuss the concept of Set in short.

Assignment-2

1. Why we need key in cryptography?
2. What is the primary advantage of symmetric key cryptography?
3. Justify the statement “Decryption using a Feistel Cipher is essentially the same as encryption”.

PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

MID TERM QUESTION PAPER

DIT UNIVERSITY DEHRADUN

B.TECH (CSE / IT) MID TERM ODD SEM 2017-18 (SEM VII)

Roll No.

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

Subject Name: Cryptography and Network Security

Time: 2 Hours

Total Marks: 50

Note: All questions are compulsory. No student is allowed to leave the examination hall before the completion of the exam. No additional answer booklet shall be issued.

- Q.1)** (a) Distinguish between substitution cipher and transposition cipher.
 (b) Differentiate between active and passive security attacks with the help of example.
 (c) Find the multiplicative inverse modulo of 37 in Z_{19} .
 (d) Use an affine cipher to encrypt the message "INDIA" with the key pair (7, 2).

[4 x 2.5= 10]

- Q.2)** (a) How encryption is achieved using the rotor cipher?
 (b) Encrypt the plaintext "FIREWALL" using 5x5 play fair cipher using the key value "CRYPTOGRAPHY".
 (c) How confidentiality is achieved in public key cryptography?
 (d) **Find the value of Euler totient function Φ (100).**

[4 x 2.5= 10]

- Q.3)** (a) Discuss the role of S-Box in DES. In DES S-Box, how 48 bit data are converted in to 32 bit data? With this S-Box extract outputs for 101011 and

001001.

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
1	16	13	8	10	3	7	2	12	5	6	11	0	17	4	15	14	9	18	25	20	31	24	19	23	27	10	2	28	22	9	1
7	11	4	1	9	12	5	2	0	6	10	13	15	3	26	16	29	14	21	30	17	25	18	31	24	19	23	27	10	2	28	22
2	1	17	7	6	10	3	11	12	15	13	8	0	5	9	14	4	16	20	3	18	25	21	31	24	19	23	27	10	2	28	22

- (b) Explain RSA algorithm and perform encryption and decryption using RSA for the following data p=7, q=11, e=17, M=8.

[2 x 5= 10]

PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------

- Q.4)** (a) Generate the cipher text for “short example” using Hill Cipher. Use the following key for the operation

$$K = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$$

- (b) Draw and explain the block diagram of DES Function.

[2 x 5= 10]

- Q.5)** (a) Briefly explain the security services and mechanisms in cryptography.
(b) State Fermat little theorem, Also Calculate the value of “ $145^{102} \bmod 101$ ” using Fermat little theorem.

[2 x 5= 10]

-----END OF PAPER -----



**Cryptography & Network
Security Course File**

Issue No.: 01

Date:

Rev No.: NIL

Rev. Date: NIL

Clause: NIL

Page:

FINAL END SEM. QUESTION PAPER

DIT UNIVERSITY DEHRADUN

B.TECH (CSE/IT) END TERM ODD SEM 2017-18 (SEM VII)

Roll No.

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

Cryptography and Network Security

Time: 3 Hours

Total Marks: 100

**Note: All questions are compulsory. No student is allowed to leave the examination hall before the completion of the exam.
No additional answer booklet shall be issued.**

- Q.1)** (a) Define Security goals and distinguish between integrity and non-repudiation?
- (b) How does firewall prevents intrusion detection?
- (c) Illustrate different ways in which an attacker can mount a DOS attack on a system.
- (d) How many transformations are there in each version of AES? Also explain the advantage of AES over DES.
- [4 x 5= 20]**
- Q.2)** (a) Apply Miller Rabin algorithm using the base 2 to test whether the number 561 is composite or not.
- (b) State the purpose of appending length of the message in MD5 hash algorithm?
- (c) Define Chinese remainder theorem and its application. Find the value of x for the following congruence equations using Chinese remainder theorem:
- X 1 mod 5
X 5 mod 8
X 3 mod 13
- (d) Consider one round version of DES. Plaintext is given in hexadecimal notations as:
0 1 2 3 4 5 6 7 8 9 A B C D E F
- (i) Derive Initial Permutation
- (ii) Derive L0, R0

[4 x 5= 20]

PREPARED BY :

REVIEWED BY :

APPROVED BY :

- Q.3)** (a) In Elgamal cryptosystem, given the prime $p=11$:
- (i) Choose an appropriate primitive root (e_1) and private key (d), and then calculate e_2 .
 - (ii) Encrypt the message "HE", use 00 to 25 for encoding.
 - (iii) Decrypt the cipher text to obtain the plaintext.
- (b)
- (i) List the main features of the SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512?
 - (ii) Differentiate between message authentication code (MAC) and message detection codes (MDC).

[2 x 10= 20]


- Q.4)** (a) List and explain about the entities that constitute Kerberos environment. Write down the message exchanges for obtaining ticket granting ticket and service granting ticket in context of Kerberos version 4. Give justifications behind choice of various elements of the message.
- (b) How a key is shared between two parties using Diffie-Hellman by exchange algorithm? Consider the Diffie-Hellman scheme with a common prime $q=11$ and a primitive root $\alpha=2$.
- (i) Show that 2 is indeed a generator.
 - (ii) If the user A has a public key $Y_A=9$, then calculate private key value for user A.
 - (iii) If the user B has a public key $Y_B=3$, then calculate the shared secret key k between A and B.

[2 x 10= 20]

- Q.5)** (a)
- (i) Describe the signature generation process of digital signature standard.
 - (ii) Describe the various services provided by PGP. How PGP is different from X.509?
- (b) Differentiate between the transport mode and tunnel mode of IP Sec and explain how authentication and confidentiality are achieved using IP Sec.

[2 x 10= 20]

-----END OF PAPER -----

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

LIST OF DEBAR STUDENTS

NO DEBAR

PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------

SCHEME OF EVALUATION PATTERN
(AS PER COURSE STRUCTURE)

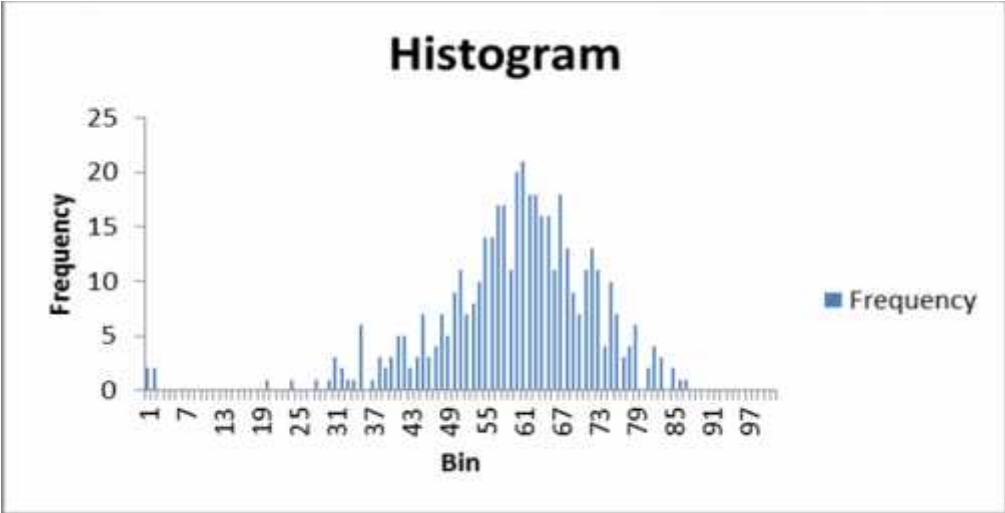
Evaluation Factors	Marks Allotted
Mid Term	20
Class Test	5
Attendance	0
Quizzes	5
Assignment	5
Viva-voce (CE)	5
Lab Assessment/Record	5
Performance (ETE)	15
End Term	40
Total	100


PREPARED BY :

REVIEWED BY :

APPROVED BY :

Result Analysis Sheet (Proposed)

1.	No. of student appeared	:	438
2.	No. of student debarred	:	0
3.	No. of Highest marks out of 100%	:	87
4.	No. of student securing highest marks	:	1
			total students
5.	Total no. of student secured	A+	13
6.	Total no. of student secured	A	34
7.	Total no. of student secured	B +	82
8.	Total no. of student secured	B	179
9.	Total no. of student secured	C+	78
10.	Total no. of student secured	C	31
11.	Total no. of student secured	D	14
12.	Total no. of student secured	E	2
13.	Total no. of student secured	F	5
14.	Overall justification by faculty:		
15.	Graphical Representation 		
16.	Action planned for improvement of student's performance (in next semester):		
17.	Remarks:		
18.			
19.			

	Cryptography & Network Security Course File	Issue No.: 01	Date:
		Rev No.: NIL	Rev. Date: NIL
		Clause: NIL	Page:

CHECKLIST

S.NO.	CONTENTS	Page No	YES	NO	N/A
1.	Syllabus				
2.	Lesson Plan				
3.	Time Table				
4.	Attendance Register				
5.	Theory Performance Sheet, Teacher's Comments, Teacher's Suggestions				
6.	Scheme of Evaluation (Course Structure) (Practicals Attendance cum Practical Performance Sheet), Teacher's Comments, Teacher's Suggestions				
7.	List of Practicals				
8.	List of Tutorials Sheets				
8.	List of Assignments				
9.	Mid Term Question Paper, End Sem. Question Paper				
10.	Scheme of evaluation Pattern				
11.	Result Analysis (Theory & Practicals (if any))				
12.	Check List				
13.	Miscellaneous, if any				

Remarks by the Course Coordinator:

Remarks by the Director/Dean/HOD:

PREPARED BY :	REVIEWED BY :	APPROVED BY :
----------------------	----------------------	----------------------