Tanzina, IT21005

Date:

Ans to the Ques no-1.

Shores algorithm runs on a quantum computer and can factor large integers and compute descrete logarithm in polynomial time

→RSA security is based on the hardness of factoring large semiprimes.

→ ECC security is based on the hardness of the elliptic curve discrete logarithm problem.

Both problems are efficiently solvable by shor's algorithm on a sufficiently large quantum computer.

Consequences:

→ Current public-key systems like RSA-2048 and ECC-256 would be broken in hours or hours or seconds on a large quantum computer.

→ Digital certificates, TLS/SSL, email encryption and blockchain systems relying on these schemes would be ~~compnosied~~ compromised.

Ans. to the Ques. no - 2

Role of QKD :

→ Uses quantum mechanics to securely exchange a secret key.

→ Example : BB84 protocol.

→ Any eavesdropping attempt disturbs the quantum state and can be detected.

Difference :

→ classical PKC relies on hard math problems.

→ QKD relies on physics law - theoretically unbreakable even by quantum computers.

→ QKD secures the key exchange, not the message encryption itself.

Tanzina · IT21005

Date

Ans. to the Ques. no - 3

Difference between lattice-based cryptography and RSA/ECC in the context of quantum resistance:

Hardness basis:

↳ RSA/ECC → based on factoring or discrete log; broken by quantum computers using shor's algorithm.

↳ Lattice-based: based on lattice problems with no known efficient quantum attack.

Security:

↳ RSA/ECC → not quantum safe.

↳ Lattice-based → considered quantum-safe.

key size:

↳ RSA/ECC → smaller keys.

↳ Lattice-based → larger keys, but still practical.

Tanzina, IT21005

Speed:

↳ Lattice → often faster for encryption/signatures than RSA with large keys.

Extra Features:

↳ Lattice allows advanced things like fully homomorphic encryption; RSA/ Ecc don't.

Ans. to the Ques. no - 4

python PRNG using time + seed:

```
import time

def custom_prng(seed):
    current_time = int(time.time() * 1000)
    combined = seed ^ current_time
    a = 1664525
    b = 1013904223
    m = 2**32
```

Tanzina, IT21005

```
random_num = (a * combined + c) % m
return random_num

seed = 12345
print("Random Number:", custom_prng(seed))
```

Output : Random Number : 2783789124

Ans. to the Ques. no - 5

Sieve of Eratosthenes algorithm:

→ Create a list of numbers from 2 to n.
→ Repeatedly remove multiples of each prime starting from 2.
→ Remaining numbers are primes.

Python Implementation:

```
def sieve(n):
    primes = [True] * (n+1)
    primes[0] = primes[1] = False
    for i in range(2, int(n** 0.5)+1):
        if primes[i]:
            for j in range(i*i, n+1, i):
```

Tanzina, IT21005

Date

S S M T W T F

$\Rightarrow 561 = 3 \times 11 \times 17$

it passes all the rules

so, this one is ch carmicheal.

$\Rightarrow 1105 = 5 \times 13 \times 17$

it also passes all the rules.

so, this one is also carmicheal.

$\Rightarrow 1729 = 7 \times 13 \times 19.$

it also carmicheal.

Tanzina, I

Ans. to the Ques. no - 7

(a) Is $\mathbb{Z}_{11}$ with $(+, \cdot)$ a ring?

Yes. $\mathbb{Z}_{11}$ (integers modulo 11) with addition and multiplication mod 11 is a ring. In fact, since 11 is prime, every nonzero element has a multiplicative inverse. So, $\mathbb{Z}_{11}$ is a field

Date:

s s m t w

Ans. to the Ques. no - 8

Remainder of -52 modulo 31 :

$-52 \bmod 31$

$-52 + 62 = 10$

$62 = 2.31$

$-52 \equiv 10 \pmod{31}$

Remainder $= 10$.

Tanzina, IT

Ans. to the Ques. no - 9

$7x \equiv 1 \pmod{26}$

As $\gcd(7, 26) = 1$, so inverse exists.

$7.15 = 105 \equiv 1 \pmod{26}$

$105 - 4.26 = 105 - 104 = 1$

Inverse $= 15$.

Ans. to the Ques. no - 10

$(-8 \times 5) \bmod 17$

$-8 \times 5 = -40$

$-40 \equiv -40 + 3 \cdot 17 = -40 + 51 = 11.$

So, $(-8 \times 5) \bmod 17 = 11.$

Ans. to the Ques. no - 11

Bézout's Theorem: For integers a, b not both zero, there exist integers x, y such that,

$ax + by = \gcd(a, b)$

If, $\gcd(a, m) = 1$

Bézout gives $ax + my = 1.$

So, $ax \equiv 1 \pmod{m}$: x is the multiplicative inverse of $a \bmod m$.

Tanzina, IT21005

Date:

Inverse of 97 modulo 385:

We find integers x, y with

$$97x + 385y = 1$$

One correct pair is

$$97.(-127) + 385.32 = 1$$

$-127 \bmod 385 = 385 - 127 = 258$

So, inverse $= 258$.

Ans. to the Ques. no-12

Existence of integer solutions for $ax+by=\gcd(a,b)$

Bézout's identity guarantees integer solutions x, y to $ax+by=\gcd(a,b)$. Constructed by the extended Euclidean algorithm.

Now, $43x \equiv 1 \pmod{240}$.

We need the inverse of 43 mod 240.

$\therefore 43 \cdot 67 + 240(-12) = 1$

$43^{-1} \equiv 67 \pmod{240}$.

Date :

S S M T W T F

Ans. to the Ques. no -13

Fermat's Little Theorem

If P is prime and gcd $(a, P) = 1$,

then, $a^{P-1} \equiv 1 \pmod{P}$

using in primality test :

Suppose, $a^{n-1} \bmod n = 1$. If not, n is composit.

If yes, n is probably prime.

561 is composite because $561 = 3 \times 11 \times 17$

Now, $5^{123} \bmod 17$

$5^{16} \equiv 1 \pmod{17}$

$123 \bmod 16 = 11$.

So, $5^{123} \equiv 5^{11}$

$5^2 \equiv 8$, $5^4 \equiv 13$, $5^8 \equiv 16$

$5^{11} \equiv 16 \times 8 \times 5 \equiv 9 \times 5 \equiv 11$.

So, $5^{123} \bmod 17 = 11$.

Tanzina, IT21005

Ans. to the Ques. no-14

Chinese Remainder Theorem:

If $m_1, m_2, \ldots, m_k$ are pairwise coprime positive integers, then for any integers $a_1, \ldots, a_k$ the system $x \equiv a_i \pmod{m_i}$ $(i = 1, \ldots, k)$

Let, $M = \prod_{i=1}^{k} m_i$,

$M_i = M / m_i$

$\gcd(M_i, m_i) = 1$; there exists an inverse y_i with $M_i y_i \equiv 1 \pmod{m_i}$.

$x = \sum_{i=1}^{k} a_i M_i y_i$

Now, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

Here, $m_1 = 3$, $m_2 = 5$, $m_3 = 7$ are pairwise coprime.

$M = 3.5.7 = 105$

$M_1 = 105 / 3 = 35$

.

Tanzina, IT21005

Tanzina, IT21005

Finding y_1 with $35 y_1 \equiv 1 \pmod 3$

$35 \equiv 2 \pmod 3$

$2y_1 \equiv 1 \pmod 3$

$y_2 \equiv 2 \pmod 3$

$\therefore a_1 M_1 y_1 = 2 \cdot 35 \cdot 2 = 140$

$M_2 = 105/5 = 21$

$21 \equiv 1 \pmod 5$

$y_2 \equiv 1$

$a_2 m_2 y_2 = 2 \cdot 21 \cdot 1 = 63.$

$M_3 = 105/7 = 15$

$15 \equiv 1 \pmod 7$

$y_3 \equiv 1$

$a_3 m_3 y_3 = 2 \cdot 15 \cdot 1 = 30$

Sum $= 140 + 63 + 30 = 233$

Reduce modulo 105 : $233 - 2 \cdot 105 = 233 - 210 = 23.$

So, the solution is,

$x \equiv 23 \pmod{105}$.

Ans. to the Ques. no - 15

CIA triad:

→ Confidentiality: keep data secret from unauthorized users. Achieved by encryption, access control, authentication.

→ Integrity: Ensure data is correct and unaltered. Achieved by checksums, hashes, digital signatures, versioning.

→ Availability: Ensure systems and data are accessible when needed. Achieved by backups, redundancy, failover, DDOS protection.

Tanzina, IT21005

Date

Ans. to the Ques. no-16

Steganography vs cryptography + common hiding techniques.

⇒ Difference:

↳ Cryptography hides the content of a message but does not hide that a message exists.

↳ Steganography hides the existence of the message by embedding it inside innocuous data. They can be combined: First encrypt the secret, then hide it.

Common techniques for hiding data in digital media

→ LSB (Least significant Bit) in images: modify least significant bits of pixel values to store bits of secret data.

Tanzina, IT21005

→ Audio steganography : alter LSBs of audio samples or use ~~impt~~ imperceptible frequency changes.

→ Video steganography : hide data across frames or in motion vectors.

→ Metadata hiding: place messages in file metadata field.

→ Text steganography : whitespace or font/ formatting changes, synonyms, or deliberate typos to encode bits.

Tanzina, IT21005

Ans. to the Ques. no 17

Key differences between phishing, malware and DoS attacks:

phishing → Tricks users into revealing sensitive information.

compromises confidentiality.

Date :

Malware → Malicious software installed on a system.

Can affect confidentiality, integrity and availability.

DoS → overloads a system or network with excessive requests to make it unavailable.

Primarily affects availability.

Tanzina, I

Ans. to the Ques. no-18

Role of GDPR in mitigating cyber attacks & protecting privacy.

User Consent: Requires organizations to get clear permission before collecting personal data.

Data Minimization: Encourages storing only necessary data.

Security measures: Mandates technical and organizational safeguards.

Breach Notification: Organizations must report breaches quickly.

Ans. to the Ques. no-19

DES encrypts 64-bit plaintext using a 56-bit key in 16 rounds.

steps:

1. Initial Permutation (IP).
2. Round functions (16 rounds).
3. Final permutation (FP).

Security role of each step:

→ IP & FP
→ Round Function
→ Key schedule

Tanzina, IT21005

Ans. to the Ques. no-20

DES first round (XOR only)

$f(R_0, k_1) = 0xF0F0F0F0 \oplus 0x0F0F0F0F = 0xFFFFFFFF$

$L_1 = R_0 = 0xF0F0F0F0$

$R_1 = L_0 \oplus f(R_0, k_1) = 0xAAAAAAAA \oplus 0xFFFFFFFF$

$= 0x55555555$

Ans. to the Ques. no-21

AES subBytes (partial S-box)

Input : [0x23, 0xA7, 0x4C, 0x19]

- 0x23 → Row 2, col 3 → 0xD4
- 0xA7 → Row A, col 7 → 0x63
- 0x4C → Row 4, col C → 0x2E
- 0x19 → Row 1, col 9 → 0xC6

Output : [0xD4, 0x63, 0x2E, 0xC6]

Tanzina, IT21005

Date :

S S M T W T F

Ans. to the Ques. no -13

Fermat's Little Theorem

If P is prime and gcd $(a, P) = 1$,

then, $a^{P-1} \equiv 1 \pmod{P}$

using in primality test :

Suppose, $a^{n-1} \bmod n = 1$. If not, n is composit.

If yes, n is probably prime.

561 is composite because $561 = 3 \times 11 \times 17$

Now, $5^{123} \bmod 17$

$5^{16} \equiv 1 \pmod{17}$

$123 \bmod 16 = 11$.

So, $5^{123} \equiv 5^{11}$

$5^2 \equiv 8$, $5^4 \equiv 13$, $5^8 \equiv 16$

$5^{11} \equiv 16 \times 8 \times 5 \equiv 9 \times 5 \equiv 11$.

So, $5^{123} \bmod 17 = 11$.

Tanzina, IT21005

Ans. to the Ques. no -22

AES AddRoundKey (XOR)

$[0x1A \oplus 0x55, 0x2B \oplus 0x66, 0x3C \oplus 0x77, 0x4D \oplus 0xB8]$

$= [0x4F, 0x4D, 0x4B, 0xC5]$

Ans. to the Ques. no -23

AES mixcolumns example:

Matrix x $[0x01, 0x02, 0x03, 0x04]$ over $GF(2^8)$:

Row 1 : $(02 \times 01) \oplus (01 \times 02) \oplus (01 \times 03) \oplus (03 \times 04) = 0x0E$

Row 2 : $(03 \times 01) \oplus (02 \times 02) \oplus (01 \times 03) \oplus (01 \times 04) = 0x0B$

Row 3 : $(01 \times 01) \oplus (03 \times 02) \oplus (02 \times 03) \oplus (01 \times 04) = 0x0D$

Row 4 : $(01 \times 01) \oplus (01 \times 02) \oplus (03 \times 03) \oplus (02 \times 04) = 0x09$

Output : $[0x0E, 0x0B, 0x0D, 0x09]$

Tanzina, IT21005

Ans. to the Ques. no - 24

Encrypts an IV with the key to get key-stream blocks, XOR with plaintext. Next key-stream block = encrypt previous keystream. Synchronization is ensured by using the same IV and keystream sequence at both ends.

Ans. to the Ques. no - 25

AES modes with error propagation:

- CBC : 1 block error → current block corrupted + 1 block partially corrupted.
- CFB : 1 byte error → current byte corrupted + next few bytes partially wrong.

Tanzina, IT21005

Tanzina, IT21005

Ans. to the Ques. no - 24

Encrypts an IV with the key to get key-stream blocks, XOR with plaintext. Next key-stream block = encrypt previous keystream. Synchronization is ensured by using the same IV and keystream sequence at both ends.

Ans. to the Ques. no - 25

AES modes with error propagation:

- CBC : 1 block error → current block corrupted +1 block partially corrupted.
- CFB : 1 byte error → current byte corrupted + next few bytes partially wrong.

Tanzina, IT21005

Ans. to the Ques. no-26

Recommended mode for large files with parallel processing CTR mode- allows independent encryption/decryption of blocks and no error propagation beyond affected block.

Ans. to the Ques. no-27

RSA encryption & decryption (M=1, e=5, n=14, d=11)

Encryption:

$C = M^e \bmod n = 1^5 \bmod 14 = 1$

The ciphertext is 1.

Decryption:

$M' = C^d \bmod n = 1^{11} \bmod 14 = 1$

The decrypted message matches the origin

So, RSA works here.

Tanzina, IT21005

Ans. to the Ques. no - 28

$H(M) = 5$, $d = 3$, $n = 33$

A digital signature is created by raising the hash to the private key power.

$S = H(M)^d \bmod n$

$= 5^3 \bmod 33$

$= 125 \bmod 33$

$= 26$

Signature = 26; which the ~~recie~~ receiver can verify using the public key.

Ans. to the Ques. no - 29

Diffle - Hellman key exchange

$p = 17, g = 3, a = 4, b = 5$

➢ Aleya's public key:

$A = g^a \bmod p = 3^4 \bmod 17 = 81 \bmod 17 = 13$

→ Badol's public key :

$B = g^b \bmod p = 3^5 \bmod 17 = 5$

As public key of Aleya = 13 and Badol = 5.

These will be exchanged to compute the shared secret.

Ans. to the Ques. no - 30

Simple Hash function

$H(x) = (\Sigma ASCII) \bmod 100$

- "AB" :

$65 + 66 = 131$

$\Rightarrow 131 \bmod 100 = 31$

- "BA" :

$66 + 65 = 131 \bmod 100 = 31$

→ Both give the same hash(31), even though the messages are different → this is called a collision

→ This shows weak hash functions are vulnerable to collisions, making them insecure for cryptographic use.

Tanzina, IT21005

Date:

S S M T W T F

Ans. to the Ques. no - 31

MAC Calculation & Forgery:

- MAC = (Message + Secretkey) mod 17 = (15 + 7) mod 17 = 22 mod 17 = 5

- If attacker changes message to 10, they'd need the key to compute correct MAC. Without key, they can't easily forge the right MAC.

Ans. to the Ques. no - 32

TLS Handshake:

1. Client Hello: Client sends supported cipher suits and a random number.

2. Server Hello: Server ~~server~~ selects cipher suite, sends certificate and random number.

3. key exchange : Client and server use asymmetric encryption (e.g., RSA or Diffie-Hellman) to securely share a session key.

4. Session key Generated: Both sides compute the same symmetric key.

5. Handshake complete: Secure communication begins using symmetric encryption.

Ans. to the ques. no - 13

SSH protocol stack

1. Transport Layer Protocol: handles encryption, integrity, compression and key exchange.

Tanziva, IT21005

2. User authentication protocol: verifies the user (password, public key, etc).

3. Connection Protocol: manages multiple channels (e.g., shell, file transfer) over the secure connection.

Ans. to the Ques. no 34

TLS Handshake steps:

Client Hello → Server Hello → Certificate → key Exchange → Session key → Encrypted Communication.

Tanzina, IT21005

Date

3. key exchange : Client and server use asymmetric encryption (e.g., RSA or Diffie-Hellman) to securely share a session key.

4. Session key Generated: Both sides compute the same symmetric key.

5. Handshake complete: Secure communication begins using symmetric encryption.

Ans. to the ques. no - 23

SSH protocol stack

1. Transport Layer Protocol: handles encryption, integrity, compression and key exchange.

Tanzina, IT21005

Tanzina, IT21005

Tanzina, IT21005

Date

Ans to the Ques. no-35

Elliptic Curve General Form

Equation:

$y^2 = x^3 + ax + b$ over a finite field.

Why in crypto: Provides strong security with small keys using the hardness of the elliptic curve discrete logarithm problem.

Ans. to the Ques. no-36

- Ecc achieves same security as RSA with much smaller keys because solving elliptic curve problems is much harder than factoring large integers.

Example: Ecc 256-bit ≈ RSA 3072-bit in security strength.

Tanzina, IT21005

Ans. to the Ques. no-37

Curve:

$$y^2 \equiv x^3 + 2x + 3 \pmod{97}$$

For, P = (3, 6)

L.H.S. $y^2 = 6^2 = 36$

R.H.S. $x^3 + 2x + 3$

$= 27 + 6 + 3$

$= 36$

Since,

$36 \equiv 36 \pmod{97}$; P lies on the curve.

Ans. to the Ques. no-38

ElGamal encryption

P = 23, g = 5, h = 8, m = 10, k = 6.

Tanzina, IT21005

Date:

- $C_1 = g^k \bmod p = 5^6 \bmod 23$

$5^2 = 23 \equiv 2$,;

$5^4 \equiv 4$;

$5^6 \equiv 4.2 = 8$

So, $C_1 = 8$.

- $C_2 = m.h^k \bmod p = 10.8^6 \bmod 23$

$8^2 = 64 \equiv 18$,

$8^4 \equiv 18^2 = 324 \equiv 2$,

$8^6 \equiv 2.18 = 36 \equiv 13$

$C_2 = 10.13 = 130 \equiv 15$

Ciphertext: $(C_1, C_2) = (8, 15)$.

Tanzina, IT21005

Date

Ans. to the Ques. no - 39

IoT devices have limited CPU, memory, power and bandwidth, so algorithms must be small, fast and low energy while still secure.

Example : Ascon (NIST LWC winner).
- lightweight AEAD and hash, designed for constrained devices.

Ans. to the Ques. no - 40

Here are three IOT-specific attacks & mitigations:

1. Firmware hijacking (malicious unautho-rized updates):

Tanzina, IT21005

Mitigate : secure boot, signed firmware + verified updates, rollback protection.

2. Physical tampering (opening device, probing/ debug ports.

Mitigate: Tamper-evident seals/enclosures, disable/lock JTAG/UART, secure elements/TPM, sensor tamper alarms.

3. Botnets (e.g., Mirai via default creds & Open Telnet).

Mitigate: Unique strong credentials, disable telnet / use SSH, rate-limit logins, auto-patching,

network segmentation ; IOT firewall / IDS . signed firmware.