SL .NO	TEAM	REG NO	NAME
1	TEAM 1	192110166	NUKANABOINA SAI VAMSI VAMSI
2		192110306	SIDDI PRAMOD KUMAR REDDY
3		192110355	BOLLU VIKAS VIKAS
4	TEAM 2	192110200	GANGAVARAM JAHNAVI
5		192110260	MEKALA DHARMIKA
6		192110275	NASINA HARITHA
7	TEAM 3	192110418	PALANKI VENKATA NAGA MUKESH
8		192110588	MUDDAPU VIJAYARAMARAJU
9		192110593	RAYIDI TIRUPATHIRAO
10	TEAM 4	192111296	BACHU.NEELIMA
11		192210239	DODDI GEETHA MADHURI
12		192210252	ISHA SINGH
13	TEAM 5	192111376	CHIMIDI PRANEETH KUMAR
14		192111448	BAKKACHENNAIAHGARI GNANESWAR REDDY

CASE STUDY

Online banking, also known as internet banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website.Online banking facilities typically have many features and capabilities in common, but also have some that are application specific. The common features fall broadly into several categories: - A bank customer can perform non-transactional tasks through online banking, including: (i) Viewing account balances (ii) Viewing recent transactions (iii) Downloading bank statements, for example in PDF format (iv) Viewing images of paid cheques (v) Ordering cheque books (vi) Download periodic account statements (vii) Downloading applications for M-banking, E-banking etc

Draw the steps and elucidate which type of authentication and encryption will be best suited for the Online Banking System.

On the server, we will have a corresponding method, such as verify_digest .. The server-sideprogram (ASP, JSP, Servlet, etc), which receives the client's form data, will call this method. This method will accept the original message and the message digest (say MD1) from the client,compute its own message digest (say MD2) and compare the two message digests (i.e. MD1 andMD2). Depending on the result of the message digest comparison, it will return an appropriate message back to the funds transfer

specifically designed for transfer of authentication data between two entities. It allows the receiving entity to authenticate the connecting entity (e.g. Client connecting to a Server) as well as authenticate itself to the connecting entity (Server to a client) by declaring the type of information needed for authentication as well as syntax. How does the recipient believe that the message was created by a known sender

Evaluate the security implications of implementing a screened host architecture versus a screened subnet firewall architecture for a medium-sized enterprise. Consider factors such as management complexity, consistency in security policies, and the potential impact of a security breach. Provide recommendations on the most suitable architecture for safeguarding information assets on the trusted network."

A hospital is transitioning to electronic health records (EHR). Discuss the role of digital signatures in securing patient data, ensuring its integrity, and providing a mechanism for healthcare professionals to

Q.1	**Q2**

Q3	**Q4**

	15		192111498	GALISETTY SHESHAGIRI
	16	TEAM 6	192121075	PALLE BHANU PRASAD BHANU PRASAD
	17		192121156L	GOKULNATH P
	18		192121158L	KIRUSHNNACHALAM G
	19	TEAM 7	192210029	GADDE VENKATA CHAITANYA KUMAR
	20		192210034	KALLU MAVEEN
	21		192210111	ABBURI YASWANTH
	22	TEAM 8	192210217	YAKKALA VAMSI KRISHNAJANA GUPTHA
	23		192210223	CHAKALI RAVI KUMAR
	24		192210229	HEMANTH KONATHALA
	25	TEAM 9	192210284	DHARMAYYAGARI JAYA SANKAR REDDY
	26		192210291	VENNAPUSA LOKESH
	27		192210386	G SANTHOSH REDDY
	28	TEAM 10	192210344	KANKANAMPATI BHUMIKA
	29		192211029	VASA BHANU SREE
	30		192211047	POTHANI KIRANMAIE
	31	TEAM 11	192210442	PUTLURU ANANDA BHIRAVA REDDY
	32		192210459	KONERU RUPESH REDDY
	33		192211256	PADALA KARTHI KESAVA REDDY
	34	TEAM 12	192211156	MEEGADA DEEPTHI REDDY
	35		192211568	KARRI GEETHA SOWMYA SRI
	36		192211668	SHAIK MAHABOOB HUSSAIN

trust the authenticity of the records.
Within a multinational manufacturing company's supply chain, provide a detailed explanation of how digital signatures are integrated to ensure the authenticity and integrity of critical documents. Discuss specific use cases, such as verifying the origin of components, preventing counterfeit products, and establishing trust between different entities in the supply chain.
In a scenario where employees frequently access corporate resources remotely using mobile devices, explicate how firewalls contribute to securing these remote connections. Deliberate the firewall configurations and policies that can protect against unauthorized access and potential attacks while maintaining a balance between security and user convenience.
In emergency situations where healthcare providers need immediate access to patient records and the ability to sign digital documents remotely, how does the implementation of digital signatures facilitate secure and timely access to patient records? Additionally, what measures are in place to ensure the authentication of healthcare professionals in remote environments, and how is the integrity of digitally signed documents maintained to support critical decision-making during emergencies?
With the advent of quantum computing, military organizations are considering the implications for cryptography. Discuss the importance of transitioning to quantum-safe cryptographic algorithms in military communications. Explore the challenges and strategies involved in preparing military networks for the post-quantum era.
Imagine a scenario where a backdoor malware infiltrates a secure communication system, compromising the confidentiality of transmitted data. Analyze the challenges in detecting and removing backdoor malware, the potential consequences of data exposure, and the strategies for strengthening the resilience of encrypted communication systems against such threats.
Drones and unmanned systems are integral to modern military operations. Explain how cryptographic measures are implemented to secure the communication links and control systems of unmanned vehicles. Discuss the challenges of ensuring the confidentiality and integrity of data transmitted between the operator and the unmanned system.
detection in identifying and preventing malicious activities carried out by insiders, including unauthorized access and data exfiltration. Discuss the balance between monitoring employee activities and respecting privacy concerns.

	37	TEAM 13	192211259	KATAKAM RAKESH REDDY
	38		192211354	KUBERA CHITHANYA KUMAR
	39		192211560	KODAM ABILASH
	40		192211680	T INDRA KUMAR

In a healthcare setting, unauthorized access to patient records can have severe consequences. How does the implementation of digital signatures enhance user authentication and access control to prevent unauthorized personnel from signing or accessing sensitive patient information?