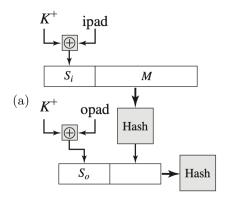
1. 2-out-of-4 Questions [12 points]For each question, please mark the two correct answers.(1) Which statements are true?

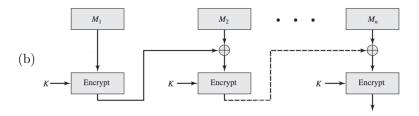
remains unchanged.

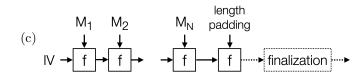
(1) Which statements are true? □ Perfect security means that an attacker cannot gain any information from observing a ciphertext. □ Canantic security requires the key to be at least as long as the plaintext. □ One-time pad does not provide integrity protection. Only perfectly-secure ciphers should be used to encrypt sensitive information in practice. (2) A secure stream cipher □ provides diffusion (each ciphertext bit depends on many plaintext bits). □ can encrypt a 1-bit long plaintext into a 1-bit long ciphertext. □ always generates the same pseudorandom sequence given the same key. □ generates a pseudorandom sequence given the same key. □ generates a pseudorandom sequence given the same key. □ generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. (3) Digital certificates □ are verified using the certificate authority's public key. □ must be sent through a secure channel to protect their integrity. □ contain the public key of the owner (i.e., subject). □ should be accepted only if they are listed on a Certificate Revocation List. (4) Which statements are typically true? □ Session keys are renewed more frequently than master keys. □ Key freshness may be proven with the help of nonces. □ based on integer factorization. □ secure against passive attacks. □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on the hardness of discrete logarithm. □ capital all vulnerabilities. □ based on the bardness of discrete logarithm. □ capital all vulnerabilities. □ privide security, systems may need to be regularly updated even if their functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly updated even if their functionality of the regularly updated even if their function				
any information from observing a ciphertext. Semantic security requires the key to be at least as long as the plaintext. Only perfectly-secure ciphers should be used to encrypt sensitive information in practice. (2) A secure stream cipher provides diffusion (cach ciphertext bit depends on many plaintext bits). can encrypt a 1-bit long plaintext into a 1-bit long ciphertext. claylways generates the same pseudorandom sequence given the same key. generates a pseudorandom sequence are recificate authority's public key. must be sent through a secure channel to protect their integrity. contain the public key of the owner (i.e., subject). should be accepted only if they are listed on a Certificate Revocation List. (4) Which statements are typically true? Sessions keys are used for encrypting master keys. Contralized secret-key distribution requires monaster keys. Contr	(1)	Which statements are true?	(7)	Digital signatures
 □ Semantic security requires the key to be at least as long as the plaintext. □ One time pad does not provide integrity protection. □ Only perfectly-secure ciphers should be used to encrypt sensitive information in practice. (2) A secure stream cipher □ provides diffusion (each ciphertext bit depends on many plaintext bits). □ can encrypt a 1-bit long plaintext into a 1-bit long ciphertext. □ generates a pseudorandom sequence given the same key. □ generates a pseudorandom sequence diven the same key. □ generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. (3) Digital certificates □ are verified using the certificate authority's public key. □ must be sent through a secure channel to protect their integrity. □ contain the public key of the owner (i.e., subject). □ should be accepted only if they are listed on a Certificate Revocation List. (4) Which statements are typically true? □ Sessions keys are used for encrypting master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Sessions keys are used for encrypting master keys. □ Sessions keys are used for encrypting master keys. □ Diffic-Hellman key exchange is based on integer factorization. □ secure against passive attacks. □ based on integer factorization. □ secure against passive attacks. □ based on integer factorization. □ secure against passive attacks. □ Diffic-Hellman key exchange is based on the factorization. □ secure against passive attacks. □ Diffic-Hellman key exchange is based on the factorization. □ secure against passiv		Perfect security means that an attacker cannot gain		can be verified using the private key.
One-time pad does not provide integrity protection.		• -		
 □ One-time pad does not provide integrity protection. □ Only perfectly-secure ciphers should be used to encrypt sensitive information in practice. (2) A secure stream cipher □ provides diffusion (cach ciphertext bit depends on many plaintext bits). □ can encrypt a 1-bit long plaintext into a 1-bit long ciphertext. □ always generates the same besudorandom sequence given the same key. □ generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. (3) Digital certificates □ are verified using the certificate authority's public key. □ must be sent through a secure channel to protect their integrity. □ contain the public key of the owner (i.e., subject). □ should be accepted only if they are listed on a Certificate Revocation List. □ Session keys are renewed more frequently than master keys. □ Session keys are renewed more frequently than master keys. □ Session keys are used for encrypting master keys. □ Sessions keys are used for encrypting master keys. □ Sessions keys are used for encrypting master keys. □ Sessions shaped on integer factorization. □ secure against passive attacks. □ Diffie-Hellman key exchange is □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ Discontralized approaches. □ based on the farthess of discrete logarithm. □ secure against passive attacks. □ Discontralized approaches. □ based on the marginate and the provide administration in parallel. □ provide security, systems may need to be system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be sometical worlded. even if the functionality of the system ca		· - · · · · · · · · · · · · · · · · · ·		
 □ Only perfectly-secure ciphers should be used to encrypt sensitive information in practice. (2) A scure stream cipher □ provides diffusion (cach ciphertext bit depends on many plaintext bits). □ can encrypt a 1-bit long plaintext into a 1-bit long ciphertext. □ always generates the same pseudorandom sequence given the same key. □ generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. (3) Digital certificates □ are verified using the certificate authority's public key. □ must be sent through a secure channel to protect their integrity. □ contain the public key of the owner (i.e., subject). □ should be accepted only if they are listed on a Certificate Revocation List. (4) Which statements are typically true? □ Session keys are renewed more frequently than master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Sessions keys are sued for encrypting master keys. □ Diffie-Hellman key exchange is based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against passive attacks. □ based on integer factorization. □ secure against passive attacks. □ based on integer factorization. □ secure against passive attacks. □ based on integer factorization. □ secure against passive attacks. □ fryitally distacts might take advantage of the design of the encryption algorithm. □ provide diffusion (each ciphertext bit depends on many plaintext bits). (1) Secure block ciphers □ take a fixed-length input and produce an arbitrary-length output. □ require at least 512-bit keys due to birthday paradox. □ allows blocks to be decrypted in parallel				
can encrypt sensitive information in practice.			Ц	provide integrity protection.
Public-key ciphers are typically more efficient than block ciphers. provides diffusion (each ciphertext bit depends on many plaintext bits). can encrypt a 1-bit long plaintext into a 1-bit long ciphertext. always generates the same pseudorandom sequence given the same key. generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. 3) Digital certificates are verified using the certificate authority's public key. must be sent through a secure channel to protect their integrity. contain the public key of the owner (i.e., subject). should be accepted only if they are listed on a Certificate Revocation List. 4) Which statements are typically true? Session keys are renewed more frequently than master keys. Sessions keys are used for encrypting master keys.			(8)	Which statements are true for public-key encryption?
Decoration of the computation of the same key. Decoration of the public key of the owner (i.e., subject). Decorating are renewed more frequently master keys. Decorating are renewed more frequently master keys. Decoration keys are renewed more frequently master keys. Decoration keys are renewed more frequently master keys. Decoration keys are renewed more frequently than master keys. Decoration keys are renewed more frequently than master keys. Decoration keys are used for encrypting master keys. Decoration keys are used for encrypting master keys. Decoration keys are supported in parallel. Decoration keys are the control over information related to them. To compromise a system, an attacker must find and exploit all vulnerabilities. Decoration keys man be doubt an undetected way. To provide security, systems may need to be recorded to many plaintext bits. Decoration (and first) to protect the integrity of the control over information related to them. To compromise a system, an attacker must find and exploit all vulnerabilities. Decoration (and first) to protect the integrity of the plaintext. (and detect replay attacks using sequence numbers. Computation must be performed before encryption (not after) to protect the integrity of computation must be performed before encryption (not after) to protect the integrity of computation must be performed before encryption (not after) to protect the integrity of computation must be performed before encryption (not after) to protect the integrity of computation must be performed before encryption (not after) to protect the integrity of must be sent through the plaintext. (and detect replay attacks using sequence numbers. Comfidentiality protection prevents passive attacks. Deconfidentiality protection prevent		, ,		Public-key ciphers are typically more efficient than
many plaintext bits).	(2)	A secure stream cipher		· - · · · · · · · · · · · · · · · · · ·
can encrypt a 1-bit long plaintext into a 1-bit long ciphertext. always generates the same pseudorandom sequence given the same key. generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. are verified using the certificate authority's public key. must be sent through a secure channel to protect their integrity. contain the public key of the owner (i.e., subject). should be accepted only if they are listed on a Certificate Revocation List. Which statements are typically true? Confidentiality protection prevents passive attacks. Dassed on integer factorization. Secure against passive attacks. Dassed on integer factorization. Secure against passive attacks. Privacy means that individuals have control over information related to them. To compromise a system, an attacker must find and exploit all vulnerabilities. System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. To provide security, systems may need to be recorded by undeted over if their functionality of the graph of the certificate authority's public key. Privacy means that individuals have control over information related to them. To provide differed over if their functionality of the system cannot be modified in an unauthorized and undetected way. To provide control over information related cover if their functionality of the plaintext. can detect replay attacks using sequence numbers. Confidentiality protect		provides diffusion (each ciphertext bit depends on		Key generation is a randomized algorithm.
long ciphertext. □ always generates the same pseudorandom sequence given the same key. □ generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. (3) Digital certificates □ are verified using the certificate authority's public key. □ must be sent through a secure channel to protect their integrity. □ contain the public key of the owner (i.e., subject). □ should be accepted only if they are listed on a Certificate Revocation List. □ Session keys are renewed more frequently than master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Chetralized secret-key distribution requires more master keys than decentralized approaches. □ Session keys are used for encrypting master keys. □ Confidentiality protection prevents passive attacks. □ Overestimating the attackers' capabilities often leads to security incidents. □ Cryptanalytic attacks against encryption require knowledge of at least one plaintext-ciphertext pair. □ Cryptanalytic attacks might take advantage of the design of the encryption algorithm. □ Secure against passive attacks. □ based on integer factorization. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ based on integer factorization. □ secure against active attacks. □ Diffie-Hellman key exchange is ubseed on integer factorization. □ Sessions keys are used for encrypting master keys. □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be may be a tracks against encryption requires howeledge o		many plaintext bits).		
always generates the same pseudorandom sequence given the same key. Generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. Computation must be performed before encryption (not after) to protect the integrity of the plaintext. Can detect replay attacks using sequence numbers. Lags can be verified using a public key. Contain the public key of the owner (i.e., subject). Should be accepted only if they are listed on a Certificate Revocation List. Confidentiality protection prevents passive attacks. Contains the public key of the owner (i.e., subject). Should be accepted only if they are listed on a Certificate Revocation List. Confidentiality protection prevents passive attacks. Contains the public key of the owner (i.e., subject). Session keys are renewed more frequently than master keys. Centralized secret-key distribution requires more master keys than decentralized approaches. Session keys are used for encrypticin (not after) to protect the integrity of the plaintext. Can detect replay attacks using sequence numbers. Lags can be verified using a public key. Confidentiality protection prevents passive attacks. Confidentiality protection prevents passive attacks. Confidentiality protection prevents passive attacks. Contains the public key. Confidentiality protection prevents passive attacks. Confidentiality protection prevents passive attacks. Confidentiality protection prevents passive attacks. Contains the public key. Confidentiality protection prevents passive attacks. Confidentiality protection prevents passive attacks using a public key. Confidentiality protection preve				
given the same key. generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. 3) Digital certificates are verified using the certificate authority's public key. must be sent through a secure channel to protect their integrity. contain the public key of the owner (i.e., subject). should be accepted only if they are listed on a Certificate Revocation List. (4) Which statements are typically true? Session keys are renewed more frequently than master keys. Centralized secret-key distribution requires more master keys than decentralized approaches. Sessions keys are used for encrypting master keys. Key freshness may be proven with the help of nonces. Sessions keys are used for encrypting master keys. Key freshness may be proven with the help of nonces. Sessions integer factorization. secure against active attacks. based on the hardness of discrete logarithm. secure against passive attacks. based on integer factorization. secure against passive attacks. based on integer factorization. secure against passive attacks. Cendidentiality protection prevents passive attacks. Chyptanalytic attacks against encryption require knowledge of at least one plaintext-ciphertext pair. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. (11) Secure block ciphers take a fixed-length input and produce an arbitrary-length output. require at least 512-bit keys due to birthday paradox. are often built on a large number of rounds. provide diffusion (each ciphertext bit depends on many plaintext bioks are repeated. allows blocks to be decrypted in parallel. is vulnerable to attacks that rearrange the blocks of the ciphertext. allows blocks to be encrypted in parallel. is based on a Feistel network. encryption and decryption algorithms are supported in hardware by many modern CPUs.				tionary nard problems.
□ generates a pseudorandom sequence that is at least 128 bits long to prevent brute-force attacks. 3			(9)	MAC
128 bits long to prevent brute-force attacks.				computation must be performed before encryption
dag length does not depend on the message length. dags can be verified using a public key. doffer a public key. doffer dags can be verified using a public key. doffer dags can be verified using a public key. doffer dags can be verified using a public key. doffer dags can be verified using a public key. doffer dags can be verified using a public key.				
□ are verified using the certificate authority's public key. □ must be sent through a secure channel to protect their integrity. □ contain the public key of the owner (i.e., subject). □ should be accepted only if they are listed on a Certificate Revocation List. (4) Which statements are typically true? □ Session keys are renewed more frequently than master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Key freshness may be proven with the help of nonces. □ Sessions keys are used for encrypting master keys. □ Key freshness may be proven with the help of nonces. □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ based on integer factorization. □ secure against active attacks. □ brivacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly undeted over if their functionality is a scurred proventies and the care integrity in the autacks are all invertible (given the correct key). Confidentiality protection prevents passive attacks. Overestimating the attackers' capabilities often leads to security incidents. Confidentiality protection prevents passive attacks. Overestimating the attackers capabilities often leads to security incidents. Confidentiality protection prevents passive attacks. Overestimating the attacks angint encryption require knowledge of at least one plaintext-ciphertex pair. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Secure block ciphers Lake fixed-length input and produce an arbitrary-length output. Counter (CTR) block cipher mode may leak information if p				can detect replay attacks using sequence numbers.
public key. must be sent through a secure channel to protect their integrity. contain the public key of the owner (i.e., subject). should be accepted only if they are listed on a Certificate Revocation List. Which statements are typically true? Session keys are renewed more frequently than master keys. Centralized secret-key distribution requires more master keys than decentralized approaches. Sessions keys are used for encrypting master keys. Key freshness may be proven with the help of nonces. Sessions keys are used for encrypting master keys. Key freshness may be proven with the help of nonces. based on the hardness of discrete logarithm. secure against passive attacks. based on integer factorization. secure against active attacks. Provide diffusion (each ciphertext bit depends on many plaintext bits). Confidentiality protection prevents passive attacks. Brute-force attacks against encryption require knowledge of at least one plaintext-ciphertext pair. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Comfidentiality protection prevents passive attacks. Brute-force attacks against encryption require knowledge of at least one plaintext-ciphertext pair. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Confidentiality protection prevents passive attacks. Brute-force attacks against encryption require attacks reason apaint active attacks. Confidentiality protection pleasite. Cryptanalytic attacks might take advantage of the design of the encryption algorithm.	(3)	Digital certificates		
must be sent through a secure channel to protect their integrity. Contain the public key of the owner (i.e., subject). Should be accepted only if they are listed on a Certificate Revocation List. Overestimating the attackers' capabilities often leads to security incidents. Brute-force attacks against encryption require knowledge of at least one plaintext-ciphertext pair. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Secure block ciphers take a fixed-length input and produce an arbitrary-length output. require at least 512-bit keys due to birthday paradox. are often built on a large number of rounds. provide diffusion (each ciphertext bit depends on many plaintext bits). (2) Counter (CTR) block cipher mode may leak information if plaintext blocks are repeated. allows blocks to be decrypted in parallel. is vulnerable to attacks that rearrange the blocks of the ciphertext. allows blocks to be encrypted in parallel. is vulnerable to attacks that rearrange the blocks of the ciphertext. allows blocks to be encrypted in parallel. is vulnerable to attacks that rearrange the blocks of the ciphertext. allows blocks to be encrypted in parallel. in ardware by many modern CPUs. encryption consists of steps that are all invertible (given the correct key).		are verified using the certificate authority's		tags can be verified using a public key.
their integrity. contain the public key of the owner (i.e., subject). should be accepted only if they are listed on a Certificate Revocation List. Which statements are typically true? Session keys are renewed more frequently than master keys. Centralized secret-key distribution requires more master keys than decentralized approaches. Sessions keys are used for encrypting master keys. Key freshness may be proven with the help of nonces. Sessions keys are used for encrypting master keys. Key freshness may be proven with the help of nonces. Sesure against passive attacks. based on the hardness of discrete logarithm. secure against passive attacks. based on integer factorization. secure against active attacks. System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. To provide security, systems may need to be recorded and and the public is a secure that individuals have control over an acceptance of the encryption and decryption algorithms are supported in hardware by many modern CPUs. contain the public key of the owner (i.e., subject). Contraint he public key of the owner (i.e., subject). Brute-force attacks against encryption require knowledge of at least one plaintext-ciphertext pair. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. Cryptanalytic attacks might take advantage of the design of the encryption algorithm. 11) Secure block ciphers take a fixed-length input and produce an arbitrary-length output. require at least 512-bit keys due to birthday paradox. provide diffusion (each ciphertext bit depends on many plaintext bits). 12) Counter (CTR) block cipher mode may leak information if plaintext blocks are repeated. allows blocks to be decrypted in parallel. Is vulnerable to attacks that rearrange the blocks of the ciphertext. allows blocks to be decrypted in parallel. In all with the provide diffusion (each ciphertext) is vulnerable to attacks that rearrange the blocks of the cip		- · · · · · · · · · · · · · · · · · · ·	(10)	Which statements are true?
 □ contain the public key of the owner (i.e., subject). □ should be accepted only if they are listed on a Certificate Revocation List. □ Brute-force attacks against encryption require knowledge of at least one plaintext-ciphertext pair. □ Cryptanalytic attacks might take advantage of the design of the encryption algorithm. □ Cryptanalytic attacks might take advantage of the design of the encryption algorithm. □ Cryptanalytic attacks might take advantage of the design of the encryption algorithm. □ Cryptanalytic attacks might take advantage of the design of the encryption algorithm. □ Secure block ciphers □ Lake a fixed-length input and produce an arbitrary-length output. □ require at least 512-bit keys due to birthday paradox. □ are often built on a large number of rounds. □ provide diffusion (each ciphertext bit depends on many plaintext bits). □ Counter (CTR) block cipher mode □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is based on a Feistel network. □ compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be recryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 	Ц		` /	
 □ should be accepted only if they are listed on a Certificate Revocation List. □ Session keys are renewed more frequently than master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Cryptanalytic attacks might take advantage of the design of the encryption algorithm. □ Secure block ciphers □ take a fixed-length input and produce an arbitrary-length output. □ require at least 512-bit keys due to birthday paradox. □ a large number of rounds. □ provide diffusion (each ciphertext bits) □ provide diffusion (each ciphertext bits) □ provide diffusion (each ciphertext bits) □ counter (CTR) block cipher mode □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encryption algorithms are supported in hardware by many modern CPUs. □ is based on a Feistel network. □ is based on a Feistel network. □ encryption consists of steps that are all invertible (given the correct key). 	П			
Certificate Revocation List. (4) Which statements are typically true? Session keys are renewed more frequently than master keys. Centralized secret-key distribution requires more master keys than decentralized approaches. Sessions keys are used for encrypting master keys. Key freshness may be proven with the help of nonces. Sessions keys are used for encrypting master keys. Sessions keys are used for encrypting allows block ciphers ake a fixed-length input and produce an arbitrary-length output. Secure block ciphers take a fixed-length input and produce an arbitrary-length output. Secure block ciphers have a fixed-length input and produce an arbitrary-length output. Secure against active deal fixed length output. Secure against active deal fixed length output. Secure against active deal fixed length ou				
Which statements are typically true?				
 □ Session keys are renewed more frequently than master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Key freshness may be proven with the help of nonces. □ Diffie-Hellman key exchange is □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly undeted even if their functionality of the system cannot be modified in an unauthorized in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 			_	
master keys. □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Key freshness may be proven with the help of nonces. □ Diffie-Hellman key exchange is	` '		Ц	v - v
 □ Centralized secret-key distribution requires more master keys than decentralized approaches. □ Sessions keys are used for encrypting master keys. □ Key freshness may be proven with the help of nonces. (5) Diffie-Hellman key exchange is □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be requirely undeted even if their functionality of the system cannot be modified even if their functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be required in paralled in part and produce an arbitrary-length output. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ provide diffusion (car cipheralize) □ sunte		- v		design of the energyption algorithm.
 □ Sessions keys are used for encrypting master keys. □ Key freshness may be proven with the help of nonces. □ Diffie-Hellman key exchange is □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly undated even if their functionality. □ take a fixed-length input and produce an arbitrary-length output. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ provide diffusion (each ciphertext bit depends on many plaintext bits). □ Sulherable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is based on a Feistel network. □ encryption con		· ·	(11)	Secure block ciphers
 □ Sessions keys are used for encrypting master keys. □ Key freshness may be proven with the help of nonces. □ Diffie-Hellman key exchange is □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly windsted against factorization and length output. □ require at least 512-bit keys due to birthday paradox. □ require at least 512-bit keys due to birthday paradox. □ allows block cipher mode □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. (13) AES □ is based on a Feistel network. □ inhardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 	Ш			take a fixed-length input and produce an arbitrary-
 □ Key freshness may be proven with the help of nonces. □ liftie-Hellman key exchange is □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ Which statements are true? □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly undeted even if their functionality of the systems are supported in hardware by many modern CPUs. □ require at least 512-bit keys due to birthday paradox. □ are often built on a large number of rounds. □ provide diffusion (each ciphertext bit depends on many plaintext bits). (12) Counter (CTR) block cipher mode □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. (13) AES □ is based on a Feistel network. □ encryption and decryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 				
 (5) Diffie-Hellman key exchange is □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. (12) Counter (CTR) block cipher mode □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ AES □ is based on a Feistel network. □ encryption and decryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 				
 □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ Which statements are true? □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly undeted even if their functionality of the functionality of the system cannot be modified in an unauthorized and undetected way. □ many plaintext bits). (12) Counter (CTR) block cipher mode □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ allows blocks to be encrypted in parallel. (13) AES □ is based on a Feistel network. □ encryption and decryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 				
 □ based on the hardness of discrete logarithm. □ secure against passive attacks. □ based on integer factorization. □ secure against active attacks. □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ AES □ is based on a Feistel network. □ is based on a Feistel network. □ encryption and decryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 	(5)	Diffie-Hellman key exchange is	Ц	
 □ based on integer factorization. □ secure against active attacks. □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ AES □ is based on a Feistel network. □ encryption and decryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 				many promoter stosy.
 □ secure against active attacks. □ may leak information if plaintext blocks are repeated. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ allows blocks to be encrypted in par			(12)	Counter (CTR) block cipher mode
□ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be recognizely undetected even if their functionality of the functionality of the recognizely undetected even if their functionality of the correct key). □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be decrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel. □ is vulnerable to attacks that rearrange the blocks of the ciphertext. □ allows blocks to be encrypted in parallel.				may leak information if plaintext blocks are repeated.
 □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly, undeted, even if their functionality functionality of the circular the ciphertext. □ allows blocks to be encrypted in parallel. □ is based on a Feistel network. □ encryption and decryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key). 		secure against active attacks.		
 □ Privacy means that individuals have control over information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly, undeted, even if their functionality functionality of the correct key). 	(6)	Which statements are true?		
information related to them. □ To compromise a system, an attacker must find and exploit all vulnerabilities. □ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly, undetected even if their functionality of the correct key).		Privacy means that individuals have control over		-
exploit all vulnerabilities. System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. To provide security, systems may need to be regularly, undetected even if their functionality (given the correct key).		·	Ц	allows blocks to be energipted in parallel.
□ System integrity means that the functionality of the system cannot be modified in an unauthorized and undetected way. □ To provide security, systems may need to be regularly, undeted, even if their functionality (given the correct key). □ System integrity means that the functionality of the encryption and decryption algorithms are supported in hardware by many modern CPUs. □ encryption consists of steps that are all invertible (given the correct key).			(13)	AES
system cannot be modified in an unauthorized and undetected way. To provide security, systems may need to be regularly, undetected even if their functionality (given the correct key).				is based on a Feistel network.
undetected way. To provide security, systems may need to be recularly undetected even if their functionality (given the correct key).	Ц			
To provide security, systems may need to be recularly, updated even if their functionality (given the correct key).			_	
		· ·		
		regularly updated even if their functionality		supports key sizes ranging from 128 to 1024 bits.

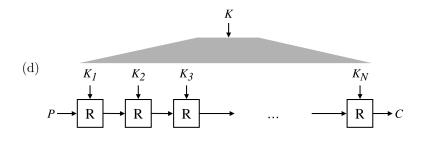
(14)	Which statements are true for cryptograp	phic (17)	Kerberos protocol
	hash functions?		requires all protocol participants to share master
	Compression functions take two fixed-length inpand produce one fixed-length output.	outs	keys with each other. proves to all protocol participants that the session
	SHA-2 is based on the "soap" construction.		key is fresh.
	Merkle-Damgård construction is a method		uses timestamps to prove key freshness. is vulnerable to impersonation attacks.
П	building iterative hash functions. Brute-force attack needs around $2^{H/2}$ steps to fin		is vulnerable to impersonation attacks.
	pre-image given an H -bit long hash value.	(18)	Cipher Block Chaining (CBC) block cipher mode
(15)	Which statements are true?		may leak information if plaintext blocks are repeated. is vulnerable to attacks that rearrange the blocks of the ciphertext.
	Authenticated encryption provides both confictiality and integrity protection.	1011-	allows blocks to be decrypted in parallel. allows blocks to be encrypted in parallel.
	3DES uses keys that are twice as long as DES ke		A cryptographic hash function
	3DES uses blocks that are three times as long DES blocks.	5 465	takes fixed-length inputs and produces variable-
	Meet-in-the-middle attack against mult		length outputs.
	encryption is always faster than brute-fe key search.		must be invertible given the secret key. is collision resistant if it is computationally infeasible to find any pair of inputs with the same output.
(16)	With RSA,		can be used to protect the confidentiality of passwords due to the one-way property.
	both encryption and decryption are based	on (20)	A key can be securely reused with a stream cipher if
	modular exponentiation. encryption and decryption are based on series	s of	the key is combined with a nonce before encryption.
	substitutions and permutations. the size of the ciphertext depends on the key.		each plaintext is encrypted with a different part of the generated pseudorandom sequence.
	modulus (part of the public and private keys) n		every plaintext is completely different.
	be a prime number.		the key was chosen uniformly at random.
2	Matching Questions [3 points]		
For	- · · · · · · · · · · · · · · · · · · ·	ter of the co	orresponding text or figure. Note that you have to use
(1)	Cryptographic primitives, protocols, and standar	rds	
	ElGamal (a	a) key-exch	ange protocol with trusted third party
	DSA (l	o) key-exch	ange protocol with digital signatures
	X.509	c) digital ce	ertificate standard
	_ CMAC (c	d) public-ke	y encryption scheme
	Needham-Schroeder (e	e) message	authentication code
	Station-to-Station (f) digital si	gnature scheme
(2)	Ciphertext length: if we encrypt a 64-bit long pl	aintext secu	urely, how long can we expect the ciphertext to be?
	AES in ECB mode (a	a) 64 bits	
	Salsa20 / ChaCha20 (l	o) 128 bits	
	RSA (e	e) 224 to 51	2 bits
	_ ECC (c	d) 2048 to 1	15,360 bits

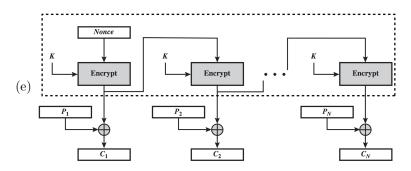
(3) Various schemes











- _ HMAC
- __ Output Feedback (OFB)
- __ Merkle-Damgård
- _ iterated block cipher
- __ CBC-MAC

	3.	Open-Ended	Questions	[5	points
--	----	------------	-----------	----	--------

For each question, please clearly indicate your final answer and show how you obtained that answer.

(1)	Bit Errors [3 points] Alice has encrypted a 128-bit message and sent it to Bob. During transmission, Mallory changed the values of the first 32 bits of the ciphertext. When Bob decrypts the modified ciphertext, at most how many bits of the plaintext may be affected by this change if the cipher is
	(a) one-time pad?
	(b) a block cipher with 64-bit blocks in Electronic Code Book (ECB) mode?
	(c) a block cipher with 64-bit blocks in Cipher Block Chaining (CBC) mode?
	(d) a block cipher with 64-bit blocks in Counter (CTR) mode?
	(a) a stock stylint with or one stocks in country (C11), mode.

(2)	Signature Forgery [2 points] Alice uses a hash-then-sign digital-signature scheme that is based on a hash function with 512-bit long hash values. Mallory would like to cheat this signature scheme by creating a malicious document that has a valid signature from Alice.
	Questions:
	(a) If Mallory has obtained a benign document with a valid signature from Alice, how many malicious documents does Mallory need to generate to have a good chance of finding one for which this signature is valid?
	(b) Suppose that Mallory can trick Alice into signing any benign document. How many documents does Mallory need to generate to have a good chance of finding two documents for which the same signature will be valid?
	(c) Suppose that Alice tries to increase the difficulty of this attack by hashing twice before signing (i.e., Alice signs $H(H(X))$ instead of $H(X)$, where X is a document and H is the hash function). How many documents does Mallory need to generate in this case to find two documents for which the same signature wil be valid?