1. The CIA of security essentially stands for Confidentiality, Integrity, and Availability. This is a very popular security model that covers essential security features that need to be offered by any secure system. Confidentiality refers to the technique of hiding information from those who are unauthorized to do so. Encryption and cryptography are two key methods that are incorporated to protect the confidentiality of a system. Integrity ensures that the data is unchanged and accurate representation of the original data. In many cases, attackers will try to intercept the communication, and make changes to the data. Availability refers to the ability to ensure that the data is accessible at all times to the authorized person. Sometimes, attack attempts are made to prevent users from accessing the data when they need to, which is also known as denial-of-service (Ic, n.d.).

   Confidentiality of a computer system is said to be in existence, if and only the authorized individuals are allowed to access the data stored on the system, while unauthorized users will be blocked (Panmore, 2015). Methods that are often incorporated to ensure confidentiality of an account include User IDs, passwords, biometric verifications, security tokens, data encryption, and two-factor authentication. Integrity, on the other hand, ensures the trustworthiness or consistency of data, and steps need to be taken to make sure that the data is not modified in any manner. Version control, user access controls, and file permissions, are proven methods by which integrity is maintained. Availability involves the maintenance of the hardware, and software environments, to ensure that the users have round-the-clock access to the system. Redundancy, disaster recovery plans, and regular upgrades are common techniques that are incorporated for ensuring availability (Techtarget, 2014).
2. The value of p = 7 and q = 11.

   Θ (n) = (p-1) x (q-1) = (7-1) x (11-1) = 6 x 10 = 60

   Inverse of 19 mod 60 = **19**

3. The plaintext message, in this case, is “HELLOWORD”, for which the set of integers is {9,6,13,13,16,24,16,19,13,5}. The value of p = 11 and q = 3.

   The value of N, which is the modulus is computed by p x q = 11 x 3 = 33

   The PHI is computed by (p-1) (q-1) = (11-1) (3-1) = 10 x 2 = 20

   E = 3

   E is found in a way that the GCD of PHI and E is 1. Therefore, the smallest value that was derived is 3.

   The value for D is computed by d=*e*^(-1) mod [(*p*-1)x(*q*-1)].

   D = 7

To find the ciphertext integer, the formulae used is $c = m^e \bmod n$

Message (Text)	Message (Integer)	Ciphertext Integers
H	9	3
E	6	18
L	13	19
L	13	19
O	16	4
W	24	30
O	16	4
R	19	28
L	13	19
D	5	26

4. The topic selected is - ‘Understanding the Kerberos System and Its Authentication Protocols’. Kerberos is an authentication system created at MIT, which was a part of the Athena project. Kerberos utilizes encryption technology as well as a trusted third-party, who serves as an arbitrator, to carry out secure authentication on open networks. Kerberos utilizes cryptographic tickets to prevent the transmission of plain text passwords via wires. This protocol uses a shared secret as well as trusted third party arbitrator to ensure validation of the client’s identity. Clients could be users, servers, or software pieces. The trusted 3rd party arbitrator is known as a Key Distribution Center, which is a essentially a server. This server keeps active instances of the Kerberos daemons. The shared secret, in this case, is essentially the user’s password that is changed into a cryptographic key. In the context of servers or software, random keys are generated (Tldp, n.d.).

References:

Tldp (n.d.). 2. An Overview Of A Kerberos Infrastructure. Retrieved from http://tldp.org/HOWTO/Kerberos-Infrastructure-HOWTO/overview.html

Ic (n.d.). What is Security Analysis?. Retrieved from http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm

Techtarget (2014). confidentiality, integrity, and availability (CIA triad). Retrieved from http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Panmore (2015). The CIA Triad: Confidentiality, Integrity, Availability. Retrieved from http://panmore.com/the-cia-triad-confidentiality-integrity-availability