Cryptography and Network Security:-

- ### What is a virus in cryptography?

  A computer **virus** is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The **virus** requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.

- ### Type of viruses:-

  1. **File infectors-** Some file infector viruses attach themselves to program files, usually selected .com or .exe files. Some can infect any program for which execution is requested, including .sys, .ovl, .prg, and .mnu files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly contained programs or scripts sent as an attachment to an email note.

  2. **Macro viruses-**These viruses specifically target macro language commands in applications like Microsoft Word and other programs. In Word, macros are saved sequences for commands or keystrokes that are embedded in the documents. Macro viruses can add their malicious code to the legitimate macro sequences in a Word file. Microsoft disabled macros by default in more recent versions of Word; as a result, hackers have used social engineering schemes to convince targeted users to enable macros and launch the virus. As macro viruses have seen a resurgence in recent years, Microsoft added a new feature in Office 2016 that allows security managers to selectively enable macro use for trusted workflows only, as well as block macros across an organization.

  3. **Overwrite viruses-**Some viruses are designed specifically to destroy a file or application's data. After infecting a system, an overwrite virus begins overwriting files with its own code. These

viruses can target specific files or applications or systematically overwrite all files on an infected device. An overwrite virus can install new code in files and applications that programs them to spread the virus to additional files, applications and systems.

4. **Polymorphic viruses-**A polymorphic virus is a type of malware that has the ability to change or mutate its underlying code without changing its basic functions or features. This process helps a virus evade detection from many antimalware and threat detection products that rely on identifying signatures of malware; once a polymorphic virus' signature is identified by a security product, the virus can then alter itself so that it will no longer be detected using that signature.

5. **Resident viruses-** This type of virus embeds itself in the memory of a system. The original virus program isn't needed to infect new files or applications; even if the original virus is deleted, the version stored in memory can be activated when the operating system loads a specific application or function. Resident viruses are problematic because they can evade antivirus and antimalware software by hiding in the system's RAM.

6. **Rootkit viruses-**A rootkit virus is a type of malware that installs an unauthorized rootkit on an infected system, giving attackers full control of the system with the ability to fundamentally modify or disable functions and programs. Rootkit viruses were designed to bypass antivirus software, which typically scanned only applications and files. More recent versions of major antivirus and antimalware programs include rootkit scanning to identify and mitigate these types of viruses.

7. **System or boot-record infectors-** These viruses infect executable code found in certain system areas on a disk. They attach to the DOS bootsector on diskettes and USB thumb

drives or the Master Boot Record on hard disks. In a typical attack scenario, the victim receives storage device that contains a boot disk virus. When the victim's operating system is running, files on the external storage device can infect the system; rebooting the system will trigger the boot disk virus. An infected storage device connected to a computer can modify or even replace the existing boot code on the infected system so that when the system is booted next, the virus will be loaded and run immediately as part of the Master Boot.

- ## How does a computer virus attack?

Once a virus has successfully attached to a program, file, or document, the virus will lie dormant until circumstances cause the computer or device to execute its code. In order for a virus to infect your computer, you have to run the infected program, which in turn causes the virus code to be executed.
This means that a virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on the same network. Stealing passwords or data, logging keystrokes, corrupting files, spamming your email contacts, and even taking over your machine are just some of the devastating and irritating things a virus can do.
While some viruses can be playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disk. Worse yet, some viruses are designed with financial gains in mind.

- ## What is acomputer worm?

- A worm has similar characteristics of a virus. Worms are also self-replicating, but self-replication of a worm is in a different way. Worms are standalone and when it is infected on a computer, it searches for other computers connected through a local area network (LAN) or Internet connection. When a worm finds another computer, it replicates itself to the new computer and continues to search for other computers on the network to replicate.

  Due to the nature of replication through the network, a worm normally consumes much system resources including network bandwidth, causing network servers to stop responding.

- ## Types of worm:-

• **Email Worms:** Email Worms spread through infected email messages as an attachment or a link of an infected website.

• **Instant Messaging Worms:** Instant Messaging Worms spread by sending links to the contact list of instant messaging applications.

• **Internet Worms:** Internet worm will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. If a computer is found vulnerable it will attempt to connect and gain access to them.

• **IRC Worms:** IRC Worms spread through IRC chat channels, sending infected files or links to infected websites.

• **File-sharing Networks Worms:**File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

- ## How do computer spread worms?

1. Email-

One of the most common ways for computer worms to spread is via email spam. In years gone by, worms could hide in the main text of an email, but as modern email clients caught on and began blocking direct embedding circa 2010, the risk for this type of attack is fairly low.

While embedded worms may be things of the past, email attachments remain popular hiding spots for worms. What may appear to be a benign work document or personal photo can, in fact, be hiding malicious code, waiting to be released when you click a link or open said attachment. Once a machine has been infected, the worm may replicate itself by emailing itself to everyone in your address book or automatically replying to emails in your inbox.

2. Operating system vulnerabilities-

Every operating system has its vulnerabilities (yes, even macOS) and some worms are specifically coded to take advantage of these weak points. Perhaps the most infamous example is Conficker, a worm first identified in 2008 which exploited a vulnerability in a network service present in many versions of Windows, including Windows 2000, Windows XP, Windows Vista, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 Beta and Windows 7 Beta. At its peak, Conficker infected as many as 15 million computers.

3. Instant messaging-

Worms can take on similarly deceptive forms in instant messaging software and take advantage of users who are probably not on high alert when using such services.

In the past, instant messaging software such as mIRC, MSN Messenger, Yahoo IM and ICQ proved to be exceptionally fertile breeding grounds for worms. In today's digital landscape, modern chat systems are just as vulnerable, with Facebook Messenger a common infection point for worms such as Dorkbot, which spreads via an executable file disguised as a JPG image.

4. Smartphones-

Globally, there were about 2.8 billion active smartphones being used at the end of 2016, according to data collated by market intelligence firm Newzoo. With these figures in mind, it should come as little surprise that worm creators are increasingly turning their attention to mobile devices.

Research from Syracuse University suggests that every major mobile operating system (including Android, iOS, Blackberry and Windows Phone) are potentially vulnerable to worms as they all support HTML5-based mobile apps. One of the key security flaws of HTML5 is that malicious code can easily be inserted into it, meaning that when a user launches an app they could also be unwittingly executing a damaging program.

Difference Between Viruses and Worms:-

Virus v/s Worm

Virus	Worm
• Attaches itself to OS or the programs	• Do not Attaches itself to OS
• Need user action to abet their propagation.	• Self propagates across a network exploiting security in widely used services.
• Damages caused is mostly local to the machine	• It harms the network and consumes n/w bandwidth.
• Spread quite slowly	• Spread much more rapidly Ex. SQL Slammer worm 75,000 victims within ten minutes.