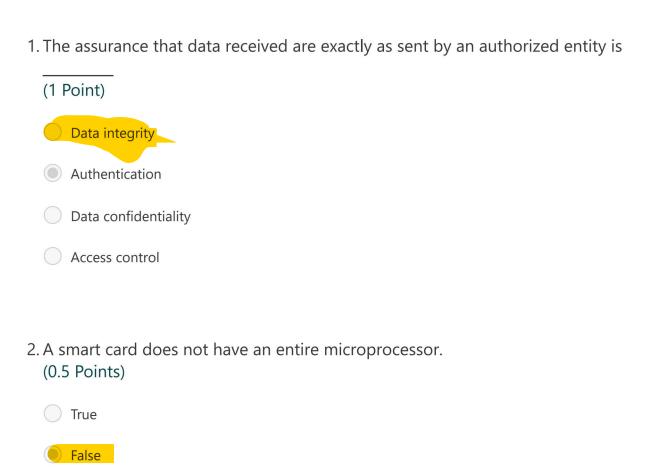
DataSecurityAndPrivacy-Quiz1 (UL_Info2_Data_Security_S5_Sec1_Fa2 1_22_HamssaHasrouny)



3. The ______ is the encryption algorithm run in reverse. (1 Point)



Plaintext	
Encryption algorithm	
Ciphertext	
4. Digital signatures and key management are the two most important applications of encryption.(1 Point)	5
Private-key	
Public-key	
Advanced	
5must accomplish encapsulation of incoming and outgoing data encryption of incoming and outgoing data and Authentication. (0.5 Points)	١,
○ VPN	
Firewall Analysis Tools	
Operating System Detection Tools	
6. The most commonly used asymmetric encryption are block ciphers. They are DET Triple DES and AES. (0.5 Points)	S,
True	
False	

7. Database access control can be managed centrally by a few privileged users. This is an example of MAC (Mandatory Access Control). (0.5 Points)
True True
False
8. The Caesar cipher of 'hawdy' encrypted using key 'f' is (1 Point)
○ MTIB
○ MTBID
MFBID
None
 The default set of rights should always follow the rule of least privilege or read- only access. (0.5 Points)
True True
○ False
10. On average, of all possible keys must be tried in order to achieve success with a brute-force attack.(1 Point)
One-fourth
Two-thirds
(Half

	Three-fourths
9	Two of the most important applications of public-key encryption are digital signatures and key management. (0.5 Points)
	True True
	☐ False
	In Differential backup, all the files created since the original full backup will always be copied again. (0.5 Points) True False
	Tuise Taise
	Symmetric encryption is used primarily to provide confidentiality (0.5 Points)
	False
	is "the process of verifying an identity claimed by or for a system entity". (1 Point)
	user authentication
	user authorization
	user control
	system management

e h	f Alice wants to send verification of her identity, she can send a message encrypted with her and anyone with her can verify that it was from her. 1 Point)
	Secret key, secret key
	Public key, private key
	Private key, public key
	Hash function, private key
	poses more management issues and can use large amounts of disk space. 0.5 Points)
	network-based IDPS
	host-based IDPS
u	prevents specific types of information from moving between an untrusted network and a trusted network. 0.5 Points)
	IDPSs
	Firewalls
	Port Scanners
u	backup involves making copies only of new files or of files that underwent some kind of change since the original full backup. 1 Point)
	full
	incremental

differential

(1 Point)

Cryptanalysis & Brute-Force attacks

	Cryptanalysis & DDoS
	Brute-force attack and CipherText
	Cryptanalysis & Caesar
23.	Public-key cryptography is symmetric. (0.5 Points)
	True
	€ False
24.	The original message or data that is fed into the algorithm is (1 Point)
	Encryption algorithm
	Decryption algorithm
	Secret key
	Plaintext
	Ciphers using substitutions or transpositions are not secure. (0.5 Points)
	True
	False
	is the scrambled message produced as output. (0.5 Points)
	Plaintext
(Ciphertext

Cryptanalysis
Secret key
27 is a procedure that allows communicating parties to verify that received or stored messages are authentic.
(1 Point)
Message authentication
Cryptanalysis
Decryption
28. Cryptanalytic attacks try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. (0.5 Points)
True
False
29 consists of striping, but no mirroring or parity. (1 Point)
RAIDO
RAID1
RAID3
RAID4
30. Packet-filtering firewalls examine the header information of data packets. Most

often based on the combination of:

(0.5 Points)

IP source and destination address
Direction (inbound or outbound)
Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests
All the choices
None of the choices
31. A is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained. (1 Point)
Cryptanalysis
Brute-force attack
Hash function
32. A message authentication code is a small block of data generated by a secret key and appended to a message. (0.5 Points)
True
False
33. Data integrity assures that information and programs are changed only in a specified and authorized manner. (0.5 Points)
True
False

34.	IDPSs can compensating for weak/missing security mechanisms in protection infrastructure (0.5 Points)
	○ True
	False False
35.	detect a violation of its configuration and activate alarm. (0.5 Points)
	Intrusion detection systems Firewalls
	Scanning and Analysis Tools
36.	is the granting of a right or permission to a system entity to access a system resource. (1 Point) Authorization
	Control
	Authentication
	Monitoring
37.	implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance. (1 Point)
	Access control
	System control

	Audit control
	Resource control
	38. Recognition by fingerprint, and retina are examples of (1 Point)
	static biometrics
	token authentication
	face recognition
	dynamic biometrics
į	39. A is created by using a secure hash function to generate a hash value for a message and then encrypting the hash code with a private key. (1 Point)
	One way hash function
	Digital signature
	Secret key
4	40 is based on the roles the users assume in a system rather than the user's identity. (1 Point)
	○ DAC
	RBAC
	MAC

This content is created by the owner of the form. The data you submit will be sent to the form owner. Microsoft is not responsible for the privacy or security practices of its customers, including those of this form owner. Never give out your password.

Powered by Microsoft Forms | Privacy and cookies | Terms of use