



Parameters	Cryptography	Cryptology
Definition	Cryptography is the process of conversion of plain text to cipher text.	Cryptology Is the process of conversion of plain text to cipher text and vice versa.
User Side	Cryptography takes place on the sender's side	It takes place on the sender and receiver side
Study Focus	It is also called the study of encryption and decryption.	Cryptography is also called the study of encryption
Message Exchange	In Cryptography, the sender sends the message to the receiver.	In Cryptology, both the sender and receiver send messages to each other.
Relationship	Cryptography can be seen as the subset of Cryptology.	Cryptology can be seen as the superset of Cryptography
Scope	Cryptography deals with the techniques of secure communication.	Cryptology deals with the study of secure communication.
Focus	Cryptography focuses on the practice of hiding information	Cryptology focuses on the theoretical and mathematical aspects of information security
	Components	Cryptography involves encryption, decryption, and

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



authentication techniques

Cryptology involves the study of codes, ciphers, and cryptanalysis is

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Parameters	Cryptography	Cryptology
Activities	Cryptography is concerned with developing algorithms and protocols	Cryptology is concerned with analyzing and breaking existing encryption methods
Applications	Cryptography is utilized in various fields such as finance, e-commerce, and national security	Cryptology is utilized in academia and research to understand and improve encryption

Quantitative Approaches	Qualitative Approaches
Results are based on objective measures	Results are based on subjective measures.
Cost and benefit issues are important	Monetary value of assets is not important.
Requires large amount of historical information like threat frequency, likelihood, etc.	Limited effort is required to develop monetary value, threat frequency
More complex process, mathematical tools are required	Relatively straight forward, mathematical tools are not needed
Mostly performed by technical and security staff	Can be performed by non-technical and non-security staff

Fy-Diploma (UR)

Sy-Diploma (UN)

Ty-Diploma (YUKH) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Substitution Cipher Technique

In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.

Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.

In substitution Cipher Technique, character's identity is changed while its position remains unchanged.

In substitution Cipher Technique, The letter with low frequency can detect plain text.

The example of substitution Cipher is Caesar Cipher, monoalphabetic cipher, and polyalphabetic cipher.

Involves replacing plaintext letters or groups of letters with ciphertext

Transposition Cipher Technique

In transposition Cipher Technique, plain text characters are rearranged with respect to the position.

Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.

While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.

While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.

The example of transposition Cipher is Rail Fence Cipher, columnar transposition cipher, and route cipher.

letters or groups of letters according to a specific algorithm or key.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)
Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/
Ty-Diploma (YU) [LIVE] (Sem 3 + sem 4) : only at 4999/-

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



The frequency distribution of the plaintext letters is typically obscured, but patterns can still be detected with statistical analysis.

Involves rearranging the order of the plaintext letters or groups of letters according to a specific algorithm or key.

The frequency distribution of the plaintext letters remains the same, but the order is scrambled, making it difficult to detect patterns with statistical analysis.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Substitution Cipher Technique	Transposition Cipher Technique
<p>Vulnerable to frequency analysis attacks, where the most commonly used letters or letter combinations in the language can be identified and used to deduce the key.</p> <p>Relatively easy to understand and implement, making it suitable for simple applications.</p>	<p>Less vulnerable to frequency analysis attacks, but still susceptible to attacks such as brute force and known plaintext attacks.</p> <p>Can be more difficult to implement and understand, but can be more secure than substitution ciphers for certain applications.</p>

Basis	Steganography	Cryptography
Definition	steganography means covered writing .	cryptography means secret writing .
popularity	Steganography is less popular than Cryptography.	While cryptography is more popular than Steganography.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Attack Name	The attack's name in Steganography is Steganalysis .	In cryptography, the Attack's name is cryptanalysis.
Data Alteration	In steganography, the structure of data is not usually altered.	While in cryptography, the structure of data is altered.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Basis	Steganography	Cryptography
Security Principles	Steganography supports Confidentiality and Authentication security principles.	Cryptography supports Confidentiality and Authentication security principles as well as Data integrity and Non-repudiation .
Visibility	In steganography, the fact that a secret communication is taking place is hidden.	While in cryptography only a secret message is hidden.
Mathematical Involvement	In steganography, not many mathematical transformations are involved.	Cryptography involves the use of number theory, mathematics, etc. to modify data
Information Handling	In Steganography the information is hidden.	In cryptography, the information is transformed.
	The hidden information is not visible.	Transformed information is visible.
	Steganography Provides Confidentiality only.	Cryptography Provides Confidentiality, Integrity, Non-repudiation.

Fy-Diploma (URJA) [LIVE] (S
Sy-Diploma (UN

Ty-Diploma (YUKTA) [LIVE] (S
All Courses : [CHECK NOW](#) [YouTube: SUBSCRIBE NOW](#) [INSTA : FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



V2V EdTech LLP | NIS (22620) | Codes

Information
on
Visibility

Security
Services

V2V

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Basis	Steganography	Cryptography
Goal	The goal of steganography is to make the information invisible to anyone who doesn't know where to look or what to look for	The main goal of cryptography is to keep the contents of the message secret from unauthorized access.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Encryption

It is a process of encoding message or information so that only authorized parties can have access to it.

It is considered as principal application of cryptography.

It simply uses algorithm to encrypt data and secret key to decrypt it.

It is all about mathematical and algorithmic in nature.

Cryptography

It is study of techniques such as encryption for secure communication in presence of third parties.

It is considered as art of creating codes using techniques of encryption and decryption.

It simply provides methods of protecting data through encryption and its related processes.

It is all about techniques and technologies in nature.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Encryption	Cryptography
<p>Its main purpose is confidentiality that means concealing content of message by translating it into code.</p>	<p>Its main purpose is to apply complex mathematics and logic to design strong encryption methods.</p>
<p>Types of encryption includes symmetric and asymmetric encryption.</p>	<p>Types of cryptography includes symmetric key cryptography and asymmetric key cryptography.</p>
<p>It provides security to data all times, maintains integrity, protects privacy, protects data across devices, etc.</p>	<p>It provides techniques like encryption techniques that can guard information and communication, cryptographic technique like MAC and digital signatures to protect information against spoofing and forgeries.</p>
<p>It follows same approach with some terms like ciphertext, plaintext, and cipher.</p>	<p>It has symmetric and asymmetric version with concept of shared and non-shared key.</p>
<p>It is useful to modern data security such as digital signatures and protect sensitive electronic data such as emails and passwords.</p>	<p>It is useful in electronic commerce, military communications, chip-based card payments, digital currencies, time stamping, etc.</p>

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Cyber Security

It is a process of keeping networks, devices, programs, data secret and safe from damage or unauthorized access.

It is all about managing cyber risks in all aspects such as people, process, technology, etc.

Its main objective is to prevent or mitigate harm or destruction of computer networks, applications, devices, and data.

It is generally used for the protection of internet-connected systems like software, hardware, and data, risk management,

Cryptography

It is a process of keeping information secret and safe simply by converting it into unintelligible information and vice-versa.

It is all about math functions and can be applied in technical solutions for increasing cybersecurity.

Its main objective is to keep plain text secret from eavesdroppers who are trying to have access to some information about the plain text.

disaster planning, access control, policies.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)
Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/
Ty-Diploma (YU

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



It is generally used for integrity, entity

authentication, data origin
authentication, non-repudiation, etc.

It protects the system against viruses, worms, unwanted programs, etc., protects the computer from being hacked,

It protects authentication and data across devices, maintains integrity, provides

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Cyber Security	Cryptography
reduces computer freezing and crashes, provides privacy to users, etc.	privacy to its best, allows two parties to communicate securely, etc.
It makes cryptography one of its subsets and uses it to design algorithms, ciphers, and security measures that usually codify and keep company and customer data protected.	It is an automated mathematical tool that is used to enhance and improve cybersecurity.
It generally involves the implementation of specific procedures to keep data safe.	It generally mitigates or reduces cyber-crime simply by using elaborate design to encrypt messages.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



	Worms	Viruses
Definition	A Worm is a form of malware that replicates itself and can spread to different computers via a Network.	A Virus is a malicious executable code attached to another executable file that can be harmless or can modify or delete data.
Objective	The main objective of worms is to eat the system's resources. It consumes system resources such as memory and bandwidth and makes the system slow in speed to such an extent that it stops responding.	The main objective of viruses is to modify the information.
Host	It doesn't need a host to replicate from one computer to another.	It requires a host is needed for spreading.
Harmful	It is less harmful as compared.	It is more harmful.
Detection and Protection	Worms can be detected and removed by the antivirus and firewall.	antivirus software is used for protection against viruses.

Fy-Diploma (URVA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



V2V EdTech LLP | NIS (22620) | Codes

**Controlled
by**

Worms can be controlled by remote.

Viruses can't be controlled by
remote.

V2V

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



	Worms	Viruses
Execution	Worms are executed via weaknesses in the system.	Viruses are executed via executable files.
Comes from	Worms generally come from the downloaded files or through a network connection.	Viruses generally come from shared or downloaded files.
Symptoms	<ol style="list-style-type: none">1. Hampering computer performance by slowing down it2. Automatic opening and running of programs3. Sending of emails without your knowledge	<ol style="list-style-type: none">1. Pop-up windows linking to malicious websites2. Hampering computer performance by slowing down it3. After booting, starting of unknown programs.
Types	Internet worms, Instant messaging worms, Email worms, File sharing worms, and Internet relay chat (IRC) worms are different types of worms.	Boot sector viruses, Direct Actionviruses, Polymorphicviruses, Macro viruses, Overwriteviruses, and File Infector viruses are different types of viruses
Examples	Examples of worms include Morris worm, storm worm, etc.	Examples of viruses include Creeper, Blaster, Slammer, etc.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)
Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY](#)
Ty-Diploma (YU
All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)
Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)
Contact No : 9326050669 / 9326881428



Interface

It does not need human action to replicate.

It needs human action to replicate.

Speed

Its spreading speed is faster.

Its spreading speed is slower as compared to worms.



Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Firewall

Firewall is implemented in both hardware and software.

Firewall deals with external threats only.

Antivirus

Antivirus is implemented in software only.

Antivirus deals with both external threats and internal threats.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Table 1.3.1 : Difference between worm and virus

Sr. No.	Virus	Worm
1.	A virus is a piece of code that attaches itself to legitimate program.	A worm is a malicious program that spread automatically. possible after removing the malware.
2.	Virus modifies the code.	Worm does not modify the code.
3.	Firewall works on monitoring and filtering.	Antivirus works on Scanning of infected files and software.
4.	Virus is a destructive in nature.	Worm is non destructive in nature.
5.	Aim of virus is to infect the code or program stored on computer system.	Aim of worm is to make computer or network unusable.
6.	Virus can infect other files.	Worm does not infect other files but it occupies memory space by replication.
7.	Virus may need a trigger for execution.	Worm does not need any trigger.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YU

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Firewall	Antivirus
Firewall checks the threat from incoming packets.	Antivirus checks the threat from malicious software.
Firewall saves the system from all kinds of threats to the system.	Antivirus saves the system only from viruses.
Firewall's programming is complex than antivirus.	Antivirus's programming is simpler as comparison to firewall.

S.No.	MALWARE	TROJAN HORSE
1.	Malware is a file or a code, designed to cause damage to a user's personal computer and network.	Trojan Horse is a form of malware that capture some important information about a computer system or a computer network.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



2. Malware is more harmful than trojan horse. Trojan horse is less harmful than Malware.
3. Malware can be detected and removed by the antivirus program. Trojan horses are detected by the antivirus software.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



4.	Malware can replicate itself and makes duplicate copy of it.	While, trojan horse can not self-replicate
5.	It can destroy data and resources, cause error and slow down the performance.	It also give unauthorized access and control of the sys to the hackers.
6.	Malware covers a lot of different malicious software.	Trojan Horse is one of the type of malware.
7.	Viruses, worms, Trojan viruses, spyware, adware, and ransomware are some of the common malware.	Back orifice, Rootkit and Beast Trojan are some of the common Trojan horses.

S.No. ROOTKIT

1. Rootkit is set of malicious program that enables administrator-level access to a computer network.

2. The main objective of rootkit is to steal the identity information, often to gain control of a system.

3. Detecting and removing a rootkit is a complex process and typically requires the use of specialized tools.

VIRUS

A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.

The main objective of virus is to modify the informati

Antivirus software are used for protection against viruses.

Fy-Diploma (UR) : only at 4999/- [BUY NOW](#)
Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)
Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



4. Rootkit is one of the type of malware. Virus is one of the type of malware.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



5.	It give unauthorized access and control of the system to the attacker.	It can control data and resources, cause error, destroy system and slow down the performance.
6.	It is more harmful.	It is less harmful as compared.
7.	TDSS, ZeroAccess, Alureon and Necurs are some of the common rootkit.	Resident and Non -resident viruses are two types of Virus.

S.No.	ROOTKIT	WORMS
1.	Rootkit is set of malicious program that enables administrator-level access to a computer network.	A Worm is a form of malware that replicates itself and can spread to different computers via Network.
2.	The main objective of rootkit is to steal the identity information, often to gain control of a system.	The main objective of worms to eat the system resources.
3.	Detecting and removing a rootkit is a complex process and typically requires the use of specialized tools.	Worms can be detected and removed by the Antivirus and firewall.
4.	Rootkit is one of the type of malware.	Worms is one of the type of malware.
5.	It is more harmful as compared.	It is less harmful as compared.

Fy-Diploma (UR)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more FREE STUDY MATERIAL

Contact No : 9326050669 / 9326881428



6. It give unauthorized access and control of the system to the attacker.

It can give unauthorized access and control of the system to the hackers.

7. TDSS, ZeroAccess, Alureon and Necurs are some of the common rootkit.

Morris Worm, Storm Worm and SQL Slammer are some of the examples of worms.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Worms

A Worm is a form of malware that replicates itself and can spread to different computers via Network.

The main objective of worms to eat the system resources.

Worms can be detected and removed by the Antivirus and firewall.

Worms are self replicating.

It doesn't need a host to replicate from one computer to another.

It can give unauthorized access and control of the system to the hackers.

It is less harmful as compared.

Morris Worm, Storm Worm and SQL Slammer are some of the examples of worms.

Trojan Horse

Trojan Horse is a form of malware that capture some important information about a computer system or a computer network.

The main objective of the trojan horse is to control the activity of the system.

Trojan horses are detected by the antivirus software.

Trojan horse are not self replicating.

It require host is needed for spreading.

It also give unauthorized access and control of the system to the hackers.

It is more harmful as compared.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UN)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Back orifice, Rootkit

and Beast Trojan are some of the common Trojan horses.

Worms are executed via weaknesses in system.

Trojan horse executes through a program and interprets as utility software.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



S.No.	VIRUS	SPYWARE
1.	A Virus is a malicious executable code attached to another executable file which can be harmless or can modify or delete data.	Spyware is a form of malware designed to collect your personal information.
2.	The main objective of virus is to modify the information.	The main objective of the spyware is to monitor the activity of the system.
3.	Antivirus software are used for protection against viruses.	Spyware can be detected and removed by the anti-spyware program.
4.	It can control data and resources, cause error, destroy system and slow down the performance.	It provides profit to the third party by collecting data of user without his awareness.
5.	It is more harmful.	It is less harmful as compared.
6.	Virus replicates itself.	Spyware does not replicate itself.
7.	Resident and Non-resident viruses are two types of Virus.	Bonzibuddy, Cydore and Downloadware some examples of spyware.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Authentication

In the authentication process, the identity of users are checked for providing the access to the system.

In the authentication process, users or persons are verified.

It is done before the authorization process.

It needs usually the user's login details.

Authentication determines whether the person is user or not.

Generally, transmit information through an ID Token.

The OpenID Connect (OIDC) protocol is an authentication protocol that is generally in charge of user authentication process.

Authorization

While in authorization process, a the person's or user's authorities are checked for accessing the resources.

While in this process, users or persons are validated.

While this process is done after the authentication process.

While it needs the user's privilege or security levels.

While it determines **What permission does the user have?**

Generally, transmit information through an Access Token.

The OAuth 2.0 protocol governs the overall system of user authorization process.



Popular Authentication Techniques-

- Password-Based Authentication
- Passwordless Authentication
- 2FA/MFA (Two-Factor Authentication / Multi-Factor Authentication)

Popular Authorization Techniques-

- Role-Based Access Controls (RBAC)
- JSON web token (JWT) authorization
- SAML Authorization
- OpenID Authorization

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Authentication	Authorization
<ul style="list-style-type: none">• Single-Sign-On(SSO)• Social authentication	<ul style="list-style-type: none">• OAuth 2.0 Authorization
<p>The authentication credentials can be changed in part as and when required by the user.</p>	<p>The authorization permissions cannot be changed by user as these are granted by the owner of the system and only he/she has the access to change it.</p>
<p>The user authentication is visible at user end.</p>	<p>The user authorization is not visible at the user end.</p>
<p>The user authentication is identified with username, password, face recognition, retina scan, fingerprints, etc.</p>	<p>The user authorization is carried out through the access rights to resources by using roles that have been pre-defined.</p>
<p>Example: Employees in a company are required to authenticate through the network before accessing their company email.</p>	<p>Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access.</p>

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



DOS

DOS Stands for Denial of service attack.

In Dos attack single system targets the victim system.

DDOS

DDOS Stands for Distributed Denial of service attack.

In DDoS multiple systems attacks the victims system..

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



DOS	DDOS
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack, The volumeBots are used to attack at the same time.
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Symmetric Key Encryption

It only requires a single key for both encryption and decryption.

Asymmetric Key Encryption

It requires two keys, a public key and a private key, one to encrypt and the other to decrypt.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Symmetric Key Encryption

The size of ciphertext is the same or smaller than the original plaintext.

The encryption process is very fast.

It is used when a large amount of data needs to be transferred.

It only provides confidentiality.

The length of key used is 128 or 256 bits

In symmetric key encryption, resource utilization is low compared to asymmetric key encryption.

It is efficient as it is used for handling large amount of data.

Security is lower as only one key is used for both encryption and decryption purposes.

Asymmetric Key Encryption

The size of ciphertext is the same or larger than the original plaintext.

The encryption process is slow.

It is used to transfer small amount of data.

It provides confidentiality, authenticity, and non-repudiation.

The length of key used is 2048 or higher

In asymmetric key encryption, resource utilization is high.

It is comparatively less efficient as it can handle a small amount of data.

Security is higher as two keys are used, one for encryption and the other for decryption.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



The Mathematical Representation is as follows-

$$P = D(K, E(K, P))$$

where $K \rightarrow$ encryption and decryption key
 $P \rightarrow$ plain text

The Mathematical Representation is as follows-

$$P = D(K_d, E(K_e, P))$$

where $K_e \rightarrow$ encryption key

$K_d \rightarrow$ decryption key

$D \rightarrow$ Decryption

Symmetric Key Encryption

$D \rightarrow$ Decryption

$E(K, P) \rightarrow$ Encryption of plain text using K

Examples: 3DES, AES, DES and RC4

Asymmetric Key Encryption

$E(K_e, P) \rightarrow$ Encryption of plain text using encryption key K_e . $P \rightarrow$ plain text

Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



S.No	AES	DES
1.	AES stands for Advanced Encryption Standard	DES stands for Data Encryption Standard
2.	The date of creation is 2001.	The date of creation is 1977.
3.	Byte-Oriented.	Bit-Oriented.
4.	Key length can be 128-bits, 192-bits, and 256-bits.	The key length is 56 bits in DES.
5.	Number of rounds depends on key length: 10(128-bits), 12(192-bits), or 14(256-bits)	DES involves 16 rounds of identical operations
6.	The structure is based on a substitution-permutation network.	The structure is based on a Fiestel network.
7.	The design rationale for AES is open.	The design rationale for DES is closed.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



S.No	AES	DES
8.	The selection process for this is secret but accepted for open public comment.	The selection process for this is secret.
9.	AES is more secure than the DES cipher and is the de facto world standard.	DES can be broken easily as it has known vulnerabilities. 3DES(Triple DES) is a variation of DES which is secure than the usual DES.
10.	The rounds in AES are: Byte Substitution, Shift Row, Mix Column and Key Addition	The rounds in DES are: Expansion, XOR operation with round key, Substitution and Permutation
11.	AES can encrypt 128 bits of plaintext.	DES can encrypt 64 bits of plaintext.
12.	It can generate Ciphertext of 128, 192, 256 bits.	It generates Ciphertext of 64 bits.
13.	AES cipher is derived from an aside-channel square cipher.	DES cipher is derived from Lucifer cipher.
14.	AES was designed by Vincent Rijmen and Joan Daemen.	DES was designed by IBM.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)
Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)
Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)
All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [CHECK NOW](#)
Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)
Contact No : 9326050669 / 9326881428



No known cryptanalytical attacks against AES
but side channel attacks against AES
implementations possible. Biclique attacks
have better complexity than brute force but
still ineffective.

15.

Known attacks against DES include
Brute-force, Linear crypt-analysis,
and Differential crypt-analysis.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



16.	It is faster than DES.	It is slower than AES.
S.No	AES	DES
17.	It is flexible.	It is not flexible.
18.	It is efficient with both hardware and software.	It is efficient only with hardware.

Categories	Plaintext	Cleartext
Definition	The unencrypted data is used as an input for the encryption process or as the output for the decryption process.	The data is unencrypted and is not intended for the encryption process.
Applications	A browser, word processor, or email	Windows stores passwords in cleartext such as autologin username and password.
Advantages	As they are so easy to work with, they can all be stored in the same folder.	Used by various higher authorities so that others can not interfere in their private affairs.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Disadvantages	No standard way to specify the data format.	It is too complicated for a human to understand.
----------------------	---	--

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Factors	DAC	MAC	RBAC	ABAC
Access Control to Information	Through owner of data	Through fixed rules	Through roles	Through attributes
Access Control Based on	Discretion of owner of data	Classification of users and data	Classification of roles	Evaluation of attributes
Flexibility for Accessing Information	High	Low	High	Very high
Access Revocation Complexity	Very complex	Very easy	Very easy	Very easy
Support for Multilevel Database System	No	Yes	Yes	Yes
Used in	Initial Unix system	The U.S. department of defense	ATLAS experiment in CERN	The Federal government

Categories

Definition

HIDS

NIDS

Type

Host IDS

Network IDS

It doesn't work in real-time

Operates in real-time

Concern

Fy-Diploma (URJA) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



HIDS is related to just a **single** system, as the name suggests it is only concerned with the threats related to the Host system/computer,

NIDS is concerned with the entire **network system**; NIDS examines the activities and traffic of all the systems in the network.

Installation Point

HIDS can be installed on **each** and **every** computer or server i.e., anything that can serve as a host.

NIDS being concerned with the **network** is installed at places like **routers** or **servers** as these are the

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Categories	HIDS	NIDS
		main intersection points in the network system
Execution Process	HIDS operates by taking the snapshot of the current status of the system and comparing it against some already stored malicious tagged snapshots stored in the database, this clearly shows that there is a delay in its operation and activities	NIDS works in real-time by closely examining the data flow and immediately reporting anything unusual.
Information About Attack	HIDS are more informed about the attacks as they are associated with system files and processes.	As the network is very large making it hard to keep track of the integrating functionalities, they are less informed of the attacks



Ease of
Installation

As it needs to be installed on **every host**, the installation process can be **tiresome**.

Few installation points make it **easier** to install NIDS



Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) _ YOUTUBE : [SUBSCRIBE NOW](#) _ INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Categories	HIDS	NIDS
Response Time	Response time is slow	Fast response time

Table 1.3.2 : Comparison between Intruders and Insiders

Sr. No.	Intruders	Insiders
1.	Intruders are authorized or unauthorized users who are trying access the system or network.	Insiders are authorized users who try to access system or network for which he is unauthorized.
2.	Intruders are hackers or crackers.	Insiders are not hackers.
3.	Intruders are illegal users.	Insiders are legal users.
4.	Intruders are less dangerous than Insiders.	Insiders are more dangerous than Intruders.
5.	Intruders have to study/gain knowledge about the security system.	Insiders have knowledge about the security system.
6.	Intruders do not have access to system.	Insiders have easy access to the system because they are authorized users.
7.	Many security mechanisms are used to protect system from Intruders.	There is no such mechanism to protect system from Insider.

Substitution Cipher Technique

Transposition Cipher Technique

Fy-Diploma (UR...)
Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4
Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 499
All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#)
Download V2V

Contact No : 9326050669 / 9326881428



In substitution Cipher Technique, plain text characters are replaced with other characters, numbers and symbols.

Substitution Cipher's forms are: Mono alphabetic substitution cipher and poly alphabetic substitution cipher.

In transposition Cipher Technique, plain text characters are rearranged with respect to the position.

Transposition Cipher's forms are: Key-less transposition cipher and keyed transposition cipher.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Substitution Cipher Technique

In substitution Cipher Technique, character's identity is changed while its position remains unchanged.

In substitution Cipher Technique, The letter with low frequency can detect plain text.

The example of substitution Cipher is Caesar Cipher, monoalphabetic cipher, and polyalphabetic cipher.

Involves replacing plaintext letters or groups of letters with ciphertext letters or groups of letters according to a specific algorithm or key.

The frequency distribution of the plaintext letters is typically obscured, but patterns can still be detected with statistical analysis.

Vulnerable to frequency analysis attacks, where the most commonly used letters or letter combinations in the language can be identified and

Transposition Cipher Technique

While in transposition Cipher Technique, The position of the character is changed but character's identity is not changed.

While in transposition Cipher Technique, The Keys which are nearer to correct key can disclose plain text.

The example of transposition Cipher is Rail Fence Cipher, columnar transposition cipher, and route cipher.

Involves rearranging the order of the plaintext letters or groups of letters according to a specific algorithm or key.

The frequency distribution of the plaintext letters remains the same, but the order is scrambled, making it difficult to detect patterns with statistical analysis.

used to deduce the key.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)
Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4
Ty-Diploma (YU) [LIVE] (Sem 5 + sem 6) : only at 4999/-

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Less vulnerable to frequency

Relatively easy to understand and implement, making it suitable for simple applications.

analysis attacks, but still susceptible to attacks such as brute force and known plaintext attacks.

Can be more difficult to implement and understand, but can be more secure than substitution ciphers for certain applications.

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Substitution Cipher Technique	Transposition Cipher Technique	
Attribute	Firewall	Ids
Function	Monitors and controls incoming and outgoing network traffic based on predetermined security rules	Monitors network traffic for suspicious activity or patterns that may indicate a security threat
Deployment	Can be deployed as a hardware appliance, software application, or cloud-based service	Can be deployed as a hardware appliance, software application, or cloud-based service
Focus	Primarily focuses on blocking unauthorized access to a network	Primarily focuses on detecting and responding to security incidents
Alerts	May generate alerts based on predefined rules for network traffic	Generates alerts based on anomalous behavior or known attack signatures
Response	Can block or allow network traffic based on predefined rules	Can alert administrators to take action in response to detected threats

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Cryptographic Mode	Nature	Error Propagation	Initialization Vector	Offering	Key Application in Real Life
ECB	Block	No	No	Confidentiality	Basic encryption for small data sets, often found in database cells
CBC	Block	Yes	Yes	Confidentiality	Widely used for data encryption in protocols like TLS
CFB	Stream	Yes	Yes	Confidentiality	Stream cipher, often used in protocols like OpenPGP
OFB	Stream	No	Yes	Confidentiality	Stream cipher, used in VPNs and disk encryption

	DES	AES
Cryptographic Strength	Low	High
Key Size	56-Bit	128,192 and 256 bit
Block Size	64- Bit	128-Bit
Rounds	16	10,12,14-based on key size

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Usage	Obsolete -Not used	Currently used industry standard
--------------	---------------------------	----------------------------------

Feature	Digital Signature	Digital Certificate
Basics / Definition	A digital signature secures the integrity of a digital document in a similar way as a fingerprint or attachment.	Digital certificate is a file that ensures holder's identity and provides security.
Process / Steps	Hashed value of original data is encrypted using sender's private key to generate the digital signature.	It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.
Security Services	Authenticity of Sender, integrity of the document and non-repudiation.	It provides security and authenticity of certificate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format

Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428



Sr. No.	Symmetric Key Cryptography	Asymmetric Key Cryptography
1.	Single key is used for encryption and decryption.	Two separate keys are used for encryption and decryption.
2.	Also known as Single Key cryptography.	Known as Public and Private Key encryption.
3.	Key should be agreed by both- sender and receiver.	No need to agree on keys.
4.	Less Security.	More Security.
5.	Simple to implement.	Hard to implement as compare to symmetric key cryptography.
6.	For example - Data Encryption Standard (DES).	For example - Digital Signature.



Fy-Diploma (URJA) [LIVE] (Sem 2) only at 4999/- [BUY NOW](#)

Sy-Diploma (UMANG) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

Ty-Diploma (YUKTI) [LIVE] (Sem 3 + sem 4) : only at 4999/- [BUY NOW](#)

All Courses : [CHECK NOW](#) YOUTUBE : [SUBSCRIBE NOW](#) INSTA : [FOLLOW NOW](#)

Download V2V APP on Playstore for more [FREE STUDY MATERIAL](#)

Contact No : 9326050669 / 9326881428