Question 1 [25 Marks]

To be answered on the last page.

1. What is the block size of AES in bits?

   A. 64
   B. 128
   C. 192
   D. 256

2. The main advantage of symmetric key cryptography (say AES) over asymmetric key cryptography (say RSA) is:

   A. Fewer keys to manage.
   B. Non-repudiation is ensured.
   C. It is usually less computationally expensive.
   D. It is usually less vulnerable to cryptanalysis.

3. In RSA, what is the value of *d* obtained by running the Euclidean algorithm when e = 5, p = 7 and q = 3?

   $\phi(n) = 6 \times 2 = 12$.

   $\frac{(\phi(n) \times i) + 1}{e}$

   A. 5
   B. -2
   C. 3
   D. 4

4. In the AES key expansion process, how many words are generated for a 128-bit encryption key, and how many of those words are used for the initial round key?

   A. 10 words, 10 words
   B. 13 words, 12 words
   C. 12 words, 11 words
   D. 11 words, 10 words

5. In an organization with 150 users, if they all wish to use symmetric key cryptography to communicate with each other, how many keys will be generated in total?

   A. 150
   B. 300
   C. 11,175
   D. 11,250

6. In RSA, the Euler's totient function (Φ) of the public modulus (N) is crucial for key generation. What does Φ(N) represent?

   A. The number of integers coprime to N
   B. The count of prime factors of N
   C. The number of bits in the modulus
   D. The number of rounds in the encryption process

7. When using public key cryptographic schemes for implementing digital signatures versus encryption, the main difference is:

   A. Digital signatures encrypt with a public key and decrypt with a private key, while encryption encrypts with a private key and decrypts with a public key
   B. Digital signatures encrypt with a private key and decrypts with a public key, while encryption encrypts with a public key and decrypt with a private key
   C. Digital signatures are applied to a plaintext, while encryption is applied to the hash.
   D. Both B and C are correct.

8. If the value of g is 3 in the Diffie Hellman Key Exchange algorithm with p=7, what will be the value of the shared secret key if the private keys are 3 and 4 respectively?

   A. 5
   B. 4
   C. 3
   D. 2

$X_A = 3, X_B = 4$

$K = (Y_B)^{X_A} \bmod n$

$Y_B = (\alpha)^{X_A} \bmod n$

$Y_B =$

9. When you're tired in class, what's the most tempting option?

   A. Ask a question to show you're still engaged
   B. Start a game of "I spy" with your neighbor
   C. Pretend to take notes while secretly napping
   D. Create a master plan to escape

10. Which of the following is a strong Cipher Suite?

    1. TLS_DHE_ECDSA_WITH_AES_256_SHA512
    2. TLS_DHE_RSA_WITH_AES_128_SHA256
    3. TLS_RSA_WITH_NULL_MD5
    4. TLS_RSA_EXPORT1024_WITH_RC4_56_SHA

    A. 1 and 2
    B. 1 and 3
    C. 3 and 4
    D. 2 and 4

11. SQL injection can occur when a web application:

A. Employs strong access control policies
B. Uses a Web Application Firewall (WAF)
C. Fails to separate user input from SQL queries
D. Utilizes client-side JavaScript validation

12. Mallory, an eavesdropper, captures the public parameters (p and g) and Alice's public key in a Diffie Hellman key exchange. However, she cannot determine Alice's private key. What information can Mallory obtain from the captured data?

A. The value of the shared secret key
B. Alice's private key
C. The value of Bob's private key
D. None of the above

13. In HTTPS, the encryption of data is typically achieved using which cryptographic protocol?

A. TLS (Transport Layer Security)
B. TCP (Transmission Control Protocol)
C. SSL (Secure Sockets Layer)
D. HTTP (Hypertext Transfer Protocol)

14. What is the purpose of SSL certificates in establishing a secure HTTPS connection?

A. They provide encryption of data transmitted between the client and the server.
B. They verify the authenticity and identity of the server.
C. They prevent cross-site scripting (XSS) attacks.
D. They protect against session hijacking.

15. Which web technology can be used to control whether a web page can store cookies on a user's device?

A. HTML
B. CSS
C. JavaScript
D. HTTPS

16. You're concerned about online tracking and take measures to protect your privacy. Despite these efforts, a website is able to identify you by collecting data such as your screen resolution, time zone, and installed browser plugins. What method of tracking is the website employing?

A. Geolocation tracking
B. Cookie tracking
C. Behavioral tracking
D. Device and browser fingerprinting

17. Cookies are small pieces of data that a website can store on a user's device. Which of the following is NOT a typical use of cookies?

A. Storing session information
B. Tracking user behavior and preferences
C. Caching web content for faster loading
D. Personalizing the user experience

18. What is a potential privacy concern associated with third-party cookies?

A. They can expose sensitive user information to unauthorized parties.
B. They can cause website performance issues and slow page load times.
C. They can lead to cross-site scripting (XSS) attacks.
D. They can result in session hijacking and unauthorized access to user accounts.

19. Which approach leverages the properties of the RSA algorithm to manipulate encrypted data and gain insights into the private key?

A. Chosen ciphertext attacks
B. Timing attacks
C. Brute force
D. Mathematical attacks

20. In a hash function, what is the output called after applying the hashing algorithm to the input data?

A. Digest
B. Cipher
C. Salt
D. Key

21. What is the primary purpose of the HTTP "Connection: keep-alive" header?

A. To terminate the connection after each request-response cycle
B. To request that the server keeps the connection open for multiple requests
C. To encrypt the communication between the client and server
D. To enable caching of resources on the client-side

22. In the context of HTTP statelessness, what is the primary challenge associated with maintaining user sessions in web applications?

A. Managing persistent connections
B. Synchronizing server and client time
C. Tracking user interactions without a memory of previous requests
D. Ensuring consistent encryption for data transfer

23. A website stores user credentials in a database. An attacker enters the following input in the login form's password field: "' OR '1' = '1". What type of SQL injection is this, and what is the attacker trying to achieve?

A. Blind SQL injection, attempting to retrieve sensitive data
B. Time-based SQL injection, delaying the application's response
C. Error-based SQL injection, causing the server to produce error messages
D. Union-based SQL injection, attempting to extract data from other tables

24. A website utilizes browser fingerprinting techniques to track users across different devices and sessions. What information is typically used to create a browser fingerprint?

A. User's name and email address
B. IP address and location
C. Installed browser extensions and plugins.
D. Website browsing history

25. During an SSL/TLS handshake, the client sends a "ClientKeyExchange" message to the server. What information does this message typically contain?

A. Secret session key
B. The client's public key
C. The server's public key
D. A digital signature

National University of Computer and Emerging Sciences

FAST School of Computing **Fall-2023** **Islamabad Campus**

Question 1 [15 Marks]

Scenario:

Two friends, Alice and Bob, want to exchange secret messages securely. They decide to use RSA for authentication and Diffie-Hellman for secure key exchange. Alice will initiate the process.

RSA Key Generation: [10 Marks]
Alice generates an RSA key pair with a modulus of 187 and a public exponent (e) of 11. Calculate Alice's private exponent (d).

Diffie-Hellman Parameters: [3 Marks]
Alice and Bob agree on using Diffie-Hellman parameters with a prime modulus (P) of 23 and a generator (G) of 5. Calculate the shared secret key (K) that they will use for encryption.

Secure Communication: [2 Marks]
After exchanging public keys and generating the shared secret key, describe how Alice and Bob can use these keys to securely exchange a message. You can provide a simple example of how the shared secret key can be used for encryption and decryption.

RSA Key Generation:

$e = 11$

$d = \frac{(\phi(n) * i) + 1}{e}$

Iteration #1:

$d = \frac{(160 * 1 + 1)}{11}$ ✗ not integer

Iteration # 2 – 8:

final answer wasn't integer, did on calculator.

Iteration #9:

$d = \frac{(160 \times 9) + 1}{11}$

$d = \frac{1441}{11} = 131$

$n = 187 = 17 \times 11$

$n = p \times q = 17 \times 11$

$\phi(n) = (17-1)^*(11-1)$

$= 16 \times 10 = 160$

$CT = PT^e \bmod n$

10 Good

Diffie-Hellman Parameters:

$p = 23$, $g = 5$

$Y_A = (\alpha)^{X_A} \bmod p$

$X = 131$

$K = (Y_B)^{X_A} \bmod p$

$Y = (5)^{131} \bmod 23$ = Ans

answer from Y goes here → $K = (Y)^{131} \bmod 23$.

This will return the shared secret key.

1.5

Values?

Secure Communication

In case bob wants to send a message to Alice

To securely exchange a message, bob will use Alice's public key for encryption and Alice will use her own private key for decryption.

2

Question 2 [10 Marks]

For each of the following identify the attack and the mitigation:

Incident	Description	Attack Type
A	You are reviewing the code for a login form on a website. The code uses user input directly in a SQL query.	SQL injection can be mitigated by having a clear boundry (binding) between code and user info.
B	An attacker intercepts the user's HTTPS connection and downgrades it to HTTP. This puts the user's online banking data at risk of interception by the attacker.	Downgrading TSL attacks which makes the downgraded version apparently look better.
C	A customer's payment information is stolen during an online purchase. The website appeared to be secure as it the URL bar displayed https, but the transaction was compromised.	SQL injection using '9' or '--;'
D	A person looking for Grammarly premium for free searchers online and finds a cookie that logs him into an account belonging to John's.	due to 'replaying attacks'. can be mitigated by implementing proper checks on SQL and making it secure.
E	Ali's online activity is being tracked online although they have disabled third party cookies.	Session hijacking can be mitigated by clearing cache and disabling all cookies from browser.

Question 3 [5 Marks]

You are a security consultant tasked with assessing the security of a community forum website. This forum allows users to search for posts and topics of interest. During your assessment, you discover a vulnerability that could potentially allow attackers to manipulate the website's database using SQL injection.

Scenario:

Let's explore a practical example of how an attacker might exploit the SQL injection vulnerability in the forum's search feature. Suppose a user wants to search for posts containing the word "security." How could an attacker use this search feature to conduct a SQL injection attack, and what malicious actions could they perform with this vulnerability?

For a user searching posts containing the word "security". The SQL query will look something like.

select posts from table_name where posts_w LIKE '%security%'

The attacker can conduct SQL injection and do something like

LIKE '; --'

This will prematurely exit the query and comment out the remaining part of the query. In this case, the hijacker will get all the posts and query will become like.

select post from table_name where posts_w like '%.%'; -- security.

here 'security' is commented out and all the posts will be selected from the table.

6