CIA-2 TYCS47

1. How can deleted emails be recovered?

How to recover deleted emails in Gmail
Here's a step-by-step guide to recovering deleted emails from your Gmail account on your desktop. The whole process should take less than 30 seconds.

Step 1- Gmail's Trash/Bin folder
Go to your Gmail inbox.
On the left screen, there is a list of folders (Inbox, Starred, Spam, etc). Your deleted emails will be in a folder called "Trash" or "Bin" (these are the same folder, but named differently depending on the user's language setting).
If you can't see a folder called "Trash" or "Bin", then click "More" at the bottom of the list.
This will show all your Gmail folders, and you will now find the correct folder.

Step 2- Recover your deleted email.
Now that you've found the folder containing your deleted emails, you can start to recover them. Look inside the folder for the email you wish to recover and click on the box to the far left of the email row to select the email.
Select ~~Move~~ your deleted email to inbox to recover it.
Once you've found and selected the right emails, click "Move to" in the row of buttons above the list of emails. From the top drop-down menu that now appears, you can select where to put the deleted email.

Move your deleted email to inbox to recover it. Moving it to any folder except the "Trash" or "Bin" folder will recover the email from deletion. If you don't want to organize the email, you can simply click the "Inbox" option, and the deleted email will be put back in your inbox.

Recover deleted Gmail emails on iOS/Android
The process for recovering deleted emails from Gmail is pretty much the same for mobile devices as on desktop.
First, find the deleted email ~~is open in a~~ the folder named "Trash" or "Bin".
When you've found the email in the folder, tap it to open it.
Once the deleted emails is opening you'll see three dots in the top-right corner of the screen.
Tap this button, and the options for email actions will appear.
You can recover deleted email in Gmail from mobile too
From these options, press "Move to." Select a new folder - "Inbox" will work fine if you don't want to organize the email elsewhere.
With this done, the email will be recovered from deletion, and won't be removed from your inbox after 30 days.

Here to recover deleted emails in Gmail after 30 days
Gmail deletes all messages that have been in the "Trash"/Bin" or the "Spam" folder for more than 30 days. This is done automatically and permanently and is impossible

Email deleted from the trash in Gmail
In the Trash folder of Gmail, there is an option for 'Delete forever'. This is a very literally-named button. Emails deleted from Gmail's Trash folder are removed permanently. There is no way to get them back. So, be careful when clicking "Delete forever" in Gmail. Emails in the Trash folder are automatically deleted after 30 days, so it is recommended to simply leave the email there. If you do need to recover the email, you'll have a window of a month to do so.

2. Explain in detail about Data Carving.

File or data carving is a term used in the field of Cyber forensics. Cyber forensics is the process of acquisition, authentication, analysis and documentation of evidence extracted from and/or contained in a computer system, computer network and digital media. Extracting data (file) out of undifferentiated blocks (raw data) is called as carving. Identifying and recovering files based on analysis of file format is known as file carving. In Cyber Forensics, carving is a helpful technique in finding hidden or deleted files from digital media. A file can be hidden in areas like clusters, unallocated clusters and slack space of the disk or digital media. To use this method of extraction, a file should have a standard file signature called a file header (start of the file). A search is performed to locate the file header signature a-

continued until the file footer(end of the file) is reached. The data between these two points will be extracted and analyzed to validate the file. The extraction algorithm uses different methods of carving depending on the file formats.

How does carving work? Data carving interacts with two types of unallocated drive spaces:-

- Unused disk space - Space that was left empty when a new partition was created on a drive.
- Reused disk space - Empty space within a new partition that was previously used by another partition.

While the system treats both of these types of spaces as free space, partitions of the second type may still contain some file data even though there's no metadata that can be used to find file locations, In this case, carving is the only way to effectively recover data.

The data carving technique can be used in two ~~sentences:~~ scenarios:

1. To recover lost or damaged files due to missing or corrupt directory entries. The possibility of fully recovering such files depends on the significance of directly entry corruption. In some cases, lost files can be recovered only fragmentarily.
2. To recover deleted files. The ability to recover deleted files depends on two factors:

- Whether the filessystem contains information on the clusters where the files were stored
- Whether these clusters were overwritten with other files

For the sake of performance, the filessystem doesn't wipe out a deleted file right away. Instead, it marks the clusters occupied by that file as free space. Therefore, data from the deleted file remains on the drive until it gets overwritten with the data of another file.

3. What Is the Difference Between Threat, Vulnerability and Risk?

What is Risk? An organization's risk profile fluctuates depending on internal and external environmental factors. It incorporates not just the potential or probalty of a negative event, by the impact that event may have on your infrastructure. And though risk can never be 100% eliminated - cybersecurity is a persistently moving target, after all - it can be managed to a level that satisfies your satisfies your organization's tolerance for risk, low, manageable and known.
What is a Threat? Today's cybersecurity land-scape rolls with an endless stream of potential threats - from malware that plants dangerous executables on your software and ransomware that locks up your systems to specially targeted Hacker attacks. All of these threats look for a way in, a vulnerability in your environment that they can exploit. Some threats, however, hold more potential for

exploitation than others. The more rich, fresh data you can access and analyze about these threats, the more strategic and impactful decisions you can make regarding your vulnerability management and remediation.

What is a Vulnerability- Vulnerabilities are weak spots within your ~~ex~~environment and your assets- weaknesses that open you up ~~to~~ potential threats and increased risk. And unfortunately, an organization can have thousands, often millions of vulnerabilities. Remediating all of them is not feasible, especially when most organizations only have the capacity to patch one out of every ten vulnerabilities. While that may sound like a losing battle, the good news is that only 2% - 5% of valnerabilities are likely to be exploited. And among those, an even smaller percentage are likely to pose an actual risk to your business, because, for instance, many of these vulnerabilities may not be actively exploited within your industry. So much for that old "everything is a risk" approach.

4. Write in brief about MD5 checksum.

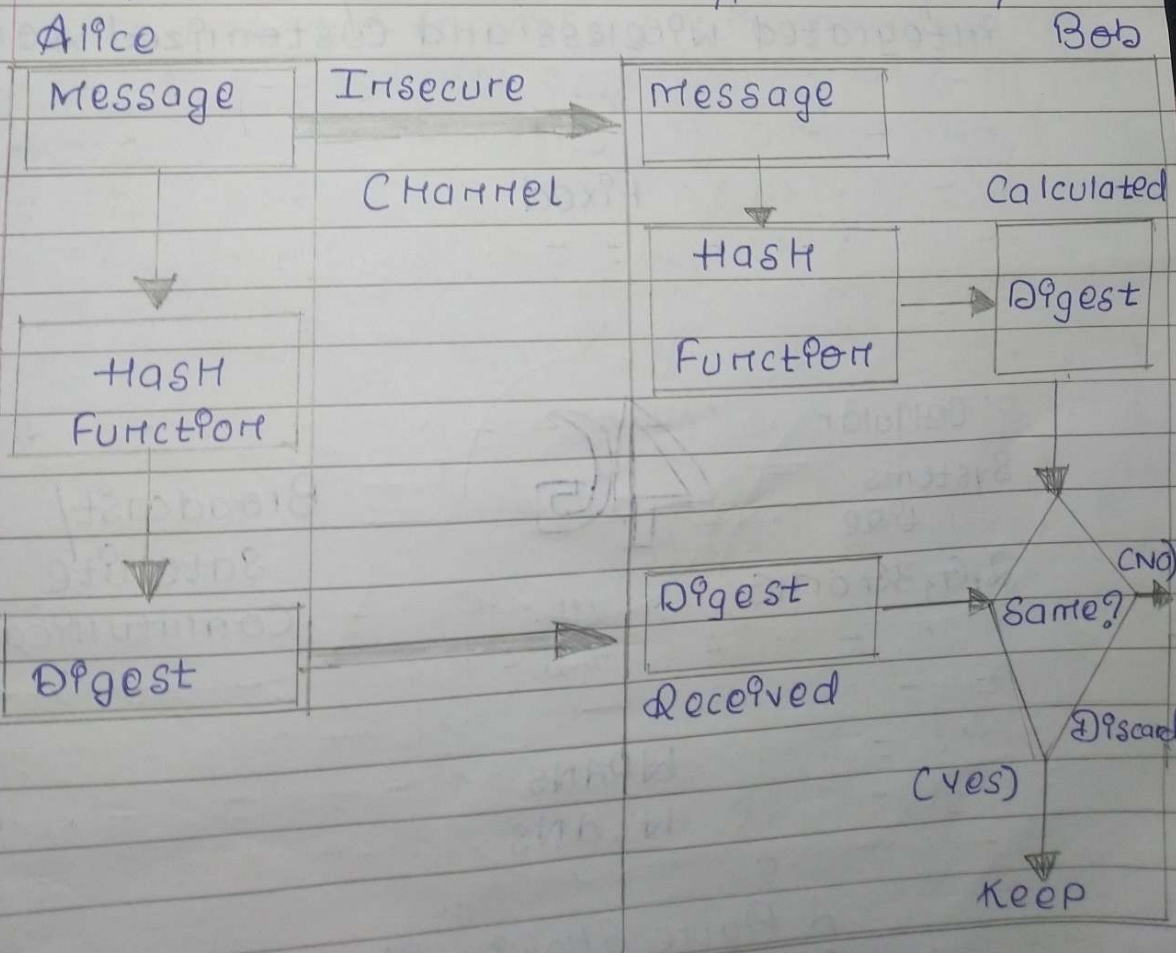
What is MD5?
The MD5 (message-digest algorithm) hashing algorithm is a one-way cyptographic function that accepts a message of any length as input and returns as output a fixed-length digest value to be used for authenticating the original message.

The MD5 hash function was originally design

for use as a secure cryptographic hash algorithm for authenticating digital signatures. But MD5 has been deprecated for uses unintentional data corruption.

What is MD5 used for?

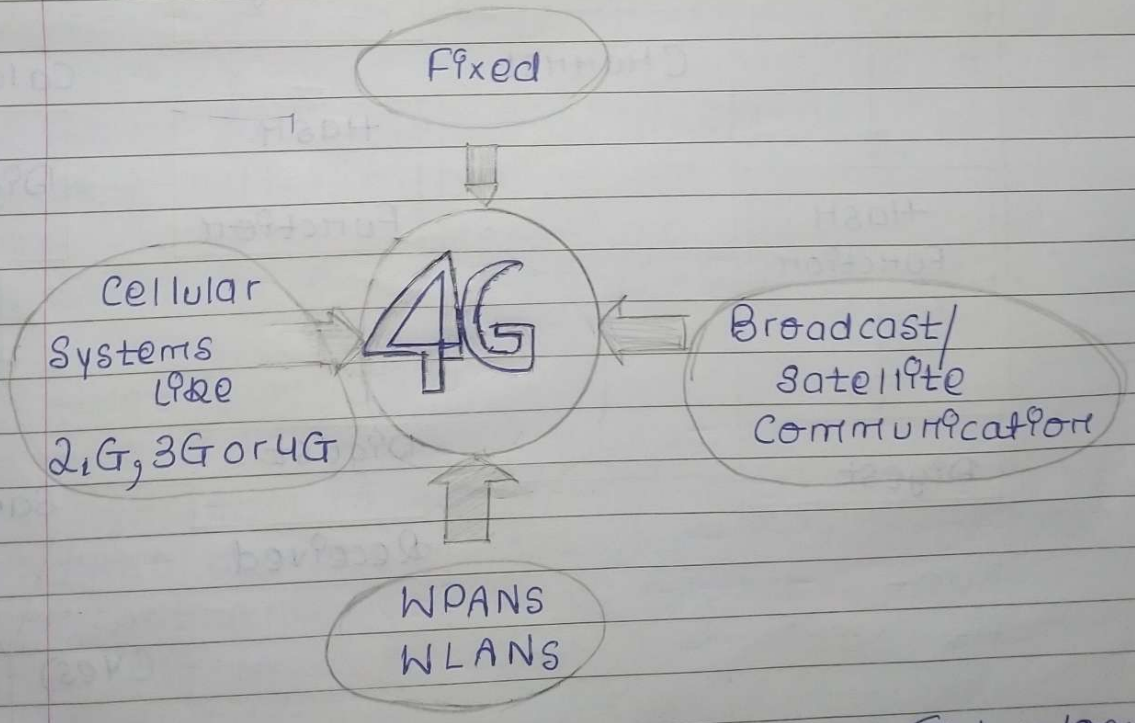
Although originally designed as a cryptographic message authentication code algorithm for use on the Internet, MD5 hashing is no longer considered reliable for use as a cryptographic checksum because security experts have demonstrated techniques capable of easily producing MD5 collisions on commercial off-the-shelf computers. An encryption collision means two files have the same hash. Hash functions are used for message security, password security, computer forensics and cryptocurrency.



5. List and explain technologies used by 4G network.

4G- Also known as "Beyond 3G" 4G refers to the fourth generation of wireless communications.

4G is all about convergence; convergence of wired and wireless networks, wireless technologies including GSM, wireless LAN, and Bluetooth as well as computers, consumer electronics, communication technology and several others. 4G is a Mobile multimedia, anytime anywhere, Global mobility support, integrated wireless solution, and customized personal service network system
4G wireless technology is also reffered to by "MAGIC" which stands for Mobile multimedia, Any-where, Global mobility solutionsever, integrated wireless and customized services.



A Figure Showing Use of 4G Technology Across Various Networks

4G is an all IP-based integrated system will be capable to provide 100 Mbps for high mobility and 1 Gbps for low mobility, with end-to-end QoS and high security, and will offering various services at any time as per user requirements, anywhere with seamless interoperability, at affordable cost. The user services include IP telephony, ultra-broadband Internet access, gaming services and High Definition Television (HDTV) streamed multimedia.

4G Requirements - As per ITU's IMT-A

- All-IP packet switched network
- Data rates up to 100 Mbps for high mobility and up to 1 Gbps for low mobility.
- Seamless connectivity and global roaming
- Interoperability with existing wireless standards
- Smooth handovers.
- High QoS.

Key components & Technologies in 4G

MIMO - OFDM

MIMO, in contrast to traditional communication systems, takes advantage of multipath propagation to increase throughput, range/coverage, and reliability. MIMO (Multipe Input Multiple Output) systems use spatial multiplexing transmitting antennas and multiple receiving antennas are used.

IPv6 - IPv4 address exhaustion is likely to be in its final stages by the time of deployment of IPv6. Hence, for 4G technology IPv6 has evolved to support a large number of devices

Smart Antennas

Smart or Intelligent antennas is also a multi-antenna concept which allows the radio beam to follow the user. This is done through beam forming which temporarily improve gain. They are also used to provide transmit and/or receive diversity.

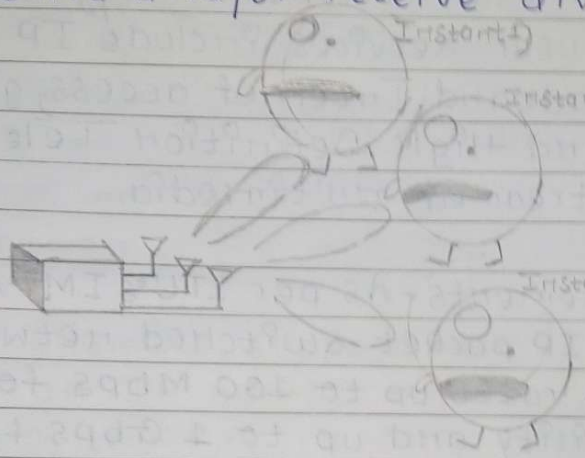


Fig. 4: A Diagram showing Concept of Smart or Intelligent Antennas

AdHoc Networks

AdHoc networks refer to spontaneous self organisation of network of devices, not necessarily connected to Internet, 4G will create Hybrid wireless networks using adHoc networks

Adaptive Modulation And Coding (AMC)

Adaptive modulation and coding mechanism reacts to instaneous variations in channel conditions and accordingly modify the modulation & coding format, AMC allows different data rates to be assigned to different users.

Adaptive Hybrid ARQ

Efficent and reliable Medium access control

(MAC) layer performance is extremely important for reliable link performance over the lossy wireless channel. To achieve this, an automatic retransmission and fragmentation mechanism called automatic Repeat Request (ARQ) is used, wherein the transmitter breaks up packets received from higher layer into smaller sub packets, which are transmitted sequentially.

Improved Modulation

Previous standards used phase-shift keying, more spectrally efficient modulation schemes such as 64-QAM (Quadrature Amplitude Modulation) is being used for 4G systems.

Software Defined Radio (SDR)

SDR is key to 4G systems. Software Defined Radio allows some of the functional modules of radio equipment like modulation/demodulation, signal generation, coding and link-layer protocols, that used to be traditionally implemented in special purpose hardware to be implemented in modifiable software or firmware operating on programmable processing technologies.

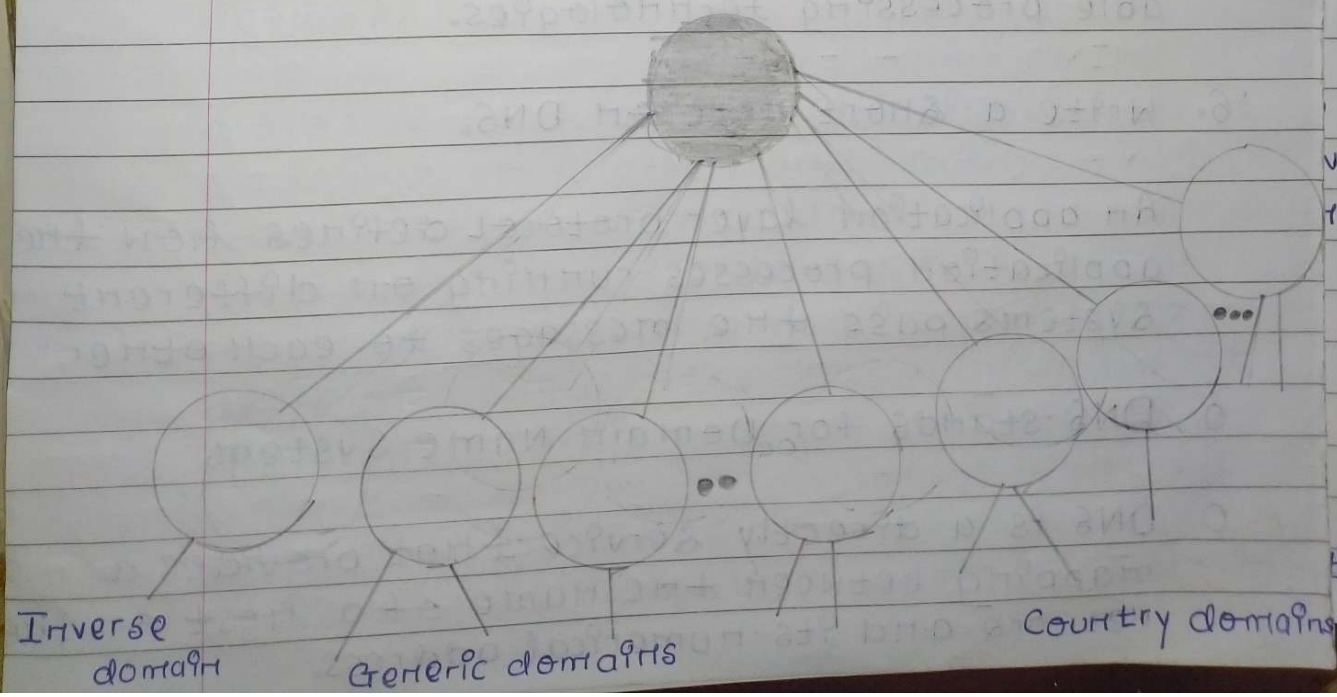
6. Write a short note on DNS.

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directly service that provides a mapping between the name of a host on the network and its numerical address.

- DNS is required for the functioning of the Internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain is more reliable than IP address.

DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.



7. Explain in detail anyone Email protocol.

- SMTP stands for Simple Mail Transfer Protocol.
- SMTP is a set of communication guidelines that allow software to transmit an electronic mail over the Internet is called Simple Mail Transfer Protocol.
- It is a program used for sending messages to other computer users based on e-mail addresses.
- It provides a mail exchange between user on the same or different computers, ~~users based~~ and it also supports:
- It can send a single message to one or more recipients.
- Sending message can include text, voice, vido or graphics.
- It can also send the messages on networks outside the Internet.
- The main purpose of SMTP is used to set up communication rules between servers. The servers have a way of identifying themselves and announcing what kind of communication they are trying to perform. The also have a way of handling the erros receiving server reply with an error message of some kind.

8. What are the different ways of password cracking?

The Top Ten Password-cracking Techniques Used by

1. Phishing

password-cracking-phishing

There's an easy way to hack, ask the user for his or her password. A phishing email leads the unsuspecting reader to a spoofed log in page associated with whatever service it is the hacker wants to access, usually by requesting the user to put right some terrible problem with their security. That page then asks their password and the hacker can go use it for their own purpose. Why bother going to the trouble of cracking the password when the user will happily give it to you anyway?

2. Social Engineering

Social engineering takes the world "ask the user" concept outside of the inbox that phishing tends to stick with and into the real world. A favourite of the social engineer is to call an office posting as an IT security tech guy and simply ask for the network access password. You'd be amazed at how often this works. Some even have the necessary goonads to don a suit and name badge before walking into a business to ask the receptionist the same question face to face.

3. Malware

Malware comes in many forms, such as a keylogger, also known as a screen scraper, which records everything you type or takes screenshots during a login process, and then forwards a copy of this file to Hacker

file and copy it, which, unless properly encrypted, will contain easily accessible saved passwords from the user's browsing history.

4. Dictionary Attack

password-cracking - dictionary

The dictionary attack uses a simple file containing words that can be found in a dictionary, hence its rather straightforward name. In other words, this attack uses exactly the kind of words that many people use as their password.

5. Rainbow Table Attack

Rainbow tables aren't as colorful as their name may imply but, for a hacker, your password could well be at the end of it. In the most straightforward way possible, you can boil a rainbow table down into a list of pre-computed hashes - the numerical value used when encrypting a password. This table contains hashes of all possible password combinations for any given hashing algorithm. Rainbow tables are attractive as it reduces the time needed to crack a password hash to simply just looking something up in a list.

6. Spidering

Savvy hackers have realized that many corporate passwords are made up of words that are connected to the business itself.

studying corporate literature, website sales material, and even the websites of competitors and listed customers can provide the ammunition to build a custom word list to use in a brute force attack. Really savvy hackers have automated the process and let a spidering application, similar to the web crawlers employed by leading search engines to identify keywords and then collect and collate the lists for them.

7. Offline Cracking

It's easy to imagine that passwords are safe when the systems they protect lock out users after three or four wrong guesses, blocking automated guessing applications. Well, that would be true if it were not for the fact that most password hacking takes place ~~o~~offline, using a set of hashes in a password file that has been 'obtained' from a compromised system.

Often the target in question has been compromised via a hack on a third party, which then provides access to the system servers and those all-important user password hash file. The password ~~hash~~ cracker can take as long as they need to try and crack the code without alerting the target system or individual user.

8. Brute Force Attack

Like the dictionary attack, the

brute force attack comes with an added bonus for the hacker. Instead of simply using words, a brute force attack lets them detect non-dictionary words by working through all possible alpa-numeric combinations from aaa1 to zzz10.

9. Shoulder surfing
password-cracking:- Shoulder-surfing
Another form of social engineering, Shoulder surfing, just as it implies, entails peeking over a person's shoulders while they're entering credentials, passwords, etc. Although the concept is very low tech, you'd be surprised how many passwords and sensitive information is stolen this way, so remain aware of your surroundings when accessing bank accounts, etc. on the go.

10. Guess
The password cracker's best friend, of course, is the predictability of the user. Unless a truly random password has been created using software dedicated to the task, a user-generated 'random' password is unlikely to be anything of the sort.

9. Define the following terms as per IT Act:

- Access
- Addressee
- Digital Signature
- Secure System

Section 2(1) in The Information Technology Act, 2000
(1) In this Act, unless the context otherwise

(a) "access", with its grammatical variations and cognate expressions, means gaining entry into, instructing or communicating with the logical, arithmetical or memory function resources of a computer, computer system or computer network;

(b) "addressee" means a person who is intended by the originator to receive the electronic record but does not include any intermediary;

(p) "digital signature" means authentication of any electronic record by a ~~sig~~ subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

"secure system" means computer hardware, software, and procedure that-

(a) are reasonably secure from unauthorised access and misuse;

(b) provide a reasonable level of reliability and correct operation;

(c) are ~~res~~reasonably suited to performing the intended functions; and

(d) adhere to generally accepted security procedures;

10. What are privacy controls? Explain its importance

Privacy controls are lists of measures that will reduce privacy risk contained in an information system. They respond to risks identified in a risk analysis process. They correspond to the impact levels identified in a privacy impact analysis (PIA). The risk manager chooses matching controls that fulfill a number of requirements.

A privacy control is chosen from one of two categories:

- a technical control;
- an administrative control.

Technical controls are controls that are part of the information technology used to process personal data. technical controls are often functions of information security such as access control, encryption, integrity protection, availability insurance. Safety functions such as fire protection, redundant power supplies and reserve hardware are part of the technical controls, too. Finally, PETs and other privacy support technology such as data hiding, steganography, mathematical data obfuscation and TET's are technical controls.

Administrative controls are all non-technical controls. Administrative controls are, for example, staff qualification management, staff security clearance, the proper administrative of data subject consent and privacy policies in harmony with the data transactions performed. The administrative ~~administrative~~ on of physical access to computing hardware and storage devices, the management of roles and privileges that lead to authorization in access control systems, and the authorization and monitoring of subcontractors are other examples of administrative controls.

Sometimes, physical controls are listed separately, implying the securing of physical access to systems. Non-technical controls gets implemented in processes, procedures, policies and operations.

WHY ~~What~~ is privacy important?

Privacy is the ability to control who can access information about our private life and our activities. Privacy is important because:

- Privacy gives us the power to choose our thoughts and feelings and who we share them with.
- Privacy protects our information we do not want shared publicly (such as health or personal finances).
- Privacy helps protect our physical safety (if our real time location data is private.)
- Privacy helps protect us as individuals, and our businesses, against entities were depend on or that are more powerful than us.
- Privacy is tied to freedom..... Could we really be free - and have free will - without privacy?