# Yarmouk Private University جامعة اليرموك الخاصة

****

**Faculty of Informatics & Communications Engineering كلية هندسة المعلوماتية والاتصالات**

|  |  |  |
| --- | --- | --- |
| **Course No**: CIE 530 | **Course Title**: Networks and systems security | **Exam Time**: 120 Min |
| **Credit Hours:** 3 (2 T +1 P) | **Lecturer**: Prof. Moutasem Shafa'amry | **Date** 23/1/2023 |
| **Department**: Comm & info. Eng. | **Semester**: 2023 | **Total** **Marks**: 50 Marks |

# Final Exam

**Question 1: Circle the correct choice for each of the following: (15 Marks)**

1. Reconnaissance, Eavesdropping and Port scanning are of which type of attacks
   1. Passive
   2. Active
2. DOS, Spoofing, Man in the Middle, ARP poisoning, Smurf attacks, Buffer overflow, and SQL

Injection are of which type of attacks

1. Passive
2. Active
3. PGP
4. stands for Pretty good privacy and was developed by Phil Zimmerman in 1995 and Offers authentication, confidentiality, compression, e-mail compatibility and segmentation
5. stands for Pretty gard privacy and was developed by Phil Zimmerman in 1995 and Offers authorization, confidentiality, compression, e-mail compatibility and segmentation
6. stands for Prince good privacy and was developed by Joan Daemen and Vincent Rijmen and Offers authentication, confidentiality, compression, e-mail compatibility and segmentation
7. which of the following is true about AES
   1. stands for Advanced Encryption Standard
   2. Symmetric block cipher
   3. Has a fixed block size of 128 bits
   4. Has a key size of 128, 192, or 256 bits
   5. was developed by Joan Daemen and Vincent Rijmen
   6. all of the above is correct
   7. all of the above is correct

1. RSA, DSA, Diffie-Hellman, El Gamal, Elliptic Curve and PKCS are
   1. Symmetric algorithms
   2. Single key algorithms
   3. Asymmetric algorithms

1. DES, AES, RC4, and RC6 are
2. Asymmetric algorithms
3. Symmetric algorithms

1. Transposition Cipher is
   * 1. replacing an alphabet with another character of the same alphabet set
     2. letters are just rearranged but No letters are replaced

1. Substitution cipher
   * 1. replacing an alphabet with another character of the same alphabet set
     2. letters are just rearranged but No letters are replaced

1. The possibility that a particular vulnerability will be exploited
   1. Risk
   2. Risk Analysis
   3. Risk mitigation
   4. Vulnerability

1. The process of selecting appropriate controls to reduce risk to an acceptable level a. Risk
   1. Risk Analysis
   2. Risk mitigation
   3. Vulnerability

1. Attempt to make a machine or network resource unavailable to its intended users. a. Sniffing
   1. Spoofing
   2. Hijacking
   3. Denial of Service (DoS) Attack

1. Sets up a fake device and trick others to send messages to it
   1. Hijacking
   2. Spoofing
   3. Phishing
   4. Pharming

1. Prevents unauthorized use or disclosure of information
   1. Availability
   2. Integrity
   3. Confidentiality
   4. Authorization

1. Defines the user’s rights and permissions on a system
   1. Availability
   2. Integrity
   3. Confidentiality
   4. Authorization

1. Encrypts bits of the message at a time, typically bit-wise.
   1. AES
   2. Substitution cipher
   3. Transposition Cipher
   4. Stream cipher

1. The attack in which redirect a website’s traffic to another fake site by changing the victim’s

DNS settings or hosts file is called

* 1. Sniffing
  2. Pharming
  3. Spoofing
  4. Hijacking
  5. Phishing

1. The attack in which Users(victims) are redirected to a fake website that looks genuine. When the victim supplies his account and password, this can be used by the attacker to the target site, is called
   1. Sniffing
   2. Pharming
   3. Spoofing
   4. Hijacking
   5. Phishing

1. DES is a standard block cipher with
   1. 64-bits Block size and 64-bit key size
   2. 128-bits Block size and 56-bit key size
   3. 64-bits Block size and 56-bit key size
   4. 128-bits Block size and 64-bit key size
   5. 128-bits Block size and 56-bit key size

**Question 2 Answer the following (10 Marks)**

* 1. Explain The Hill encryption algorithm (5Marks)

………………………………………………………………………………………………………………………………………………………………….

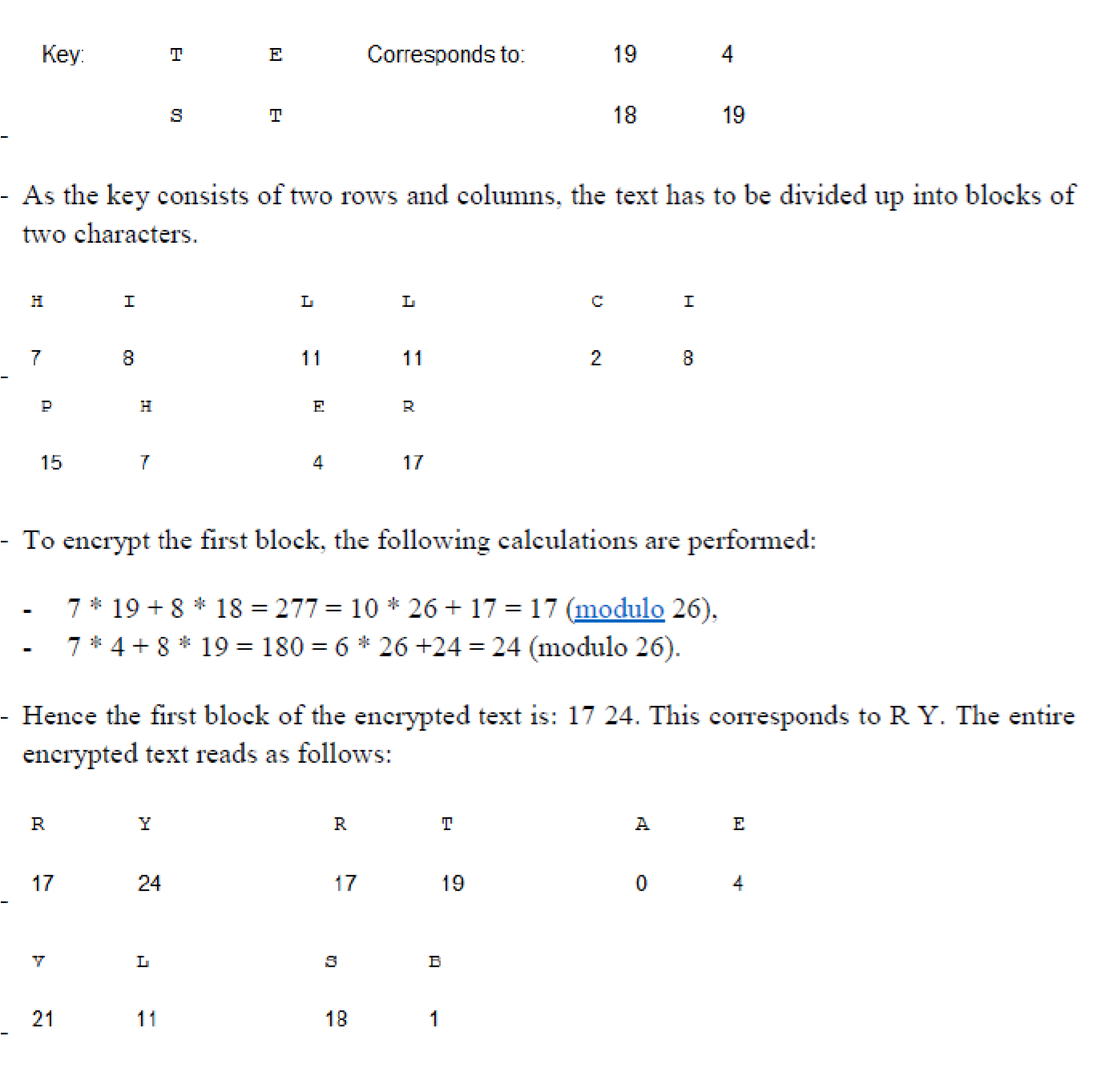
In this algorithm the key is a quadratic matrix: this means it has the same number of rows and columns. This number is called the dimension of the matrix. The plaintext is divided into blocks of equal size (one block consists of as many characters as the key has rows). The last block sometimes has too few characters: In this case the last block is padded to have the length of the matrix dimension -- by default it's filled up with the first character of the used alphabet. This algorithm operates on the numerical values of the charcters from the selected alphabet.

………………………………………………………………………………………………………………………………………………………………….

.

* 1. Encrypt the text **HILLCIPHER** with the key **TEST** using The Hill encryption algorithm

Show all steps (5 Marks)

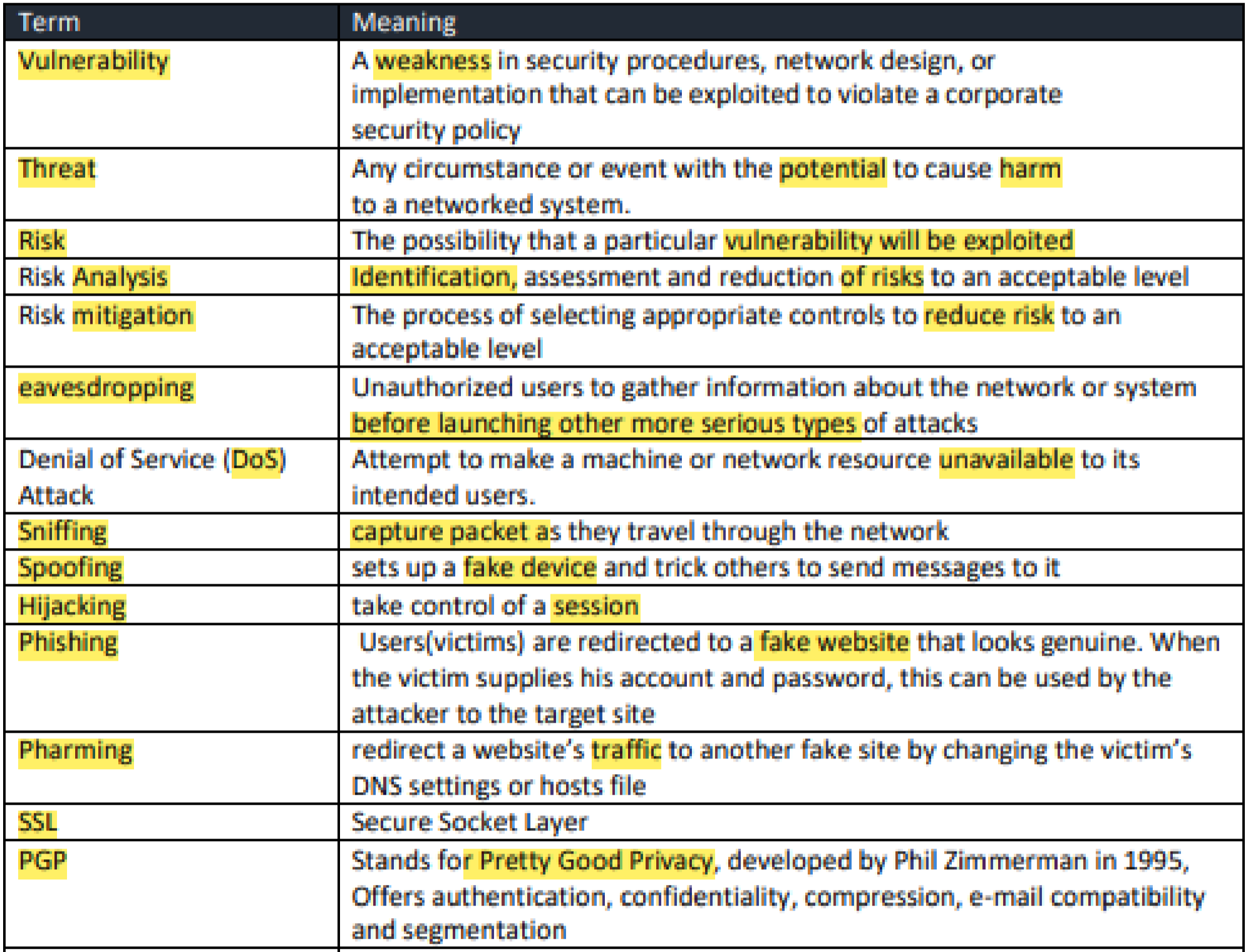


**Question 3 fill the table with 5 symmetric algorithms and their key size(10 Marks) ANSWER**

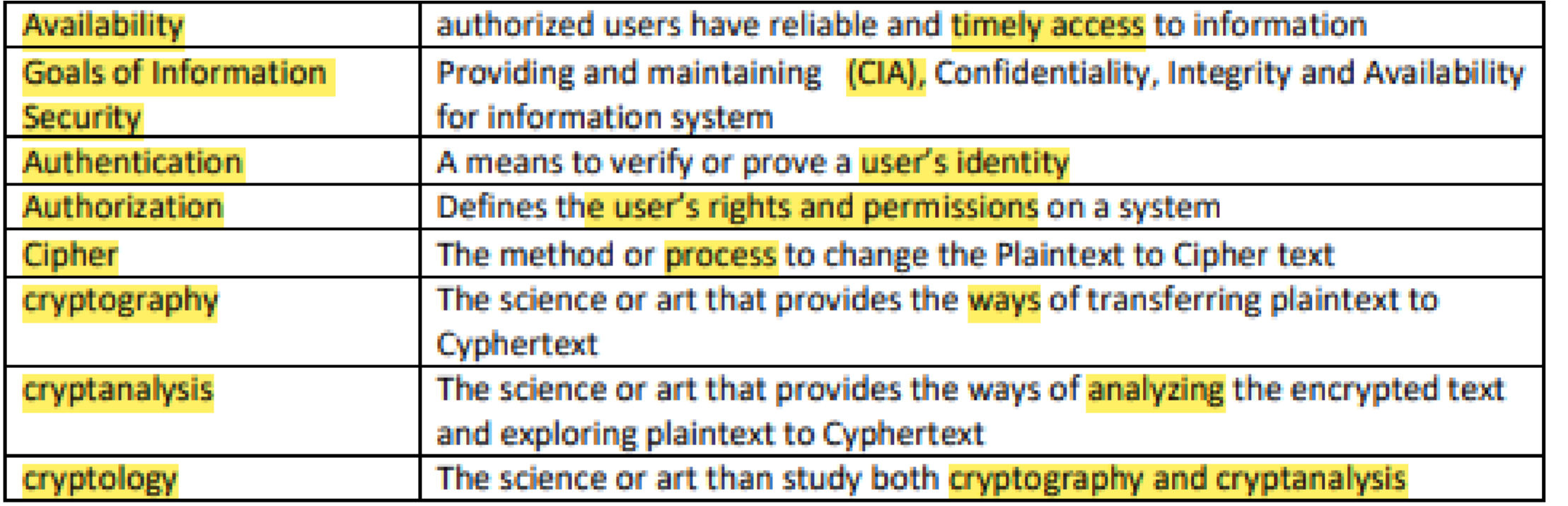
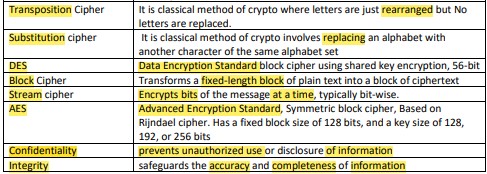
|  |  |
| --- | --- |
| DES | 56-bit keys |
| Triple DES (3DES) | 112-bit and 168-bit keys |
| AES | 128, 192, and 256-bit keys |
| RC6 | 128, 192, and 256-bit keys |
| IDEA | 128-bit keys |

**Question 4 match the following terms with their meaning (15 Marks)**

**ANSWER (From this table)**



End of the Questions



Good Luck

Prof. Moutasem Shafa’amry

# Yarmouk Private University

**Faculty of Informatics & Communications جامعة اليرموك الخاصة**

## Engineering كلية الهندسة المعلوماتية والاتصالات

|  |  |  |
| --- | --- | --- |
| **Course No**: CIE 530 | **Course Title**: Networks and systems security | **Exam Time**: 90 Min |
| **Credit Hours:** 3 (2 T +1 P) | **Lecturer**: Prof. Moutasem Shafa'amry | **Date** 13/08/2022 |
| **Department**: Comm & info. Eng. | **Semester**: Summer 2021-2022 | **Total** **Marks**: 20 Marks |

# Mid-Term Exam

**Question 1: Circle the correct choice for each of the following: (10 Marks)**

1. DES is a standard block cipher with
   1. 64-bits Block size and 64-bit key size
   2. 128-bits Block size and 56-bit key size
   3. 64-bits Block size and 56-bit key size
   4. 128-bits Block size and 64-bit key size
   5. 128-bits Block size and 56-bit key size
2. Attempt to make a machine or network resource unavailable to its intended users. a. Sniffing
   1. Spoofing
   2. Hijacking
   3. Denial of Service (DoS) Attack
3. Sets up a fake device ad trick others to send messages to it
   1. Hijacking
   2. Spoofing
   3. Phishing
   4. Pharming
4. The possibility that a particular vulnerability will be exploited
   1. Risk
   2. Risk Analysis
   3. Risk mitigation
   4. Vulnerability
5. Defines the user's rights and permissions on a system
   1. Availability
   2. Integrity
   3. Confidentiality
   4. Authorization
6. The process of selecting appropriate controls to reduce risk to an acceptable level a. Risk
   1. Risk Analysis
   2. Risk mitigation
   3. Vulnerability
7. Prevents unauthorized use or disclosure of information.
8. Availability
9. Integrity
10. Confidentiality
11. Authorization
12. Encrypts bits of the message at a time, typically bit-wise.
    1. AES
    2. Substitution cipher
    3. Transposition Cipher
    4. Stream cipher
13. The attack in which redirect a website's traffic to another fake site by changing the victim's

DNS settings or hosts file is called

* 1. Sniffing
  2. Pharming
  3. Spoofing
  4. Hijacking
  5. Phishing

1. The attack in which Users(victims) are redirected to a fake website that looks genuine. When the victim supplies his account and password, this can be used by the attacker to the target site, is called
   1. Sniffing
   2. Pharming
   3. Spoofing
   4. Hijacking
   5. Phishing

Good Luck

Prof. Moutasem Shafa’amry

# Yarmouk Private University

**Faculty of Informatics & Communications جامعة اليرموك الخاصة**

## Engineering كلية الهندسة المعلوماتية والاتصالات

|  |  |  |
| --- | --- | --- |
| **Course No**: CIE 530 | **Course Title**: Networks and systems security | **Exam Time**: 90 Min |
| **Credit Hours:** 3 (2 T +1 P) | **Lecturer**: Prof. Moutasem Shafa'amry | **Date** 13/12/2021 |
| **Department**: Comm & info. Eng. | **Semester**: Fall 2021-2022 | **Total** **Marks**: 20 Marks |

# Mid-Term Exam

**Question 1: Circle the correct choice for each of the following: (10 Marks)**

1. The possibility that a particular vulnerability will be exploited
   * 1. Risk
     2. Risk Analysis
     3. Risk mitigation
     4. Vulnerability
2. The process of selecting appropriate controls to reduce risk to an acceptable level a. Risk
   * 1. Risk Analysis
     2. Risk mitigation
     3. Vulnerability
3. Attempt to make a machine or network resource unavailable to its intended users. a. Sniffing
   * 1. Spoofing
     2. Hijacking
     3. Denial of Service (DoS) Attack
4. Sets up a fake device and trick others to send messages to it
   * 1. Hijacking
     2. Spoofing
     3. Phishing
     4. Pharming
5. Prevents unauthorized use or disclosure of information
   * 1. Availability
     2. Integrity
     3. Confidentiality
     4. Authorization
6. Defines the user’s rights and permissions on a system
   * 1. Availability
     2. Integrity
     3. Confidentiality
     4. Authorization
7. Encrypts bits of the message at a time, typically bit-wise.
   1. AES
   2. Substitution cipher
   3. Transposition Cipher
   4. Stream cipher
8. The attack in which redirect a website’s traffic to another fake site by changing the victim’s

DNS settings or hosts file is called

* 1. Sniffing
  2. Pharming
  3. Spoofing
  4. Hijacking
  5. Phishing

1. The attack in which Users(victims) are redirected to a fake website that looks genuine. When the victim supplies his account and password, this can be used by the attacker to the target site, is called
   1. Sniffing
   2. Pharming
   3. Spoofing
   4. Hijacking
   5. Phishing
2. DES is a standard block cipher with
   1. 64-bits Block size and 64-bit key size
   2. 128-bits Block size and 56-bit key size
   3. 64-bits Block size and 56-bit key size
   4. 128-bits Block size and 64-bit key size
   5. 128-bits Block size and 56-bit key size

**Question 2 Ansewr the following (10 Marks)**

1. Explain The Hill encryption algorithm (5Marks)

………………………………………………………………………………………………………………………………………………………………….

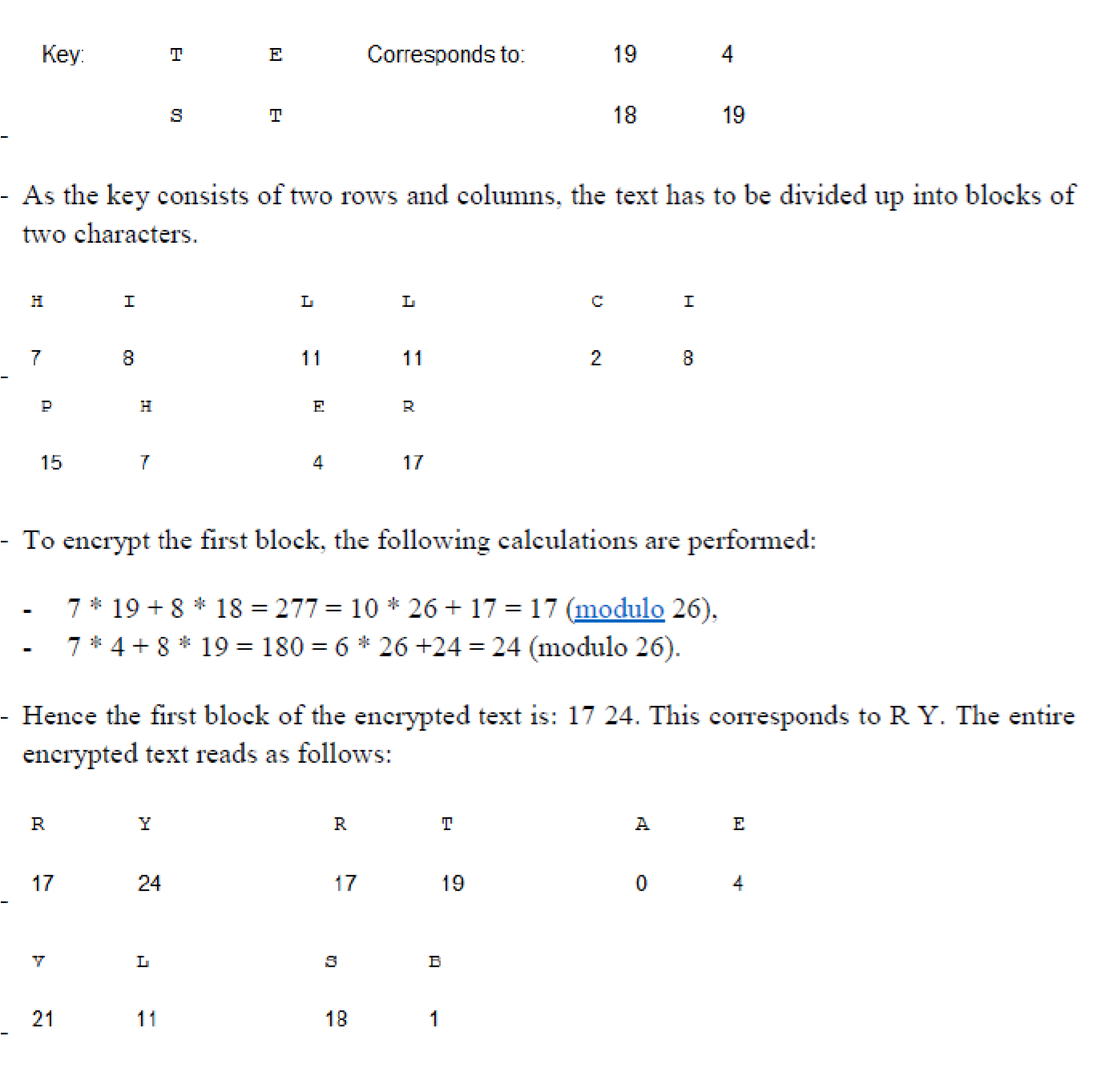
In this algorithm the key is a quadratic matrix: this means it has the same number of rows and columns. This number is called the dimension of the matrix. The plaintext is divided into blocks of equal size (one block consists of as many characters as the key has rows). The last block sometimes has too few characters: In this case the last block is padded to have the length of the matrix dimension -- by default it's filled up with the first character of the used alphabet. This algorithm operates on the numerical values of the charcters from the selected alphabet.

………………………………………………………………………………………………………………………………………………………………….

.

1. Encrypt the text **HILLCIPHER** with the key **TEST** using The Hill encryption algorithm

Show all steps (5 Marks)



End of the Questions

Good Luck

Prof. Moutasem Shafa’amry