**CIDM 6341 : Cybersecurity Spring 2020**

Mid-term Exam

Take Home

*The objectives of this test is to evaluate your ability (i) to identify threats posed to information security and the more common attacks associated with those threats, and selecting the appropriate counter measures, (ii) to assess risk based on probability of occurrence and likely impact, and recognize the existing conceptual frameworks for evaluating risk controls and formulate a cost benefit analysis (iii) to recognize the important role of access control in computerized information systems, and identify widely-used access control techniques, and (iv) to list and explain the major protocols used for secure communications.*

Please answer the following FIVE questions out of SIX questions. Each question carries equal point (20) and has three parts **(a) [ 4 – 6 points]** terms and definition, **(b) [10 points]** large question (with example, illustration, case-study), and **(c) [ 6 -4 points]** small question – technical question.

Here is one example question:

**Q2: Cryptography**

1. **[ 4 points]** Differentiate between active and passive attacks in cyber security.
   1. **Active Attacks:**
      1. Disguising on entity (process, files, registry value…etc) as something else
      2. Replay previous messages
      3. Modify messages in transit
      4. Add, or delete messages
      5. Denial of service attacks
   2. **Passive Attacks**
      1. Obtain Message Contents
      2. Monitor traffic flow
2. **[ 10 points]** Illustrate the Vigenere Cipher technique: (i) Encrypt the English message below with the key (ABCD), and (ii) Suppose in the receiver end, you do not have the key, can you use frequency distribution (table 1) to decrypt the encrypted message?

Message : CRYPTOISSHORTFORCRYPTOGRAPHY

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
| 8.15 | 1.44 | 2.76 | 3.79 | 13.11 | 2.92 | 1.99 | 5.26 | 6.35 | 0.13 | 0.42 | 3.39 | 2.54 |
| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 7.10 | 8.00 | 1.98 | 0.12 | 6.83 | 6.10 | 10.47 | 2.46 | 0.92 | 1.54 | 0.17 | 1.98 | 0.08 |

Below is the Vigenere Cipher plain text, key and encrypted cipher

CRYPTOISSHORTFORCRYPTOGRAPHY

Encrypted with key "ABCD"

CSASTPKVSIQUTGQUCSASTPIUAQJB

Method used to encrypt is with the Vigenere Cipher table.

This would be easy to decrypt without the key because the key length is only 4. Also since we chose to use ABCD, Then the first letter in every four letters is the same as the actual plain text. Which you can see above. This would take some time but decryption would be able to be done without having the key provided.

The frequency of the letters also totals to 12.35%. Using the process for finding the frequencies is possibly to decrypt the message.

**(c) [ 6 points]** “Very often digital signatures are used with hash functions” is it true? Explain.

1. This is true
2. The hash is signed instead of the message.
   1. The hash function has to be pre image resistant, strong collision resistant and weak collision resistant.
3. The purpose of using a digital signature is to sign the hash, if the certificate does not match then you would not be able to continue the communication in order to read the message, even though the message itself is not encrypted.
4. The reason why this is, during the handshake if the cert request does not pass then there is a rejection that takes place. In curl the error code would be either a curl error 35 or curl error 60, dependent on where the failure occurred. You can also view the handshake request in Wireshark. Though this can be seen but not decrypted in Wireshark since the first response is rejected if the cert does not match.