****

**Computer Science Department**

**Information Systems Security (11464)**

**First Exam, Spring 2017/2018**

**March 31, 2018**

Time Allowed: 60 minutes

**Instructor Name:** …………………………………………

**Section Time: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |

**Student Number:**

|  |  |  |
| --- | --- | --- |
| **Question** | **Points** | **Score** |
| **1** | **3** |  |
| **2** | **4** |  |
| **3** | **4** |  |
| **4** | **3** |  |
| **5** | **3** |  |
| **6** | **3** |  |
| **Total** | **20** |  |

**Part I: Multiple Choices questions (6 x 0.5 = 3 Points)**

**Question 1: Answer all the following questions by choosing the most correct statement**

1. **\_\_\_\_\_ \_\_\_\_\_ is any action that compromises the security of information owned by an organization.**
2. Security mechanism
3. Security attack
4. Security policy
5. Security service
6. **\_\_\_\_\_\_\_\_ \_ attack involves an adversary repeating a previously captured user response.**
7. Client
8. Replay
9. Trojan horse
10. Eavesdropping
11. **When using Hash Functions, there are multiple ways in which the message can be authenticated using a hash code. All of the following are correct except:**
12. The message digest can be encrypted using symmetric encryption.
13. The message digest can be encrypted using public-key encryption
14. The message digest can be encrypted using private-key encryption
15. when A has a message to send to B, it calculates the hash function over the concatenation of the secret key and the message
16. All of them are correct.
17. **A digital certificate will typically include all of the following except:**
18. A copy of the public key
19. A copy of the private key
20. Information about the owner of the key: the owner’s name, etc.
21. Information about the digital certificate: a serial number, expiry date, etc.
22. Information about the CA itself: CA name, its own digital signature, etc.
23. **When properly applied, the one-time pad is the only known truly unbreakable cipher because it is using**
24. a strong symmetric key
25. an asymmetric key
26. Public Key Infrastructure (Public and Private keys)
27. a key of the same length of the message and for just one time
28. None of the above
29. **A countermeasure or security mechanism is a process (or a device incorporating such a process) that is designed to**
30. Prevent from a security attack.
31. Detect a security attack
32. Recover from a security attack
33. All of the above

**Part II: Essay questions (8 Points):**

**Question 2:** The following table shows **“Network security attacks”.** Fill the comparison table that compares among those Attacks in terms of (definition, classification (Passive/Active), its effects on the security services and what are the countermeasures or mehanisms to overcome it). **(4 Points)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Attack** | **Definition** | **Type of attack** | **Security Services** | **Countermeasure** |
| **1** | **Interception or Eavesdropping attack** |  |  |  |  |
| **2** | **Interruption attack** |  |  |  |  |
| **3** | **Replay attack** |  |  |  |  |
| **4** | **Repudiation Attack** |  |  |  |  |

**Question 3:** Alice wants to send a message M to Bob. How can she ensure the following properties, using asymmetric cryptography: **(4 Points)**

* 1. Confidentiality
  2. Integrity but not confidentiality
  3. Confidentiality and integrity
  4. Confidentiality, integrity and non-repudiation

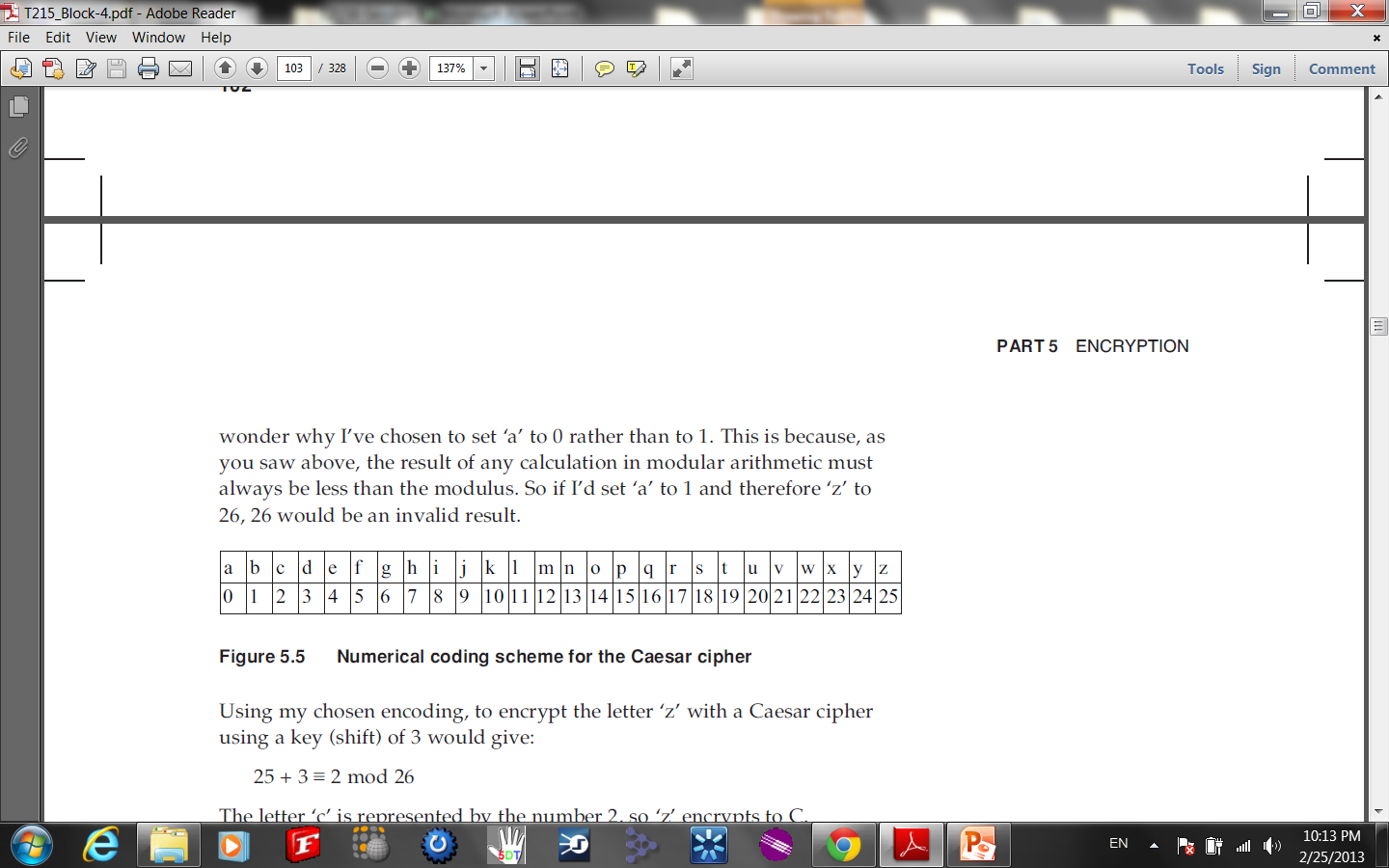
**Part III: Problem Solving (9 Points)**

**Note:** You should show all the required steps and rules to solve these problems.

**Question 4:** Using a computer that can perform 12 calculations per second, how long would it take to try all possible permutations (Brute Force Attack) of 7 different letters? Give the answer in minutes. (Note: you can solve the question without using a calculator) **(3 Points)**

**Question 5: *Caesar Cipher – Answer only one branch; either a or b (not both)* (3 Points)**

Use the following table to help you find the code of letters:



1. Decrypt the following cipher text using **Caesar Cipher** with key 2600000000058 “**YARWLNBBBDVJHJDWRENABRCH**”. Write the answer as a readable sentence. Show your work (the modular arithmetic of every letter decryption).
2. On a Caesar cipher text captured by an intruder, cryptanalysis showed that the letter with the highest frequency of the ciphertext is the letter “**N**”. If the captured message contains the phrase “**YARWLNBBBDVJHJDWRENABRCH**” then decrypt it. Write the answer as a readable sentence. Show your work (the modular arithmetic of every letter decryption).

**Question 6:** Decrypt the ciphertest “**SMPSMENNEELEOADY**” using **Row Transposition Cipher**  if the key is “**253614**”. Show your steps; including the calculation of the number of rows and columns of the matrix, partitioning the ciphertext, populating the matrix and then writing down the plaintext. **(3 Points)**