Sunday March 06, 2022

EAST WEST UNIVERSITY
Department of Computer Science and Engineering
B.Sc. in Computer Science and Engineering Program
In-Course Assessment-1, Spring 2022 Semester

Course:	**CSE487 Cybersecurity, Law and Ethics, Section-1 and 2**
Instructor:	**Rashedul Amin Tuhin, Senior Lecturer, CSE Department**
Full Marks:	**30 (15 will be counted for final grading)**
Due:	**23:55 Thursday March 10, 2022**

Notes: There are **SIX** questions, answer ALL of them. Course Outcome (CO), Cognitive Level, Mark, for each question are mentioned at the right margin.

This is an **outcome-based take-home exam with complex engineering problems, usage of modern tools and reporting**. You are encouraged to do your own research to solve the given problems. **Each question requires at least 1 hour of attention.**

Formatting: Font: Times New Roman, Size: 10-12pt, Line Spacing: Single

Submission method: Turn-in one PDF file only, via Google Classroom through the assignment named "*In-Course Assessment-1*". Filename example: *2020-3-60-000.ICA1.pdf* **Please do not submit Google Doc files or links. Download it as PDF and submit that PDF. Do not forget to write your student ID at the header of your answer script.**

Late submission policy: There will be no penalty if submitted within 5 minutes of the stipulated time. However, for every additional 5-minute delays in submission, 20% marks will be deducted.

Plagiarism policy: There will be no penalty if the similarity is up to 25% including references. For every additional 15% similarity, 20% marks will be deducted.

Cryptanalysis (Hash decryption) [EP1, EP2, EP4]

Q1. Given that, **[CO2, C4, Mark: 05]**

hash(x)= 6da96dec2995ce9f2756f1ceb4f883b3e957f56fb5a649a6e3c02586207939be

a. **Identify** the hash function from the digest length and the set of unique characters. [01]

Attack surface minimization/Hints:
The input to the hash function, x, is an ASCII string. It could be something related to the course codes of your B.Sc. in CSE program at EWU. So, the input contains 3 UPPERCASE LETTERS and 3 DIGITS. No salt was used for the hash function. Utilize this information and use *Crunch* to generate a dictionary.

b. **Identify** the size of the dictionary? **Find** the time required to brute-force this in your computer. [01]

You can further minimize the attack surface by taking only the valid course codes as inputs.

c. Use your favorite programming language to **generate** a Rainbow Table, taking the course codes of the core CSE courses of your B.Sc. in CSE program. Use standard libraries like *hashlib* or *cryptography* library functions. [02]

d. **Find** the value of x. [01]

Analyzing TLS (HTTPS decryption): [EP1, EP2, EP4]

Q2. **Capture a TLS session with *Wireshark*:** **[CO2, C4, Mark: 05]**

Clear your browser history and cookies and run *Wireshark* to start capturing your network traffic. Download the Academic Calendar PDF from the EWU website. After downloading, stop the capture on *Wireshark*, and use appropriate filters to display this communication only (Follow TCP stream). Save the capture file,

Hints:

Use *ipconfig* command [*ifconfig* in Linux] to discover your computer's IPv4 address. Get the public IPv4 address of www.ewubd.edu by ping or by the following procedure: Right click on the webpage and click *Inspect element* and go to the *Network* tab, then reload the page. Select any HTTP GET request and identify the IPv4 address of *www.ewubd.edu* from the *Headers*.

Analyze the TCP stream in Wireshark and answer the following:

a. **Identify** the TCP 3-way handshake packets.

b. **Provide** the NAT assignment (ip:port <--> ip:port). e.g., 192.168.0.3:12345 <--> 123.45.67.89:123 for the connection.

c. **Identify** the first encrypted packet.

d. **Identify** the packet numbers of the *Client Hello* and *Server Hello* packets.

e. **Provide** the cipher suites offered by the client.

f. **Identify** the cipher suite selected by the server.

g. **Identify** the negotiated TLS version.

h. **Identify** the packet in which EWUBD.EDU offered its certificate.

i. **Perform** HTTPS decryption demonstrating the release of message contents attack.
Hint: https://www.comparitech.com/net-admin/decrypt-ssl-with-wireshark/
[01]

Public Key Infrastructure [EP1, EP4]

Q3. **Analyze** the SSL Certificate of EWUBD.EDU (either from the Wireshark capture file or from the padlock icon at the address bar of the browser), and answer the following questions: **[CO1, C3, Mark: 05]**

a. **Identify** the intended purpose of this certificate.

b. **Identify** the issuer of this certificate, with the CA trust chain of the SSL Certificate issued to EWUBD.EDU.

c. **Identify** the validity of the certificate: Is this certificate valid for *www.ewubd.edu.bd* ?When will this certificate expire?

d. **Identify** the hashing algorithm used to create the certificate.
e. **Identify** the algorithm used by the CA to sign the certificate.
f. **Provide** the public key of EWUBD.EDU and identify the length.
g. **Identify** the public key algorithm that was used to generate public-private keypair.
h. **Identify** certificate revocation points. If the CA wants to revoke the certificate before the expiration date, how will it be announced.
i. **Demonstrate** the certificate verification process performed by your browser to ensure that it is communicating with the authentic EWUBD.EDU. [01]

Asymmetric Key Cryptography: RSA Algorithm [EP1, EP2, EP4]

Q4. Alice and Bob want to establish a secure connection so that no one except them can understand the contents of their messages. **[CO1, C3, Mark: 05]**

a. **Demonstrate** how Alice and Bob can establish a secure connection using the RSA Algorithm with prime numbers smaller than 100. **Provide** the Public and Private keypairs of both Alice and Bob. [03]
b. **Explain** how *Confidentiality* and *Non-Repudiation* are ensured to prevent *MITM* attacks. [01]
c. **Compare** the values of e (*encryptor/exponent*) and n (*modulus*) for your case, with the public key of EWUBD.EDU [01]

X.800 OSI Security Architecture [EP1]

Q5. With the help of diagrams, **provide examples of** the *Security services* and *Security attacks* as per the *X.800 OSI Security Architecture*. Consult **RFC4949** if required. **[CO1, C3, Mark: 05]**

Symmetric Encryption [EP1, EP2, EP4]

Q6. Assume that Alice and Bob have already established a secure communication channel using the RSA algorithm, which is an asymmetric encryption. However, they still want to establish a symmetric session key for the subsequent communications. **[CO1, C3, Mark: 05]**

a. **Explain** why they would still want to establish another secure connection with each other with a symmetric key. [0.5]
b. **Demonstrate** a *Diffie-Hellman Key Exchange* between Alice and Bob, through a clear channel where Eve is eavesdropping. Use prime numbers less than 100. [02]
c. **Explain** how security requirements are achieved by *Diffie-Hellman Key Exchange*. [0.5]
d. **Demonstrate** how confidentiality and integrity can be compromised if only *Diffie-Hellman Key Exchange* protocol is used alone. [02]