

Amit Shah  
18012010008

## Cyber security Assignment

Q Explain digital signatures also tell its advantage?

As A digital signature is a mathematical scheme for demonstrating the authenticity of digital message or documents. It is a virtual fingerprint that is unique to a person and are used to identify signers and secure data in digital documents. It is a type of electronic signature that ensure compliance with legal regulation by providing the validity and authenticity of a digital documents and signature identity. digital signature can provide proof of origin, time identity and status of a digital document. A signature confirms that the data emitted from the signer and has not been tampered with during transit.

Advantage of digital signature :-

- (1) Save time :- Digital signature are cost and time free because it verify by data so it check faster than paper.
- (2) Cost savings -
- (3) work flow efficiency
- (4) Better customer experience
- (5) Future validity
- (6) Security
- (7) Environment benefits etc

Q 2 What do you mean by information security? explain with the help of example.



Information security (InfoSec) enables organizations to protect digital and analog information. InfoSec provides coverage for cryptographic mobile computing social media, as well as infra-structure and networks containing private financial and corporate information. Cyber security, on the other hand, protects both raw and meaningful data, but only from internet based threats.

Organisations implement information security for a wide range of reasons. Example -

Berkshire Bank is an example of a company that decided to restructure its data loss prevention (DLP) strategy. The company wanted to gain access to more detailed reporting on events. Their old system only provided general information when threats were prevented but the company wanted to know specific about each event. To prevent that Berkshire bank adopted enablement solution to provide managed DLP coverage.

Q Define the term Information Assurance.

Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. There are commonly five terms associated with the definition of information assurance.

- (a) Integrity
- (b) Availability
- (c) Authentication

- (d) Confidentiality
- (e) Non repudiation

IA is a field in and of itself. It can be thought of as a specialty of information technology because an IA specialist must have a thorough understanding of IT and how information systems work and are interconnected with all of the threats that are now common in the IT world: worms, phishing attacks, social engineering, identity theft and more. A focus on protection against these threats is required. IA is that focus - the final pillar is non-repudiation.