Cryptography and Network Security

Unit: 4

Cyber Security

ANC0301

(B Tech III[rd] Sem)

Sujeet Singh Bhadouria
Assistant Professor
(CSE)
NIET, Gr. Noida

Faculty Profile

FACULTY PROFILE
Name of Faculty: Sujeet Singh Bhadouria

Designation & Department: Assistant Professor, CSE

Qualification: Ph.D (Pre-Submission) M.Tech

Experience: 10 Years of teaching experience

Area of Interest: Computer Network

Reviewer: IET Communications ISSN 1751-8644 (SCI & SCOPUS INDEX)
Research Publications:
International Journal 09
Paper Presentation 06
International Patent 01 (Granted)
National Patent 04

Evaluation Scheme

Sl. No.	Subject Codes	Subject Name	Periods			Evaluation Scheme				End Semester		Total	Credit
			L	T	P	CT	TA	TOTAL	PS	TE	PE		
WEEKS COMPULSORY INDUCTION PROGRAM													
1	AAS0301A	Engineering Mathematics-III	3	1	0	30	20	50		100		150	4
2	ACSE0306	Discrete Structures	3	0	0	30	20	50		100		150	3
3	ACSE0304	Digital Logic & Circuit Design	3	0	0	30	20	50		100		150	3
4	ACSE0301	Data Structures	3	1	0	30	20	50		100		150	4
5	ACSE0302	Object Oriented Techniques using Java	3	0	0	30	20	50		100		150	3
6	ACSE0305	Computer Organization & Architecture	3	0	0	30	20	50		100		150	3
7	ACSE0354	Digital Logic & Circuit Design Lab	0	0	2				25		25	50	1
8	ACSE0351	Data Structures Lab	0	0	2				25		25	50	1
9	ACSE0352	Object Oriented Techniques using Java Lab	0	0	2				25		25	50	1
10	ACSE0359	Internship Assessment-I	0	0	2				50			50	1
11	ANC0301/ ANC0302	Cyber Security*/ Environmental Science*(Non Credit)	2	0	0	30	20	50		50		100	0
12		MOOCs** (For B.Tech. Hons. Degree)											
		GRAND TOTAL										**1100**	**24**

Syllabus

Introduction:

Introduction to Information Systems: Types of Information Systems, Development of Information Systems, Need for Information Security, Threats to Information Systems, Information Assurance, Guidelines for Secure Password and WI-FI Security and social media and Windows Security, Security Risk Analysis and Risk Management.

Application Layer Security:

Data Security Considerations-Backups, Archival Storage and Disposal of Data, Security Technology-Firewall, Intrusion Detection, Access Control, Security Threats -Viruses, Worms, Trojan Horse, Bombs, Trapdoors, Spoofs, E-mail Viruses, Macro Viruses, Malicious Software, Network and Denial of Services Attack, Security, Threats to E-Commerce: Electronic Payment System, e- Cash, Issues with Credit/Debit Cards.

Syllabus

Secure System Development:

Application Development Security, Architecture & Design, Security Issues in Hardware: Data Storage and Downloadable Devices, Mobile Protection, Security Threats involving in social media, Physical Security of IT Assets, Access Control, CCTV and Intrusion Detection Systems, Backup Security Measures.

Cryptography and Network Security:

- Public key cryptography: RSA Public Key Crypto with implementation in Python, Digital Signature Hash Functions, Public Key Distribution.
- Symmetric key cryptography: DES (Data Encryption Standard), AES (Advanced Encryption Standard), Secure hash algorithm (SHA-1).
- Real World Protocols: Basic Terminologies, VPN, Email Security Certificates, Transport Layer Security (TLS), IP security, DNS Security.

Syllabus

Security Policy:

- Policy design Task, WWW Policies, Email based Policies, Policy Revaluation Process-Corporate Policies-Sample Security Policies, Publishing and Notification Requirement of the updated and new Policies.
- Recent trends in security.

Applications

There are many cyber security real-life examples where financial organizations like banks and social organizations, weather channels etc. have faced cyber-attacks and have lost valuable information and resources. To fix these problems, you'll need comprehensive cyber security awareness.

According to KPMG, the annual compensation for cyber security heads ranges from 2 Cr to 4 Cr annually. The industry also reports a satisfaction level of 68%, making it a mentally and financially satisfying career for most.

Course Objective

Students will learn about :

- Security of Information system and Risk factors.
- Examine security threats and vulnerability in various scenarios.
- Understand concept of cryptography and encryption technique to protect the data from cyber-attack
- Provide protection for software and hardware.

Course Outcome

COURSE OUTCOME NO.	COURSE OUTCOMES	Bloom's Knowledge Level (KL)
CO1	Analyze the cyber security needs of an organization.	K4
CO2	Identify and examine software vulnerabilities and security solutions.	K1, K3
CO3	Comprehend IT Assets security (hardware and Software) and performance indicators.	K2
CO4	Measure the performance and encoding strategies of security systems.	K3, K5
CO5	Understand and apply cyber security methods and policies to enhance current scenario security.	K2, K3

Program Outcomes

1. Engineering knowledge
2. Problem analysis
3. Design/development of solutions
4. Conduct investigations of complex problems
5. Modern tool usage
6. The engineer and society
7. Environment and sustainability

Program Outcomes…(cont.)

8. Ethics

9. Individual and team work

10. Communication

11. Project Management and Finance

12. Life Long learning

CO-PO Mapping

CO-PO Mapping

PO No. → / CO No. ↓	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	2	1	2	-	-	-	1	2	1	2	2
CO2	2	2	2	2	2	1	-	1	2	1	2	2
CO3	2	2	1	2	2	-	-	1	2	1	2	2
CO4	2	2	1	2	2	1	-	1	2	1	2	2
CO5	2	2	1	2	2	-	-	1	2	1	2	2

*3= High *2= Medium *1=Low

Program Specific Outcomes

Program Specific Outcomes (PSOs) are what the students should be able to do at the time of graduation. The PSOs are program specific. PSOs are written by the department offering the program.

On successful completion of B. Tech. (CSE) Program, the Information and Technology engineering graduates will be able to:

PSO1 : Work as a software developer, database administrator, tester or networking engineer for providing solutions to the real world and industrial problems.

PSO2 : Apply core subjects of information technology related to data structure and algorithm, software engineering, web technology, operating system, database and networking to solve complex IT problems

PSO3 : Practice multi-disciplinary and modern computing techniques by lifelong learning to establish innovative career

PSO4 : Work in a team or individual to manage projects with ethical concern to be a successful employee
or employer in IT industry.

PSO Mapping

Program Specific Outcomes and Course Outcomes Mapping

CO	PSO1	PSO2	PSO3	PSO4
CO1	2	2	-	2
CO2	2	2	1	2
CO3	2	2	-	2
CO4	2	2	-	2
CO5	2	2	-	2

*3= High *2= Medium *1=Low

Program Educational Objectives

- The Program Educational Objectives (PEOs) of an engineering degree program are the statements that describe the expected achievements of graduates in their career, and what the graduates are expected to perform and achieve during the first few years after graduation.

PEO1: To have an excellent scientific and engineering breadth so as to comprehend, analyze, design and solve real-life problems using state-of-the-art technology.

PEO2: To lead a successful career in industries or to pursue higher studies or to understand entrepreneurial endeavors.

PEO3: To effectively bridge the gap between industry and academics through effective communication skill, professional attitude and a desire to learn.

Result Analysis

Faculty Name	Subject Name	Code	Result
Ms Ruchika Sharma	Cyber Security	ANC0301	100%

Question Paper Template

(SEM:…..SESSIONAL EXAMINATION –I)(2021-2022)

Subject Name: ……..

Time: 1.15Hours **Max. Marks:30**

General Instructions:

- All questions are compulsory. Answers should be brief and to the point.
- This Question paper consists of .....pages & ...5.....questions.
- It comprises of three Sections, A, B, and C. You are to attempt all the sections.
- Section A -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- Section B - Question No-3 is Short answer type questions carrying 5 marks each. You need to attempt any two out of three questions given.
- Section C -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. You need to attempt any one part a. or b.
- Students are instructed to cross the blank sheets before handing over the answer sheet to the invigilator.
- No sheet should be left blank. Any written material after a blank sheet will not be evaluated/checked.

		SECTION – A	[8]	
1.	**Attempt all parts**		**(4×1=4)**	**CO**
	a.		**(1)**	
	b.		**(1)**	
	c.		**(1)**	
	d.		**(1)**	
2.	**Attempt all parts**		**(2×2=4)**	**CO**
	a.		**(2)**	
	b.		**(2)**	

Question Paper Template

		SECTION – B		
3.	**Answer any two of the following-**		**[2×5=10]**	**CO**
	a.		**(5)**	
	b.		**(5)**	
	c.		**(5)**	
		SECTION – C		
4	**Answer any one of the following-(Any one can be applicative if applicable)**		**[2×6=12]**	**CO**
	a.	**Question-**	**(6)**	
	b.	**Question-**	**(6)**	
5.	**Answer any one of the following-**			
	a.		**(6)**	
	b.		**(6)**	

Question Paper Template

		SECTION – A		CO
1.	Attempt all parts-		[10×1=10]	
	1-a.	Question-	-1	
	1-b.	Question-	-1	
	1-c.	Question-	-1	
	1-d.	Question-	-1	
	1-e.	Question-	-1	
	1-f.	Question-	-1	
	1-g.	Question-	-1	
	1-h.	Question-	-1	
	1-i.	Question-	-1	
	1-j.	Question-	-1	
2	Attempt all parts-		[5×2=10]	CO
	2-a.	Question-	-2	
	2-b.	Question-	-2	
	2-c.	Question-	-2	
	2-d.	Question-	-2	
	2-e.	Question-	-2	

Question Paper Template

SECTION – B				CO
3	Answer any five of the following-		[5×6=30]	
	3-a.	Question-	-6	
	3-b.	Question-	-6	
	3-c.	Question-	-6	
	3-d.	Question-	-6	
	3-e.	Question-	-6	
	3-f.	Question-	-6	
	3-g.	Question-	-6	

Question Paper Template

SECTION – C				CO
4	Answer any one of the following-		[5×10=50]	
	4-a.	Question-	-10	
	4-b.	Question-	-10	
5	Answer any one of the following-			
	5-a.	Question-	-10	
	5-b.	Question-	-10	
6	Answer any one of the following-			
	6-a.	Question-	-10	
	6-b.	Question-	-10	
7	Answer any one of the following-			
	7-a.	Question-	-10	
	7-b.	Question-	-10	
8	Answer any one of the following-			
	8-a.	Question-	-10	
	8-b.	Question-	-10	

Prerequisite/Recap

- Basics recognition in the domain of Computer Science.
- Concept of network and operating system.
- Commands of programming language.

Content (Unit-4)

- Public key cryptography: RSA Public Key Crypto with implementation in Python, Digital Signature, Hash Functions, Public Key Distribution.
- Symmetric key cryptography: DES (Data Encryption Standard), AES (Advanced Encryption Standard), Secure hash algorithm (SHA-1).
- Real World Protocols: Basic Terminologies, VPN, Email Security Certificates, Transport Layer Security, TLS, IP security, DNS Security.

Unit Objective/Outcomes

Topic	Objective
RSA IMPLEMENTATION IN PYTHON	To implement RSA in python language.
DIGITAL SIGNATURE	Digital signatures are used to meet three important goals of information security: integrity, authentication, and non-repudiation.
HASH FUNCTIONS	Cryptographic Hash Functions are used to achieve a number of Security goals like Message Authentication, Message Integrity, and are also used to implement Digital Signatures (Non-repudiation), and Entity Authentication.
PUBLIC KEY DISTRIBUTION	In public key cryptography, the key distribution of public keys is done through public key servers.
DES	Data Encryption is used to deter malicious or negligent parties from accessing sensitive data. An important line of defense in a cyber security architecture, encryption makes using intercepted data as difficult as possible.
AES	Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key -- to encrypt and decrypt a message and protect it from unauthorized access or use.

Topic Mapping with CO

Topic	CO
RSA IN PYTHON	CO4
DIGITAL SIGNATURE	CO4
HASH FUNCTIONS	CO4
PUBLIC KEY DISTRIBUTION	CO4
DES	CO4
AES	CO4

Introduction (CO4)

- Modern life depends on online services, so having a better understanding of cyber security threats is vital.
- The course will improve your online safety in the context of the wider world, introducing concepts like malware, trojan virus, network security, cryptography, identity theft, and risk management.

1. https://www.javatpoint.com/cyber-security-introduction
2. https://www.edureka.co/blog/what-is-cybersecurity/
3. http://natoassociation.ca/a-short-introduction-to-cyber-security/

Introduction(CO4)

- **Cryptography :**

It is the art of secret writing.

- **Network :**

Network is collection of computers linked/connected together via connecting network devices like modem, routers, bridge, repeater etc.

- **Network Security :**

Nowadays, everything is performed on Internet, so it is necessary to provide security for the data which is transferred between computer systems.

"Providing security for the data over the network."

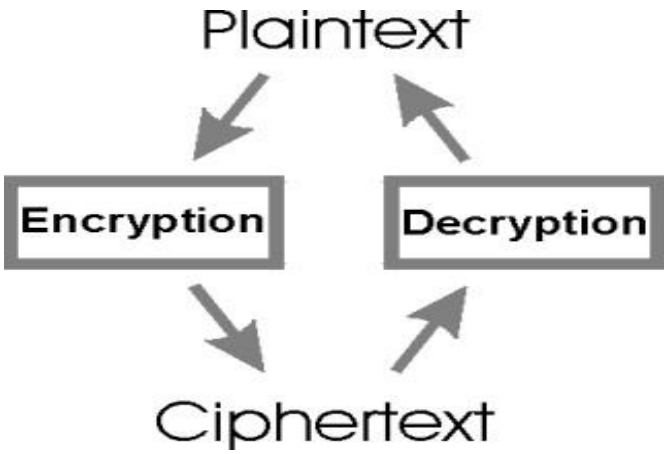
Introduction

Plain Text :

Normal text that can be read by user and is in readable format.

Cipher Text :

It is in unreadable format and user have to convert cipher text to plain text.



Introduction

2 Ways of Encryption

- **Stream ciphers :**

In stream ciphers the encryption is done bit by bit.

- **Block ciphers :**

In block ciphers the encryption is done block by block, where a block is group of bits.

Introduction

There are 2 mechanisms for encryption.

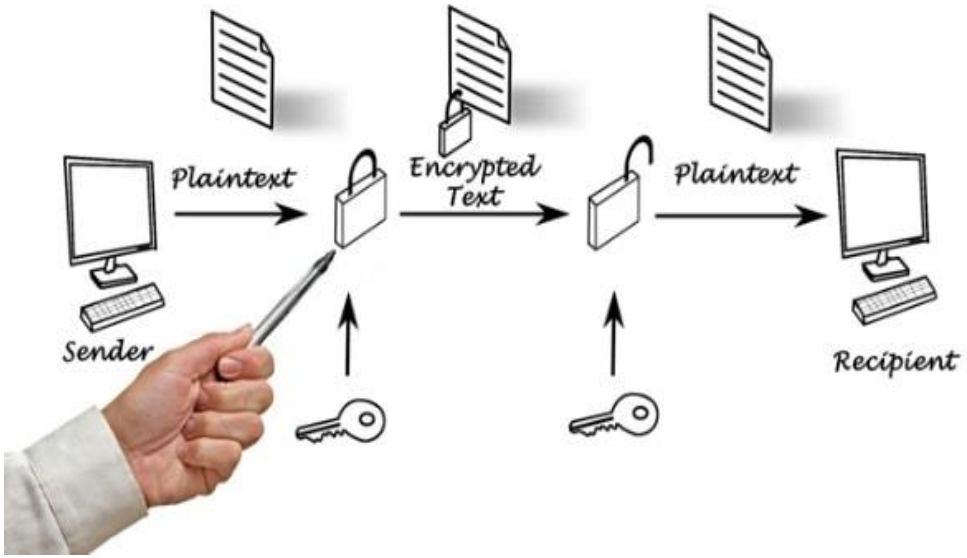
1. Asymmetric key encryption or public key encryption.

A pair of public key and private key is used for encryption and decryption.

Introduction

2. Symmetric key encryption or secret key encryption or single key encryption.

Same key is used for encryption and decryption.



RSA Algorithm(CO4)

RSA is the most common public-key algorithm, named after its inventors Rivest, Shamir, and Adelman (RSA).RSA encryption algorithm is a type of public-key encryption algorithm. To better understand RSA, lets first understand what is public-key encryption algorithm.

Public key encryption algorithm:

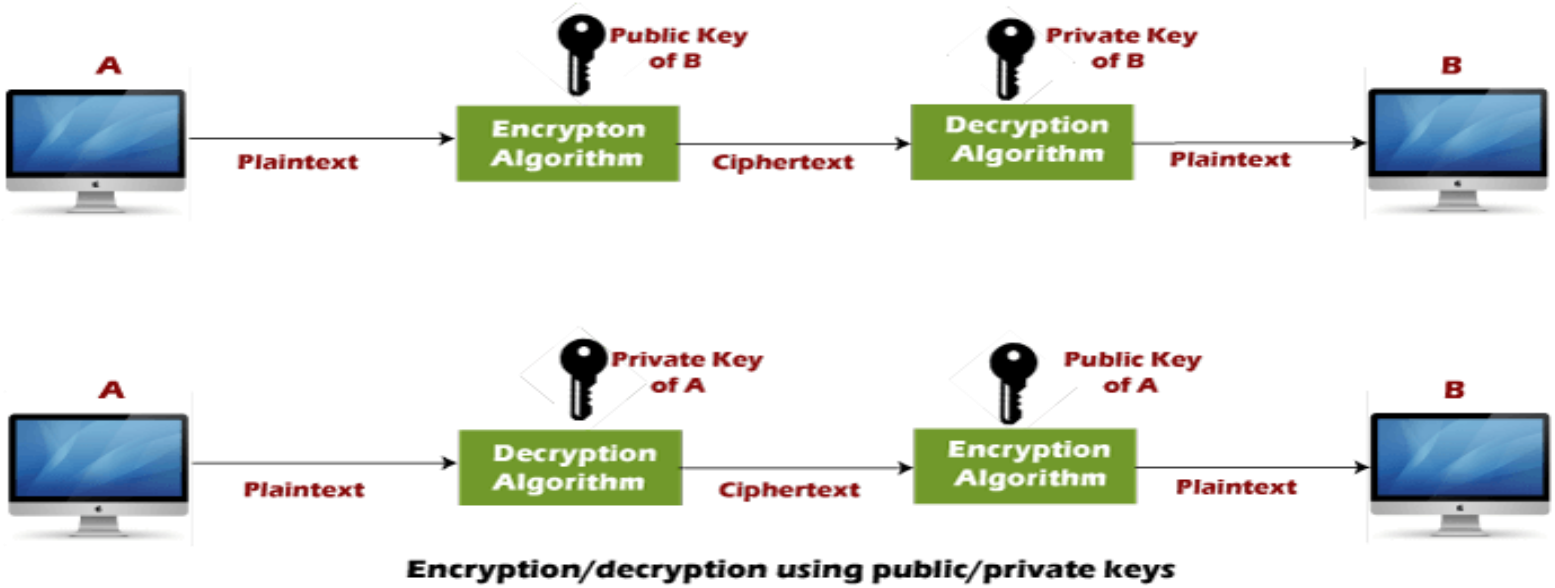
Public Key encryption algorithm is also called the Asymmetric algorithm. Asymmetric algorithms are those algorithms in which sender and receiver use different keys for encryption and decryption. Each sender is assigned a pair of keys:

- Public key
- Private key

The Public key is used for encryption, and the Private Key is used for decryption. Decryption cannot be done using a public key. The two keys are linked, but the private key cannot be derived from the public key. The public key is well known, but the private key is secret and it is known only to the user who owns the key. It means that everybody can send a message to the user using user's public key. But only the user can decrypt the message using his private key.

RSA Algorithm(CO4)

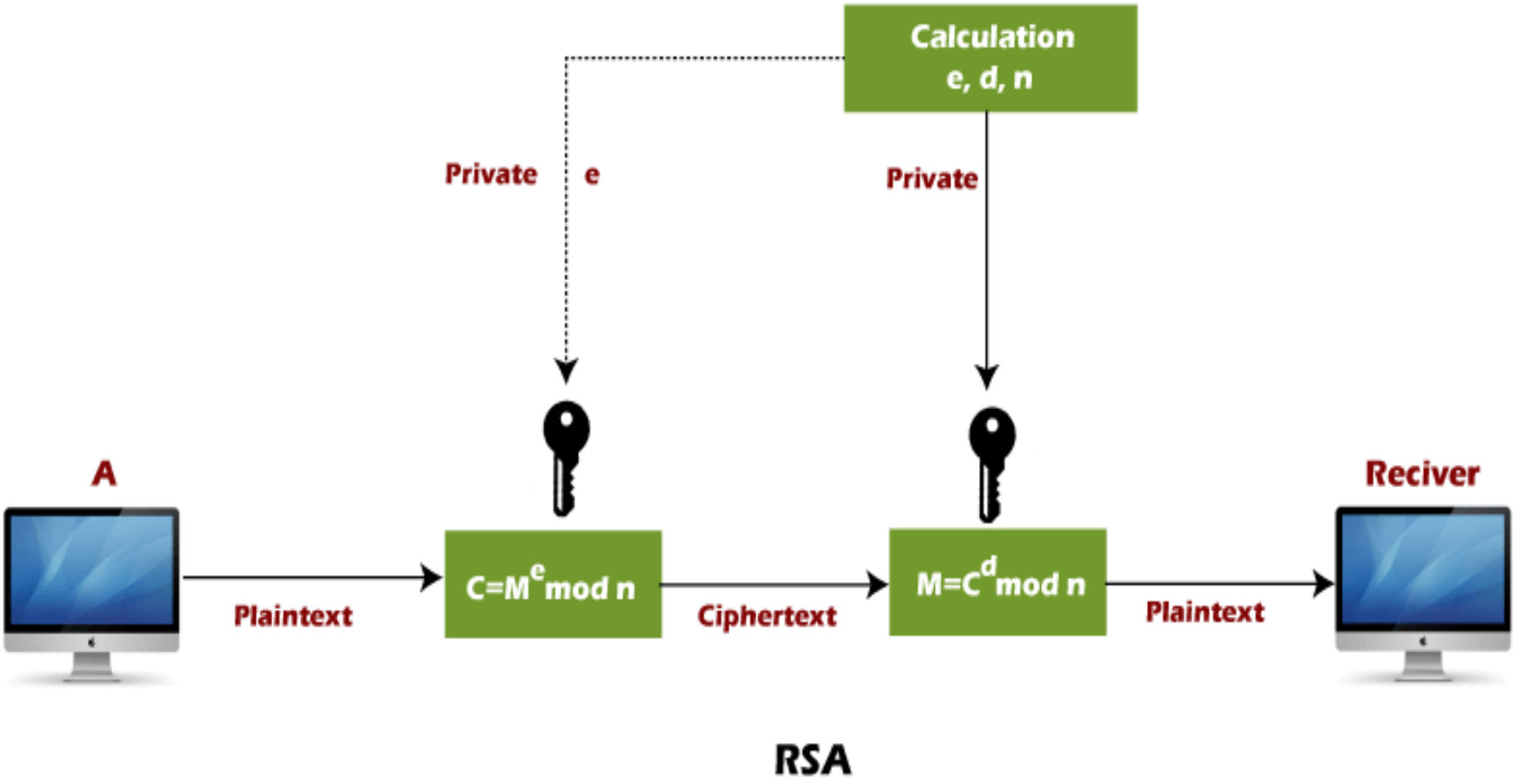
The Public key algorithm operates in the following manner:



Encryption/decryption using public/private keys

- The data to be sent is encrypted by sender A using the public key of the intended receiver
- B decrypts the received ciphertext using its private key, which is known only to B. B replies to A encrypting its message using A's public key.
- A decrypts the received ciphertext using its private key, which is known only to him.

RSA Algorithm(CO4)



RSA

RSA Algorithm(CO4)

- RSA algorithm uses the following procedure to generate public and private keys:

- Select two large prime numbers, p and q.
- Multiply these numbers to find n = p x q, where n is called the modulus for encryption and decryption.
- Choose a number e less than n, such that n is relatively prime to (p - 1) x (q - 1). It means that e and (p - 1) x (q - 1) have no common factor except 1. Choose "e" such that 1<e < ϕ (n), e is prime to ϕ (n),
- gcd (e,d(n)) =1
- If n = p x q, then the public key is <e, n>. A plaintext message m is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.

RSA Algorithm(CO4)

- $C = m^e \bmod n$

Here, m must be less than n. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.

- To determine the private key, we use the following formula to calculate the d such that:
- $D_e \bmod \{(p - 1) \times (q - 1)\} = 1$
- Or
- $D_e \bmod \phi (n) = 1$
- The private key is <d, n>. A ciphertext message c is decrypted using private key <d, n>. To calculate plain text m from the ciphertext c following formula is used to get plain text m.
- $m = c^d \bmod n$

RSA Algorithm(CO4)

- 1. Two large prime numbers are considered. Let them be p,q.
- 2. Calculate n = p q and (ϕ) phi = (p-1) (q-1).
- 3. Select e, public key, such that 1 < e < phi and gcd (e, phi) = 1,i.e e is not a factor of (p-1) and(q-1).
- 4. Calculate d, the private key, such that de =1 mod phi.
- One key is (n, e) and the other key is (n, d). The values of p, q, and phi should also be kept secret.
- n is considered to be the modulus.
- e is considered to be the public key.
- d is considered to be the secret key.

RSA Algorithm

Encryption

Sender A does the following:

1. Get the recipient B's public key (n, e).
2. Identify the plaintext message as a positive integer m.
3. Calculate the cipher text c = m^e mod n.
4. Transmits the cipher text c to receiver B.

Decryption

Recipient B is supposed to perform the following functions:

1. Make a consideration to adapt his or her own private key (n, d) and depict a complete computation in plain text m = c^d mod n.
2. Perform a conversion of the integer so that it can be in plain text form

RSA Public key crypto in python

Encryption:

$m^e \bmod(n) = 89^3 \bmod 77 = 166 = c$

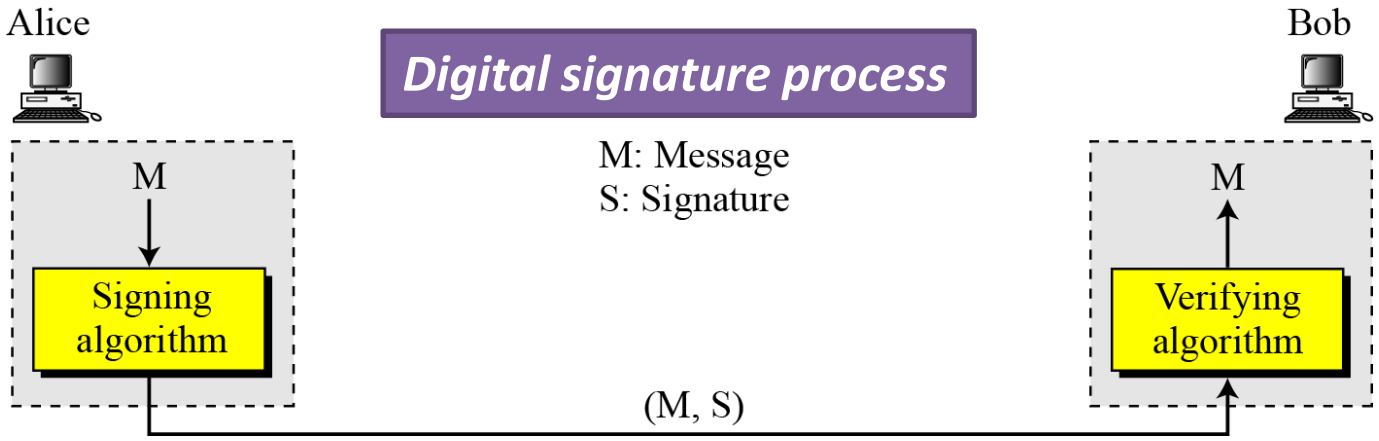
```
01  import math
02
03  message = int(input("Enter the message to be encrypted: "))
04
05  p = 11
06  q = 7
07  e = 3
08
09  n = p*q
10
11  def encrypt(me):
12      en = math.pow(me,e)
13      c = en % n
14      print("Encrypted Message is: ", c)
15      return c
16
17  print("Original Message is: ", message)
18  c = encrypt(message)
```

OUTPUT:-

```
Enter the message to be encrypted: 89
Original Message is:  89
Encrypted Message is:  166
```

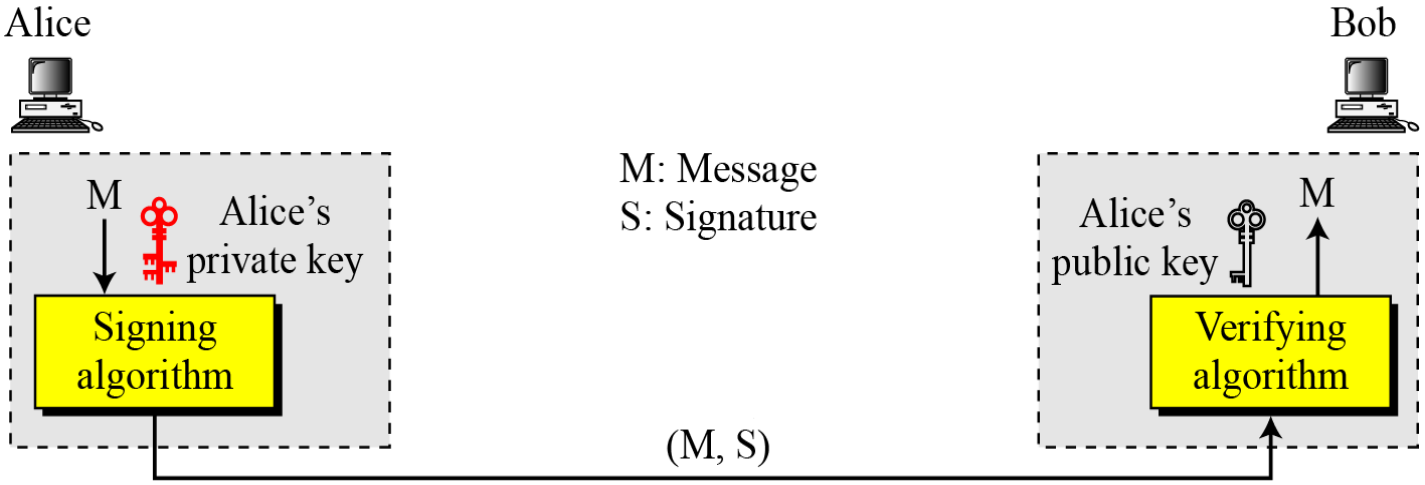
Digital Signature (CO4)

In digital signature process the sender uses a signing algorithm to sign the message. The message and the signature are sent to the receiver. The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted; otherwise, it is rejected.



Digital Signature

Adding key to the digital signature process

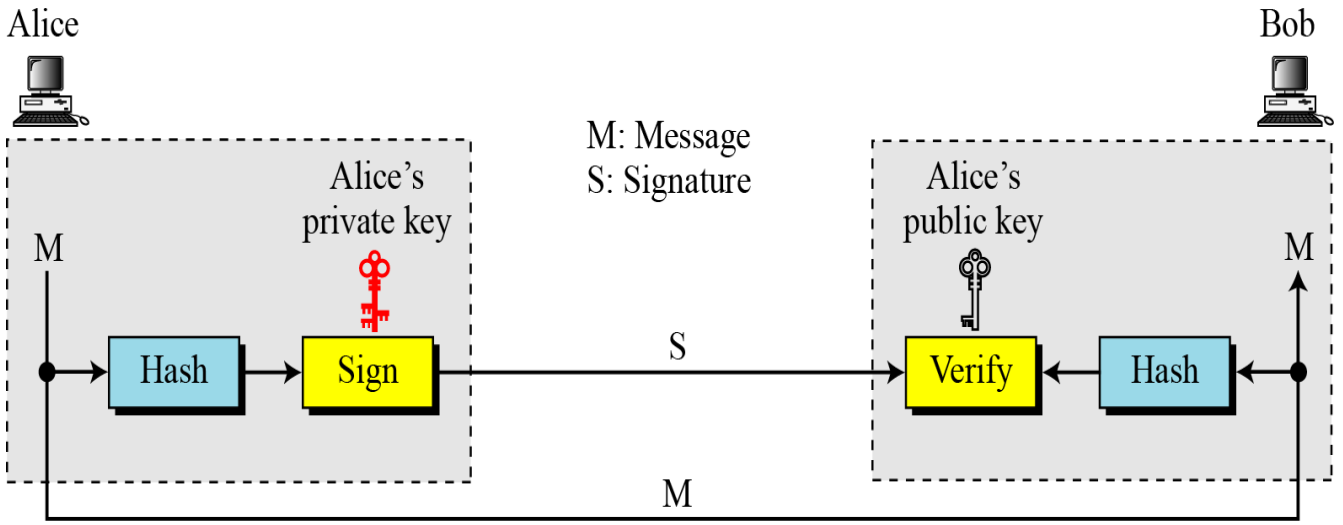


Note

A digital signature needs a public-key system. The signer signs with her private key; the verifier verifies with the signer's public key.

Digital Signature

Signing the digest



Note

A cryptosystem uses the private and public keys of the receiver: a digital signature uses the private and public keys of the sender.

Hash Function(CO4)

A cryptographic hash function is an algorithm that takes an arbitrary amount of data input—a credential—and produces a fixed-size output of enciphered text called a hash value, or just "hash." That enciphered text can then be stored instead of the password itself, and later used to verify the user.

Certain properties of cryptographic hash functions impact the security of password storage.

- **Non-reversibility, or one-way function.** A good hash should make it very hard to reconstruct the original password from the output or hash.

Hash Function

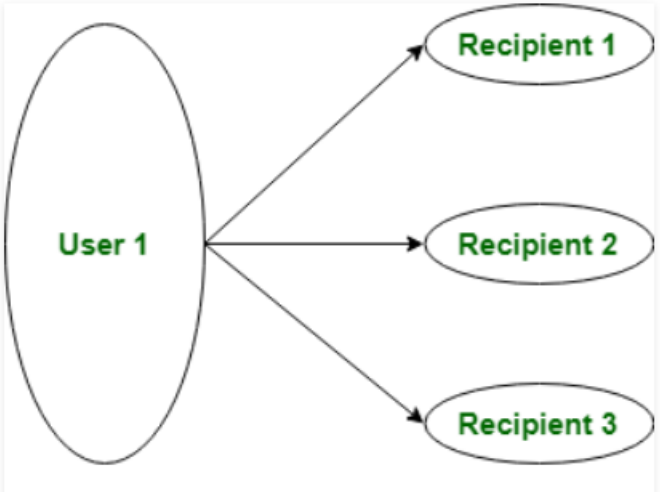
- **Diffusion, or avalanche effect**. A change in just one bit of the original password should result in change to half the bits of its hash. In other words, when a password is changed slightly, the output of enciphered text should change significantly and unpredictably.
- **Determinism.** A given password must always generate the same hash value or enciphered text.
- **Collision resistance.** It should be hard to find two different passwords that hash to the same enciphered text.
- **Non-predictable.** The hash value should not be predictable from the password.

Public-key Distribution

In cryptography it is a very tedious task to distribute the public and private key between sender and receiver. If key is known to the third party (forger/eavesdropper) then the whole security mechanism becomes worthless.
So, there comes the need to secure the exchange of keys.
Public key can be distributed in 4 ways: Public announcement, Publicly available directory, Public-key authority, and Public-key certificates. These are explained as following below.

1.Public Announcement:

Here the public key is broadcasted to everyone. Major weakness of this method is forgery. Anyone can create a key claiming to be someone else and broadcast it. Until forgery is discovered can masquerade as claimed user.



Public-key Distribution

2. Publicly Available Directory:
In this type, the public key is stored at a public directory. Directories are trusted here, with properties like Participant Registration, access and allow to modify values at any time, contains entries like {name, public-key}.Directories can be accessed electronically still vulnerable to forgery or tampering.

3. Public Key Authority:
It is similar to the directory but, improve security by tightening control over distribution of keys from directory. It requires users to know public key for the directory. Whenever the keys are needed, a real-time access to directory is made by the user to obtain any desired public key securely.

4. **Public Certification:**
This time authority provides a certificate (which binds identity to the public key) to allow key exchange without real-time access to the public authority each time. The certificate is accompanied with some other info such as period of validity, rights of use etc. All of this content is signed by the trusted Public-Key or Certificate Authority (CA) and it can be verified by anyone possessing the authority's public-key.

Data Encryption Standard (DES) CO4

DES Algorithm

This is the most common encryption. It mainly consists of two common inputs in the encryption function, which includes the key and the plain text.

The plain text must be a 64-bit combination in length where the key should be having a length of 56 bits.

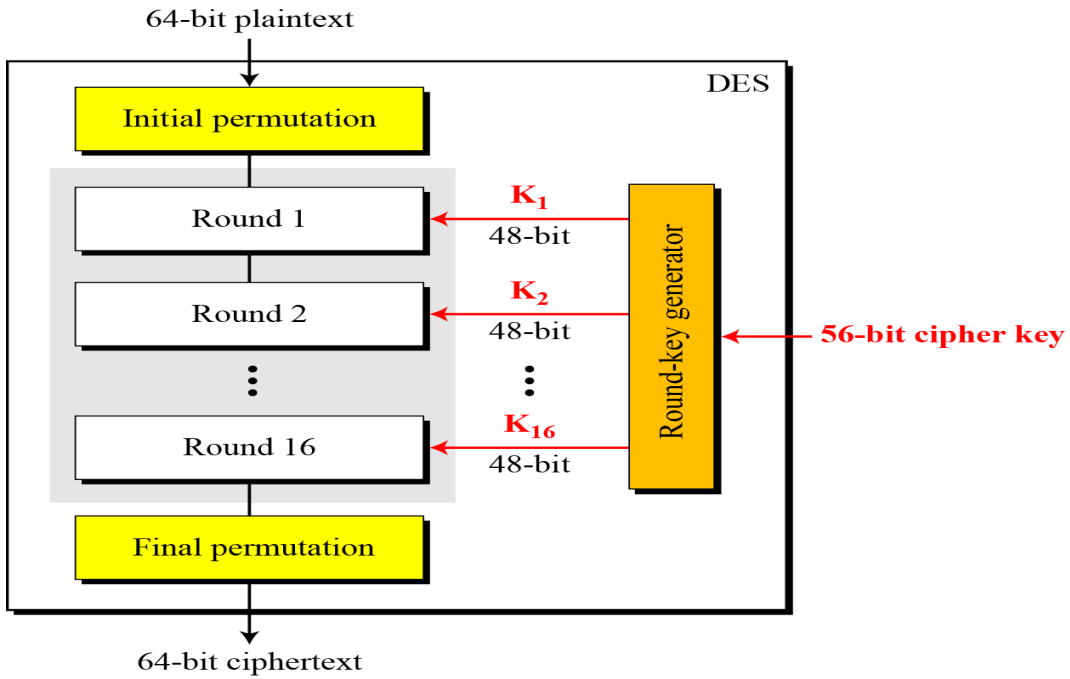
The 64 bits of plain text will first go through initial permutation which can then rearrange the bits. Second, a 16 round of a similar function is articulated.

This will include both permutation and substitution functionalities. This is then followed by a pre-output which is swapped at 32 bits position and passes through a final permutation so as to come up with an end set of 64-bit text cipher.

Data Encryption Standard (DES) CO4

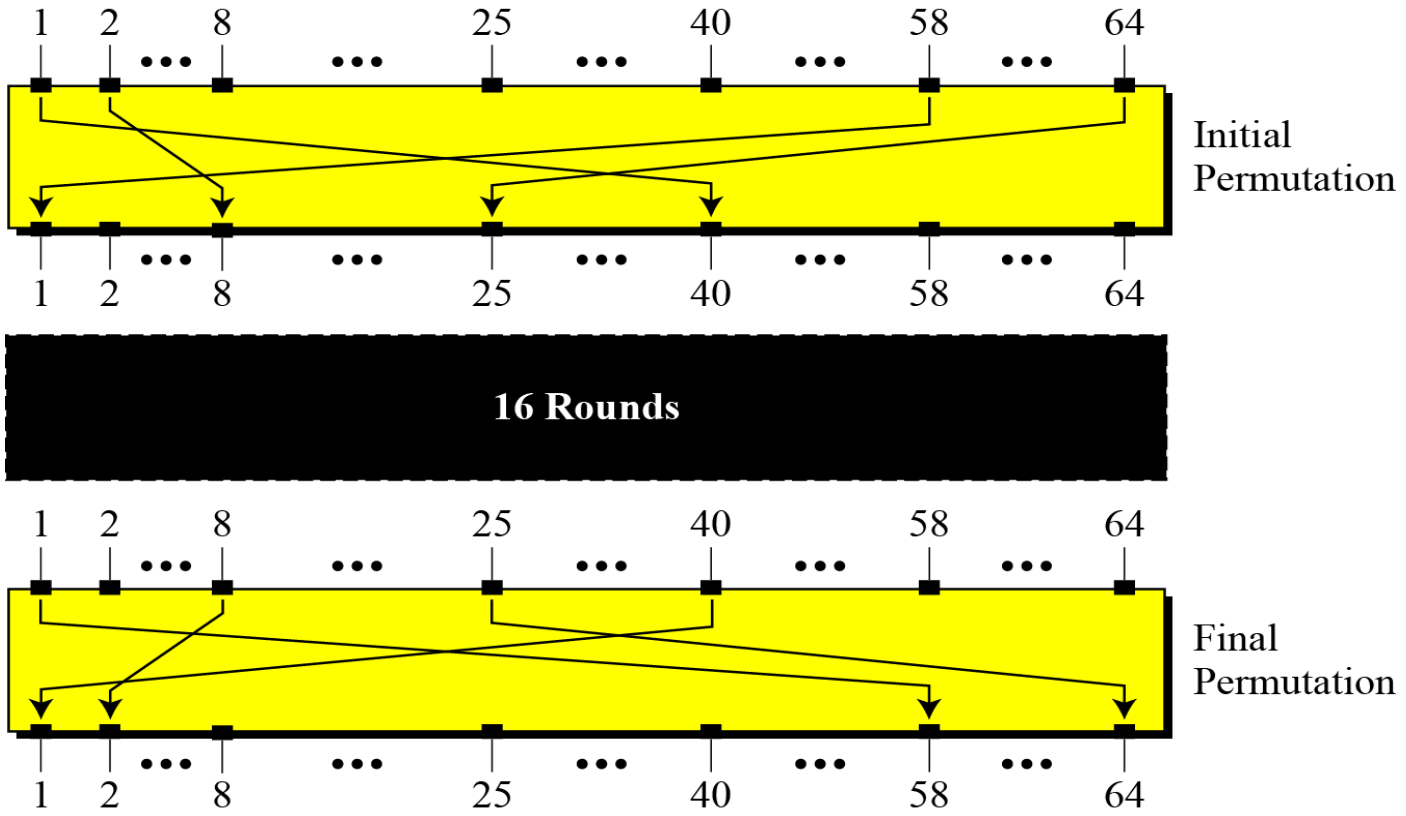
The encryption process is made of two permutations (P-boxes), which we call initial and final permutations, and sixteen Feistel rounds.

General structure of DES



Data Encryption Standard (DES)

Initial and final permutation steps in DES



Data Encryption Standard (DES)

Initial and final permutation tables

Initial Permutation	*Final Permutation*
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

Advanced Encryption Standard (AES)-CO4

This type of encryption was mainly chosen for use in the year 2001.

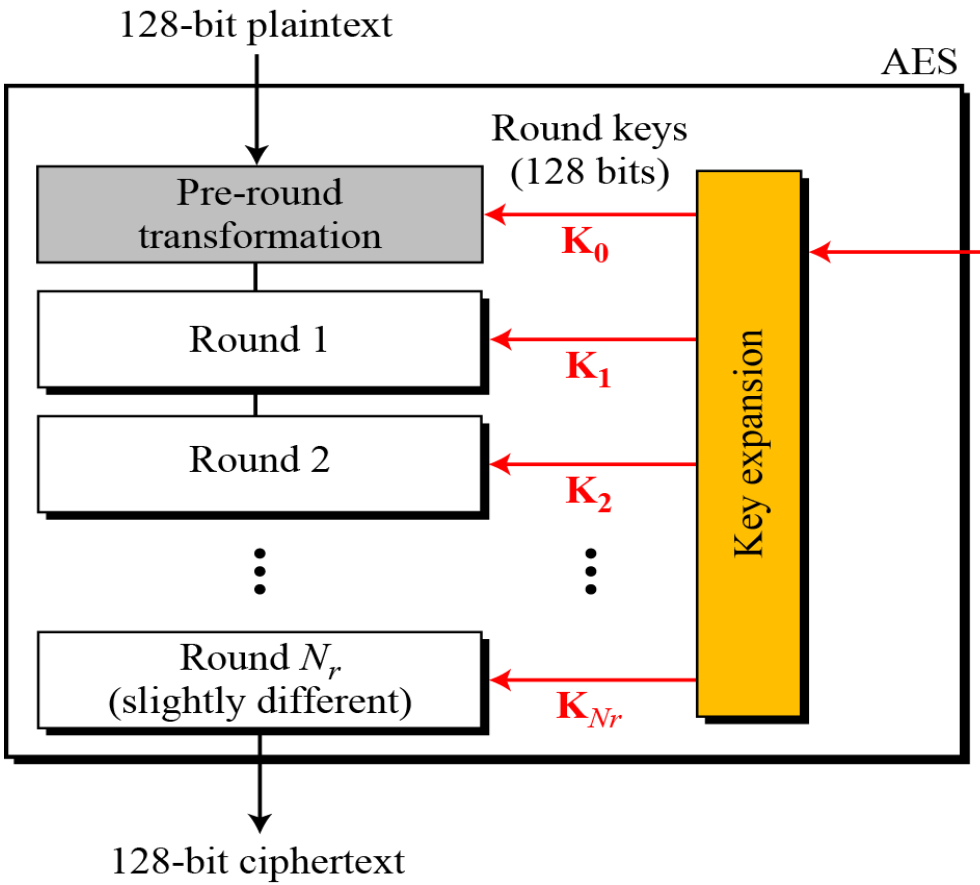
It is also regarded as an iterated block cipher, which consists of 10, 12, and 14 key size rounds with respective key sizes of 128, 192, and 256 bits.

This mode provides an optimal performance symmetric key encryption and decryption.

It is 6 times faster than triple DES.

AES encryption cipher

General design of AES encryption cipher



Cipher key
(128, 192, or 256 bits)

Nr	Key size
10	128
12	192
14	256

Relationship between number of rounds and cipher key size

SHA : Secure Hash Algorithms (CO4)

The Secure Hash Algorithm 1 (SHA-1) is a cryptographic computer security algorithm. It was created by the US National Security Agency in 1995, after the SHA-0 algorithm in 1993, and it is part of the Digital Signature Algorithm or the Digital Signature Standard (DSS).
SHA-1 produces a 160-bit hash value or message digests from the inputted data (data that requires encryption), which resembles the hash value of the MD5 algorithm.
It uses 80 rounds of cryptographic operations to encrypt and secure a data object.

Some of the protocols that use SHA-1 include:

- Transport Layer Security (TLS)
- Secure Sockets Layer (SSL)
- Pretty Good Privacy (PGP)

SHA : Secure Hash Algorithms

- Pretty Good Privacy (PGP)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Internet Protocol Security (IPSec)

SHA-1 is commonly used in cryptographic applications and environments where the need for data integrity is high. It is also used to index hash functions and identify data corruption and checksum errors.

Real world Protocols

- A cryptographic protocol (also known as encryption protocol or security protocol) is an abstract or an existing protocol that performs a security-related function and applies cryptographic methods.
- A protocol describes how the cryptographic algorithms should be used to secure information.
- Real world protocols are used have security while transmitting data from one end to another end. Some of them includes –

VPN, Email Security Certificates, Transport Layer Security (TLS), IP security (IPSec), DNS Security.

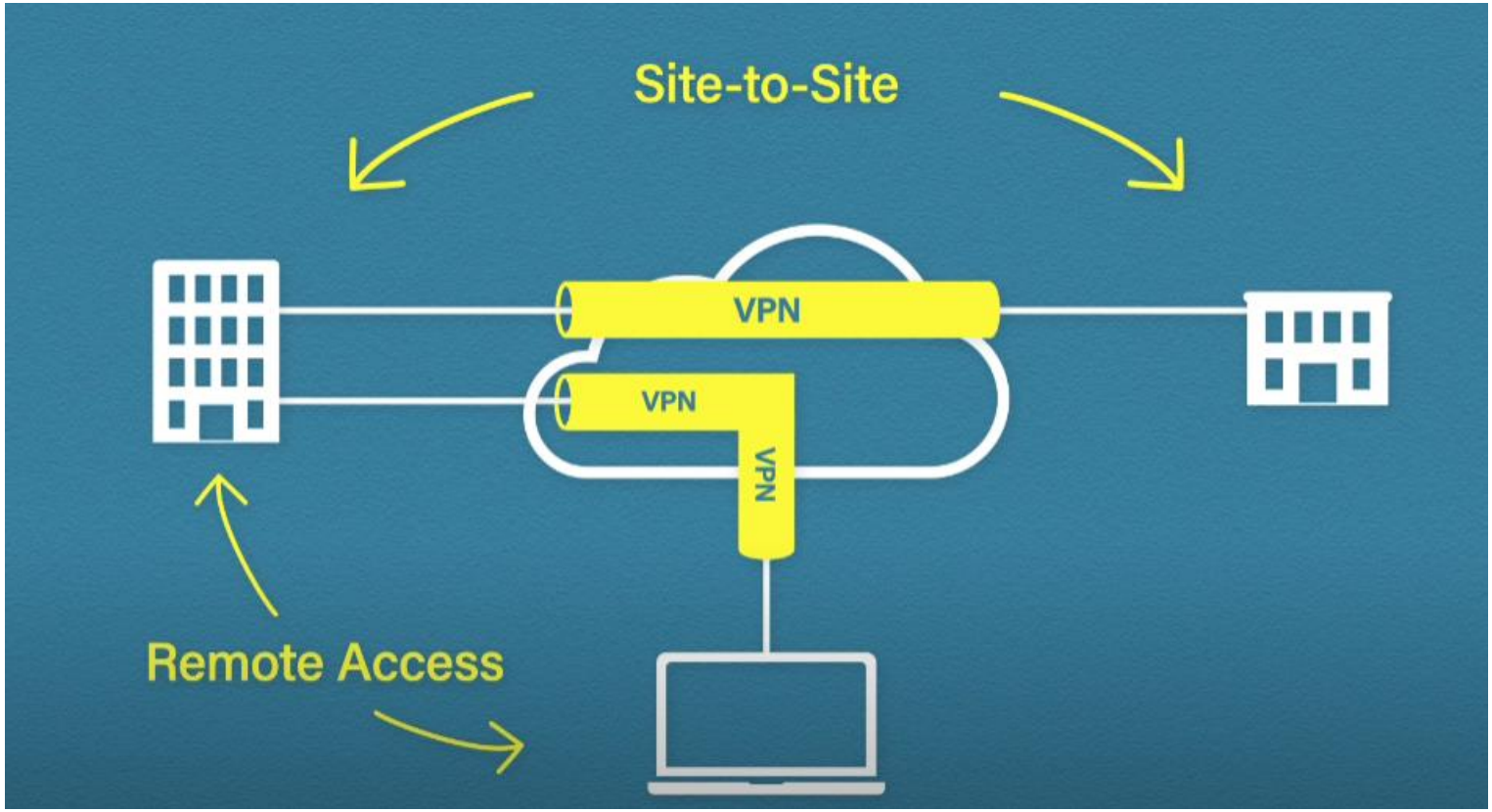
Virtual Private Network (VPN)

VPN is a private communication network, which is the most secure, remote method of connecting a computer to a private network with the help of a public network, such as the Internet.

It creates the virtual tunnel through which the data travels from one computer to the other over the network.

Due to this, an attacker gets the way to use the remote client to relay attacks through the VPN tunnel.

Site to Site and Remote-Access VPNs



E-mail Security Certificates (CO4)

E-mail security can be defined as the use of various techniques to secure sensitive information in email communication and accounts against unauthorized access, loss, or compromise.

For this there is a need of E-mail security certificates also known as S/MIME (Secure Multipurpose Internet Mail Extensions)

E-mail Security Certificates

- S/MIME (Secure Multipurpose Internet Mail Extensions) keeps your emails protected during transition.
- S/MIME uses cryptography to digitally sign and encrypt your email to prevent interception from any unauthorised person.
- Email certificates, also known as S/MIME certificates are digital certificates that can be used to sign and encrypt email messages.
- When you encrypt and email using an email certificate, only the person that you send it to can decrypt and read the email.
- The recipient can also be sure that the email hasn't been changed in any way.

E-mail Security Certificates

S/MIME includes two security features :

Email encryption : It encrypt the content of the email sent between two S/MIME enabled users to make it unreadable to anyone other than the intended recipient.

Digital signature : It digitally signed the email send between two S/MIME enabled users to eliminate any risk of spoofing.

Transport Layer Security (TLS) CO4

- Transport Layer Security (TLS) encrypts data sent over the Internet to ensure that eavesdroppers and hackers are unable to see what you transmit which is particularly useful for private and sensitive information such as passwords, credit card numbers, and personal correspondence.
- TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the Internet.
- It is mostly familiar to users through its use in secure web browsing, and in particular the padlock icon that appears in web browsers when a secure session is established.
- However, it can and indeed should also be used for other applications such as e-mail, file transfers, video/audioconferencing, instant messaging and voice-over-IP, as well as Internet services.

IP Security (CO4)

IPSec is a security protocol which is used to provide security at the network layer of the networking system.
IPSec authenticates and encrypts the data packets over an IP network.
IPSec is a security protocol which is used to provide security at the network layer of the networking system.
IPSec authenticates and encrypts the data packets over an IP network.

IP Security

Features of IPSec:

It guards the overall data packet produced at the IP layer inclusive of the higher layer headers.

IPSec works in between two different networks, therefore, adoption of security features is easier to implement without making any changes in the running applications.

Provisions host-based security as well.

The most frequent task of IPSec is to secure VPN network (a virtual private network) between two different network entities.

DNS Security

- The Domain Name System (DNS) is the protocol that makes the Internet usable by allowing the use of domain names. DNS is widely trusted by organizations, and DNS traffic is typically allowed to pass freely through network firewalls.
- As a result, the security of DNS is a critical component of network security.
- DNS is important because it links the domain name to the IP. Internet criminals can exploit these weaknesses and are capable of creating false DNS records. These fake records can trick users into visiting fake websites, downloading malicious software, or worse.

Faculty Video Links, Youtube & NPTEL Video Links and Online Courses Details

- https://www.youtube.com/watch?v=E47ew_IsqaM
- https://www.youtube.com/watch?v=gDtlbGK13xM
- https://www.youtube.com/watch?v=xFzaoJjzXJQ
- https://youtu.be/RQOJgEA5e1k
- https://youtu.be/GKqOWCK71K4
- https://youtu.be/zDDkNq6kpRE

Daily Quiz

1. In which of the following, a person is constantly followed/chased by another person or group of several peoples?

A. Phishing
B. Bulling
C. Stalking
D. Identity theft

2. Which one of the following can be considered as the class of computer threats?

A. Dos Attack
B. Phishing
C. Soliciting
D. Both A and C

Daily Quiz

3. The best way to minimize your digital footprint is to:

A. Take fewer photos with your smartphone.

B. B. Travel less with your smartphone.

C. C. Post less on social media

4. What is most valuable to companies looking to sell you something?

A. Your phone number.

B. B. Your email address.

C. C. Your physical address

Daily Quiz

5. What's the best way to secure a weak password like "monkey123"?

A. Add an uppercase numeral and a special character, such as $.

B. Don't reuse it anywhere else or share it with anyone.

C. Enable two-factor authentication

6. When using a VPN, what's the one thing that you cannot hide from ISPs, hackers, and the government?

A. The fact that you're using a VPN.

B. Your identity.

C. Your data.

Daily Quiz

7. Which of the following is considered as the unsolicited commercial email?

A. Virus
B. Malware
C. Spam
D. All of the above

8. Which one of the following is a type of antivirus program?

A. Quick heal
B. Mcafee
C. Kaspersky
D. All of the above

Daily Quiz

9. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_____:

A. Antivirus
B. Firewall
C. Cookies
D. Malware

10. Which of the following refers to exploring the appropriate, ethical behaviors related to the online environment and digital media platform?

A. Cyber low
B. Cyberethics
C. Cybersecurity
D. Cybersafety

Weekly Assignment

1. Differentiate DES and AES?
2. Describe SHA-1 Algorithm.
3. Write and explain the Digital Signature Algorithm.
4. Explain the Transport layer security.
5. Explain RSA algorithm with example.
6. Differentiate between Symmetric and Asymmetric key Cryptosystem.
7. Describe S/MIME protocol for emails.

Faculty links

1. https://www.youtube.com/watch?v=lECb8emmN0M&list=PL71FE85723FD414D7&index=26

- ***NPTEL Video link***

1. https://nptel.ac.in/courses/106105162

Glossary Questions

Fill the right options:

Secure Hash Algorithm, 2, 128, 64, Integrity

1. No of keys in public key cryptography _____
2. SHA stands for _____
3. Key sizes for AES and DES (respectively are)____ and ____
4. Digital certificate ensures_____ property of CIA triad.

MCQ s

1. A _____ is used to verify the integrity and authenticity of a message.

(a) Decryption algorithm

(b) Message digest

(c) MAC

(d) Both (b) and (c)

2. Which of the following is the latest version of the SHA algorithm?

(a) SHA-512

(b) SHA-256

(c) SHA-128

(d) SHA-1

MCQ s

3. The purpose of hash function is to ensure _____.

(a) Message integrity

(b) Message authentication

(c) Both (a) and (b)

(d) None of these

4. Choose the odd one out.

(a) RC5

(b) Blowfish

(c) ECC

(d) MAC

MCQ s

5. When two different messages yield the same message digest, it is called _____.

(a) Attack

(b) Collision

(c) Hash

(d) None of these

6. Which of these is a kind of attack possible on digital signatures?

(a) Ciphertext-only attack

(b) Known-message attack

(c) Key-only attack

(d) Both (b) and (c)

MCQ s

7. An attacker needs to perform _____ operations in order to determine collision in SHA-1.

(a) 2^{64}

(b) 2^{80}

(c) 2^{256}

(d) 2^{72}

8. Which of these is not a variation of a digital signature?

(a) Timestamped signature

(b) Blind signature

(c) Encrypted digital signature

(d) Undeniable digital signature

MCQ s

9. Which of these statements is not correct about DSS?

(a) It was published by the National Institute of Standards and Technology.

(b) It uses three functions to create a digital signature.

(c) An elaborated version of DSS was named as FIPS 186-2.

(d) It uses Secure Hash Algorithm (SHA).

10. Which of these is a kind of attack possible on digital signatures?

(a) Ciphertext-only attack

(b) Known-message attack

(c) Key-only attack

(d) Both (b) and (c)

MCQ s

11. Which of the following is a property of a digital signature?

(a) It must be able to verify the author.

(b) It must be able to verify the date and time of the signature.

(c) It must be able to authenticate the contents of the message at the time of the signature.

(d) All of these

12. RSA _____ be used for digital signatures.

(a) can

(b) cannot

(c) must

(d) must not

MCQ s

13. The sender encrypts the message with his or her private key to achieve _____.

(a) Authentication

(b) Confidentiality

(c) Both (a) and (b)

14. Which of the following pair of keys is used to create and verify the digital signature, respectively?

(a) Signer's private key and verifier's public key

(b) Verifier's public key and verifier's private key

(c) Signer's private key and signer's public key

(d) Signer's public key and signer's private key

MCQ s

15. Which of the following services is not provided by digital signatures directly?

(a) Message authenticity

(b) Message confidentiality

(c) Message integrity

(d) Nonrepudiation

16. Which of the following is /are offered by the Hash functions?

a. Authentication

b. Non repudiation

c. Data Integrity

d. All of the above

MCQ s

17. Which of the following is not possible through hash value?

a. Password Check

b. Data Integrity check

c. Digital Signatures

d. Data retrieval in its original form

18. Which of the following is not a property of Hash Function?

a) Pre-Image Resistance

b) Compression

c) Fixed Length Output

d) None of the above

MCQs

19. Which of the following is not a property of Hash Function?

a) Pre-Image Resistance

b) Compression

c) Fixed Length Output

d) None of the above

20. Which of the following names can we use for denoting the output of the hash function?

a) Hash value

b) Hash Code

c) Message Digest

d) All of the above

Past Sessional Papers

Printed page: 2 Subject Code:ANC0301

Roll No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute)

Affiliated to Dr. A.P. J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow

Course : B.Tech Branch : CSE.

Semester : III Sessional Examination : Second Year- (2021 - 2022)

Subject Name: Cyber Security

Time: 1.15Hours [SET- A] Max. Marks:30

General Instructions:

- This Question paper consists of .....pages & .....questions.It comprises of three Sections, A, B, and C
- **Section A** -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- **Section B** - Question No-3 is Short answer type questions carrying 5 marks each. Attempt any two out of three questions given.
- **Section C** -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. Attempt any one part a or b.

		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system b. Illusion detection system c. Intrusion detection system d. None	(1)	CO2
	d.	4. Full form of VIRUS? a. Various Information Resource Under Support b. Very Information Resource Under Support c. Vital Information Resource Under Seize d. none	(1)	CO2

Past Sessional Papers

2.	All questions are compulsory		[2×2=4]	
	a.	Differentiate virus and worms?	(2)	CO2
	b.	Define zero day attack?	(2)	CO2
		SECTION – B	[10Marks]	
3.	Answer any two of the following-		[2×5=10]	
	a.	What is a firewall? Mention all types of Firewalls.	(5)	CO2
	b.	What is spoofing ? What are its different types?	(5)	CO2
	c.	What is e-commerce. Name some e -commerce site. How is payment done while the transaction of goods here?	(5)	CO2
		SECTION – C	[12Marks]	
4	Answer any one of the following-		[1×6=6]	
	a.	What is a Trojan horse in Network security and how it got its name?	(6)	CO2
	b.	Explain intrusion detection system?	(6)	CO2
5.	Answer any one of the following-		[1×6=6]	
	a.	Differentiate between Debit card and Credit card?	(6)	CO2
	b.	Explain the advantages and disadvantages of E-cash?	(6)	CO2

Past Sessional Papers

Printed page: 2 Subject Code: ANC0301

Roll No:

NOIDA INSTITUTE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA
(An Autonomous Institute)

Affiliated to Dr. A.P. J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow

Course: B.Tech Branch: CSE

Semester: 3rd Sessional Examination: 2nd Sessional Year- (2021 – 2022)

Subject Name: Cyber Security

Time: 1.15Hours [SET- B] Max. Marks: 30

General Instructions:

- This Question paper consists of .....pages & .....questions.It comprises of three Sections, A, B, and C
- Section A -Question No- 1 is objective type questions carrying 1 mark each, Question No- 2 is very short answer type carrying 2 mark each. You are expected to answer them as directed.
- Section B - Question No-3 is Short answer type questions carrying 5 marks each. Attempt any two out of three questions given.
- Section C -Question No. 4 &5are Long answer type (within unit choice) questions carrying 6marks each. Attempt any one part a or b.

		SECTION – A	[08Marks]	
1.	All questions are compulsory		(4×1=4)	
	a.	1. How many layers are there in OSI model? a. 4 b. 7 c. 3 d. 8	(1)	CO2
	b.	2. Data security considerations are? a. Backups b. Archival storage c. Disposal of data d. All	(1)	CO2
	c.	3. Full form of IDS? a. Invention detection system b. Illusion detection system c. Intrusion detection system d. None	(1)	CO2
	d.	4. Full form of VIRUS? a. Various Information Resource Under Support b. Very Information Resource Under Support c. Vital Information Resource Under Seize d. none	(1)	CO2

Past Sessional Papers

2.	All questions are compulsory		(2×2=4)	
	a.	Define zero day attack.	(2)	CO2
	b.	Differentiate virus , worms, Trojan horse and logic bombs?	(2)	CO2
		SECTION – B	[10Marks]	
3.	Answer any two of the following-		(2×5=10)	
	a.	What is spoofing? Explain different types of spoofing?	(5)	CO2
	b.	Explain the working of IDS System with the help of the diagram.	(5)	CO2
	c.	Explain virtual private networks in detail?	(5)	CO2
		SECTION – C	[12Marks]	
4	Answer any one of the following-		(1×6=6)	
	a.	What is the data security consideration? Explain in this reference Data backup security, Data archival security and Data disposal consideration.	(6)	CO2
	b.	Discuss Electronic Payment System and its types. Explain the threats to E Commerce.	(6)	CO2
5.	Answer any one of the following-		(1×6=6)	
	a.	What is Firewall and explain the types of Firewall?	(6)	CO2
	b.	Differentiate between Debit card and Credit card?	(6)	CO2

Old Question Papers

Printed Pages:01 | Sub Code: RUC 501

Paper Id: 199503 | Roll No.

B TECH

(SEM V) THEORY EXAMINATION 2018-19

CYBER SECURITY

Time: 3 Hours | ***Total Marks: 70***

Note: **1.** Attempt all Sections. If require any missing data; then choose suitably.

SECTION A

1. **Attempt *all* questions in brief.** **2 x 7 = 14**

a. Write a short note on the Copyright Act?
b. What do you mean by physical Security for informationSystems?
c. Describe Intellectual Property Issues (IPR).
d. Write short notes on "Patent Law".
e. What do you mean by WWW policy?
f. Give small notes on Corporate Policy.
g. Differentiate between Cyber Security and Information Security.

SECTION B

2. **Attempt any *three* of the following:** **7 x 3 = 21**

a. What are the key differences between Symmetric and Asymmetric encryption?
b. Explain Information Security Governance in detail and process involved in the Risk Management?
c. Explain briefly about Application Development Security with guidelines.
d. Elaborate the term Access Control. What is include in authorization process for (File, Program, Data rights) and explain the all types of controls.
e. What do you understand by security structure (Architecture) and design?

Old Question Papers

SECTION C

3. **Attempt any *one* part of the following:** **7 x 1 = 7**

(a) What do you mean by Intellectual Property? Describe various means using which Intellectual Property may be protected to an extent.

(b) Explain Confidentiality, Integrity and Availability in terms of cyber security.

4. **Attempt any *one* part of the following:** **7 x 1 = 7**

(a) What are the approaches followed in developing Information System (IS)? Explain the difference between security and threats.

(b) What is the need of information Security also explain the term ISMS?

5. **Attempt any *one* part of the following:** **7 x 1 = 7**

(a) Explain the role of Security in Internet and Web Services.

(b) What is Intrusion Detection System? Explain with Block Diagram.

6. **Attempt any *one* part of the following:** **7 x 1 = 7**

(a) Explain in Detail about Secure Information System Development.

(b) Describe the working principle of CCTV.

7. **Attempt any *one* part of the following:** **7 x 1 = 7**

(a) What are the Data Security Considerations? Explain in this reference Data Backup Security.

(b) What is Public Key Cryptography? Define its Advantage and Disadvantage.

Old Question Papers

Printed Pages : 1 **Roll No.** | | | | | | | | | | | **AUC002**

COMMON TO ALL BRANCHES
THEORY EXAMINATION (SEM-IV) 2016-17
CYBER SECURITY

Time : 3 Hours *Max. Marks : 100*

Note : Be precise in your answer.

SECTION – A

1. Attempt all of the following questions: **10 x 2 = 20**

(a) What is CIA (Confidentiality, Integrity and Availability) trade?
(b) What are the threats to information system?
(c) What is System Development Life Cycle (SDLC)?
(d) Define the terms RTGS and NEFT.
(e) What do you mean by virus, worm and IP spoofing?
(f) How cyber security is different from computer security?
(g) State the difference between Risk Management and Risk Assessment.
(h) Explain briefly about disposal of data.
(i) Define IT asset and the security of IT Assets.
(j) What is the need of cyber laws in India?

Old Question Papers

SECTION – B

2. **Attempt any five parts of the following question:** **5 x 10 = 50**

(a) What are biometric? How can a biometric be used for access control? Discuss the criteria for selection of biometrics.

(b) What is Intrusion Detection System (IDS)? Explain its type in detail.

(c) What are the backup security measures? Discuss its type.

(d) What are the basic fundamental principles of information security? Explain.

(e) Write a short note on CCTV and its applications.

(f) What is Electronic cash? How does cash based transaction system differ from credit card based transactions?

(g) What do you mean by Virtual Private Networks? Discuss authentication mechanism used in VPN.

(h) **Write a short note on:**

(i) Database Security **(ii)** Email Security **(iii)** Internet Security

SECTION – C

Attempt any two of the following questions: **2 x 15 = 30**

3. What is Electronic Data Interchange (EDI)? What are the benefits of EDI? How can it be helpful in governance?

4. What is digital signature? What are the requirements of a digital signature system? List the security services provided by digital signature.

5. Explain the following in detail :

(i) Private Key cryptosystem and Public key cryptosystems.

(ii) Firewall.

Expected Questions for University Exam

1. Distinguish between known and unknown vulnerabilities. How are they managed?
2. Illustrate the techniques used in securing mail system against spam.
3. Explain importance of web security.
4. Why security policies should be developed?
5. Explain key aspects in maintaining cloud security.

Summary

- This PPT provides the important ideas of current world's security problems. As the world is moving towards a digital era, users are increasing utilizing the web services, email systems, mobile devices and the cloud services.
- The major topics covered are Development of Policies, WWW Policies, Email Security Policies, mobile security , cloud security.
- The users should also be aware of selecting and using cloud resources and services. Hence, a proper maintenance and utilization of security measures is essential in preventing users against various attacks.

References

1. Charles P. Pfleeger, Shari Lawerance Pfleeger, “Analysing Computer Security ”, Pearson Education India.
2. V.K. Pachghare, “Cryptography and information Security”, PHI Learning Private Limited, Delhi India.
3. Dr. Surya Prakash Tripathi, Ritendra Goyal, Praveen kumar Shukla ,”Introduction to Information Security and Cyber Law” Willey Dreamtech Press.(prefer)
4. https://img2.helpnetsecurity.com/dl/reviews/157870264X.pdf
5. https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
6. https://onlinecourses.swayam2.ac.in/cec20_cs09/unit?unit=96&lesson=112

Thank You