



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

Important Instructions to examiners:

- 1) The answers should be examined by key words and not as word-to-word as given in the model answer scheme.
- 2) The model answer and the answer written by candidate may vary but the examiner may try to assess the understanding level of the candidate.
- 3) The language errors such as grammatical, spelling errors should not be given more Importance (Not applicable for subject English and Communication Skills).
- 4) While assessing figures, examiner may give credit for principal components indicated in the figure. The figures drawn by candidate and model answer may vary. The examiner may give credit for any equivalent figure drawn.
- 5) Credits may be given step wise for numerical problems. In some cases, the assumed constant values may vary and there may be some difference in the candidate's answers and model answer.
- 6) In case of some questions credit may be given by judgement on part of examiner of relevant answer based on candidate's understanding.
- 7) For programming language papers, credit may be given to any other program based on equivalent concept.

Q. No	Sub Q.N.	Answer	Marking Scheme
1.	a) i) Ans.	Attempt any three of the following: Explain 'Data Obfuscation'. Data obfuscation: 1. Data obfuscation involves protection of sensitive information with technique other than encryption. 2. Data obfuscation is one of the solutions for data theft. Obfuscate means to make the data unclear. 3. It is an effective method which involves chopping the text into segments and re-arranging it. 4. Sometimes data is obfuscated by using a simple substitution cipher. 5. A good example of data obfuscation would be an audit report on a medical system. In this report only required field of patients are disclosed to the auditor. Details which are not required such as patient's contact no and address are made obfuscate.	12 4M Relevant Explan ation 4M
	ii) Ans.	Explain following with reference to information security. a) Security policy b) Standards c) Guidelines d) Procedures	4M



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>a) Security policy: Information security policy consists of higher level statements related to the protection of information across the business by senior management. Businesses may have a single encompassing policy or several specific policies that target different areas like</p> <ol style="list-style-type: none"> 1. Senior Management Statement of Policy 2. Regulatory Policy 3. Advisory Policy 4. Informative Policy <p>b) Standards: Standard consists of specific low level mandatory controls that help to enforce and support the information security policy. Standard helps to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software. For example, a password standard may set out rules for password complexity and a Windows standard may set out the rules for hardening Windows clients.</p> <p>c) Guidelines:</p> <ol style="list-style-type: none"> 1. It should consist of recommended, non-mandatory controls that help to support standards or serve as a reference when no applicable standard is in place. 2. It should be viewed as best practices that neither are nor usually requirements, but are strongly recommended. 3. It can be consisting of additional recommended controls that support a standard or help to fill in the gaps where no specific standard applies. 4. A standard may require specific technical controls for accessing the internet securely and separate guidelines may be outline the best practices for using it. <p>d) Procedures: Procedures are the detailed, step by step activities that are followed to implement a process or configure system for compliance to a guideline. They may also be step by step security processes, which assure repeatability and accountability of personnel performing the procedure.</p>	<p><i>Explan ation of each term 1M</i></p>
iii) Ans.	<p>Give any four applications of cryptography. Applications of cryptography are:</p>	<p>4M</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>1. Data Hiding: The original use of cryptography is to hide something that has been written.</p> <p>2. Digital Code: Cryptography can also can be applied to software, graphics or voice that is, it can be applied to anything that can be digitally coded.</p> <p>3. Electronic payment: When electronic payments are sent through a network, the biggest risk is that the payment message will alter or bogus messages introduced and the risk that someone reads the messages may be minor significance.</p> <p>4. Message Authentication: One cannot entirely prevent someone from tampering with the network and changing the message, but if this happens it can certainly be detected. This process of checking the integrity of the transmitted message is often called message authentication. The most recent and useful development in the uses of cryptography is the digital signature.</p>	<p><i>Any four correct applications of cryptography, each application 1M</i></p>
	<p>iv) Ans.</p>	<p>Describe any four virus attacks.</p> <p>1.DOS: A Denial of Service attack is a type of cybercrime where internet site is made unavailable by using multiple computers which make repeated requests to the server.</p> <p>2.SPAM: It is an irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.</p> <p>3.Malicious insider: An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.</p> <p>4.Phishing: It is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.</p> <p>5.Botnet: It is a network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.</p>	<p>4M</p> <p><i>Description of any four virus attacks, each attack 1M</i></p>
1.	<p>b) i) Ans.</p>	<p>Attempt any one of the following:</p> <p>Describe three pillars of information security.</p> <p>Three pillars of information security:</p>	<p>6 6M</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

1. Confidentiality
2. Integrity
3. Availability

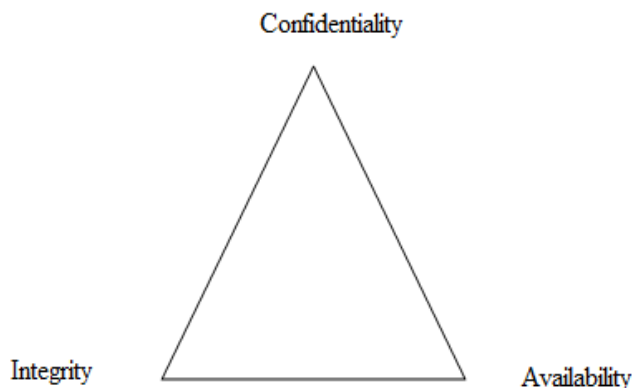


Fig: Three pillars of Information Security

1. Confidentiality:

It is used as an attempt to prevent the intentional or unintentional unauthorized disclosure of message contents. Loss of confidentiality can occur in many ways such as through the intentional release of private company information or through a misapplication of networks right.

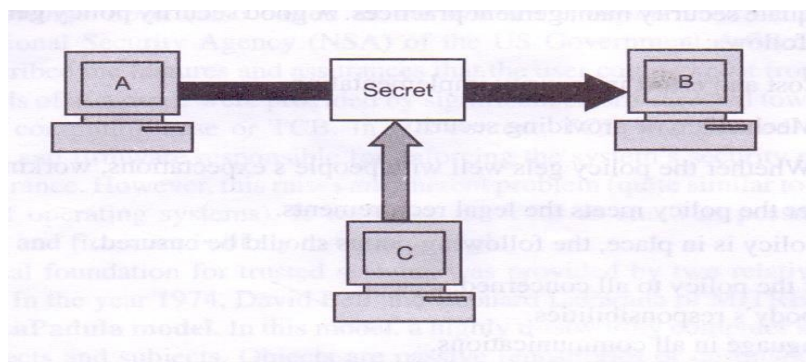


Fig: Loss of Confidentiality

2. Integrity:

The concept of integrity ensures that

- i. Modifications are not made to data by unauthorized person or processes.
- ii. Unauthorized modifications are not made to the data by authorized

*Correct
descripti
on of
each
pillar
with
neat
diagram
2M*



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

- person or processes.
iii. The data is internally and externally consistent.

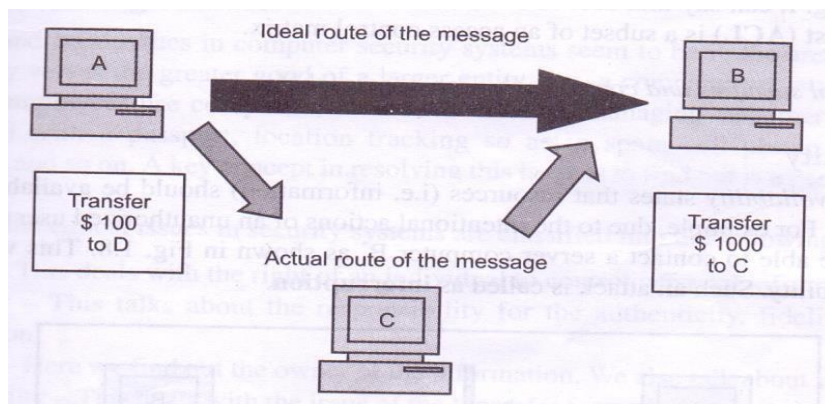


Fig: Loss of Integrity

3. Availability:

The concept of availability ensures the reliable and timely access to data or computing resources by the appropriate person. Availability guarantees that the systems are up and running when they are needed. In addition, this concept guarantees that the security services needed by the security practitioner are in working order.

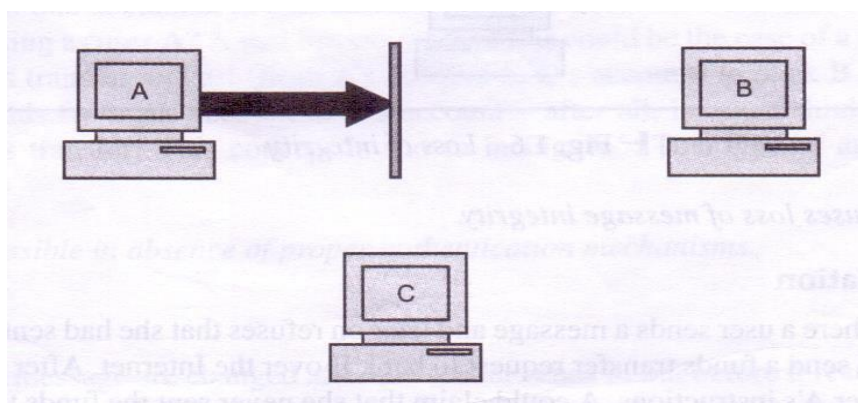


Fig: Attack on availability

<p>ii)</p> <p>Ans.</p>	<p>Describe any six protection mechanisms in ‘Trusted Computing Base’.</p> <p>Protection Mechanisms in a Trusted Computing Base are as follows:</p> <p>1. Process Isolation: Each process has its own address space to store data and code of application. We can prevent other processes from</p>	<p>6M</p>
------------------------	---	------------------



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>accessing the other process's data. It will prevent data leakage as well as modification in the memory.</p> <p>2. Principle of least privilege: For allowing normal functioning it will limit the access to minimum level. This will prevent data exploitation.</p> <p>3. Hardware Segmentation: It is the process of dividing memory into multiple segments or sections. For every process, Kernel allocates some memory to store its process data, application code, and application data. It will prevent the user processes from accessing other process's memory.</p> <p>4. Layering: Dividing process of operation into number of layers to perform various functions is called as Layering.</p> <ol style="list-style-type: none"> Each layer is responsible for particular type of actions. Lower layers will perform all basic functions while higher layers will perform more complex and protected functions <p>5. Abstraction: By ignoring implementation details it will provide security. It will define particular set of permissible values as well as operations for an object.</p> <p>6. Data / Information hiding: It is the process of assuring that when data or information at one level is available at another level (Higher or Lower), then it cannot be available to another level (Higher or Lower)</p> <p>7. Information Storage: It is the process of retaining the physical state of information for specific interval time, for example at the time of poor fluctuation.</p> <p>8. Closed and open System: In closed system very less interfaces are available that can connect to other systems. Users have limited access to application and programming language in this system.</p> <p>9. Multitasking, Multiprogramming , Multiprocessing :</p> <ol style="list-style-type: none"> Capability of running multiple tasks at a time in synchronized way is called Multitasking. Capability of allowing execution of multiple programs is called Multiprogramming. Capability of a processor of allowing simultaneous execution of multiple programs called Multiprocessing. <p>10. Finite State Machine: It is a device which stores a current state of process at that time.</p> <ol style="list-style-type: none"> Output of finite state of machine is based upon the input given to device. New state is depending upon the old state and input. 	<p style="text-align: center;"><i>Description of any six protection mechanisms in trusted computing base 1M Each</i></p>
2.	i)	<p>Attempt any two of the following:</p> <p>Describe levels of information classification and explain any three criteria for classification of information.</p>	<p style="text-align: center;">16 8M</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	Ans.	<p>Levels of information classification are:</p> <p>1. Unclassified Information that is neither sensitive nor classified. The public release of this information does not violate confidentiality.</p> <p>2. Sensitive but Unclassified (SBU) Information that has been designated as a minor secret but may not create serious damage if disclosed.</p> <p>3. Confidential The unauthorized disclosure of confidential information could cause some damage to the country's national security.</p> <p>4. Secret The unauthorized disclosure of this information could cause serious damage to the country's national security.</p> <p>5. Top secret This is the highest level of information classification. Any unauthorized disclosure of top secret information will cause grave damage to the country's national security.</p> <p>Criteria for information Classification:</p> <p>1. Value It is the most commonly used criteria for classifying data in private sector. If the information is valuable to an organization it needs to be classified.</p> <p>2. Age The classification of the information may be lowered if the information value decreases over the time.</p> <p>3. Useful Life If the information has been made available to new information, important changes to the information can be often considered.</p> <p>4. Personal association If the information is personally associated with specific individual or is addressed by a privacy law then it may need to be classified.</p>	<p><i>Description of levels of information classification</i></p> <p>5M</p> <p><i>Any three criteria for classification of information</i></p> <p>3M</p>
	ii) Ans.	<p>Explain 'play fair cipher' encryption process with the help of following points.</p> <p>a) Preparing plain text b) Preparing a key matrix c) Encryption process- Operation rules – with suitable example.</p> <p>a) Preparing plain text:</p> <p>1. To prepare plain text write all letters of plain text in lowercase, in pairs without punctuation. 2. In plain text if j is present, all j's are replaced with i's.</p>	<p>8M</p> <p><i>Playfair cipher encryption</i></p> <p>on</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>3. In plain text if double letters occur in a pair, divide them by X or a Z.</p> <p>For e.g. ‘full’ in a plain text becomes ‘fulxl’.</p> <p>4. If there are an odd number of letters in plain text, an extra letter is chosen and it is added at the end.</p> <p>b) Preparing a key matrix:</p> <p>1. A key matrix is a five-by-five matrix of letters constructed using a keyword.</p> <p>2. The key phrase is first written without repeating any letters. The remaining letters of the alphabet are filled in the alphabetic order.</p> <p>c) Encryption process:</p> <p>The plain text is encrypted two letters at a time using the following steps:</p> <p>1. Each letter in a pair that is on the same row is replaced by the letter to the right.</p> <p>2. Letters in the same column are replaced by the next letter below in the same column.</p> <p>3. When the letters are neither in the same row nor in the same column, then the substitution based upon their intersection. Start with the first letter and move across until it is lined up with the second letter. Then start with the second, and move up or down until it is lined up with the first. Perform the transformation for each pair of letters in the modified plain text and remove the spaces.</p> <p>Example:</p> <p>Plaintext: We live in a world full of beauty.</p> <p>Keyword: Another</p> <p>Step 1: Preparing plain text</p> <p>The plain text matrix is:</p> <table><tr><td>we</td><td>li</td><td>ve</td><td>in</td><td>aw</td></tr><tr><td>or</td><td>ld</td><td>fu</td><td>lx</td><td>lo</td></tr><tr><td>fb</td><td>ea</td><td>ut</td><td>yz</td><td></td></tr></table> <p>Step 2: Preparing key matrix</p> <p>The key matrix is:</p> <table><tr><td>A</td><td>N</td><td>O</td><td>T</td><td>H</td></tr><tr><td>E</td><td>R</td><td>B</td><td>C</td><td>D</td></tr><tr><td>F</td><td>G</td><td>I/J</td><td>K</td><td>L</td></tr><tr><td>M</td><td>P</td><td>Q</td><td>S</td><td>U</td></tr><tr><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr></table>	we	li	ve	in	aw	or	ld	fu	lx	lo	fb	ea	ut	yz		A	N	O	T	H	E	R	B	C	D	F	G	I/J	K	L	M	P	Q	S	U	V	W	X	Y	Z	<p><i>process: preparin g plain text-2M</i></p> <p><i>preparin g a key matrix- 2M</i></p> <p><i>Encryption process- 2M</i></p> <p><i>Example -2M</i></p>
we	li	ve	in	aw																																						
or	ld	fu	lx	lo																																						
fb	ea	ut	yz																																							
A	N	O	T	H																																						
E	R	B	C	D																																						
F	G	I/J	K	L																																						
M	P	Q	S	U																																						
V	W	X	Y	Z																																						



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>Step 3: Encryption By following the above rules for encryption of plain text the cipher text is: VRFKAFGONVNBULLMIZIHIEFESHZY</p>	
	<p>iii) Ans.</p>	<p>List any six ‘Data Recovery Tools’ and explain ‘Data Recovery Procedure’.</p> <p>Data recovery tools:</p> <ol style="list-style-type: none"> 1. NTFS Data recovery tools 2. FAT data recovery tool 3. Digital Camera Data recovery tool 4. Removable media data recovery tool 5. Recovery of deleted files 6. Recovery of formatted partition <p>Data Recovery Procedure:</p> <p>1. NTFS Data Recovery Tools: NTFS Recovery is a fully automatic utility that recovers data from damaged or formatted disks. It is designed with a home user in mind. You don't need to have any special knowledge in disk recovery. Example: - Diskinternal_s NTFS Data Recovery tool. The tool supports</p> <ul style="list-style-type: none"> • A disk volume containing valuable info was damaged due to a system malfunction. • A disk volume was damaged due by a dangerous virus. • Windows cannot access a disk drive. • Disk was damaged • You have mistakenly formatted a disk volume • Files or folders are not readable • Corrupt or damaged partition table <p>2. FAT Data Recovery Tools: FAT Recovery is a fully automatic utility that recovers data from damaged or formatted disks. The program scans the disk first and then restores the original structure of files and folders. Example: - Diskinternal_s FAT Data Recovery tool. Works for all:</p> <ul style="list-style-type: none"> • Formatted drive (to NTFS, to/from FAT32/FAT16) • Inaccessible drive • Drive not booting • Missing or deleted file or directory 	<p>8M</p> <p><i>List of Data recovery tools 3M</i></p> <p><i>Data recovery procedure 5M</i></p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<ul style="list-style-type: none"> • Corrupt or damaged partition table. • Damaged Dynamic Disks <p>FAT Recovery is fully wizard-based, meaning there is no technical knowledge needed. Any person can recover data from damaged or formatted disks on their own, without hiring a technician. FAT Recovery does not write anything to the damaged disk, therefore you can try the program without any risk of losing data you want to be recovered. It does not matter whether Windows recognizes a disk or not, nor does it matter if all directory information is missing – all recoverable data will be recovered and the original disk structure will be restored. Because the program scans every single sector, it never misses recoverable data. Another important advantage of FAT Recovery is its capability to recover data from virtual disks, and it does not matter if the data was deleted prior to recovery or not. FAT Recovery supports the following file systems - FAT12, FAT16, FAT32, and VFAT. Files up to 64 KB are recovered by FAT Recovery.</p> <p>3. Digital Camera Data recovery tool: Digital camera data recovery has the leading photo recovery software for memory card used by digital camera or phone. It can effectively recover lost, deleted, corrupted or formatted photos and video files from various memory cards. It supports almost all memory card types including SD Card, MicroSD, SDHC, CF (Compact Flash) Card, xD Picture Card, Memory Stick and more. Example: - Diskinternals Digital Camera Data Recovery tool.</p> <p>Features</p> <ul style="list-style-type: none"> • Recover deleted photos from memory cards • Recover lost photos from memory cards • Recover lost movies from memory cards • Recover photos from formatted memory cards • Recover photos from damaged, unreadable or defective memory cards • Recover pictures from removable storage including flash drives • Recover images, video files from mobile phones <p>4. Removable media data recovery tool: The process of recovery is a very straightforward one - insert disk, press "Recover" and get the files you need. The software is easy to use and does not require any additional skills. We tried to make working with it as comfortable as possible. The program starts working automatically and doesn't require the additional set up change. Comfortable Recovery</p>	
--	--	---	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>Wizard will do everything for you. The result of the Wizard work is the list of all the recoverable files. All you have to do is to choose the necessary files and press a Recover button. The innovational scanning technology economizes greatly your time that otherwise would be spent on a damaged disc recovery.</p> <p>The advanced users can use a manual recovering. In this case you can work individually with each session\track and chose the file system depending on session.</p> <p>Example:-</p> <ul style="list-style-type: none">• Card Recovery• PhotoRec• Recover My Files• Recuva <p>5. Procedure to recover deleted files:</p> <p>If the file is deleted from the recycle bin, or by using shift + delete button, the simplest and easiest way to recover deleted file is by using a data recover software. If the file has been partially over written, there are some data recovery software applications which will perform better to recover the maximum of data.</p> <p>It is important to save the recovered file in a separate location like a flash drive. A file can only be permanently lost if it is over written. So do not over write, do not install or create new data on the file location.</p> <p>6. Procedure to recover formatted partition:</p> <p>If the hard drive is formatted, then people generally use a bootable CD to start the system. But if the system is booted and installed something like an operating system, on the formatted drive then there is more chances of losing the data forever.</p> <p>Formatting is to add deletion mark on all files or even empty FAT and system couldn't identify any content of disk partition. Formation nevertheless doesn't perform any operation upon data. Though directory is empty, data still exists. By utilizing data recovery software, user could retrieve all those data.</p> <p>Partition damage could probably render users considerable losses not only in terms of data, but economically also. Partition data loss is likely to bring about tens of millions of economic loss for user. Therefore, user should attach great attention on data protection while using computer. To recover files from a formatted drive through data recovery software is not a very complicated process, but it can be lengthy, and will need:</p>	
--	--	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		1. An enclosure (to convert hard drive into USB external drive). 2. A bootable system with preferably a high storage capacity hard drive. 3. A disk image creator and a virtual disk creator. 4. Data recovery software. 5. Sufficient storage space on devices other than the formatted drive.	
3.	i) Ans.	Attempt any four of the following: Explain ‘Bell-Lapadula’ model of information security. Bell LaPadula Model: The Bell-La Padula (BLP) model is a classic mandatory access-control model for protecting confidentiality. The BLP model is derived from the military multilevel security paradigm, which has been traditionally used in military organizations for document classification and personnel clearance. The BLP model has a strict, linear ordering on the security of levels of documents, so that each document has a specific security level in this ordering and each user is assigned a strict level of access that allows them to view all documents with the corresponding level of security or below. Working: The security levels in BLP form a partial order, <Each object, x, is assigned to a security level, L(x). Similarly, each user, u, is assigned to a security level, L(u). Access to objects by users is controlled by the following two rules: Simple security property. A user u can read an object x only if $L(x) < L(u)$ A user u can write (create, edit, or append to) an object x only if $L(u) < L(x)$ The simple security property is also called the —no read up rule, as it prevents users from viewing objects with security levels higher than their own. The property is also called the —no write down rule. It is meant to prevent propagation of information to users with a lower security level.	16 4M Relevant Explan ation 4M
	ii) Ans.	Explain working of ‘Biometric System’ with neat sketch. Biometrics refers to metrics related to human characteristics and traits. Biometrics authentication is used in computer science as a form of identification and access control.	4M



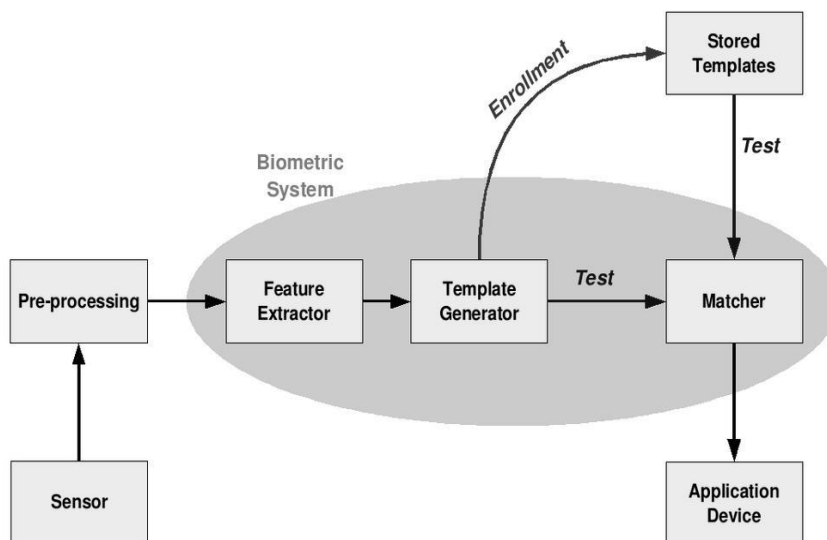
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518



***Correct
diagram
2M***

1. The block diagram illustrates the two basic modes of a biometric system. First, in verification (or authentication) mode the system performs a one-to-one comparison of captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person. In the first step, reference models for all the users are generated and stored in the model database.

2. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison.

3. Second, in identification mode the system performs a one-to-many comparison against biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as

***Explana
tion 2M***



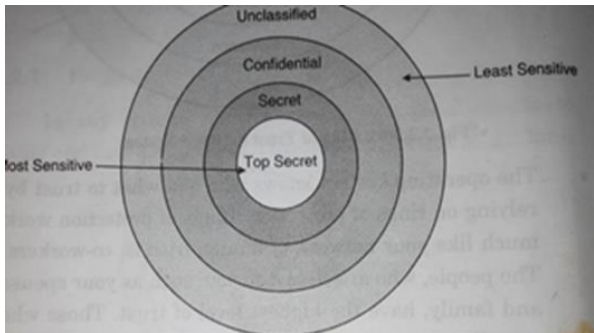
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>passwords, PINs or keys are ineffective.</p> <p>4. The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust.</p> <p>5. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way.</p> <p>6. During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements.</p>	
	<p>iii) Ans.</p>	<p>Describe ‘Ring of Trust’ in stand-alone system.</p> <p>Here the outer most layers contain less security whereas higher level of security is implemented in inner rings.</p> <p>The operating system knows who and what to trust by relying on rings of protection.</p> <p>The Protection ring model the operating system provides with various level at which to execute Code or to restrict that code’s access.</p> 	<p>4M</p> <p><i>Relevant Explan ation with diagram 4M</i></p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>The layer number increases and the level of trust decreases.</p> <p>Layer 0: The most level of trust.</p> <p>The OS kernel resides at this level.</p> <p>Any process running at this level is called operating in Privileged Mode.</p> <p>Layer 1: It contains Non Privileged portion of the operating system.</p> <p>Layer 2: At this level I/O drivers, low level operations and utilities reside.</p> <p>Layer 3: At this level applications and procedures operate.</p> <p>Users usually interact with this level.</p> <p>Operations working at this level generally called working in User Mode.</p>																															
	<div>iv)</div> <div>Ans.</div>	<p>Explain ‘Simple Row Transposition’ Technique of encryption with suitable example.</p> <p><i>(Note: keyword with/without alphabetical order shall be considered in the example)</i></p> <p>Transposition technique replaces one alphabet with another and also performs some permutation over the plain text alphabet.</p> <p>Algorithm Steps:-</p> <ol style="list-style-type: none">1. Write the plain text message row by row in a rectangle of a predefined size (keyword size)2. Read the message column by column, however, it need not be in the order of columns, it can be any random order.3. The message thus obtained is the cipher text message. <p>Example: Plain Text: —Come Home Tomorrow”</p> <p>Keyword: ZEBRAS</p> <p>Consider a rectangle with six column and. Therefore, when the message is written in the rectangle row by row it will look as follow</p> <table><tr><td>Column 1</td><td>Column 2</td><td>Column 3</td><td>Column 4</td><td>Column 5</td><td>Column 6</td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td>C</td><td>O</td><td>M</td><td>E</td><td>H</td><td>O</td></tr><tr><td>M</td><td>E</td><td>T</td><td>O</td><td>M</td><td>O</td></tr><tr><td>R</td><td>R</td><td>O</td><td>W</td><td></td><td></td></tr></table> <p>Now, decide the order of columns as some random order, say, 4, 6, 1, 2, 5, 3 Then read the text in the order of these columns.</p> <p>The cipher text obtained from it would be : EOW OO CMR OER HM MTO</p> <p>While Decryption phase the cipher is written back in same rectangle with same size and all ciphers are placed as per the key.</p>	Column 1	Column 2	Column 3	Column 4	Column 5	Column 6							C	O	M	E	H	O	M	E	T	O	M	O	R	R	O	W			<div>4M</div> <div>Explanation 2M</div> <div>Relevant Example 2M</div>
Column 1	Column 2	Column 3	Column 4	Column 5	Column 6																												
C	O	M	E	H	O																												
M	E	T	O	M	O																												
R	R	O	W																														



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

v) Ans.	<p>Describe any four ‘Cyber Crimes’. Different types of cyber crimes are:</p> <ol style="list-style-type: none"> 1. Hacking 2. Cracking 3. Viruses, Virus Attacks 4. Pornography 5. Spam 6. Spying 7. Obscene or offensive content 8. Mail Bomb 9. Bug exploit <p>1. Hacking Every act committed towards breaking into a computer and/or network is hacking and it is an offence. Hackers write or use readymade computer programs to attack the target computer. They possess the desire to destruct and they get enjoyment out of such destruction. Some hackers hack for personal monetary gains, such as stealing credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. Government websites are hot on hacker’s target lists and attacks on government websites receive wide press coverage.</p> <p>2. Cracking A cracker is someone who breaks into someone else computer system, often on a network by passing passwords or licenses in computer programs or in other ways intentionally breaches computer security. A cracker can be doing this for Profit maliciously, for some altruistic purpose or cause, or because the challenge is there. The term —cracker" is not to be confused with —hacker.</p> <ul style="list-style-type: none"> • Hackers generally deplore cracking. <p>3. Viruses, Virus Attacks A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections as it travels. Like a human virus, a computer virus can range in severity: some may cause only mildly annoying effects while others can damage your hardware, software or files. A computer virus is one kind of threat to the security and integrity of computer systems. A Computer virus can cause the loss or alteration of programs or data, and can compromise their Confidentiality. A computer virus can spread from program to program, and from system to system, without direct human intervention.</p> <p>4. Pornography Child Pornography is a very inhuman and serious cybercrime offence. It</p>	<p>4M</p> <p><i>Each Point explanat ion 1M</i></p>
------------	--	---



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>includes the following:</p> <p>Any photograph that can be considered obscene and/or unsuitable for the age of child viewer.</p> <p>Film, video, picture. Computer generated image or picture of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct .Internet is the most frequently used tool for such criminals to reach children and practice child sex abuse. The spreading use internet and its easy accessibility to children has made them viable victim to cybercrime. There is a type of humans called Pedophiles who usually allure the children by obscene Pornographic contents and then they approach them for sex. Then they take their naked photographs while having sex. Such people sometime misguide children telling them that they are of the same age and win their confidence. Then they exploit the children either by forcing them to have sex or selling their pictures over internet.</p> <p>5. Spam</p> <p>Spam or Junk mail, is the (unwanted) sending out of mass emails for commercial or fraudulent purposes, which is unethical and illegal. Anti-Spam laws are being enforced in most countries which will hopefully limit the use of annoying electronic communications.</p> <p>6. Spying</p> <p>Credit Card copying (Skimming) is another cyber crime that comes under spying as well as fraud. As a person swipes his card at the ATM, or presents his card at a restaurant or shop for billing, the swipe machine may have a skimmer attached to it which transfers confidential information to the card to a third party, other than the credit card company.</p> <p>7. Obscene or offensive content</p> <p>Obscenity becomes a criminal activity where creating, distributing, accessing and spreading obscene material exploits human beings in any manner, especially when it is accessed by children.</p> <p>8. Mail Bombs</p> <p>Email —bombing" is characterized by abusers repeatedly sending an identical email message to a particular address. A mail bomb is the sending of a massive amount of email to a specific person or system. A huge amount of mail may simply fill up the recipient_s disk space on the server or, in some cases, may be too much for a server to handle</p>	
--	--	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>and may cause the server to stop functioning. Mail bombs not only inconvenience the intended target but they are also likely to inconvenience everybody using the server. Senders of mail bombs should be wary of exposing themselves to reciprocal mail bombs or to legal actions.</p> <p>9. Bug Exploits: An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or something electronic (usually computerized). Such behavior frequently includes things like gaining control of a computer system.</p>	
4.	<p>a) i) Ans.</p>	<p>Attempt any three of the following: Describe any four strategies of “Risk Control”. Risk control is the application of controls to reduce the risks to an organization's data and information systems. <i>It includes four strategies:</i> 1. Defend the defend control strategy attempts to prevent the exploitation of the vulnerability. This is the preferred approach and is accomplished by means of countering threats, removing vulnerabilities from assets, limiting access to assets, and adding protective safeguards. 2. The transfer control strategy attempts to shift risk to other assets, other processes, or other organizations. 3. The terminate control strategy directs the organization to avoid those business activities that introduce uncontrollable risks the mitigate control strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation. 4. The accept control strategy is the choice to do nothing to protect a vulnerability and to accept the outcome of its exploitation.</p>	<p>12 4M</p> <p><i>Any four strategies of risk control</i> 4M</p>
	<p>ii) Ans.</p>	<p>Explain ‘Virtual Private Network’ with neat sketch. Virtual Private Network (VPN): VPN is a mechanism of employing encryption, authentication and integrity protection so that we can use a public network (the Internet) as Information Technology it is a private network. VPN offers high amount of security and yet does not require any special cabling on behalf of the organization that wants to use it. Thus VPN combines the advantages of public network (cheap and easily available) with those of a private network (secure and reliable). Suppose an organization has two networks, Network 1 and Network 2 which are</p>	<p>4M</p> <p><i>Explanation 2M</i></p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

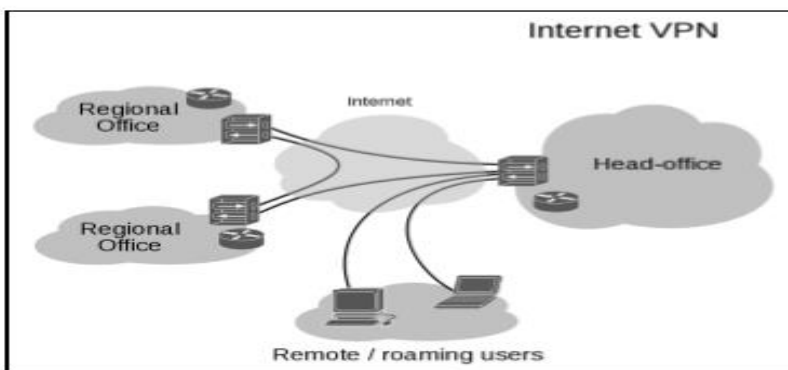
WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

physically apart from each other and we want to connect them using the VPN approach. In such case we set up two firewalls, Firewall1 and Firewall2



*Diagram
2M*

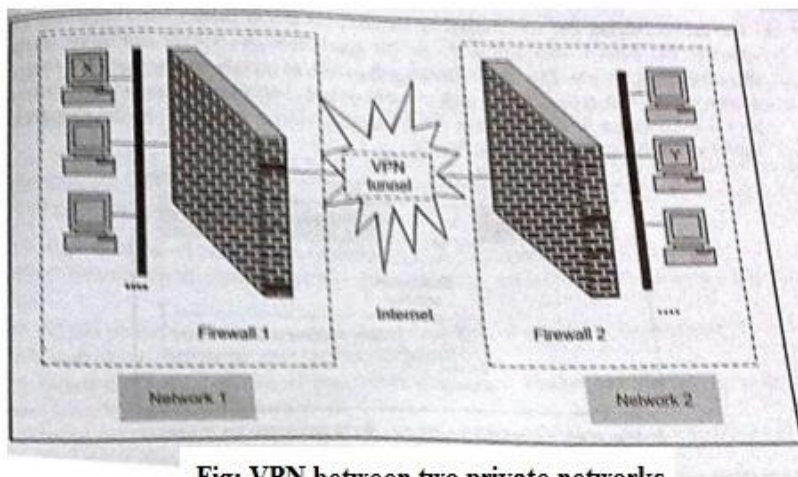
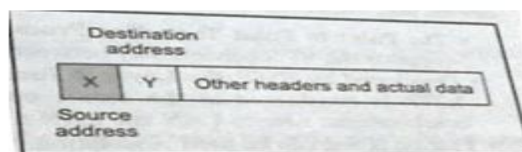


Fig: VPN between two private networks

Let us assume that host X on Network 1 wants to send a data packet to host Y on Network 2. This transmission would work as follows:
Host X creates the packet, inserts its own IP address as the source address and the IP address of host Y as the destination address.

Step 1: Original Packet





MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

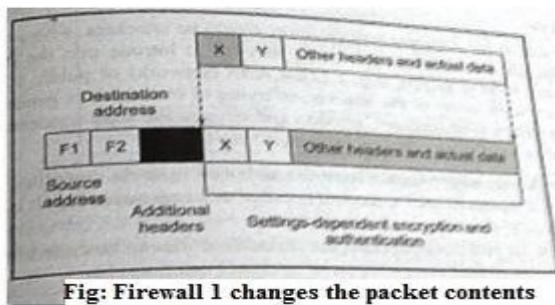
WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

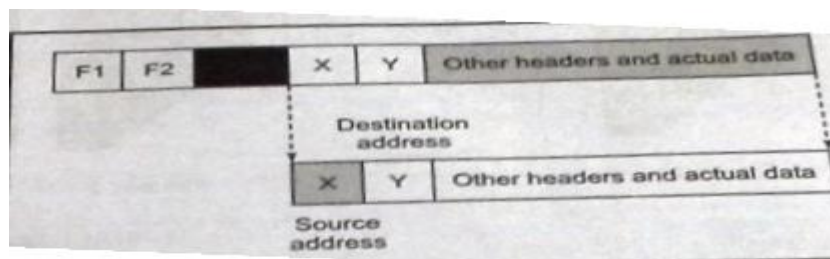
17518

2) The packet reaches Firewall 1. As we know, Firewall1 now adds new headers to the packet. In these new headers it changes the source IP address of the packet from that of host X to its own address (i.e. the IP address of Firewall1 say F1). It also changes the destination IP address of the packet from that of host Y to the IP address of Firewall say F2). It also performs the packet encryption and authentication depending on the settings and send the modified packet over the Internet.



Step 2 Firewall 1 changes the packet contents

3) The packet reaches Firewall2 over the Internet via one or more routers. Firewall2 discards the outer header and performs the appropriate decryption and other cryptographic functions as necessary. This yields the original packet as was created by host X in step 1. It looks for the destination and delivers the packet to host Y. Step 3: Firewall 2 retrieves the original packet contents.



- 1) PPTP (Point to Point Tunneling Protocol) It is used on Windows NT Systems. It mainly supports the VPN connectivity between a single user and a LAN.
- 2) L2TP (Layer 2 Tunneling Protocol) L2TP is considered as the secure open standard for VPN connections. It works for both combinations: user to LAN and Lan-to-Lan.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	3) IPSEC This is used between two communicating devices.	
iii) Ans.	<p>Explain ‘Trusted Computing Base’.</p> <p>The trusted computing base (TCB) is the sum total of all software and hardware required to enforce security</p> <ol style="list-style-type: none"> Typically, all of hardware, the core OS that is involved in protection, and all programs that operate with system privileges Desirable properties: – Small – Separable, well-defined – Independently-auditable Reference Monitor. A reference monitor is a separable module that enforces access control decisions All sensitive operations are routed through the reference monitor <div data-bbox="380 806 1240 1310" data-label="Diagram"> </div> <ol style="list-style-type: none"> The monitor then decides if the operation should proceed. It stands between Subjects and Objects and its role is to verify the subject, meets the minimum requirements for an access to an object as shown in figure. In Unix/Linux security kernel acts as a Reference Monitor which will handle all user application requests for access to system resources. In trusted system Object is something that people want to access. These objects (data) are labeled according to their level of sensitivity. Subjects (users) should have same level of classification while accessing object. <p>The reference monitor has three properties:</p> <ol style="list-style-type: none"> It cannot be bypassed and controls all access. It cannot be altered and is protected from modification or change. It can be verified and tested to be correct. 	<p>4M</p> <p><i>Explanation with neat diagram</i> 4M</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<div>iv) Ans.</div>	<div>Explain ‘One Time Pad’ with suitable example. One time pad also known as Vernam Cipher, is implemented using random set of non- repeating characters as the input cipher text. The most significant point here is that once an input cipher text for transposition is used, it is never used again for any other messages hence the name one time pad. The length of the input cipher text is equal to the length of the original plain text. The algorithm used in the Vernam cipher / one time pad is described as follows: 1. Treat each plain text alphabet as a number in an increasing sequence i.e. A = 0, B = 1, ...Z =25. 2. Do the same for each character of the input cipher text. 3. Add each number corresponding to the plain text alphabet to the corresponding input cipher text alphabet number. 4. If the sum thus produced is greater than 26, then subtract 26 from it. 5. Translate each number of the sum back to the corresponding alphabet. This gives the output cipher text. Example: Message: WE LIVE IN A WORLD FULL OF BEAUTY The key is given as: Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ Solution:<table><tr><td>PLAINTEXT</td><td>W</td><td>E</td><td>L</td><td>I</td><td>V</td><td>E</td><td>I</td><td>N</td><td>A</td><td>W</td><td>O</td><td>R</td><td>L</td><td>D</td><td>F</td><td>U</td><td>L</td><td>O</td><td>F</td><td>B</td><td>E</td><td>A</td><td>U</td><td>T</td><td>Y</td></tr><tr><td></td><td>22</td><td>04</td><td>11</td><td>8</td><td>21</td><td>4</td><td>8</td><td>13</td><td>0</td><td>22</td><td>14</td><td>17</td><td>11</td><td>3</td><td>5</td><td>20</td><td>11</td><td>11</td><td>14</td><td>5</td><td>1</td><td>4</td><td>0</td><td>20</td><td>19</td><td>24</td></tr><tr><td>OTP KEY</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td></tr><tr><td></td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td></tr><tr><td>RESULT</td><td>22</td><td>5</td><td>13</td><td>11</td><td>25</td><td>9</td><td>14</td><td>20</td><td>8</td><td>31</td><td>24</td><td>28</td><td>23</td><td>16</td><td>19</td><td>35</td><td>27</td><td>28</td><td>32</td><td>24</td><td>21</td><td>25</td><td>22</td><td>43</td><td>43</td><td>49</td></tr><tr><td>MOD 26</td><td>22</td><td>5</td><td>13</td><td>11</td><td>25</td><td>9</td><td>14</td><td>20</td><td>8</td><td>5</td><td>24</td><td>2</td><td>23</td><td>16</td><td>19</td><td>9</td><td>1</td><td>2</td><td>6</td><td>24</td><td>21</td><td>25</td><td>22</td><td>17</td><td>17</td><td>23</td></tr><tr><td>CIPHERTEXT</td><td>W</td><td>F</td><td>N</td><td>L</td><td>Z</td><td>J</td><td>O</td><td>U</td><td>I</td><td>F</td><td>Y</td><td>C</td><td>X</td><td>Q</td><td>T</td><td>J</td><td>B</td><td>C</td><td>G</td><td>Y</td><td>V</td><td>Z</td><td>W</td><td>R</td><td>R</td><td>X</td></tr></table> The ciphertext is “WFNLZJOUIFYCXQTJBCGYVZWRRX”</div>	PLAINTEXT	W	E	L	I	V	E	I	N	A	W	O	R	L	D	F	U	L	O	F	B	E	A	U	T	Y		22	04	11	8	21	4	8	13	0	22	14	17	11	3	5	20	11	11	14	5	1	4	0	20	19	24	OTP KEY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	RESULT	22	5	13	11	25	9	14	20	8	31	24	28	23	16	19	35	27	28	32	24	21	25	22	43	43	49	MOD 26	22	5	13	11	25	9	14	20	8	5	24	2	23	16	19	9	1	2	6	24	21	25	22	17	17	23	CIPHERTEXT	W	F	N	L	Z	J	O	U	I	F	Y	C	X	Q	T	J	B	C	G	Y	V	Z	W	R	R	X	<div>4M</div> <div>Explanation 2M</div> <div>Example 2M</div>
PLAINTEXT	W	E	L	I	V	E	I	N	A	W	O	R	L	D	F	U	L	O	F	B	E	A	U	T	Y																																																																																																																																																																						
	22	04	11	8	21	4	8	13	0	22	14	17	11	3	5	20	11	11	14	5	1	4	0	20	19	24																																																																																																																																																																					
OTP KEY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z																																																																																																																																																																					
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25																																																																																																																																																																					
RESULT	22	5	13	11	25	9	14	20	8	31	24	28	23	16	19	35	27	28	32	24	21	25	22	43	43	49																																																																																																																																																																					
MOD 26	22	5	13	11	25	9	14	20	8	5	24	2	23	16	19	9	1	2	6	24	21	25	22	17	17	23																																																																																																																																																																					
CIPHERTEXT	W	F	N	L	Z	J	O	U	I	F	Y	C	X	Q	T	J	B	C	G	Y	V	Z	W	R	R	X																																																																																																																																																																					
4.	<div>b) i) Ans.</div>	<div>Attempt any one of the following: Explain working of ‘Digital Signature’ with neat sketch. Digital Signatures: 1. Digital signature is a strong method of authentication in an electronic form.</div>	<div>6 6M</div>																																																																																																																																																																																												



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

2. It includes message authentication code (MAC), hash value of a message and digital pen pad devices. It also includes cryptographically based signature protocols.
3. Digital Signature is used for authentication of the message and the sender to verify the integrity of the message.
4. Digital Signature may be in the form of text, symbol, image or audio.
5. In today's world of electronic transaction, digital signature plays a major role in authentication. For example, one can fill his income tax return online using his digital signature, which avoids the use of paper and makes the process faster.
6. Asymmetric key encryption techniques and public key infrastructure are used in digital signature.
7. Digital signature algorithms are divided into two parts-
 - a. Signing part: It allows the sender to create his digital signature.
 - b. Verification part: It is used by the receiver for verifying the signature after receiving the message.

Explanation 4M

Generation and Verification of digital signatures:

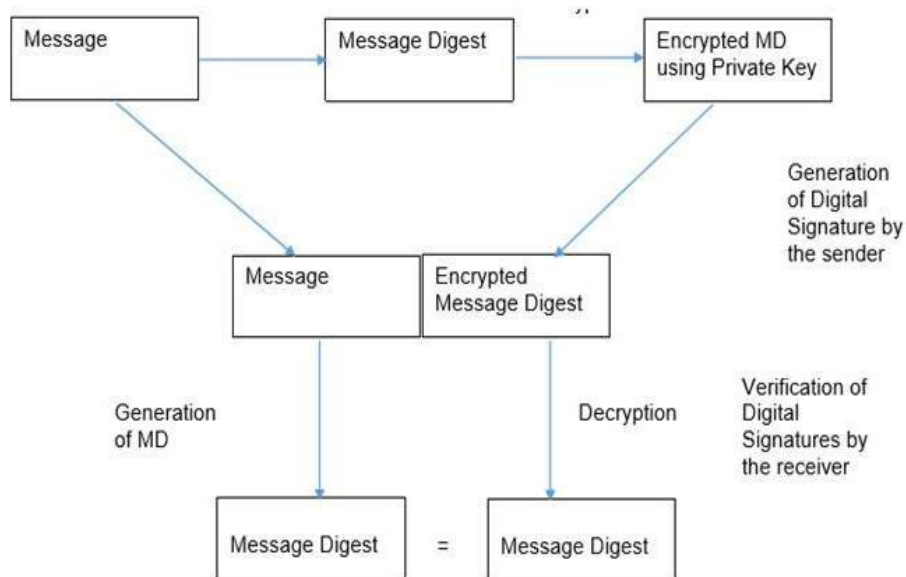


Diagram 2M

Procedure:

1. Message digest is used to generate the signature. The message digest (MD) is calculated from the plaintext or message.
2. The message digest is encrypted using user's private key.



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>3. Then, the sender sends this encrypted message digest with the plaintext or message to the receiver.</p> <p>4. The receiver calculates the message digest from the plain text or message he received.</p> <p>5. Receiver decrypts the encrypted message digest using the sender's public key. If both the MDs are not same then the plaintext or message is modified after signing.</p>	
	<p>ii) Ans.</p>	<p>Describe any six 'authentication protocols'.</p> <p>1) CHAP: It is a Challenge Handshake Authentication Protocol. This protocol is used by servers to validate the identity of remote client. CHAP verifies the identity by using 3- way handshaking and by using shared secret.</p> <p>After establishment of link, the server sends a challenge message to the client.</p> <p>Then client responds with a value obtained by using a one-way hash function.</p> <p>Server compares the response i.e. hash value with its own calculated hash value.</p> <p>If the value matches, then the authentication is acknowledged or else the connection is terminated.</p> <p>2) EAP: It is Extensible Authentication Protocol and mainly used for wireless networks and point to point connections. It may support various authentication mechanisms like tokens, certificate, one-time password, smart cards etc. In EAP protocol</p> <ul style="list-style-type: none"> • A user requests connection to WLAN through an access point. • Then the access point requests identification (ID) data from the user and transmits that data to an authentication server. • The authentication server then request the access point for proof of the validity of the ID. • After the verification from the user, access point sends it back to the authentication server and the user is connected to the network. <p>3) PAP: It is Password Authentication Protocol. It is used by Point to Point Protocol to validate users before allowing them access to server resources. In this protocol, a user's name and password are transmitted over a network and compared to a table of name- password pairs. It is a two way handshaking protocol.</p> <ul style="list-style-type: none"> • Client sends username and password. • Server sends "authentication-ack", if credentials are OK or 	<p>6M</p> <p><i>Descript ion of any six protocol 1M each</i></p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p style="text-align: center;">“authentication-nak”.</p> <p>4) SPAP: It is Shiva Password Authentication Protocol and it is an encrypting authentication protocol used by Shiva remote access servers. SPAP offers a higher level of security than other authentication protocols such as PAP, but it is not as secure as CHAP.</p> <p>5) DES: It is a Data Encryption Standard (DES) is the classic among the symmetric block cipher algorithms. DES was developed in the 1970s as a US-government standard for protecting non-classified information. DES encrypts 64-bit clear-text blocks under the control of 56-bit keys. Each key is extended by a parity byte to give a 64-bit working key. It uses both substitutions as well as transposition techniques of cryptography.</p> <p>6) RADIUS: It is a Remote Authentication Dial-In User Service protocol. It is a client/server protocol and used for authentication and authorization of users who are dialing in remotely to servers on the network.</p> <ul style="list-style-type: none">• RADIUS client sends username and encrypted password to the RADIUS server.• RADIUS server responds with Accept, Reject, or Challenge.• The RADIUS client acts upon services and services parameters bundled with Accept or Reject. <p>7) S/KEY: It is a one-time password system developed for operating systems like UNIS. One-time password allows you to log on only once with a password, after which that password is no longer valid. Instead of memorizing passwords, list of passwords are given and that may be maintained by hardware device. Each time you login, you ask the hardware device for the next password.</p> <p>8) TACACS: It is a Terminal Access Controller Access Control System. It is an older authentication protocol used mainly in UNIX networks. It allows a remote access server to pass a user's login password to an authentication server to check whether access can be allowed to a given system or not. TACACS is an encryption protocol and therefore less secure.</p> <p>9) MS-CHAP(MD4): It is a Microsoft Challenge Handshake</p>	
--	---	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>Authentication Protocol (MS-CHAP). It is based on CHAP and was developed to authenticate remote Windows- based workstations. It uses the Message Digest 4 (MD4) hashing algorithm and the Data Encryption Standard (DES) encryption algorithm to generate the challenge and response. It also provides mechanisms for reporting connection errors and for changing the user's password. It only works on Microsoft Systems.</p> <p>10) SKID (SKID2 and SKID3): SKID2 and SKID3 are secret key identification protocols. SKID2 provides unilateral entity authentication whereas SKID3 provides mutual entity authentication.</p>	
5.	<p>i) Ans.</p>	<p>Attempt any two of the following: Describe 'ITACT- 2000'.</p> <p>The IT Act 2000 gives very good solution to the cyber crimes these solutions are provided in the following ways. In this Act several sections and Chapters are there which are defined in the following manner:</p> <p>1. Chapter 1 the preliminary chapter of IT Act 2000 gives all of the information about the short title, territory up to which it is extendable, and the basic application of related laws.</p> <p>2. Chapter 2 to 7 of this Act defines 'access', 'addressee', 'adjudicating officer', 'affixing digital signature', 'Asymmetric Cryptography', 'cyber', 'computer', 'digital signature', 'Digital Signature Certificate' and other numerous basic terms, which are defined in its appendix.</p> <p>3. Other chapters of this Act define those crimes which can be considered as cognizable offences, i.e. for which the police can arrest the wrongdoer immediately.</p> <p>4. Section 80 of this Act gives a freedom to the police officer to search, arrest the offender who is indulged in that crime or going to commit it.</p> <p>5. Section 65 to 70 covers all of the cognizable offences, namely, 'tampering of documents', 'hacking of the personal computer', 'obscene information transmission or publication', 'failure of compliance by certifying authority or its employees, of orders of the Controller of certifying authorities', 'Access or attempt to access by any unauthorized person, a protected system notified by Govt. in the Official Gazette' in which non-bailable warrant is issued or no warrant is required.</p> <p>6. Section 71 indicates the offence 'Misrepresentation of material fact</p>	<p>16 8M</p> <p>Any relevant 6 points 6M</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>from the controller or Certifying Authority for obtaining any license or Digital Signature Certificate’.</p> <div><p>Some IT Act Offences</p><table><tr><th>Section</th><th>Brief nature of offence</th><th>Punishment</th><th>Cognizable/ Non- Cognizable</th><th>Bailable/non- bailable</th></tr><tr><td>65</td><td>Tampering of documents</td><td>Imprisonment up to 3 yrs or fine up to 2 lakh or both.</td><td>Cognizable</td><td>Non-bailable</td></tr><tr><td>66</td><td>Hacking the personal computer</td><td>Imprisonment up to 3 yrs or fine up to 2 lakh, or both.</td><td>Cognizable</td><td>Non-bailable</td></tr><tr><td>67</td><td>Obscene information transmission or publication</td><td>In 1st conviction Imprisonment may be extended up to 5 yrs and a fine up to 1 lakh. On second /subsequent conviction with Imprisonment may be extended up to 10 yrs and fine up to 2 lakh.</td><td>Cognizable</td><td>Non-bailable</td></tr><tr><td>68</td><td>Failure of compliance by certifying Authority or its employees, of orders of the Controller of certifying authorities</td><td>Imprisonment, not exceeding 3 yrs or fine not exceeding 2 lakh, or both.</td><td>Cognizable</td><td>Non-bailable</td></tr><tr><td>69</td><td>Failure by any person to assist any govt. agency which is intercepting any information transmitted through any computer resource to decrypt information</td><td>Imprisonment, which may be extended to 7 yrs.</td><td>Cognizable</td><td>Non-bailable</td></tr><tr><td>70</td><td>Access or attempt to access by any unauthorized person, a protected system notified by Govt. in the Official Gazette.</td><td>Imprisonment, which may be extended to 10 yrs. and fine.</td><td>Cognizable</td><td>Non-bailable</td></tr><tr><td>71</td><td>Misrepresentation of material fact from the controller or Certifying Authority for obtaining any license or Digital Signature Certificate.</td><td>Imprisonment, which may be extended to 2 yrs, or fine extended up to 1 lakh, or both.</td><td>Non-Cognizable</td><td>Bailable</td></tr></table></div>	Section	Brief nature of offence	Punishment	Cognizable/ Non- Cognizable	Bailable/non- bailable	65	Tampering of documents	Imprisonment up to 3 yrs or fine up to 2 lakh or both.	Cognizable	Non-bailable	66	Hacking the personal computer	Imprisonment up to 3 yrs or fine up to 2 lakh, or both.	Cognizable	Non-bailable	67	Obscene information transmission or publication	In 1 st conviction Imprisonment may be extended up to 5 yrs and a fine up to 1 lakh. On second /subsequent conviction with Imprisonment may be extended up to 10 yrs and fine up to 2 lakh.	Cognizable	Non-bailable	68	Failure of compliance by certifying Authority or its employees, of orders of the Controller of certifying authorities	Imprisonment, not exceeding 3 yrs or fine not exceeding 2 lakh, or both.	Cognizable	Non-bailable	69	Failure by any person to assist any govt. agency which is intercepting any information transmitted through any computer resource to decrypt information	Imprisonment, which may be extended to 7 yrs.	Cognizable	Non-bailable	70	Access or attempt to access by any unauthorized person, a protected system notified by Govt. in the Official Gazette.	Imprisonment, which may be extended to 10 yrs. and fine.	Cognizable	Non-bailable	71	Misrepresentation of material fact from the controller or Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment, which may be extended to 2 yrs, or fine extended up to 1 lakh, or both.	Non-Cognizable	Bailable	<p>Any two offence s 2M</p>
Section	Brief nature of offence	Punishment	Cognizable/ Non- Cognizable	Bailable/non- bailable																																						
65	Tampering of documents	Imprisonment up to 3 yrs or fine up to 2 lakh or both.	Cognizable	Non-bailable																																						
66	Hacking the personal computer	Imprisonment up to 3 yrs or fine up to 2 lakh, or both.	Cognizable	Non-bailable																																						
67	Obscene information transmission or publication	In 1 st conviction Imprisonment may be extended up to 5 yrs and a fine up to 1 lakh. On second /subsequent conviction with Imprisonment may be extended up to 10 yrs and fine up to 2 lakh.	Cognizable	Non-bailable																																						
68	Failure of compliance by certifying Authority or its employees, of orders of the Controller of certifying authorities	Imprisonment, not exceeding 3 yrs or fine not exceeding 2 lakh, or both.	Cognizable	Non-bailable																																						
69	Failure by any person to assist any govt. agency which is intercepting any information transmitted through any computer resource to decrypt information	Imprisonment, which may be extended to 7 yrs.	Cognizable	Non-bailable																																						
70	Access or attempt to access by any unauthorized person, a protected system notified by Govt. in the Official Gazette.	Imprisonment, which may be extended to 10 yrs. and fine.	Cognizable	Non-bailable																																						
71	Misrepresentation of material fact from the controller or Certifying Authority for obtaining any license or Digital Signature Certificate.	Imprisonment, which may be extended to 2 yrs, or fine extended up to 1 lakh, or both.	Non-Cognizable	Bailable																																						
<p>ii) Ans.</p>	<p>Explain stepwise working of ‘Kerberos’ with neat sketch.</p> <p>Kerberos is a network authentication protocol and it is designed to provide strong authentication for Client /Server Applications. It uses secret- key Cryptography.</p> <p>Kerberos is a protocol which was created by MIT as a solution to network security problems. It uses strong cryptography hence a client can prove its identity to a server and vice versa over an in secure network connection.</p> <p>Basics of Kerberos</p> <p>The basic Kerberos Model has the following participants:</p> <ul style="list-style-type: none">• A Client• A Server• A key distribution center (KDC) consisting of,<ul style="list-style-type: none">○ An Authentication Server (AS)	<p>8M</p> <p>correct steps descripti on 4M</p>																																								



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>○ A Ticket Granting Server (TGS)</p> <p>○ Database with strong passwords.</p> <p>Kerberos Process: Suppose client wants to communicate with server.</p> <ul style="list-style-type: none"> • User logs in to gain network access. • This user will need a ticket to get tickets (TGT). • In kerberos, the key distribution center (KDC) has an authentication service (AS) which gives TGT such that user has to decrypt the response with the password hash. • The user then sends the same and asks for service ticket. • The ticket granting service (TGS) will send service ticket. <p>This service ticket is used to authenticate the user at the network server side so that the user can make use of the server or client server session begins.</p> <p style="text-align: center;">The kerberos ticket exchange process</p>	<p><i>Diagram with correct steps 4M</i></p>
<p>iii) Ans.</p>	<p>Describe various ways to ‘Physical Access Control’.</p> <p>Perimeter Security Controls: Controls on the perimeter of the data center are designed to prevent unauthorized access to the facility. These types of controls, may have different “states” or behaviors based on the time of day or the day of the month. A gate may allow controlled access during the day but be locked or closed at night, for example.</p>	<p>8M</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>Fences in some respects model the various levels of security in the virtual world. Turnstiles are less effective than either gates or fences. Mantraps, as the name implies, are enclosed areas with a secure door on either end that literally “trap” an individual between doors.</p> <p>Badging: Issued by a site security office, the photo identification badge is a perimeter security control mechanism that not only authenticates an individual but also continues to identify the individual while inside the facility. Most sites issuing photo identification require that the individual displays the badge where it is most visible, usually on the upper torso. The badge alone is no guarantee that unauthorized individual are denied access- badges can be stolen and photos replaced- but combined with other perimeter controls, the badge offers a familiar and comfortable sense of security in most organizations.</p> <p>Keys and Combination Locks: Keys and combination locks are how most people know physical security, mainly because they are the least complicated and expensive devices. Beyond the mechanical door lock opened with a key, locks are now programmable and opened with a combination of keys (e.g., the five-key pushbutton lock once popular in IT operations), a security badge with a magnetic strip, or some other mechanism. Locks are typically unguarded and are meant to delay an intruder, not absolutely deny him access. For that reason, you rarely find these devices any more in areas where a high level of access authorization is required.</p> <p>Security Dogs: What some home security experts don’t tell you is that dogs are not just a man’s best friend, but they can also make great security guards! Dogs can be unflinchingly loyal and rely on all of their senses to detect intruders. They can also be trained to perform specialized services such as sniffing out drugs or explosives at airports or alerting the blind to fire before it engulfs them. The image of the German shepherd tethered to the door behind an auto junkyard may be the first thing that comes to mind when thinking about security dogs, but dogs are a highly effective and threatening perimeter security control when handled properly and humanely.</p> <p>Lighting:</p>	<p><i>Any four relevant controls each 2M</i></p>
--	---	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>Lighting is another form of perimeter protection that discourages intruders or other unauthorized individuals from entering restricted areas. You are likely familiar with how shopping malls use streetlights to discourage parking lot break-ins, and many homeowners have motion-detector lights installed on garages and back porches. Critical buildings and installations should use some form of lighting as a deterrent, whether it be floodlights, streetlight, or searchlights. According to the National Institute of Standards and Technology, critical areas (e.g., fire escapes, emergency exits, and so forth) require safety lighting to be mounted 8 feet high and burn with a candlepower of 2 candelas (the equivalent of a strong spotlight).</p> <p>Smart Cards:</p> <p>A smart card resembles a regular payment (credit) card with the major difference that it carries a semiconductor chip with logic and nonvolatile memory. Unlike a security access card (badge with magnetic strip), the smart card has many purposes, including storing value for consumer purchases, medical identification, travel ticketing and identification, and building access control. The card may also store software that detects unauthorized tampering and intrusions to the chip itself and, if detected, can lock or destroy the contents of the chip to prevent disclosure or unauthorized uses.</p> <p>Alarm Systems:</p> <p>The implementation of a series of the aforementioned intrusion detectors is referred to as an alarm system. A local alarm system sets off an alarm on the premises, alerting guards on the premises to respond. Private security firms manage central-station systems, such as home alarms from ADT and other well-known home security companies. They monitor a system 24 hours a day and respond to alerts from a central location.</p> <p>Company established, owned, and operated alarm systems (also called dedicated alarm systems) resemble a commercial central station system in that it serves many customers but differs because the focus is on the company exclusively. Dedicated systems may be more sophisticated than a local alarm system and share many of the same features as the centralized version. Additional alarms may be triggered at police or fire stations, with the permission and knowledge of the company being protected.</p> <p>Biometrics:</p>	
--	--	--



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>The use of biometrics (Greek for “life measurements”) in conjunction with more standard forms of authentication such as fixed passwords and PINs is beginning to attract attention as the cost of the technology decreases and its sophistication increases. In fact, the traditional scheme of password-based computer security could lose stature as the use of smart card-based cryptographic credentials and biometrics authentication become commercially viable. Some companies such as the American Biometrics Corporation claim that using an individual’s unique physical characteristics along with other identification and authentication (I & A) techniques can almost unequivocally authenticate a user. Biometrics authentication uses characteristics of the human face, eyes, voice, fingerprints, hands, signature, and even body temperature, each technique having its own strengths and weaknesses.</p>	
6.	<p>i) Ans.</p>	<p>Attempt any four of the following: Describe ‘Cyber crime investigation process’. Cyber crime investigation process: The computer crime investigation should start immediately following the report of any alleged criminal activity. Many processes ranging from reporting and containment to analysis and eradication should be accomplished as soon as possible after the attack. An incident response plan should be formulated, and a Computer Emergency Response Team (CERT) should be organized before the attack. The incident response plan will help set the objective of the investigation and will identify each of the steps in the investigative process. Detection and Containment Before any investigation can take place, the system intrusion or abusive conduct must first be detected. Report to Management All incidents should be reported to management as soon as possible. Prompt internal reporting is imperative to collect and preserve potential evidence. It is important that information about the investigation be limited to as few people as possible.. Determine if Disclosure is Required Determine if a disclosure is required or warranted due to laws or regulations. Investigation Considerations Once the preliminary investigation is complete and the victim organization has made a decision related to disclosure, the organization must decide on the next course of action.</p>	<p>16 4M</p> <p><i>Any relevant descripti on 4M</i></p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

		<p>Obtaining and Serving Search Warrants. If it is believed that the suspect has crucial evidence at his or her home or office, a search warrant will be required to seize the evidence.</p> <p>Surveillance Two forms of surveillance are used in computer crime investigations: physical and computer. Physical surveillance can be generated at the time of the abuse, through CCTV security cameras, or after the fact. Computer surveillance is achieved in a number of ways. It is done passively through audit logs or actively by way of electronic monitoring.</p> <p>The goal of the investigation is to identify all available facts related to the case. The investigative report should provide a detailed account of the incident, highlighting any discrepancies in witness statements. The report should be a well-organized document that contains a description of the incident.</p> <p>Computer forensics is the study of computer technology as it relates to the law. This generally means analyzing the system by using a variety of forensic tools & processes, and that the examination of the suspect system may lead to other victims and other suspects.</p>	
	<p>ii) Ans.</p>	<p>Describe 'Information Technology Infrastructure Library (ITIL). The Information Technology Infrastructure Library (ITIL) is a collection of best practices in IT service management (ITSM), and focuses on the service processes of IT and considers the central role of the user. It was developed by the United Kingdom's Office of Government Commerce (OGC). Since 2005, ITIL has evolved into ISO/IEC 20000, which is an international standard within ITSM.</p> <p>An ITIL service management self-assessment can be conducted with the help of an online questionnaire maintained on the website of the IT Service Management Forum. The self-assessment questionnaire helps evaluate the following management areas:</p> <ol style="list-style-type: none"> Service Level Management Financial Management Capacity Management Service Continuity Management Availability Management Service Desk Incident Management Problem Management Configuration Management 	<p>4M</p> <p>Relevant description with neat diagram 4M</p>



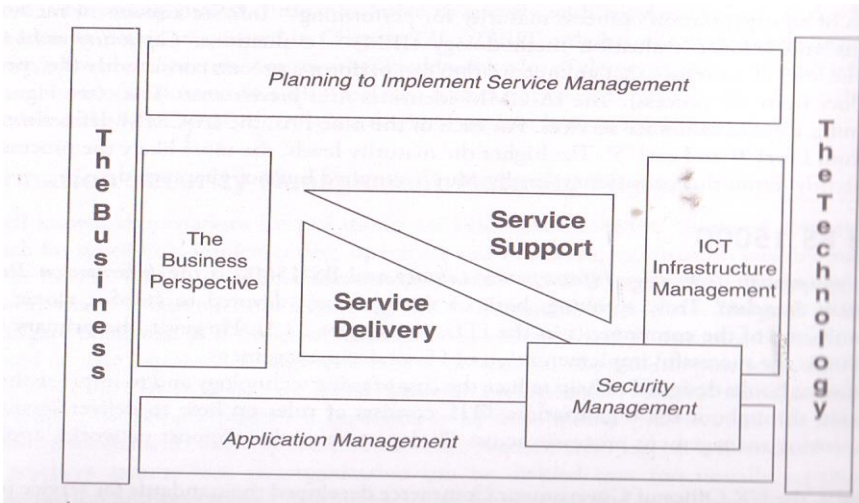
MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>j) Change Management k) Release Management</p> 	
<p>iii) Ans.</p>	<p>Explain ITSEC (Information Technology Security Evaluation Criteria) with its target of evaluation levels.</p> <p>ITSEC is developed by European country for security evaluation criteria.</p> <ol style="list-style-type: none"> ITSEC focuses more on integrity and availability. It tries to provide a uniform approach to product and system. ITSEC will also provide security targets like: <ol style="list-style-type: none"> Policy for system security Required mechanism for security Required rating to claim for minimum strength Level for evaluating targets –functional as well as evaluation <p>ITSEC classes contain hierarchical structure where every class will be added to the class above it. This class contains some particular function.</p> <p>F-IN This class will provide high integrity. F-AV This class will provide high availability. F-DI This class will provide high data integrity. F-DX This class is used for networks. Of provide high integrity while exchanging data in networking.</p>	<p>4M</p> <p>ITSEC explanation 2M</p> <p>Evaluative levels 2M</p>



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<p>ITSEC uses following I classes from E0 to E6 to evaluate the security.</p> <p>E0 – Minimal protection.</p> <p>E1 – Security target and informal architecture design must be produced.</p> <p>E2 – An informal detail design and test document must be produced.</p> <p>E3 – Source code or hardware drawing to be produced. Correspondence must be shown between source codes of detailed design.</p> <p>E4 – Formal model of Security and Semi – formal specification of Security function architecture and detailed design to be produced.</p> <p>E5 – Architecture design explain the inter relationship between security component.</p> <p>E6 – Formal description of architecture and Security function to be produced.</p> <p>Information could leak from those users who were cleared to see it, down to those users who are not.</p>											
<p>iv)</p> <p>Ans.</p>	<p>Differentiate between – ‘Qualitative Risk Analysis’ and ‘Quantitative Risk Analysis’.</p> <table><tr><th>Qualitative Risk Analysis</th><th>Quantitative Risk Analysis</th></tr><tr><td>1.It is a collaborative process of assigning relative values to assets, assessing their risk exposure, and estimating the cost of controlling the risk.</td><td>1. It is a process for assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats.</td></tr><tr><td>2. It utilizes relative measures and approximate costs rather than precise valuation and cost determination.</td><td>2. It is used to determine potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk</td></tr><tr><td>3. Assets can be rated based on criticality - very important, important, not-important etc. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc. Threats can be rated based on scale of likely - likely, unlikely, very likely etc.</td><td>3. Assets can be rated as the cost of replacing an asset, the cost of lost productivity, or the cost of diminished brand reputation.</td></tr><tr><td>4. In this 100% qualitative risk analysis is feasible.</td><td>4. In this 100% quantitative risk analysis is not possible.</td></tr></table>	Qualitative Risk Analysis	Quantitative Risk Analysis	1.It is a collaborative process of assigning relative values to assets, assessing their risk exposure, and estimating the cost of controlling the risk.	1. It is a process for assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats.	2. It utilizes relative measures and approximate costs rather than precise valuation and cost determination.	2. It is used to determine potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk	3. Assets can be rated based on criticality - very important, important, not-important etc. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc. Threats can be rated based on scale of likely - likely, unlikely, very likely etc.	3. Assets can be rated as the cost of replacing an asset, the cost of lost productivity, or the cost of diminished brand reputation.	4. In this 100% qualitative risk analysis is feasible.	4. In this 100% quantitative risk analysis is not possible.	<p>4M</p> <p>Any 4 points 1M each</p>
Qualitative Risk Analysis	Quantitative Risk Analysis											
1.It is a collaborative process of assigning relative values to assets, assessing their risk exposure, and estimating the cost of controlling the risk.	1. It is a process for assigning a numeric value to the probability of loss based on known risks, on financial values of the assets and on probability of threats.											
2. It utilizes relative measures and approximate costs rather than precise valuation and cost determination.	2. It is used to determine potential direct and indirect costs to the company based on values assigned to company assets and their exposure to risk											
3. Assets can be rated based on criticality - very important, important, not-important etc. Vulnerabilities can be rated based on how it is fixed - fixed soon, should be fixed, fix if suitable etc. Threats can be rated based on scale of likely - likely, unlikely, very likely etc.	3. Assets can be rated as the cost of replacing an asset, the cost of lost productivity, or the cost of diminished brand reputation.											
4. In this 100% qualitative risk analysis is feasible.	4. In this 100% quantitative risk analysis is not possible.											



MAHARASHTRA STATE BOARD OF TECHNICAL EDUCATION
(Autonomous)
(ISO/IEC - 27001 - 2005 Certified)

WINTER – 2016 EXAMINATION

Model Answer

Subject Code:

17518

	<div>v)</div> <div>Ans.</div>	<div>Consider plain text – “INFORMATION” and convert given plain text into cipher text using ‘Caesar Cipher’ with shift of position three – Write down steps in encryption.</div> <div>Plaintext: INFORMATION</div> <div>Key: 3 (shift)</div> <div>A translation chart for the given plain text is as follows:</div> <table><tr><td>Plaintext</td><td>a</td><td>b</td><td>c</td><td>d</td><td>e</td><td>f</td><td>g</td><td>h</td><td>i</td><td>j</td><td>k</td><td>l</td><td>m</td></tr><tr><td>Ciphertext</td><td>D</td><td>E</td><td>F</td><td>G</td><td>H</td><td>I</td><td>J</td><td>K</td><td>L</td><td>M</td><td>N</td><td>O</td><td>P</td></tr><tr><td>Plaintext</td><td>n</td><td>o</td><td>p</td><td>q</td><td>r</td><td>s</td><td>t</td><td>u</td><td>v</td><td>w</td><td>x</td><td>y</td><td>z</td></tr><tr><td>Ciphertext</td><td>Q</td><td>R</td><td>S</td><td>T</td><td>U</td><td>V</td><td>W</td><td>X</td><td>Y</td><td>Z</td><td>A</td><td>B</td><td>C</td></tr><tr><td>Given Plaintext</td><td>I</td><td>N</td><td>F</td><td>O</td><td>R</td><td>M</td><td>A</td><td>T</td><td>I</td><td>O</td><td>N</td><td></td><td></td></tr><tr><td>Ciphertext</td><td>L</td><td>Q</td><td>I</td><td>R</td><td>U</td><td>P</td><td>D</td><td>W</td><td>L</td><td>R</td><td>Q</td><td></td><td></td></tr></table> <div>Cipher text is LQIRUPDWLRQ</div>	Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z	Ciphertext	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	Given Plaintext	I	N	F	O	R	M	A	T	I	O	N			Ciphertext	L	Q	I	R	U	P	D	W	L	R	Q			<div>4M</div> <div>Accurate full translation on chart of alphabet with accurate shift 2M, correct cipher text 2M</div>
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m																																																																										
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P																																																																										
Plaintext	n	o	p	q	r	s	t	u	v	w	x	y	z																																																																										
Ciphertext	Q	R	S	T	U	V	W	X	Y	Z	A	B	C																																																																										
Given Plaintext	I	N	F	O	R	M	A	T	I	O	N																																																																												
Ciphertext	L	Q	I	R	U	P	D	W	L	R	Q																																																																												