### 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
- 2. The main advantage of symmetric key cryptography (say AES) over asymmetric key cryptography (say RSA) is: RSA) is:
  - A. Fewer keys to manage.
  - B. Non-repudiation is ensured.
  - C. It is usually less computationally expensive.
- 3. In RSA, what is the value of d obtained by running the Euclidean algorithm when e=5, p=7 and q=3?
  - A. 5
- q(n)=6x2=12.

- 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
- 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

FAST School of Computing

Fall-2023

Islamabad Campus

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

- \* 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
  - 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
  - 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.
- 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.

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
    - 2 and 4

**FAST School of Computing** 

Fall-2023

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?
    - X. 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.
    - . 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
  - 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

Fall-2023

Islamabad Campus

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

- A. Storing session information
- B./ Tracking user behavior and preferences
- . Caching web content for faster loading
- D. Personalizing the user experience
- 18. What is a potential privacy concern associated with third-party cookies?
  - 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
  - Tracking user interactions without a memory of previous requests
  - D. Ensuring consistent encryption for data transfer

FAST School of Computing

Fall-2023

Islamabad Campus

- 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?
  - M. 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

FAST School of Computing

Fall-2023

Islamabad Campus

#### Scenario:

#### Question 1 [15 Marks]

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.

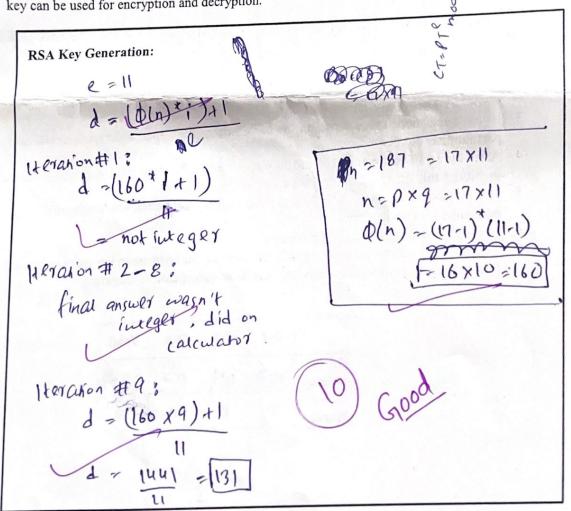
RSA Key Generation: [10 Marks]

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.

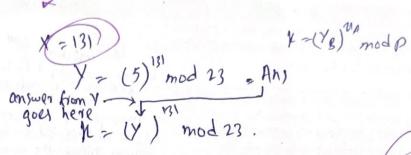
After exchanging public keys and generating the shared secret key, describe how Alice and Bob can use these keys to securely exchange a message. You can provide a simple example of how the shared secret key can be used for encryption and decryption.



Fall-2023

Islamabad Campus

## Diffie-Hellman Parameters: = 131) Y = (YB) 21 mod p



This will retorn the shared secret key. Values ?

#### Secure Communication

In case bob wank to send a message to Alice securely exchange a message, bob will use Alice's public ney for energyption and Alice will use her own private key for Lecryphon



FAST School of Computing

Fall-2023

Islamabad Campus

#### Question 2 [10 Marks]

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

Incident	and the intigation:				
A	You are reviewing the code for a login form on a website. The code uses user input directly in a SQL query.				
В	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.	by having a tray boundry (bine between code and wer into.  Down gradier TSI accepts which in ales the daingraded version apparantly look better.)			
С	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.	capt sal injection using			
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 actachs'. can be mitigated by implementing proper checks on			
E	Ali's online activity is being tracked online although they have disabled third party cookies.	sersion hijaching it secure.  Sersion hijaching can be mitigated by clearing cacle.  and disaling an cookies ton			

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?

Fall-2023

Islamabad Campus

For a mer sparching posts comaining the word "security". The sal query will look something like.

Select posts from table-name where posts-w DLIKE "% second?"

The actacher can conduct soll injection and do something likk

LIVE ;-- )

This will premarriely east the query and comment out the remaining part of the query in this case, the hijacher will get an the posts and goory will become like.

select post from taste name where posts w like 17. 7. 7; -- security

here security is commensed out and as the posts will be serected from the table.

Best of Luck @ \*