1. 2-out-of-4 Questions [12 points]

For each question, please mark the *two* correct answers.

(1) Which statements are true?

- ☑ Perfect security means that an attacker cannot gain any information from observing a ciphertext.
- ☐ 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.
- ☑ 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.
- ☑ 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.

(6) 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 updated even if their functionality remains unchanged.

(7) Digital signatures

- ☐ can be verified using the private key.
- ☑ may be created using elliptic curve cryptography.
- ☐ are more efficient computationally than message authentication codes.
- ☑ provide integrity protection.

(8) Which statements are true for public-key encryption?

- ☐ Public-key ciphers are typically more efficient than block ciphers.
- ☑ Key generation is a randomized algorithm.
- ☐ Encryption requires the private key.
- ☑ Public-key ciphers are typically built on computationally hard problems.

(9) MAC

- ☐ computation must be performed before encryption (not after) to protect the integrity of the plaintext.
- ☑ can detect replay attacks using sequence numbers.
- ☑ tag length does not depend on the message length.
- ☐ tags can be verified using a public key.

(10) Which statements are true?

- ☑ Confidentiality protection prevents passive attacks.
- ☐ 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.

(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 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 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).
- ☐ supports key sizes ranging from 128 to 1024 bits.

(14) Which statements are true for cryptographic hash functions?

- ☑ Compression functions take two fixed-length inputs and produce one fixed-length output.
- ☐ SHA-2 is based on the "soap" construction.
- ☑ Merkle-Damgård construction is a method of building iterative hash functions.
- ☐ Brute-force attack needs around $2^{H/2}$ steps to find a pre-image given an H-bit long hash value.

(15) Which statements are true?

- ☑ Authenticated encryption provides both confidentiality and integrity protection.
- ☑ 3DES uses keys that are twice as long as DES keys.
- ☐ 3DES uses blocks that are three times as long as DES blocks.
- ☐ Meet-in-the-middle attack against multiple encryption is always faster than brute-force key search.

(16) With RSA,

- ☑ both encryption and decryption are based on modular exponentiation.
- ☐ encryption and decryption are based on series of substitutions and permutations.
- ☑ the size of the ciphertext depends on the key.
- ☐ modulus (part of the public and private keys) must be a prime number.

(17) Kerberos protocol

- ☐ requires all protocol participants to share master keys with each other.
- ☑ proves to all protocol participants that the session key is fresh.
- ☑ uses timestamps to prove key freshness.
- ☐ is vulnerable to impersonation attacks.

(18) Cipher Block Chaining (CBC) block cipher mode

- ☐ may leak information if plaintext blocks are repeated.
- ☑ is vulnerable to attacks that rearrange the blocks of the ciphertext.
- ☑ allows blocks to be decrypted in parallel.
- ☐ allows blocks to be encrypted in parallel.

(19) A cryptographic hash function

- ☐ takes fixed-length inputs and produces variable-length outputs.
- ☐ 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.
- ☑ can be used to protect the confidentiality of passwords due to the one-way property.

(20) A key can be securely reused with a stream cipher if

- ☑ the key is combined with a nonce before encryption.
- ☑ each plaintext is encrypted with a different part of the generated pseudorandom sequence.
- ☐ every plaintext is completely different.
- ☐ the key was chosen uniformly at random.

2. Matching Questions [3 points]

For each question, please fill out each __ with the letter of the corresponding text or figure. Note that you have to use each letter exactly once in each question.

(1) Cryptographic primitives, protocols, and standards

d ElGamal	(a) key-exchange protocol with trusted third party
f DSA	(b) key-exchange protocol with digital signatures
c X.509	(c) digital certificate standard
e CMAC	(d) public-key encryption scheme
a Needham-Schroeder	(e) message authentication code
b Station-to-Station	(f) digital signature scheme

(2) Ciphertext length: if we encrypt a 64-bit long plaintext securely, how long can we expect the ciphertext to be?

b AES in ECB mode	(a) 64 bits
a Salsa20 / ChaCha20	(b) 128 bits
d RSA	(c) 224 to 512 bits
c ECC	(d) 2048 to 15,360 bits

(3) Various schemes

a HMAC

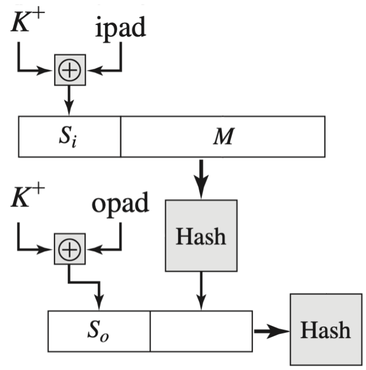
e Output Feedback (OFB)

c Merkle-Damgård

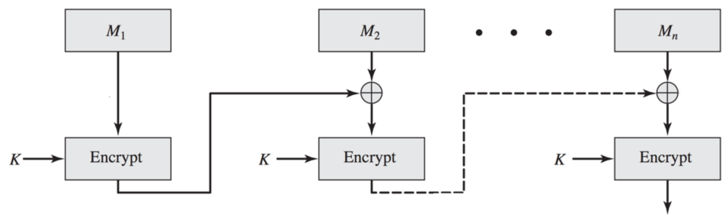
d iterated block cipher

b CBC-MAC

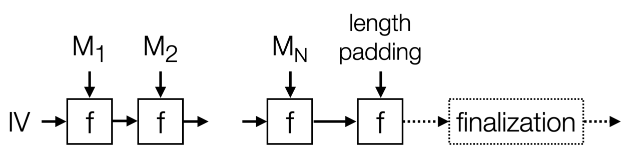
(a)



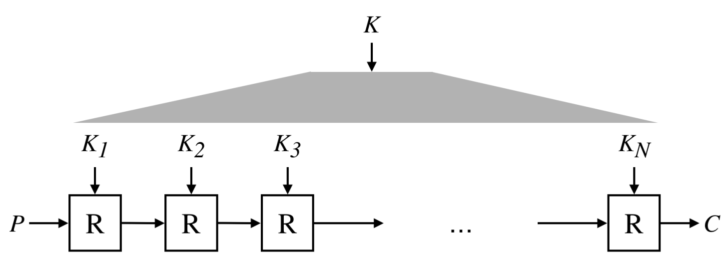
(b)



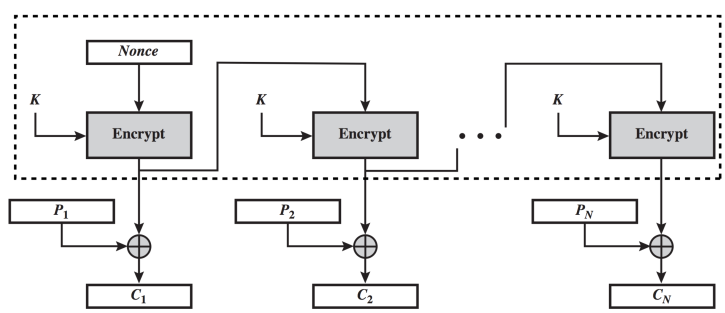
(c)



(d)



(e)



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? encrypt/decrypt each bit independently → only plaintext bits that correspond to modified ciphertext bits are affected → 32

(b) a block cipher with 64-bit blocks in Electronic Code Book (ECB) mode? encrypt/decrypt each block independently → only modified block is affected → 64

(c) a block cipher with 64-bit blocks in Cipher Block Chaining (CBC) mode? decryption involves bitwise XOR with previous cipher block → modified block is completely affected, in the next block bits that are XORed to modified bits are affected → 96

(d) a block cipher with 64-bit blocks in Counter (CTR) mode? same as one-time pad → 32

(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?
each document has the right hash with probability $\frac{1}{2^{512}}$ $\rightarrow$ Mallory needs to generate $\sim 2^{512}$ documents so that on average one will have the right hash and, hence, valid signature

(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?
birthday paradox $\rightarrow$ Mallory needs to generate $\sim 2^{256}$ to have a good chance of finding a collision

(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?
if two documents X and Y have the same hash value $h = H(X) = H(Y)$, then they will also have the same double-hash: $H(H(X)) = H(h) = H(H(Y))$ $\rightarrow$ for any set of documents, the probability of collision is at least as high with double-hashing than without $\rightarrow$ Mallory needs to generate at most $\sim 2^{256}$ (exact answer not required)