# CSE487-X Sample Questions Sets for Midterm-1 Exam

## X.800 OSI Security Architecture [EP1]

**Q1.**

***a.*** Provide examples of different attack surfaces. Develop an attack tree for the student portal system of your university. [05]

***b.*** Describe subcategories the X.800 OSI Security Architecture with examples. [05]

**[CO1, C3, Mark: 10]**

## Cryptanalysis [EP1, EP2]

**Q2.** The given paragraph was encrypted with a shift cipher. **Find** the value of the key. **Show** the mathematical equation for the encryption of the given ciphertext. [02.5]

**CO1, C3, Mark: 05]**

**Decrypt** the ciphertext. [02.5]

***Wuymul wcjbyl Gynbix ch qbcwb yuwb fynnyl ch nby jfuchnyrn cm lyjfuwyx vs u fynnyl migy zcryx hogvyl iz jimcncihm xiqh nby ufjbuvyn. Nby gynbix cm hugyx uznyl Dofcom Wuymul, qbi omyx cn ch bcm jlcpuny willymjihxyhwy.***

## Security Protocol Design [EP1, EP2, EP4]

**Q3.**

***a.*** **Explain** the issues related to symmetric encryption. [02]

***b.*** **Demonstrate** a hybrid protocol that uses both symmetric and asymmetric encryptions, with the help of a diagram and appropriate mathematical notations. [03]

**[CO1, C3, Mark: 05]**

## Symmetric Key Establishment [EP1, EP2]

**Q4.**

***a.*** **Demonstrate** a *Diffie-Hellman Key Exchange* between Alice and Bob, through a clear channel where Eve is eavesdropping. Use prime numbers between 100 and 150. [04]

***b.*** **Explain** the limitations of *Diffie-Hellman Key Exchange* algorithm. [01]

**[CO2, C4, Mark: 05]**

## Cybersecurity Knowledge Depth [EP1, EP2, EP4]

**Q5.**

***a.*** In the Bandit wargame, how do you proceed from one level to another?

***b.*** Differentiate between transposition cipher and substitution cipher.

***c.*** Which encryptions are used by the WIFI connections?

***d.*** Calculate the time difference of brute forcing a password of 8 characters and 9 characters with 1000 passwords per second rate.

***e.*** What is XCA?

**[CO2, C3, Mark: 05]**

## X.800 OSI Security Architecture [EP1]

**Q1.**

***a.*** Provide examples of different attack surfaces. Develop an attack tree for the student portal system of your university. [05]

***b.*** Identify the different security attacks prevented by the security mechanisms defined in X.800. [05]

**[CO1, C3, Mark: 10]**

## Cryptanalysis [EP1, EP2]

**Q2.** **Decode** the encoded ciphertext. **CO1, C3, Mark: 05]**

***RWlkIE11YmFyYWs=***

## Security Protocol Design [EP1, EP2, EP4]

**Q3.**

***a.*** **Explain** the issues related to symmetric encryption.

***b.*** **Demonstrate** a hybrid protocol that uses both symmetric and asymmetric encryptions, with the help of a diagram and appropriate mathematical notations.

**[CO1, C3, Mark: 05]**

## Symmetric Key Establishment [EP1, EP2]

**Q4.**

***a.*** **Demonstrate** a *Diffie-Hellman Key Exchange* between Alice and Bob, through a clear channel where Eve is eavesdropping. Use prime numbers between 100 and 150. [04]

***b.*** **Explain** the limitations of *Diffie-Hellman Key Exchange* algorithm. [01]

**[CO2, C4, Mark: 05]**

## Cybersecurity Knowledge Depth [EP1, EP2, EP4]

**Q5.**

***a.*** What is the relation between CAPTCHA and DDOS attack?

***b.*** Calculate $\Phi$ (65).

***c.*** How do you discover the MTU in your TCP connection?

***d.*** What are the hard problems that are the basis of cryptography?

***e.*** What is the relation between S/MIME and Base64?

**[CO2, C3, Mark: 05]**

| Index | Binary | Char | Index | Binary | Char | Index | Binary | Char | Index | Binary | Char |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 000000 | A | 16 | 010000 | Q | 32 | 100000 | g | 48 | 110000 | w |
| 1 | 000001 | B | 17 | 010001 | R | 33 | 100001 | h | 49 | 110001 | x |
| 2 | 000010 | C | 18 | 010010 | S | 34 | 100010 | i | 50 | 110010 | y |
| 3 | 000011 | D | 19 | 010011 | T | 35 | 100011 | j | 51 | 110011 | z |
| 4 | 000100 | E | 20 | 010100 | U | 36 | 100100 | k | 52 | 110100 | 0 |
| 5 | 000101 | F | 21 | 010101 | V | 37 | 100101 | l | 53 | 110101 | 1 |
| 6 | 000110 | G | 22 | 010110 | W | 38 | 100110 | m | 54 | 110110 | 2 |
| 7 | 000111 | H | 23 | 010111 | X | 39 | 100111 | n | 55 | 110111 | 3 |
| 8 | 001000 | I | 24 | 011000 | Y | 40 | 101000 | o | 56 | 111000 | 4 |
| 9 | 001001 | J | 25 | 011001 | Z | 41 | 101001 | p | 57 | 111001 | 5 |
| 10 | 001010 | K | 26 | 011010 | a | 42 | 101010 | q | 58 | 111010 | 6 |
| 11 | 001011 | L | 27 | 011011 | b | 43 | 101011 | r | 59 | 111011 | 7 |
| 12 | 001100 | M | 28 | 011100 | c | 44 | 101100 | s | 60 | 111100 | 8 |
| 13 | 001101 | N | 29 | 011101 | d | 45 | 101101 | t | 61 | 111101 | 9 |
| 14 | 001110 | O | 30 | 011110 | e | 46 | 101110 | u | 62 | 111110 | + |
| 15 | 001111 | P | 31 | 011111 | f | 47 | 101111 | v | 63 | 111111 | / |

**Base64 Alphabet**

## ASCII Code: Character to Binary

| | | | | | |
|---|---|---|---|---|---|
| 0 | 0011 0000 | O | 0100 1111 | m | 0110 1101 |
| 1 | 0011 0001 | P | 0101 0000 | n | 0110 1110 |
| 2 | 0011 0010 | Q | 0101 0001 | o | 0110 1111 |
| 3 | 0011 0011 | R | 0101 0010 | p | 0111 0000 |
| 4 | 0011 0100 | S | 0101 0011 | q | 0111 0001 |
| 5 | 0011 0101 | T | 0101 0100 | r | 0111 0010 |
| 6 | 0011 0110 | U | 0101 0101 | s | 0111 0011 |
| 7 | 0011 0111 | V | 0101 0110 | t | 0111 0100 |
| 8 | 0011 1000 | W | 0101 0111 | u | 0111 0101 |
| 9 | 0011 1001 | X | 0101 1000 | v | 0111 0110 |
| A | 0100 0001 | Y | 0101 1001 | w | 0111 0111 |
| B | 0100 0010 | Z | 0101 1010 | x | 0111 1000 |
| C | 0100 0011 | a | 0110 0001 | y | 0111 1001 |
| D | 0100 0100 | b | 0110 0010 | z | 0111 1010 |
| E | 0100 0101 | c | 0110 0011 | . | 0010 1110 |
| F | 0100 0110 | d | 0110 0100 | , | 0010 0111 |
| G | 0100 0111 | e | 0110 0101 | : | 0011 1010 |
| H | 0100 1000 | f | 0110 0110 | ; | 0011 1011 |
| I | 0100 1001 | g | 0110 0111 | ? | 0011 1111 |
| J | 0100 1010 | h | 0110 1000 | ! | 0010 0001 |
| K | 0100 1011 | I | 0110 1001 | ' | 0010 1100 |
| L | 0100 1100 | j | 0110 1010 | " | 0010 0010 |
| M | 0100 1101 | k | 0110 1011 | ( | 0010 1000 |
| N | 0100 1110 | l | 0110 1100 | ) | 0010 1001 |
| | | | | space | 0010 0000 |

### X.800 OSI Security Architecture [EP1]

**Q1.** ***c.*** Explain the security mechanisms defined in X.800. [05] **[CO1, C3, Mark: 10]**

***d.*** Identify the different security attacks prevented by the security mechanisms defined in X.800. [05]

### Cryptanalysis [EP1, EP2]

**Q2.** We received the following ciphertext which was encoded with a shift cipher: **CO1, C3, Mark: 05]**

```
lzwhdsaflwplzsktwwfwfujqhlwvloauwoalzskzaxluahzwjmka
fylogvaxxwjwflcwqkgfuwoalzkwnwfsfvsysafoazwdwnwfozau
zakksewskwfujqhlafygfuwoalzlzwugetafwvcwqwayzlwwf
```

**Perform** an attack against the cipher based on a letter frequency count.

How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?

### Security Protocol Design [EP1, EP2, EP4]

**Q3.**

***c.*** **Explain** the issues related to symmetric encryption. **[CO1, C3, Mark: 05]**

***d.*** **Demonstrate** a hybrid protocol that uses both symmetric and asymmetric encryptions, with the help of a diagram and appropriate mathematical notations.

### Symmetric Key Establishment [EP1, EP2]

**Q4.**

***c.*** **Demonstrate** a *Diffie-Hellman Key Exchange* between Alice and Bob, through a clear channel where Eve is eavesdropping. Use prime numbers larger than 200. [04] **[CO2, C4, Mark: 05]**

***d.*** **Explain** which security services are ensured by *Diffie-Hellman Key Exchange*. [01]

### Cybersecurity Knowledge Depth [EP1, EP2, EP4]

**Q5.**

***f.*** How many symmetric keys all nodes need to hold if there are total 100 users? **[CO2, C3, Mark: 05]**

***g.*** Calculate Φ (91).

***h.*** How do you discover the MTU in your TCP connection?

***i.*** Why did Facebook go down for five hours in 2021?

***j.*** What is CVE?

### X.800 OSI Security Architecture [EP1]

**Q1.** **Illustrate** different categories of passive and active security attacks, with diagrams. Provide examples of each type of attacks. **[CO1, C3, Mark: 10]**

### Cryptanalysis [EP1, EP2]

**Q2.** We received the following ciphertext which was encoded with a shift cipher: **CO1, C3, Mark: 05]**

*awpldpozyzeepwwjzfcqctpyolmzfeespvpjlyodaztwespqfywpeespxotdnzgpcespvpjzyesptczhy*

**Perform** an attack against the cipher based on a letter frequency count.

How many letters do you have to identify through a frequency count to recover the key? What is the cleartext?

### Security Protocol Design [EP1, EP2, EP4]

**Q3.** Assume that Alice and Bob have already established a secure communication channel using the RSA algorithm, which is an asymmetric encryption. **[CO1, C3, Mark: 05]**

- ***a.*** **Explain** the reasons they would want to use symmetric encryption.
- ***b.*** **Demonstrate** such a hybrid protocol using a diagram and appropriate mathematical notations.

### Symmetric Key Establishment [EP1, EP2]

**Q4.**

- ***a.*** **Demonstrate** a *Diffie-Hellman Key Exchange* between Alice and Bob, through a clear channel where Eve is eavesdropping. Use prime numbers larger than 50. [04] **[CO2, C4, Mark: 05]**
- ***b.*** **Explain** which security services are ensured by *Diffie-Hellman Key Exchange*. [01]

### Cybersecurity Knowledge Depth [EP1, EP2, EP4]

**Q5.**

- ***a.*** How is LSB steganography linked with DDOS attack? **[CO2, C3, Mark: 05]**
- ***b.*** Why using cracked software is much riskier nowadays?
- ***c.*** What is the minimum number of people required in a party that there is a 50% chance of two persons share the same birthday?
- ***d.*** How can PGP secure your emails?
- ***e.*** Why did you use *hashcat* and *crunch*?

### Dictionary/Brute-force Attack (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.

***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:

**Identify the IP address:** 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 tab.

***a.*** **Analyze** the TCP stream in Wireshark and answer the following:

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

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

***d.*** **Identify** the first encrypted packet.

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

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

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

***h.*** **Identify** the negotiated TLS version.

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

***j.*** **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 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 within 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 Man-In-The-Middle 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.** 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]**

*c.* **Explain** why they would still want to establish another secure connection with each other with a symmetric key. [0.5]

*d.* **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]

*e.* **Explain** which security requirements are achieved by Diffie-Hellman Key Exchange. [0.5]

*f.* **Demonstrate** how confidentiality and integrity can be compromised if only Diffie-Hellman Key Exchange protocol is used alone. [02]