Sheet 1 on Chapter 1

1. Draw a block diagram for the brute-force attack and give a short comment on the relation between the key-space, the speed of the attacking computer, and the time needed to break a given ciphertext. {Refer to the PowerPoint file of Assignment #1}
2. Answer the following MCQ on chapter 1

|  |  |
| --- | --- |
| 1 | .............. is the assurance that communicating entity is the one claimed  a) integrity b) confidentiality c) authentication d) non-repudiation |
| 2 | ………… attack may slow down or totally interrupt the service of a system.  a) traffic analysis b) DoS c) repudiation d) all of the above |
| 3 | ……… means that changes need to be done only by authorized entities and through authorized mechanisms.  a) integrity b) availability c) confidentiality d) authentication |
| 4 | ………… is a passive attack.  a) modification b) repudiation c) snooping d) masquerading |
| 5 | ………….. prevents either sender or receiver from denying a transmitted message.  a) data integrity b) authentication c) nonrepudiation d) access control |
| 6 | Denial of service is a/an…….….  a) passive attack b) active attack  c) attack on message integrity d) None of the above |
| 7 | In the network security model, the role of the trusted third party can be:  a) arbiter (to solve disputes) b) distributer of keys  c) encrypting/decrypting messages d) both (a) and (b) |
| 8 | Masquerade is a/an ……….  a) passive attack b) active attack  c) attack on message integrity d) both (b) and (c) |
| 9 | Modification of message contents represents a threat to ………..  a) integrity b) availability c) confidentiality d) none of the above |
| 10 | The objective of computer security is to provide … ……….. of information system resources.  a) integrity b) availability c) confidentiality d) all of the above |
| 11 | The mechanism(s) for data confidentiality are …………   1. Encryption 2. Routing control 3. Digital signature 4. Both (a) and (b) |
| 12 | 1. Assurance that data received is as sent by an authorized entity. 2. Authentication 3. Access Control 4. Data Confidentiality 5. Data Integrity |
| 13 | Resource accessible and usable.   1. Authentication 2. Data Integrity 3. Non-Repudiation 4. Availability |
| 14 | Prevention of the unauthorized use of a resource.   1. Authentication 2. Access Control 3. Data Confidentiality 4. Non-Repudiation |
| 15 | Protection against denial by one of the parties in a communication.   1. Authentication 2. Data Confidentiality 3. Non-Repudiation 4. Availability |
| 16 | Protection of data from unauthorized disclosure.   1. Authentication 2. Data Confidentiality 3. Data Integrity 4. Availability |
| 17 | In the network access control model, the gatekeeper is typically a ………   1. biometric authentication 2. username and password 3. firewall 4. all the above |
| 18 | In the network access control model, internal security controls such as ……….. are needed to ensure that only authorized users can access designated information or resources.   1. biometric authentication 2. username and password 3. firewall 4. both (a) and (b) |

1. Compute the following using modular arithmetic {For a mathematical background, refer to page 108, section 4.3 of the textbook}. Check your results with the “MOD()” function in an Excel sheet.
2. 35 mod 26
3. (4 – 21) mod 26
4. 573 mod 91
5. Compute the following using the XOR logical operator.
6. (01100101) XOR (11110000)
7. (110101) XOR (010101)
8. (1100) XOR (0111)