IT INFRASTRUCTURE MANAGEMENT
WEEK 8 ASSIGNMENT

1. List the classification of various Trojan horses.

1. Remote access Trojans
2. Data sending Trojans
3. Destructive Trojans
4. Proxy Trojans
5. FTP Trojans
6. Security software disabler Trojans
7. Denial-of-Service (DoS) attack Trojans

2. List the categories of cryptographic algorithms and explain them.Some of the algorithms are discussed here:

Secret Key Cryptography (SKC)
Public Key Cryptography (PKC)
Hash Functions (HF)
Digital Signature

Secret Key Cryptography

A single key is used in SKC for both encryption and decryption of data.
In this form of cryptography, the key must be known to both the sender and the receiver.
If the key is compromised, the security offered by secret key cryptography is violated.
SKC assumes that the two communicating parties rely upon each other and are not to disclose the key and to protect it against modification.
SKC is categorized as stream ciphers and block ciphers.
Stream ciphers operate on a single bit at a time with different key.
On the other hand; a block cipher encrypts the data block wise.
It encrypts one block at a time, using the same key.
In general, a block cipher always generates the same cipher text when using the same key with the same plain text, whereas in a stream cipher, the same plain text encrypts to different cipher text when using the different keys.
The below figure shows that the sender uses the key to encrypt the plain text and sends the cipher text to the receiver.
In order to decrypt the message, the receiver also applies the same key.
As this scheme uses a single key for both encryption and decryption, secret key cryptography is also called symmetric cryptography.
A significant disadvantage of symmetric cryptography is the key management necessary to use them securely.

Public Key Cryptography

This concept has been introduced to solve the problem found in secret key cryptography.
Each person in this technique gets two keys known as the public and the private key.
Each person's public key is publicly known and the private key is kept secret.

Hence, the need for the both parties involved in communication to share secret information is eliminated.
All communication takes place only with the public key and no communication uses the private key.

Hash Function

It is also called message digests and it is a one-way encryption algorithm that does not use any key to encrypt or decrypt the message.
This technique generates a fixed length hash value based upon the plain text.
The hash function makes it impossible to recover the contents of the plain text.
It uses a digital fingerprint of a file's contents, in order to ensure that the file has not been changed by an intruder or any type of virus.

Digital Signature

A digital signature is a type of asymmetric cryptography.
It enables the receiver to believe that the one who has sent the message is the claimed person.
In many respects, it is equivalent to traditional handwritten signature.
But a digital signature is more difficult to forge than a handwritten signature since a digital signature is created and verified by cryptography, a branch of applied mathematics.
It transforms the messages into cipher text and back to plain text.
Digital signature uses the public key cryptography technique.

3. Highlight the importance of cryptography.

When the data is transmitted over the network, it passes a number of intermediate servers before it reaches the destination.
This data is stored on servers for months and at any stage, it is vulnerable to interception.
Therefore, the best way is the use of cryptography technique.
In simple terms, cryptography is the process of altering the original messages to hide their meaning from opponents who might intercept them.
Cryptography can be referred to as encryption which is the process of converting plain text into cipher text.
The reverse is decryption that converts cipher text to plain text.
Cryptography relies upon two basic components: an algorithm and a key.
Algorithms are complex mathematical structures and keys are strings of bits.
In order to communicate over the internet, two parties must use the same algorithm and key.
Communications through the internet, for example e-Commerce or e-mail may not be secure, if there is no encryption.
Hackers may be able to read messages or even modify the messages, if cryptography technique is not used.

4. Compare any Four antivirus software and list all the features and functionalities supported by them.

Bitdefender
Bitdefender is a Romanian cybersecurity company which provides different antivirus packages for private users and businesses. It provides cross-platform products such as Small Office Security ($99.98), Premium Security ($149.99) or Total Security ($99.99) promising high quality in terms of

security, features, and ease-of-use. Prices vary depending on the number of devices you need to secure, but they are generally fairly high. The software is easy to use and includes a dashboard that's nicely laid out which makes using it on touch-based devices much easier. The features that make Bitdefender stand out include:

- Real-time scanner delivers an always-on security shield and offers strong performance thanks to the integrated cloud scanner without burdening system performance
- Automatic updates: programs are updated hourly and achieve a higher hit rate to detect different types of malware
- Safepay offers special security for financial transactions
- Spam protection filters irrelevant messages in email inbox
- Weak point scanner shows weaknesses in a computer system

Norton by NortonLifeLock

Norton is an antivirus program series by US software developer NortonLifeLock (previously Symantec). The company acquired Peter Norton Computing in 1990 and kept the Norton product name ever since. Norton Security products are of a high-quality standard and provide customers with a wide range of security features for multiple device types. The products aren't free, but they offer great performance, user-friendly interfaces and direct support at a low cost. The most important features of the Norton Security antivirus software are:

- Real-time protection against all types of malware attacks
- Intelligent firewall for Windows and Mac
- Exclusive Norton expert support and virus protection guarantee (money return guarantee in case of irremovable virus attack)
- Password manager

Avira

Avira is a well-known German software company that offers various antivirus software products for private users and companies. It provides both free and fee-based products for PC, Mac, Android, and iOS. Avira Pro, Avira Internet Security, and Avira Prime are good options for private users. Avira also offers packages for businesses such as the Avira Antivirus for Endpoint and Avira Antivirus for small business editions. All packages provide good protection and excellent support at a fair price. The company's Free Security Suite has been ranked among the best free antivirus programs for years. It includes the most important essential protection features.

The key features Avira packages offer include:

- Automatic software and driver updates (not in Pro version)
- Real-time protection and repair function
- Security for online transactions and credit card payments
- Intelligent ad blocker

Kaspersky

With establishments in over 30 countries worldwide, a team of more than 4,000 highly qualified specialists and expertise in security software since 1997, Russian software company Kaspersky Lab has a lot of experience in producing high-quality software security solutions for private users and businesses. The company's product portfolio ranges from classic antivirus software for the family desktop to complex enterprise protection for businesses with more than 1,000 employees. Some of its editions such as Security Cloud Personal and Internet Security also incorporate cross-platform support, whilst others have been adapted to suit operating systems including Windows, macOS, Android or iOS.

Among the most important features of Kaspersky products are:

- Browser encryption for secure online shopping and banking (Windows or macOS)
- Webcam and VPN security in case of insecure WLAN (not included in Anti Virus version)
- Phishing protection

- Password manager (not included in all editions)
- Special protection for servers and workstations (Business edition)