Vidyalankar Institute of Technology
Semester VI – Computer Engineering – Mid Semester Assessment – 3

Date: 08/04/2024	Cryptography & System Security	30 Marks/1 hour

1	Solve any five (2 marks each)		CO
	A	Differentiate between MD5 SHA1 w.r.t output size.	CO3
	B	Draw the Diagram of MAC for checking message integrity.	CO3
	C	Demonstrate DDOS attack with proper diagram.	CO5
	D	If attacker can break the firewall security, it can easily compromise with IDS/IPS, how one can protect IDS/IPS from such scenario?	CO5
	E	What is DNS poisoning? Demonstrate with diagram.	CO5
	F	An ABC organization needs to hide all its internal machine IPs with an outside network, how it can do it? Give an example.	CO5
	G	How many chaining variables are needed in SHA-1 algorithm and of what size?	CO3
	H	SSL uses symmetric key encryption, justify with example.	CO5
2	Solve anyone (10 marks each)		
	A	An e-commerce company, has been experiencing network disruptions during peak hours of online sales. Upon investigation, the network administrators suspect that the disruptions may be due to multiple SYN packets. Demonstarte this attack and tell how network administrators got aware of this Attack	CO5
	B	ABC Enterprises is considering upgrading its network security infrastructure and is contemplating implementing a stateful inspection firewall. As part of the evaluation process, the IT security team is tasked with understanding the capabilities and benefits of this type of firewall. Explain what a stateful inspection firewall is with proper diagram and example.	CO5
3	Solve anyone (10 marks each)		
	A	A prominent financial institution, is considering implementing HMAC (Hash-based Message Authentication Code) for securing its online banking transactions. Demonstrate with diagram how HMAC is useful both at sending and receiving side to maintain integrity.	CO3
	B	Demonstrate the entire working of MD5 algorithm in detail.	CO3

CO3	Apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.
CO5	Understand network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols like SSL, IPSec, and PGP.

Vidyalankar Institute of Technology
Semester VI – Computer Engineering – Mid Semester Assessment – 3

Date: 08/04/2024	Cryptography & System Security	30 Marks/1 hour

1	Solve any five (2 marks each)		CO
	A	Differentiate between MAC SHA1 w.r.t output size.	CO3
	B	Draw the Diagram of MAC for checking message integrity.	CO3
	C	Demonstrate DDOS attack with proper diagram.	CO5
	D	If attacker can break the firewall security, it can easily compromise with IDS/IPS, how one can protect IDS/IPS from such scenario?	CO5
	E	What is DNS poisoning? Demonstrate with diagram.	CO5
	F	An ABC organization needs to hide all its internal machine IPs with an outside network, how it can do it? Give an example.	CO5
	G	How many chaining variables are needed in SHA-1 algorithm and of what size?	CO3
	H	SSL uses symmetric key encryption, justify with example.	CO5
2	Solve any one (10 marks each)		
	A	An e-commerce company, has been experiencing network disruptions during peak hours of online sales. Upon investigation, the network administrators suspect that the disruptions may be due to multiple SYN packets. Demonstarte this attack and tell how network administrators got aware of this Attack	CO5
	B	ABC Enterprises is considering upgrading its network security infrastructure and is contemplating implementing a stateful inspection firewall. As part of the evaluation process, the IT security team is tasked with understanding the capabilities and benefits of this type of firewall. Explain what a stateful inspection firewall is with proper diagram and example.	CO5
3	Solve any one (10 marks each)		
	A	A prominent financial institution, is considering implementing HMAC (Hash-based Message Authentication Code) for securing its online banking transactions. Demonstrate with diagram how HMAC is useful both at sending and receiving side to maintain integrity.	CO3
	B	Demonstrate the entire working of MD5 algorithm in detail.	CO3

CO3	Apply the knowledge of cryptographic checksums and evaluate the performance of different message digest algorithms for verifying the integrity of varying message sizes.
CO5	Understand network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols like SSL, IPSec, and PGP.