CyberRookie CSX Fundamentals - Section 3: Security Architecture Principles

Defense in depth	the practice of layering defenses to provide added protection
Perimeter	a well-defined (if mostly virtual) boundary between the organization and the outside world
Network or System-centric	the emphasis is on placing controls at the network and system levels to protect the information stored within
Data-centric	which emphasizes the protection of data regardless of its location
The perimeter	is an important line of defense that protects the enterprise against external threats, and its design should reflect a proactive stance toward preventing potential risk.
Internet Perimeter	An important component of the security perimeter which ensures secure access to the Internet for enterprise employees and guest users residing at all locations, including those involved in telecommuting or remote work.
Internet Perimeter	should route traffic between enterprise and Internet, no exes, monitor network ports, detect/block traffic from infected internal computers, control outbound traffic, identify/block anomalous traffic, eliminate threats like malware, enforce filtering policies.
Internet Perimeter	should always provide protection for VPNs, WANs, and WLANs
VPN protection should include	Terminating VPN traffic from remote users, provide a hub for terminating VPN traffic from remote sites, terminate traditional dial in users.
VPN Traffic	First filtered at the egress point to the specific IP addresses and protocols that are part of the VPN service. A remote user can only gain access after being authenticated.
WAN traffic	security is provided by input/output system (IOS) features. Unwanted traffic can be blocked from the remote branch using input access lists, and IP spoofing can be mitigated through L3 filtering.
In distributed and decentralized IT architectures	the third-party risk is likely to increase, often as a function of moving critical applications, platforms and infrastructure elements into the cloud.
Focus of cybersecurity is shifting toward contracts and service level agreements (SLAs)	for platforms, storage infrastructure and cloud-based data repositories
Cybercrime and cyberwarfare perpetrators	continue to aim at "weak spots" in architectural elements and systems
3rd party cloud providers	are facing an increased risk of attacks and breaches due to the agglomeration and clustering of sensitive data and information
APTs and cybercrime	always rely on preparatory research and insight into the target enterprise which raises the level of exposure for weak or unsecured parts of the overall architecture.
Vulnerable spots include	legacy systems, unpatched parts of the architecture, "dual persona" use of mobile devices and many others.
Architectural approaches	articulate the organization, roles, entities and relationships that exist or should exist to perform a set of business processes.
Process models and framework models	two models of security architecture
Framework security architecture models	describe the elements of architecture and how they relate to one another
Process security architecture modules	is more directive in its approach to the processes used for the various elements.
Zachman Framework	developing a who, what, where, when and how matrix which contains columns showing aspects of the enterprise that can be described or modeled. Rouser various viewpoints from which those aspects can be considered.
Zachman Framework	This approach provides a logical structure for classifying and organizing design elements, which improves the completeness of security architecture.
SABSA	Sherwood Applied Business Security Architecture

25. **TOGAF**	The Open Group Architecture Framework
26. **The Open Group Architecture Framework**	developed by Open Group in 1990s, high level an holistic approach addresses security as an essential component of the overall enterprise design.
27. **The Open Group Architecture Framework**	objective is to ensure that architectural development projects meet business objectives, that they are systematic and that their results are repeatable
28. **OSI Model**	Open Systems Interconnect model
29. **OSI Model**	is used to describe networking protocols and considered a reference to standardize the development of actual networks. OSI was the first nonproprietary open definition for networking.
30. **OSI Model**	defines groups of functionality required for network computers into layers, with each layer implementing a standard protocol for its functionality.
31. **OSI Layers**	Physical, Data-link, Network Transport, Session, Presentation, Application.
32. **Physical Layer**	Manages signals among network systems
33. **Data Link Layer**	Divides data into frames that can be transmitted by the physical layer
34. **Network Layer**	Translates network addresses and routes data from sender to receiver
35. **Transport Layer**	Ensures that data are transferred reliably in the correct sequence
36. **Session Layer**	Coordinates and manages user connections
37. **Presentation Layer**	Formats, encrypts and compresses data
38. **Application Layer**	Mediates between software applications and other layers of network services
39. **Transmission Control Protocol/Internet Protocol (TCP/IP)**	protocol suite used as the de facto standard for the Internet includes both network-oriented protocols and application support
40. **Equipment for Application, Presentation and Session Layer**	Gateway
41. **Equipment for Transport Layer**	Layer 4 Switch
42. **Equipment for Network Layer**	Router, Layer 3 switch
43. **Equipment for Data link Later**	Layer 2 swtich, bridge, Wireless AP, NIC
44. **Equipment for Physical Layer**	Hub, Repeater, NIC
45. **Application Layer functions**	provides user interface. file, print, message, database and application services
46. **Presentation layer functions**	Presents data handles processing such as encryption. Data encryption, compression and translation services.
47. **Session layer functions**	Keeps the data different applications separate. Dialog control
48. **Transport layer functions**	Provide reliable or unreliable delivery. End-to-end connection
49. **Network layer function**	Provides logical addressing which routers use for path determination. Routing
50. **Data link layer function**	combines packets into bytes and bytes into frames. Provides access to media using MAC Address. Performs error detection, not error correction. Framing
51. **Physical layer function**	Moves bits between devices, specifics voltage, wire speed and pin-out of cables. Physical topography
52. **TCP/IP protocols for application, presentation and session layer**	HTTP, FTP, SMTP, TFTP, NFS, NSP, SNMP, Telnet, LPD, X Windows, DNS, DHCP
53. **TCP/IP protocols for transport layer**	TCP and UDP
54. **TCP/IP protocols for Network Layer**	ICMP, ARP, RARP, and IP
55. **TCP/IP protocols for Data link layer**	Ethernet, Fast Ethernet, FDDI, Token Ring, Point-to-point
56. **Defense in depth, security in depth or protection in depth.**	using several controls to protect an asset
57. **Defense in depth**	important concept in designing an effective information security strategy or architecture.
58. **The number of types of layers needed in defense in depth**	a function of asset value, criticality, the reliability of each control and the degree of exposure.

59.	**Advantages of using a defense in depth strategy**	increasing the effort required for a successful attack and creating additional opportunities to detect or delay an attacker
60.	**Types of Defense**	Concentric Rings (nested layering), overlapping redundancy, segregation or compartmentalization
61.	**Concentric Rings**	Creates a series of nested layers that must be bypassed in order to complete an attack. Each layer delays the attacker and provides opportunities to detect the attack.
62.	**Overlapping Redundancy**	Two or more controls that work in parallel to protect an asset. Provides multiple, overlapping points of detection. This is most effective when each control is different.
63.	**Segregation or compartmentalization**	Compartmentalizes access to an asset, requiring two or more processes, controls or individuals to access or use the asset. This is effective in protecting very high value assets or in environments where trust is an issue.
64.	**Horizontal defense in depth**	where controls are placed in various places in the path of access for an asset, which is functionally equivalent to concentric ring model above
65.	**Vertical defense in depth**	where controls are placed at different system layers—hardware, operating system, application, database or user levels
66.	**Defense in depth questions**	What vulnerabilities are addressed by each layer or control? How does the layer mitigate the vulnerability? How does each control interact with or depend on the other controls?
67.	**Firewall**	a system or combination of systems that enforces a boundary between two or more networks, typically forming a barrier between a secure and an open environment such as the Internet.
68.	**Firewalls**	Companies should build these as one means of perimeter security for their networks.
69.	**Firewall**	It applies rules to control the type of networking traffic flowing in and out
70.	**Firewalls**	should allow individuals on the corporate network to access the Internet and simultaneously prevent others on the Internet from gaining access to the corporate network to cause damage.
71.	**Deny-all philosophy**	which means that access to a given resource will be denied unless a user can provide a specific business reason or need for access to the information resource.
72.	**Accept-all philosophy**	under which everyone is allowed access unless someone can provide areas for denying access.
73.	**Firewalls**	separate networks from one another and screen the traffic between them.
74.	**Firewalls**	control the most vulnerable point between a corporate network and the Internet, and they can be as simple or complex as the corporate information security policy demands.
75.	**Firewalls**	Block, limit, prevent monitor and encrypt access
76.	**Network firewall types**	Packet filtering Application firewall systems, Stateful inspection
77.	**Packet filtering firewalls**	a screening router examines the header of every packet of data traveling between the Internet and the corporate network
78.	**Packet filtering firewalls**	are best suited for smaller networks. Organizations with many routers may face difficulties in designing, coding and maintaining the rule base.
79.	**packet filtering firewalls**	filtering rules are performed at the network layer
80.	**Packet Filtering Firewalls Advantages**	Simplicity of one network "choke point", Minimal impact on network performance, Inexpensive or free
81.	**Packet Filtering Firewalls Disadvantages**	Vulnerable to attacks from improperly configured filters, Vulnerable to attacks tunneled over permitted services, All private network systems vulnerable when a single packet filtering router is compromised
82.	**Common attacks against packet filter firewalls are:**	IP spoofing, Source routing specification, Miniature fragment attack.

83.	**IP spoofing**	the attacker fakes the IP address of either an internal network host or a trusted network host. This enables the packet being sent to pass the rule base of the firewall and penetrate the system perimeter.
84.	**Source routing specification**	centers around the routing that an IP packet must take when it traverses the Internet from the source host to the destination host. It is possible to define the route so it bypasses the firewall
85.	**Miniature fragment attack**	an attacker fragments the IP packet into smaller ones and pushes it through the firewall. Only the first sequence of fragmented packets will be examined, allowing the others to pass without review
86.	**application- and circuit-level gateways**	allow information to flow between systems but do not allow the direct exchange of packets. Therefore, application firewall systems provide greater protection capabilities than packet filtering routers.
87.	**Two types of application firewall systems**	Windows NT and Unix. They work at the application level of the OSI model.
88.	**Two types of application firewall systems**	Application-level gateways and Circuit-level gateways
89.	**Application-level gateways**	systems that analyze packets through a set of proxies—one for each service. HTTP Proxy
90.	**Circuit-level gateways**	Commercially, these are quite rare. Because they use one proxy server for all services, they are more efficient and also operate at the application level
91.	**Circuit-level gateway may be a better choice**	When network performance is a concern
92.	**Circuit-level gateways**	TCP and UDP sessions are validated, typically through a single, general-purpose proxy before opening a connection.
93.	**application-level gateways,**	which require a special proxy for each application-level service
94.	**Application-level gateways and Circuit-level gateways**	systems employ the concept of bastion hosting in that they handle all incoming requests from the Internet to the corporate network, such as FTP or web requests.
95.	**Bastion hosts**	are heavily fortified against attack.
96.	**application-based firewall systems**	are set up as proxy servers to act on the behalf of someone inside an organization's private network
97.	**proxy server**	acting as a go between. Contacts the Internet server, and then this server sends the information from the Internet server to the computer inside the corporate network
98.	**proxy server**	can maintain security by examining the program code of a given service (e.g., FTP, Telnet). It then modifies and secures it to eliminate known vulnerabilities and also log all traffic between the Internet and the network.
99.	**NAT capability**	feature available on both types of firewall systems
100.	**Application Firewalls Advantages**	Provide security for commonly used protocols, Generally hide the network from outside untrusted networks, Ability to protect the entire network by limiting breakins to the firewall itself, Ability to examine and secure program code
101.	**Application Firewalls Disadvantages**	Poor performance and scalability as Internet usage grows
102.	**Stateful inspection firewall or dynamic packet filtering**	tracks the destination IP address of each packet that leaves the organization's internal network
103.	**Stateful inspection firewall**	Whenever a response to a packet is received, its record is referenced to ascertain whether the incoming message was made in response to a request that the organization sent out
104.	**Stateful inspection firewall**	This is done by mapping the source IP address of an incoming packet with the list of destination IP addresses that is maintained and updated. This approach prevents any attack initiated and originated by an outsider.
105.	**stateful inspection firewalls**	provide control over the flow of IP traffic.

106.	**Advantages of Stateful Inspection Firewalls**	Provide greater control over the flow of IP traffic, Greater efficiency in comparison to CPU-intensive, full-time application firewall systems
107.	**Disadvantages of Stateful Inspection Firewalls**	Complex to administer
108.	**Stateless filtering**	does not keep the state of ongoing TCP connection sessions. it has no memory of what source port numbers the sessions' client selected
109.	**Stateful firewalls**	keep track of TCP connections. The firewall keeps an entry in a cache for each open TCP connection.
110.	**Stateless firewalls**	perform more quickly than stateful firewalls, but they are not as sophisticated.
111.	**Examples of Firewall Implementations**	Screened-host firewall, Dual-homed firewall, Demilitarized zone (DMZ) or screened-subnet firewall.
112.	**Screened-host firewall**	Utilizing a packet filtering router and a bastion host, this approach implements basic network layer security (packet filtering) and application server security (proxy services).
113.	**Screened-host firewall**	An intruder in this configuration must penetrate two separate systems before the security of the private network can be compromised. This firewall system is configured with the bastion host connected to the private network with a packet filtering router between the Internet and the bastion host
114.	**Dual-homed firewall**	This is a firewall system that has two or more network interfaces, each of which is connected to a different network. Usually acts to block or filter some or all of the traffic trying to pass between the networks
115.	**Demilitarized zone (DMZ) or screened-subnet firewall**	This is a small, isolated network for an organization's public servers, bastion host information servers and modem pools. Connects the untrusted network to the trusted network, but it exists in its own independent space to limit access and availability of resources.
116.	**Problems faced by organizations that have implemented firewalls**	Configuration errors, Monitoring demands, Policy maintenance, Vulnerability to application- and input-based attacks.
117.	**Firewalls**	may be implemented using hardware or software platforms.
118.	**Hardware Firewall**	will provide performance with minimal system overhead. Although hardware-based firewall platforms are faster, they are not as flexible or scalable as software-based firewalls
119.	**Software-based firewalls**	are generally slower with significant systems overhead
120.	**For the firewall it's better to use**	Applications rather than normal servers
121.	**Virtual local area networks (VLANs)**	groups of devices on one or more logically segmented LAN.
122.	**Common technique for implementing network security**	is to segment an organization's network so that each segment can be separately controlled, monitored and protected.
123.	**VLAN**	is set up by configuring ports on a switch, so devices attached to these ports may communicate as if they were attached to the same physical network segment, although the devices are actually located on different LAN segments.
124.	**VLAN**	based on logical rather than physical connections and, thus, it allows great flexibility. Enables administrators to segment network resources for optimal performance by restricting users' access of network resources to the necessary individuals only.
125.	**creating separate zones**	controls can be applied at a more granular level based on the systems, information and applications in each area.
126.	**separate zones**	can create defense in depth where additional layers of authentication, access control and monitoring can take place.
127.	**Demilitarized zone (DMZ)**	which places limited systems, applications and data in a public-facing segment

128.	**DMZ**	Utilizing two packet filtering routers and a bastion host, this approach creates the most secure firewall system because it supports network- and application-level security while defining a separate DMZ network.
129.	**DMZ**	functions as a small, isolated network for an organization's public servers, bastion host information servers and modem pools.
130.	**The key benefits of a DMZ are**	An intruder must penetrate three separate devices, Private network addresses are not disclosed to the Internet, Internal systems do not have direct access to the Internet
131.	**Integral parts of cybersecurity**	Monitoring, detection and logging
132.	**Two types of attack vectors**	ingress and egress
133.	**Ingress**	network communications coming in
134.	**Egress**	network communications going out
135.	**data loss prevention program**	helps an organization protect its information and prevent the exfiltration of sensitive data.
136.	**DLP solutions cover three primary states of information**	Data at rest, Data in motion, data in use
137.	**Data at rest**	stored data
138.	**Data in motion**	to data traveling through the network
139.	**Data in use**	data movement at the user workstation level
140.	**Malicious software**	is one of the most common attack vectors used by adversaries to compromise systems.
141.	**Heuristic-based methods of detecting unknown malware**	use specific techniques to identify common malicious code behaviors and flag them as suspicious.
142.	**Anti-malware can be controlled through many different mechanisms**	Restriction of outbound traffic, Policies and awareness training, Multiple layers of anti-malware software
143.	**intrusion detection system**	Another element to securing networks complementing firewall implementation
144.	**An IDS**	works in conjunction with routers and firewalls by monitoring network usage anomalies
145.	**Network-based IDSs**	identify attacks within the monitored network and issue a warning to the operator.
146.	**Host-based IDSs**	are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack. Can detect the modification of executable programs, detect the deletion of files and issue a warning when an attempt is made to use a privileged command
147.	**Components of an IDS**	Sensors responsible for collecting data in the form of network packets, log files, system call traces, Analyzers that receive input from sensors, an administration console, a user interface
148.	**Types of IDSs include**	Signature-based, Statistical-based, Neural networks
149.	**Broad categories of IDSs**	Network-based IDSs and Host-based IDSs
150.	**Signature-based**	These IDS systems protect against detected intrusion patterns. The intrusive patterns they can identify are stored in the form of signatures.
151.	**Statistical-based**	These systems need a comprehensive definition of the known and expected behavior of systems.
152.	**Neural networks**	An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database. It is similar to the statistical model but with added self-learning functionality.
153.	**Signature-based IDSs**	are not able to detect all types of intrusions due to the limitations of their detection rules.
154.	**statistical-based IDS systems**	may report many events outside of the defined normal activity that are still normal activities on the network
155.	**signature and statistical-based**	A combination of these models provides better protection.
156.	**Features available in an IDS include**	Intrusion detection, Ability to gather evidence on intrusive activity, Automated response (e.g., termination of connection, alarm messaging), Security policy, Interface with system tools, Security policy management

157.	**IDS cannot help with the following weaknesses**	Weaknesses in the policy definition (see Policy section), Application-level vulnerabilities, Back doors into applications, Weaknesses in identification and authentication schemes
158.	**intrusion prevention system (IPS)**	predicts an attack before it occurs.
159.	**intrusion prevention system (IPS)**	monitoring key areas of a computer system and looking for "bad behavior," such as worms, Trojans, spyware, malware and hackers.
160.	**intrusion prevention system (IPS)**	complements firewall, antivirus and antispyware tools to provide complete protection from emerging threats.
161.	**intrusion prevention system (IPS)**	able to block new (zero-day) threats that bypass traditional security measures since it does not rely on identifying and distributing threat signatures or patches.
162.	**IDS policy**	should establish the action to be taken by security personnel in the event that an intruder is detected.
163.	**IDS policy actions**	Terminate the access and Trace the access
164.	**Terminate the access**	If there is a significant risk to the organization's data or systems, immediate termination is the usual procedure.
165.	**Trace the access**	If the risk to the data is low, the activity is not immediately threatening, or analysis of the entry point and attack method is desirable, the IDS can be used to trace the origin of the intrusion.
166.	**IDS and IPS**	can be directly integrated so that one product sends alert data to another
167.	**IPSs**	designed to not only detect attacks, but also to prevent the intended victim hosts from being affected by the attacks
168.	**IPS**	should prevent malicious programs from causing a system to delete all the files in a system directory
169.	**advantages of IPSs include**	Protection at the application layer, Prevention of attacks rather than simply reacting to them, Defense in depth, Real-time event correlation
170.	**IPSs**	can generate false positives that can create serious problems if automated responses are used.
171.	**Encryption**	is the process of converting a plaintext message into a secure-coded form of text, called ciphertext
172.	**ciphertext**	cannot be understood without converting back, via decryption—the reverse process—to plaintext
173.	**a key**	special encryption/decryption password
174.	**encryption**	is subject to governmental laws and regulations that limit the key size or define what may not be encrypted.
175.	**cryptography**	Encryption is part of a broader science of secret languages
176.	**cryptography**	Protect information stored on computers from unauthorized viewing and manipulation, Protect data in transit over networks from unauthorized interception and manipulation, Deter and detect accidental or intentional alterations of data, Verify authenticity of a transaction or document
177.	**encryption**	is limited in that it cannot prevent the loss of data.
178.	**encryption**	should be regarded as an essential, but incomplete, form of access control that should be incorporated into an organization's overall computer security program.
179.	**Key elements of cyptographic systems include**	Encryption algorithm, Encryption key, Key length
180.	**Encryption algorithm**	Mathematically based function or calculation that encrypts or decrypts data.
181.	**Encryption key**	Piece of information similar to a password that makes the encryption or decryption process unique. A user needs the correct key to access or decipher a message, as the wrong key converts the message into an unreadable form.
182.	**Key length**	Predetermined length for the key. The longer the key, the more difficult it is to compromise in a brute force attack where all possible key combinations are tried.
183.	**Effective cryptographic systems depend upon a variety of factors**	Algorithm strength, Secrecy and difficulty of compromising a key, Nonexistence of back doors, Inability to decrypt parts of a ciphertext message and prevent known plaintext attacks, Properties of the plaintext known by a perpetrator

184.	**There are two types of cryptographic systems**	Symmetric Key Systems and Asymmetric Key Systems
185.	**Symmetric Key Systems**	These use single, secret, bidirectional keys that encrypt and decrypt
186.	**Asymmetric Key Systems**	These use pairs of unidirectional, complementary keys that only encrypt or decrypt. Typically, one of these keys is secret, and the other is publicly known.
187.	**Public key systems**	are asymmetric cryptographic systems.
188.	**keys and hash values**	are used to transform a string of characters into a shorter or fixed-length value or key that represents the original string
189.	**Symmetric key cryptographic systems**	are based on a symmetric encryption algorithm, which uses a secret key to encrypt the plaintext to the ciphertext and the same key to decrypt the ciphertext to the corresponding plaintext
190.	**Symmetric key**	the key is said to be symmetric because the encryption key is the same as the decryption key
191.	**Data Encryption Standard (DES)**	most common symmetric key cryptographic system
192.	**DES**	is based on a public algorithm that operates on plaintext in blocks (strings or groups) of bits
193.	**DES**	this type of algorithm is known as a block cipher.
194.	**DES**	uses blocks of 64 bits.
195.	**DES**	is no longer considered a strong cryptographic solution because its entire key space can be forced when every key is tried by large computer systems within a relatively short period of time.
196.	**DES**	is being replaced with AES
197.	**AES**	public algorithm that supports keys from 128 bits to 256 bits.
198.	**2 main advantages to symmetric key cryptosystems such as DES or AES**	The user only has to remember/know one key for both encryption and decryption, Symmetric key cryptosystems are generally less complicated and, therefore, use up less processing power than asymmetric techniques. They are ideally suited for bulk data encryption.
199.	**disadvantages to symmetric key cryptosystems such as DES or AES**	Difficulty distributing keys and Limitations of shared secret
200.	**Triple DES or 3DES**	One form of advanced encryption algorithm
201.	**Triple DES**	provides a relatively simple method of increasing the key size of DES to protect information without the need to design a completely new block cipher algorithm.
202.	**asymmetric encryption process**	two keys work together as a pair. One key is used to encrypt data; the other is used to decrypt data.
203.	**asymmetric encryption**	Either key can be used to encrypt or decrypt, but once the key has been used to encrypt data, only its partner can be used to decrypt the data
204.	**asymmetric encryption**	The key that was used to encrypt the data cannot be used to decrypt it. Thus, the keys are asymmetric in that they are inversely related to each other.
205.	**asymmetric keys**	generate a single product from two large prime numbers, making it impractical to factor the number and recover the two factors
206.	**asymmetric keys**	often used for short messages such as encrypting DES symmetric keys or creating digital signatures
207.	**asymmetric encryption**	one key—the secret or private key—is known only to one person.
208.	**asymmetric encryption**	a message that has been sent encrypted by the secret (private) key of the sender can be deciphered by anyone with the corresponding public key
209.	**asymmetric encryption**	A message that has been sent encrypted using the public key of the receiver can be generated by anyone, but can only be read by the receiver.
210.	**Elliptical Curve Cryptography (ECC)**	a variant and more efficient form of public key cryptography and is gaining prominence as a method for increasing security while using minimum resources.
211.	**Elliptical Curve Cryptography (ECC)**	demands less computational power and therefore offers more security per bit
212.	**Elliptical Curve Cryptography (ECC)**	works well on networked computers requiring strong cryptography. However, it has some limitations such as bandwidth and processing power.

213.	**Quantum cryptography**	is the next generation of cryptography that may solve some of the existing problems associated with current cryptographic systems, specifically the random generation and secure distribution of symmetric cryptographic keys
214.	**Quantum cryptography**	based on a practical application of the characteristics of the smallest "grains" of light (photons) and the physical laws governing their generation, propagation and detection.
215.	**AES**	has replaced the DES as the cryptographic algorithm standard
216.	**Rijndael**	is a symmetric block cipher with variable block and key length
217.	**Rijndael**	as the algorithm for the AES.
218.	**AES**	the block length was fixed to 128 bits, and three different key sizes (128, 192 and 256 bits) were specified
219.	**three different versions of AES**	AES-128, AES-192 and AES-256
220.	**AES**	cipher is based on substitution bytes, shifting rows, mixing columns and adding round keys that are repeated for 10 rounds
221.	**Decryption**	is computed by applying inverse functions of the round operations.
222.	**digital signature**	is an electronic identification of a person or entity created by using a public key algorithm.
223.	**checksum or digital signature algorithm**	To verify the integrity of the data, a cryptographic hashing algorithm is computed against the entire message or electronic document, which generates a small fixed string message, usually about 128 bits in length
224.	**message digest**	which generates a small fixed string message, usually about 128 bits in length
225.	**Common types of message digest algorithms**	SHA1, SHA2, MD2, MD4 and MD5
226.	**message digest algorithms**	algorithms are one-way functions, unlike private and public key encryption algorithms
227.	**cannot be reversed**	process of creating message digests
228.	**message digest algorithms**	meant for digital signature applications where a large electronic document or string of characters, such as word processor text, a spreadsheet, a database record, the content of a hard disk or a JPEG image has to be compressed in a secure manner before being signed
229.	**MD2**	optimized for 8-bit machines
230.	**MD4 and MD5**	32-bit machines
231.	**verifies the identity of the sender**	is to encrypt the message digest using the sender's private key, which "signs" the document with the sender's digital signature for message authenticity
232.	**To decipher a message digest**	the receiver would use the sender's public key, proving that the message could only have come from the sender
233.	**Once the message digest is decrypted**	the receiver will recompute the hash using the same hashing algorithm on the electronic document and compare the results with what was sent, to ensure the integrity of the message
234.	**digital signature is a cryptographic method that ensures**	Data integrity, Authentication, Nonrepudiation
235.	**Data integrity**	Any change to the plaintext message would result in the recipient failing to compute the same message hash.
236.	**Authentication**	The recipient can ensure that the message has been sent by the claimed sender since only the claimed sender has the secret key.
237.	**Nonrepudiation**	The claimed sender cannot later deny generating and sending the message.
238.	**Digital signatures and public key encryption**	are vulnerable to man-in-the-middle attacks wherein the sender's digital signature private key and public key may be faked
239.	**PKI**	performs the function of independently authenticating the validity of senders' digital signatures and public keys.
240.	**VPN**	is an example of applied cryptography that typically exchanges secure data over the Internet. Encryption is needed to make the connection virtually private.
241.	**IPSec**	popular VPN technology
242.	**IPSec**	which commonly uses the DES, Triple DES or AES encryption algorithms.

243.	**DES**	uses 56-bit keys
244.	**Triple DES**	applies the (56-bit) key three times to achieve an effective key length of 168
245.	**AES**	is a new standard adopted in 2001 that uses keys that can be 128, 192 or 256 bits long and a block size of 128 bits
246.	**Wired Equivalency Protocol - WEP**	most commonly used method for wireless local area networks
247.	**WPA and WPA2**	increasing number of organizations and vendors are replacing WEP with this
248.	**WPA and WPA2**	which uses dynamic keys and an authentication server with credentials to increase protection against hackers.
249.	**WEP and WPA**	comply with the evolving versions of the 802.11 wireless standard specified by the Institute of Electrical and Electronics Engineers (IEEE),
250.	**WPA**	key is protected with a passphrase that does not have a rigorously enforced length
251.	**WPA**	is a subset of the developing 802.11i standard
252.	**ECC**	suited for small devices because the algorithm, by combining plane geometry with algebra, can achieve stronger authentication with smaller keys compared to traditional methods, such as RSA, which primarily use algebraic factoring
253.	**ECC**	is not as rigorous as traditional public key algorithms because it has a shorter history than algorithms like RSA
254.	**ACLs**	cannot prevent improper use of information by systems administrators, as the latter can have total control of a computer
255.	**Encryption**	can fill the security gap, and it can also protect data from hackers who, by means of malicious software, can obtain systems administration rights
256.	**Encryption**	also helps to protect data when a computer or a disk falls into the wrong hands
257.	**PKI**	allows a trusted party to issue, maintain and revoke public key certificates
258.	**PKI**	allows users to interact with other users and applications to obtain and verify identities and keys from trusted sources.
259.	**Key elements of the PKI infrastructure are**	Digital certificates, Certificate authority, Registration authority
260.	**Digital certificates**	is composed of a public key and identifying information about the owner of the public key. Purpose is to associate a public key with the individual's identity in order to prove the sender's authenticity.
261.	**Certificate authority or CA**	is an authority in a network that issues and manages security credentials and public keys for message signature verification or encryption. Attests to the authenticity of the owner of a public key
262.	**Registration authority or RA**	is an authority in a network that verifies user requests for a digital certificate and tells the CA to issue it
263.	**The status and values of a current user's certificate should include**	A distinguishing username, An actual public key, The algorithm used to compute the digital signature inside the certificate, A certificate validity period
264.	**Digital certificate process**	requires the sender to "sign" a document by attaching a digital certificate issued by a trusted entity. The receiver of the message and accompanying digital certificate relies on the public key of the trusted third-party certificate authority (CA) to authenticate the message. The receiver can link the message to a person, not simply to a public key, because of their trust in this third party.
265.	**Types of CAs**	Organizationally empowered, which have authoritative control over those individuals in their name space, Liability empowered, for example, choosing commercially available options (such as VeriSign) in obtaining a digital certificate
266.	**CA**	is responsible for managing the certificate throughout its life cycle.
267.	**RA functions**	Verifying information supplied by the subject, Verifying the right of the subject to requested certificate attributes, Verifying that the subject actually possesses the private key being registered and that it matches the public key requested for a certificate (generally referred to as proof of possession [POP])

268.	**RA functions**	Reporting key compromise or termination cases where revocation is required, Assigning names for identification purposes, Generating shared secrets for use during the initialization and certificate pick-up phases of registration, Initiating the registration process with the CA on behalf of the subject end entity, Initiating the key recovery processing
269.	**RA functions**	Distributing the physical tokens (such as smart cards) containing the private keys and Certification practice statement
270.	**Certification practice statement**	is a detailed set of rules governing the CA's operations. It provides an understanding of the value and trustworthiness of certificates issued by a given CA
271.	**Certificate revocation list – CRL**	is an instrument for checking the continued validity of the certificates for which the CA has responsibility.
272.	**Use of cryptosystems by applications**	generally involves a combination of private/public key pairs, secret keys, hash functions and digital certificates.
273.	**cryptosystems by applications**	purpose of applying these combinations is to achieve confidentiality, message integrity or nonrepudiation by either the sender or recipient
274.	**cryptosystems by applications**	process generally involves the sender hashing the message into a message digest or pre-hash code for message integrity, which is encrypted using the sender's private key for authenticity, integrity and non-repudiation
275.	**Sender encrypts message**	using his/her secret key
276.	**the secret key**	is encrypted with the recipient's public key, which has been validated through the recipient's digital certificate and provides message confidentiality
277.	**recipient decrypts message**	using his/her private key to decrypt the senders secret key
278.	**uses senders secret key**	to decrypt the message, to expose it
279.	**SSL**	is a session- or connection-layered protocol widely used on the Internet for communication between browsers and web servers, in which any amount of data is securely transmitted while a session is established.
280.	**SSL**	provides end-point authentication and communications privacy over the Internet using cryptography
281.	**SSL**	only the server is authenticated while the client remains unauthenticated.
282.	**Mutual authentication**	requires PKI deployment to clients.
283.	**SSL involves a number of basic phases**	Peer negotiation for algorithm support, Public key, encryption-based key exchange and certificate-based authentication, Symmetric cipher-based traffic encryption
284.	**HTTPS**	uses public key certificates to verify the identity of end points
285.	**SSL**	uses a hybrid of hashed, private and public key cryptographic processes to secure transactions over the Internet through PKI
286.	**SSL**	Confidentiality, Integrity, Authentication (e.g., between client and server)
287.	**SSL handshake protocol**	based on the application layer but also provides for the security of the communication sessions
288.	**SSL handshake protocol**	Multiple connections can belong to one SSL session and the parties participating in one session can take part in multiple simultaneous sessions.
289.	**S/HTTP**	transmits individual messages or pages securely between a web client and server by establishing an SSL-type connection
290.	**S/HTTP**	directs the message to a secure port number rather than the default web port address. This protocol utilizes SSL secure features but does so as a message rather than as a session-oriented protocol.
291.	**IPSec**	is used for communication among two or more hosts, two or more subnets, or hosts and subnets.
292.	**IPSec transport method**	the data portion of each packet—referred to as the encapsulation security payload (ESP)—is encrypted to achieve confidentiality
293.	**IPSec tunnel method**	the ESP payload and its header are encrypted

294.	**IPSec nonrepudiation**	an additional authentication header (AH) is applied.
295.	**security associations - SAs**	define which security parameters should be applied between the communicating parties as encryption algorithms, keys, initialization vectors, life span of keys, etc.
296.	**Either IPSec Mode**	security associations (SAs) are established.
297.	**To increase IPSec security**	use asymmetric encryption via Internet Security Association and Key Management Protocol/Oakley (ISAKMP/Oakley), which allows the key management, use of public keys, negotiation, establishment, modification and deletion of SAs and attributes
298.	**SSH**	is a client-server program that opens a secure, encrypted command-line shell session from the Internet for remote logon
299.	**SSH**	uses strong cryptography to protect data, including passwords, binary files and administrative commands, transmitted between systems on a network
300.	**SSH**	typically implemented by validating both parties' credentials via digital certificates
301.	**SSH**	is useful in securing Telnet and FTP services. It is implemented at the application layer, as opposed to operating at the network layer (IPSec implementation).
302.	**Secure Multipurpose Internet Mail Extensions (S/MIME)**	a standard secure email protocol that authenticates the identity of the sender and receiver, verifies message integrity, and ensures the privacy of a message's contents, including attachments.
303.	**Secure Electronic Transactions (SET)**	is a protocol developed jointly by VISA and MasterCard to secure payment transactions among all parties involved in credit card transactions
304.	**Secure Electronic Transactions (SET)**	an application-oriented protocol that uses trusted third parties' encryption and digital signature processes, via a PKI of trusted third-party institutions, to address confidentiality of information, integrity of data, cardholder authentication, merchant authentication and interoperability
305.	**secrecy of keys**	what the security of encryption methods relies mainly on
306.	**randomness of key generation**	also a significant factor in the ability to compromise a key
307.	**IPSec**	establishes VPNs via transport and tunnel mode encryption methods
308.	**The number and types of layers needed is a function of**	asset value, criticality, the reliability of each control and the degree of exposure
309.	**key benefits of the DMZ system**	An intruder must penetrate three separate devices, Private network addresses are not disclosed to the Internet, Internal systems do not have direct access to the Internet
310.	**Internet perimeter should**	Detect and block traffic from infected internal end points, Eliminate threats such as email spam, viruses and worms, Control user traffic bound toward the Internet, Monitor and detect network ports for rogue activity