Your Name: **\*\*\***

*References: Text Book, Cryptography and Network Security: Principles and Practice by Williams Stallings.*

Q1: In cryptography, what is a cipher?

Answer : A , an encrypted message

a) An encrypted message – Cryptography or cipher is one the many study schemes used for encrypted message.  In cryptography, the plain text is converted into ciphertext or encoded message using cipher algorithm. *Text book, Page #86*

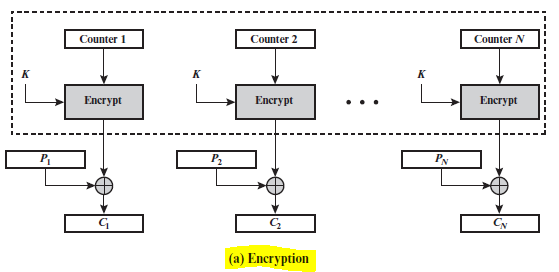
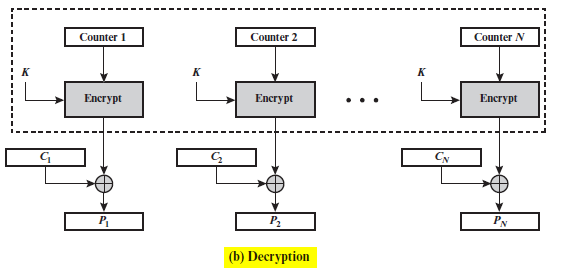
b) An algorithm for performing encryption and decryption - The areas of cryptography(encryption) and cryptanalysis(decryption) together are called **cryptology. T**his choice is not the answer as it mentions only about algorithm performing encryption and decryption.

c) A zero - cipher is not a digit zero, but we do have zero-access encryption([source](https://protonmail.com/blog/zero-access-encryption/)) and zero-knowledge proof in cryptography ([wiki](https://en.wikipedia.org/wiki/Zero-knowledge_proof)).

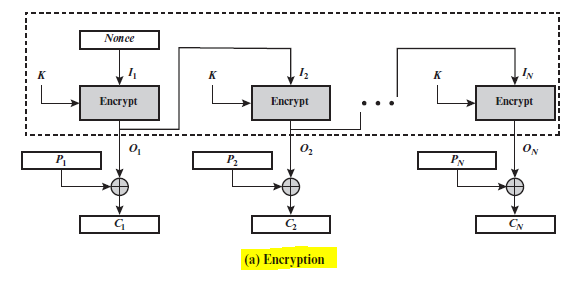
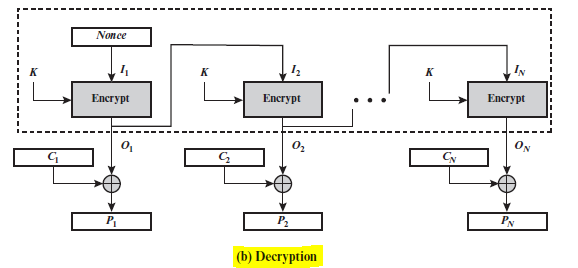
d) A code – cipher is not a code, it’s a message that’s encrypted using defined algorithm.

Q2: Consider the modes of operation for a block cipher. Which of the following modes of operation creates a keystream to be XORed with the plaintext for encryption?

Answer : D, all of the above *Text Book, Page#214-223*

**Figure.1a &1b** Counter (CTR) Mode

**Figure.2a &2b** Output Feedback (OFB) Mode

1. Counter Mode – In this mode of operation, each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block. (figure 1a & 1b & async video 4.15)
2. Output Feedback Mode – Input is processed *s* bits at a time. The input to the encryption algorithm is the preceding encryption output, and full blocks are used. (figure 2a & 2b & async video 4.14)
3. Stream Mode – (async video 4.9) Stream ciphers and stream modes of operation work by generating a key stream. [for encryption] This key stream is XORed with the plaintext in order to generate the ciphertext. [for decryption] The key stream is XORed with the ciphertext in order to generate the plaintext.
4. All of the above. – true
5. None of the above.

Q3: What is the foundation of all security on the Internet? [Hint: in your explanations of the not correct options, for each

not correct option explain how the option depends upon your chosen answer.] Answer : B, Trust We might try to achieve security goals of confidentiality and authentication but there will always be ways to break into the system. So, trust is the fundamental requirement.

1. Cryptography Encryption and Decryption - Cryptography consists of two processes: Encryption and decryption. Encryption Is the process of converting a plaintext (readable) message to ciphertext (unreadable) form. Decryption Is the process of converting the ciphertext (unreadable) message to its original (readable) form. We could try encrypting and decrypt messages but with out trust, we couldn’t achieve the authenticity of the message.
2. Trust - Trust is the foundation of security in cyberspace. To achieve an organization’s security goals and objectives, organization should implement technical mechanisms to achieve high trust for its cyberspace. Example: One factor authentication vs multi-factor authentications solutions.
3. Authentication - We use authentication and digital signature concepts to achieve Authenticity ,to prove that the claimed user identity is valid (authentication) and/or that the claimed source of a data unit is valid (data origin authentication). This is one of the added ways to ensure trust.
4. Public Key Certificates – A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate

has sole control and access to the corresponding private key.

1. Digital Signatures - Provides an electronic means of guaranteeing authenticity of the sending party and assurance that encrypted documents have not been altered during transmission. So, Digital signature achieves the following two security goals: Integrity and Authenticity. But, still the sender can deny having sent the message. So, Trust is fundamentally required.

Q4: What does it mean to be secure? Answer: D, All of the above.

a) Security means the coercive capability to stop an aggressor. Security is freedom from war, and the ability to deter

or defeat aggressive attacks.

b) Security refers to safety from vulnerabilities (both external and internal) that could harm the state, societies within

the state, and the values of those societies.

c) Security means freedom to enjoy the things that are most important to human survival and wellbeing, such as

food, health care, and the opportunity to live well.

d) All of the above – true, Security can be defined as the state of being free from danger and not exposed to damage from accidents or attacks.

e) None of the above.

Q5: Consider the modes of operation for a block cipher. Which of the following modes of operation allows for the decryption

on each block to be performed in parallel? [Hint: explain each of the identified modes of operation and in 1-2 sentences

describe how decryption operates (identify the parallelism for your answer(s) if any).] Answer : D, All of the above.

Page #214 Table7.1& pg#220

1. Counter Mode - allows parallel operation of encryption/decryption as explained in question 2
2. Cypher Block Chaining Mode – In this mode of operation, the input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext. We can perform parallelism for decryption but not for encryption.
3. Electronic Codebook Mode – Each block of plaintext bits is encoded independently using the same key. It allows parallelism for both encryption and decryption.
4. All of the above. – true, in all the modes specified above, we can perform decryption in parallel.

e) None of the above.

Q6: Which of the following are properties of a secure hash function? [Hint: explain each of the properties and explain why

your chosen property(ies) is (are) required of a secure hash function.]

Answer : D, all of the above ([source](https://www.denimgroup.com/resources/blog/2007/11/properties-of-1/)))

a) The hash value is preimage resistant. : for a given a hash value h, it should be hard to find any message m such that h = hash(k, m). This specific property is called preimage resistant.

b) The hash value is second preimage resistant. : we call a hash value to be second preimage resistant when for a given message m1, it should be hard to find a different message m2 such that hash(k, m1) = hash(k, m2).

c) The hash values are collision resistant. : Similarly, we call a hash value to be collision resistant when for a given two messages m1 and m2, it should be “hard” to find a hash such that hash(k, m1) = hash(k, m2), where k is the hash key.

d) All of the above. – true, a secure hash function has all the three properties : collision resistance, preimage resistance, and second preimage resistance.

e) None of the above.

Q7: Which of the following best describes someone who gains illegal access to a computer system? [Hint: go beyond any

single definition of a term and look at each term’s historical and other meanings to identify the best answer.]

Answer : A Hacker

a) Hacker - Is a person who gains unauthorized access to a computer or network and uses knowledge of computer technology and security settings for benign or malicious purposes.

b) Identity Thief – an imposter who commits crime by obtaining key pieces of personal identification information, such as Social Security or driver's license numbers, to impersonate someone else

c) Intruder – The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers). Source : text book page#42

d) Cyber-terrorist – Is someone who intimidates or coerces a government or organization to advance his or her political or social objectives by launching computer-based attacks against computers, networks, and the information stored on them

Q8: Which of the following are ethical issues facing the use of technology in business today? [Hint: explain why each of

the possible answers a, b and c either is or is not an ethical issue.]

Answer– D all of the above (check textbook online chapter 24 http://goo.gl/36TAJP

a) e-mail privacy – privacy is not fully present in company emails; the employer could monitor your conversations for security reasons, within the company which could be seen as violating the employee’s privacy and ultimately leads to not being totally honest communication. So, there is this ethical dilemma if the employers should monitor employees’ emails.

b) Software piracy – it’s a serious venerability that a software developer could take the code with him and implement the same(duplicate) or distribute a copyrighted software anywhere. This is an ethical concern plagued in the IT industry.

c) Intellectual property rights and copyrights – similar to software piracy, the human intellect (knowledge gained) could be used to reproduce without copyrights.

d) All of the above - yes

e) None of the above

Q9: Which of the following are desired characteristics of a pseudorandom number generator? [Hint: explain why each of the

answers a, b and c either is or is not a desired characteristic and why.] D, all of the above

a) Scalability – textbook- page#255, Scalability is one of the requirements to achieve randomness for PRNG

b) Backward Predictability – A given sequence of numbers can be reproduced at a later date if the starting point in the sequence is known(Deterministic).

c) A Shared Initialization Vector - In cryptography, an initialization vector (IV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom.

d) All of the above, true

e) None of the above

**Pseudorandom number generator(PRNG):** An algorithm that is used to produce an open-ended sequence of bits is referred to as a PRNG. A common application for an open-ended sequence of bits is as input to a symmetric stream cipher. PRNG takes as input a fixed value, called the **seed**, and produces a sequence of output bits using a deterministic algorithm.

**Characteristics of PRNG**([Source](https://www.geeksforgeeks.org/pseudo-random-number-generator-prng/)):

* **Efficient:** PRNG can produce many numbers in a short time and is advantageous for applications that need many numbers
* **Deterministic:** A given sequence of numbers can be reproduced at a later date if the starting point in the sequence is known. Determinism is handy if you need to replay the same sequence of numbers again at a later stage.
* **Periodic:** PRNGs are periodic, which means that the sequence will eventually repeat itself. While periodicity is hardly ever a desirable characteristic, modern PRNGs have a period that is so long that it can be ignored for most practical purposes

**Scalability:** Any test applicable to a sequence can also be applied to subsequences extracted at random. If a sequence is random, then any such extracted subsequence should also be random. Hence, any extracted subsequence should pass any test for randomness. We have SPRNG package to address scalability. PLFG (parallelize lagged Fibonacci generators) is a highly efficient and scalable parallel pseudo-random number generator. ([source](https://link.springer.com/content/pdf/10.1007/3-540-45545-0_68.pdf))

Q10: Which of the following is primarily used to provide integrity protection for a message sent between Alice and Bob?

[Hint: for each of the answers a, b and c, explain how it is typically used and the security functionality (e.g., integrity)

that is provided with that typical usage. For those choices that may be used to provide integrity protection, explain how

it is used to provide integrity protection if that is not its typical usage.] Answer: A, Hash Function

a) Hash function

b) Private key operation - Private Key operations are called symmetric key cryptography or operations.

c) Symmetric key operation – same as choice b.

d) All of the above

e) None of the above

**Hash functions** are the building blocks for modern cryptography. It is used in a wide variety of security applications and Internet protocols. A hash function is a cryptographic algorithm which is used to transform large random size data to small fixed size data. The data output of the hash algorithm is called hash value or digest. The basic operation of hash functions does not need any key and operate in a one-way manner. The one-way operation means that it is impossible to compute the input from a particular output. The basic uses of hash functions are:

* Generation and verification of digital signatures
* Checksum/Message integrity checks
* Source integrity services via MAC
* Derivation of sub-keys in key-establishment protocols & algorithms
* Generation of pseudorandom numbers

In general terms, the principal object of a hash function is data integrity. source: textbook, (page#340)

**Symmetric-key algorithms** also referred as secret-key(**private-key**) algorithms use a single cryptographic key for encryption and decryption purposes. They convert data in a way that is problematic for an opponent to decrypt the data without the key. Symmetric keys are securely generated and distributed to the sender and receiver and are unknown to any other entity. But if a symmetric-key algorithm is being used by more than one receiver then the key has to be shared with all entities. If the key is compromised from one entity, communication of all the entities will be compromised. Symmetric Algorithms are further divided into Block & Stream algorithms. A block algorithm breaks the input into fixed-size blocks and then progresses the crypto operations. Stream algorithms perform “bit-by-bit” crypto operations.  Primary purposes of symmetric key algorithms are:

* Confidentiality is achieved as encryption and decryption is performed using single key.
* Integrity and source authentication are achieved by using Message Authentication Codes because the MAC is generated and validated by the same key.
* Generation of pseudorandom random numbers ([Source](https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms))

Q11: Which of the following can be used to increase the strength of a specific cipher? [Hint: explain how each of the answers

a, b and c either can or cannot be used to make a cipher more secure. ask yourself if any of the answers would cause the cipher to be changed as a result - in which case, it doesn’t increase the strength of a specific cipher.] Answer D, All of the above

a) Shared Secret Key

b) Keep Algorithm Details Secret

c) Use a Key with a Larger Number of Bits

d) All of the above

e) None of the above

One measure of a cipher’s ability to protect data is its cipher strength, with the number of bits in the encryption key.

**Shared secret Key** A shared secret is a cryptographic key or Data that is only known to the parties involved in a secured communication. The shared secret can be anything from passwords or pass phrases, to a random number or any array of randomly chosen data. It is another important mechanism in cryptography as it allows secure communication to happen between two or more parties. Without a shared secret among the parties, there is no way for each party to guarantee the identity of the other.([Source](https://www.techopedia.com/definition/10330/shared-secret))

**The algorithm** is the set of rules that dictates how enciphering and deciphering take place, so by keeping the algorithm details secret may help us in securing the process from hackers.

**Use a Key with a Larger Number of Bits**  The larger the number, the more secure the cipher. ([source](https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc_50%2FGUID-B17C6AF6-C913-44A3-815B-5047C7B103D5.html))

Q12: Which of the following are basic block cipher design principles? [Hint: explain why each of the answers a, b and c

either is or is not a basic design principle.] Answer: D, all of the above. Text book, page#136

a) Use both linear and non-linear functions.

b) Use one or two more rounds than the minimum to achieve randomness.

c) Have good avalanche properties.

d) All of the above

e) None of the above

The three aspects of Block cipher design principles: The number of rounds, design of the function F, and key scheduling.

**Use one or two more rounds than the minimum to achieve randomness**(**Number of Rounds**): The cryptographic strength of a Feistel cipher derives from three aspects of the design: the number of rounds, the function F, and the key schedule algorithm. Let us look first at the choice of the number of rounds. The greater the number of rounds, the more difficult it is to perform cryptanalysis, even for a relatively weak F. In general, the criterion should be that the number of rounds is chosen so that known cryptanalytic efforts require greater effort than a simple brute-force key search attack. This criterion was certainly used in the design of DES. Schneier [SCHN96] observes that for 16-round DES, a differential cryptanalysis attack is slightly less efficient than brute force: The differential cryptanalysis attack requires 255.1 operations,10 whereas brute force requires 255. If DES had 15 or fewer rounds, differential cryptanalysis would require less effort than a brute-force key search. This criterion is attractive, because it makes it easy to judge the strength of an algorithm and to compare different algorithms. In the absence of a cryptanalytic breakthrough, the strength of any algorithm that satisfies the criterion can be judged solely on key length.

**Use both linear and non-linear functions(Design of Function F) :** The heart of a Feistel block cipher is the function F, which provides the element of confusion in a Feistel cipher. Thus, it must be difficult to “unscramble” the substitution performed by F. One obvious criterion is that F be nonlinear, as we discussed previously. The more nonlinear F, the more difficult any type of cryptanalysis will be.

There are several measures of nonlinearity, which are beyond the scope of this book. In rough terms, the more difficult it is to approximate F by a set of linear equations, the more nonlinear F is.

Several other criteria should be considered in designing F. We would like the algorithm to have good avalanche properties. Recall that, in general, this means that a change in one bit of the input should produce a change in many bits of the output. A more stringent version of this is the **strict avalanche criterion (SAC)** [WEBS86], which states that any output bit *j* of an S-box (see Appendix S for a discussion of S-boxes) should change with probability 1/2 when any single input bit *i* is inverted for all *i, j*. Although SAC is expressed in terms of S-boxes, a similar criterion could be applied to F as a whole. This is important when considering designs that do not include S-boxes.

Q13: Which of the following is an authenticated encryption (AE), also called authenticated encryption with associated data

(AEAD), cipher? [Hint: provide a brief description for each of the named ciphers, and a published reference paper for

each.]

a) Grain 128-A

b) Hummingbird 2

c) Keyak

d) All of the above

e) None of the above

Answer : D, All of the above

**Grain-128a** The Grain 128a stream cipher was first proposed at Symmetric Key Encryption Workshop (SKEW) in 2011 as an improvement of the predecessor Grain 128, which added security enhancements and optional message authentication using the Encrypt & MAC approach. One of the important features of the Grain family is that the throughput can be increased at the expense of additional hardware. Grain 128a consists of two large parts: Pre-output function and MAC. The pre-output function has an internal state size of 256 bits, consisting of two registers of size 128 bit: NLFSR and LFSR. The MAC supports variable tag lengths w such that 0 less than w and less than equal to 32. The cipher uses a 128-bit key. The cipher supports two modes of operation: with or without authentication, which is configured via the supplied IV\_0 such that if IV\_0 = 1 then authentication of the message is enabled, and if IV\_0 = 0 authentication of the message is disabled.[wiki](https://en.wikipedia.org/wiki/Grain_128a), [reference](https://www.semanticscholar.org/paper/Grain-128a%3A-a-new-version-of-Grain-128-with-%C3%85gren-Hell/dff6d125ac7b256b08dd72b376f7d8be425cd57a)

**Hummingbird-2** is an authenticating encryption primitive that has been designed particularly for resource-constrained devices such as RFID tags, wireless sensors, smart meters and industrial controllers. Hummingbird-2 can be implemented with very small hardware or software footprint and is therefore suitable for providing security in low-cost ubiquitous devices. Hummingbird-2 is resistant to all previously known cryptanalytic attacks. The Hummingbird-2 does not directly fall to either traditional stream cipher or block cipher categories as it inherits properties from both. Since Hummingbird-2 operates on 16-bit blocks, more efficiency can be realized in applications that chirp small messages, such as RFID devices or wireless sensors. This also makes it easy to layer in security in various protocol schemes. The Hummingbird-2 cipher has a 128-bit secret key K and a 128-bit internal state R which is initialized using a 64-bit Initialization Vector IV . These variables are accessed as vectors of 16-bit words: K = (K1, K2, K3, K4, K5, K6, K7, K8), R = (R1, R2, R3, R4, R5, R6, R7, R8), IV = (IV 1, IV 2, IV 3, IV 4). Hummingbird-2 is entirely built from operations on 16-bit words: the exclusive or operation on words (⊕), addition modulo 65536 () and a nonlinear mixing function f(x).([Reference](https://eprint.iacr.org/2011/126.pdf))

**Keyak** is an authenticated crypto system that is based on the Keccak sponge primitive. It is a candidate for the authenticated encryption standard in [NIST’s Caesar competition](https://competitions.cr.yp.to/caesar.html). Keccak is the recent new standard for a hashing algorithm, SHA-3. The sponge primitive is a neat construction. By itself, it is a secure hashing primitive, but can easily be extended to provide encryption, pseudo random number generation, and authentication primitives. Keyak is made of a set of four authenticated encryption functions with support for message associated data. It builds on round-reduced versions of the Keyak-f [800] and Keyak-f [1600] permutations. It uses the duplex construction on top of one of these permutations. The mode that runs on duplex construction is the DuplexWrap which is almost similar to SpongeWrap. In addition, DuplexWrap defines an explicit forget call(calling it is optional) to ensure forward secrecy. Because of this forget call it is not possible to get the key from the intermediate state. But the forgery attack is possible by generating valid ciphertext tag pair for a different message using same key and nonce [source](https://eprint.iacr.org/2015/331.pdf)

Other References : <https://eprint.iacr.org/2014/792.pdf>;

[article](https://conorpp.com/keyak-a-candidate-for-the-authenticated-encryption-standard)

Q14: In public key cryptography, one key is made public (the public key) and one key is made private (the private key). Which

of the following statements is true of public key ciphers?

a) The public key encrypts only, so it must take the plaintext as input.

b) The private key is used only for decryption of ciphertext encrypted with the public key.

c) In RSA in theory, once the keys are calculated, if the ‘public key’ is kept secret and the ‘private key’ is made

public, the cipher is not secure.

d) All of the above

e) None of the above

Answer : D, all of the above

**Public Key Cryptography** uses two set of keys. Private (secret) known only to the owners and Public keys known to anyone. The security goals are confidentiality and authentication. The Encryption is done with sender private (secret) key and receiver public key. The Decryption is done with receiver private (secret) key and sender public key. The public encryption relies on the difficulty of deriving the private key form the public key. It is more complex and slower than symmetric encryption. However, public encryption is widely used in e-commerce, because only the message’s recipient can decrypt the message. Public encryption needs the additional required security. 1) Integrity The original text message can’t be changed without knowing the private key. But the encrypted message can be alerted in the transient without noticing at the receiver side. 2) Authenticity Adding digital signature to the message ensure the identity of the sender. Source: Unit 6 presentation.

**RSA** is the one of the first public key cryptosystem and widely used for secure data transmission. In the RSA approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length. This hash code is then encrypted using the sender’s private key to form the signature. Both the message and the signature are then transmitted. The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender’s public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid. Because only the sender knows the private key, only the sender could have produced a valid signature. We should never publish the private key as it makes the cipher insecure. ( Source : text book, RSA page#427)

Q15: Which of the following are attacks that can be mitigated by a secure message authentication code? [Hint: for each answer

a, b and c, describe the attack and show how a message authentication code mitigates (or not) the attack.]

a) Message authentication code modification – secure MAC authenticator could mitigate such a modification.

b) Message modification – Is an attack where changes to the contents of a message, including insertion, deletion, transposition, and modification.

c) Source repudiation – Is an attack where denial of transmission of message by source. Text book page#383

d) All of the above

e) None of the above

Answer : D, All of the above

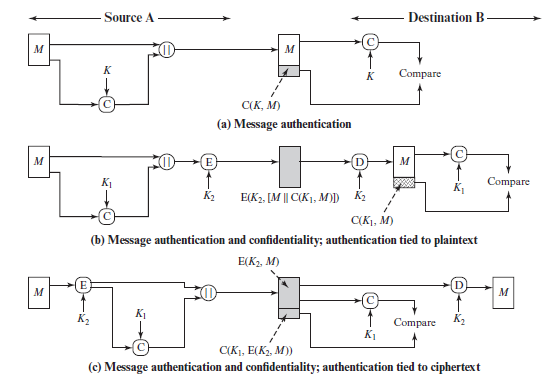
**Message authentication code (MAC),** sometimes known as a *tag***:** Is a function of the message and a secret key that produces a fixed-length value that serves as the authenticator. It’s an alternative authentication technique involves the use of a secret key to generate a small fixed-size block of data, known as a **cryptographic checksum** or MAC, that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key *K*. When A has a message to send to B, it calculates the MAC as a function of the message and the key: MAC = C(*K*, *M*) where *M* = input message, C = MAC function, *K* = shared secret key, MAC = message authentication code. The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message, using the same secret key, to generate a new MAC. The received MAC is compared to the calculated MAC.(Figure 3). If we assume that only the receiver and the sender know the identity

of the secret key, and if the received MAC matches the calculated MAC, then **1.** The receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the MAC, then the receiver’s calculation of the MAC will differ from the received MAC. Because the attacker is assumed not to know the secret key, the attacker cannot alter the MAC to correspond

to the alterations in the message. **2.** The receiver is assured that the message is from the alleged sender. Because

no one else knows the secret key, no one else could prepare a message with a proper MAC. If the message includes a sequence number (such as is used with HDLC, X.25, and TCP), then the receiver can be assured of the proper sequence because an

attacker cannot successfully alter the sequence number. In summary, any message modification can be mitigated by Secure MAC.



*Figure 3.*

For a secure unforgeable message authentication code(MAC), it should be computationally infeasible to compute a valid tag of the given message without knowledge of the key, even if for the worst case, we assume the adversary can forge the tag of any message except the given one. MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of [non-repudiation](https://en.wikipedia.org/wiki/Non-repudiation) offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages.

**NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin -** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

**Source repudiation:** Since MACs are based on symmetric principles, they do not provide non-repudiation but can counter repudiation, through digital signature. If the sender and receiver get involved in a dispute over message origination, MACs cannot provide a proof that a message was indeed sent by the sender. Though no third party can compute the MAC, still sender could deny having sent the message and claim that the receiver forged it, as it is impossible to determine which of the two parties computed the MAC.

Q16 (6 points) Explain the birthday paradox and provide an example illustrating it’s detrimental impact on the security of a system.

Create a table illustrating the birthday paradox for variables of bit size n = 16, 32, 64, 128, 256 and 512. [Hint: your

answer should include at least two paragraphs and a table created in Word. Calculate the table values yourself.]

Birthday Paradox: It describes the probabilistic occurrence for breaking on-way hashing algorithm. Hashing a text result into a value that is supposed to be unique. But, when you use smaller key length to hash text, two or more texts may result into same hash value. That is called Collison. This is better explained with a birthday example. In a room of handful of people, there are chances of having exact same birthdate. In mathematical terms, those chances are as follows.

If you are looking exact birthdate, in that room to have 50% or greater chances to have that date as two people’s birthdate, you need to have 253 people in that room

The probability of 50% or greater to have any matching birthdays in a room, you only need 23 people in that room.

Why do we care about these birthday collisions? this exact collision can occur for hashing algorithm also. The main way that an attacker of hashing algorithm, can find the corresponding hashing value that matches a specific message is through a brute force attack. If he/she finds a message with a specific hash value, it is equivalent to finding someone with specific birthday. If he/she finds two messages with same hash values, it is equivalent to finding two people with the same birthday.

The output of a hashing algorithm is n-bits in length, and to find a message through a brute force attack that results in a specific hash would require 2n random messages. Then to take this one step further, finding two messages that hash to the same value would require 2n/2 messages to be reviewed. That means that if an attacker has one hash value and wants to find a message that hashes to the same hash value, the process could take him years. However, if he just wants to find any two messages with the same hashing value, it could only take him only couple of hours.

If the n is longer, the occurrence of two same hash values for two different texts will significantly lower. In MD-5 hashing algorithm, which is 128-bit in length, the even or greater probability of occurring same hash value for two texts is 264. That is significantly large value, but still it is shorter in comparison to other hashing algorithms. SHA1 is 160-bit hashing algorithm. In this algorithm that same probability will go to 280. Even with that large value, SHA1 is broken with recent computing power. Now the industry is using SHA2, SHA512, and SHA1024. As the length of the hash value grows, the brute force attack gets complex.

|  |  |  |
| --- | --- | --- |
| Bit length of Hashing algorithm | Number of brute force attempts to un-hash the value | Probability of having 50% of greater chances of occurring two values with same hash value |
| 16 | 216 | 28 messages to review |
| 32 | 232 | 216 |
| 64 | 264 | 232 |
| 128 | 2128 | 264 |
| 256 | 2256 | 2128 |
| 512 | 2512 | 2256 |

*Table 1.*

Q17 (7 points) Computer networks are designed following a layered model. For the five layer network model, for each layer identify at least one specific security protocol that is used for communications at that layer. Identify at least one peer reviewed

published paper or RFC standard (look to RFCs first) that defines security for a particular layer and in 2-3 paragraphs

explain the security protocol. Note that unique security protocols exist at every layer, including the Physical Layer. [Hint:

search peer reviewed publications and standards for security at each layer. Use a table to summarize each layer security.]

In Q17, for each layer (5 layers), pick one protocol. Then summarize the main tasks and features of that protocol. Therefore, you describe 5 different protocols.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Network Layers | Transportation Protocol | Corresponding Security protocol | Descriptions | Peer reviewed paper |
| Application | HTTP | HTTPS | HTTPS (HTTP over SSL or HTTP Secure) is the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) as a sublayer under regular HTTP application layering. HTTPS encrypts and decrypts user page requests as well as the pages that are returned by the Web server. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks. | [Article](https://ieeexplore.ieee.org/abstract/document/4768661) |
| Transport | TCP | SSL | The salient features of SSL protocol are as follows −  SSL provides network connection security through −  **Confidentiality** − Information is exchanged in an encrypted form.  **Authentication** − Communication entities identify each other through the use of digital certificates. Web-server authentication is mandatory whereas client authentication is kept optional.  **Reliability** − Maintains message integrity checks.  SSL is available for all TCP applications.  Supported by almost all web browsers.  Provides ease in doing business with new online entities.  Developed primarily for Web e-commerce. | [Article](http://www.rfc-editor.org/info/rfc6101) |
| Network | IP | IPSec | The popular framework developed for ensuring security at network layer is Internet Protocol Security (IPsec).  **Features of IPsec**   * IPsec is not designed to work only with TCP as a transport protocol. It works with UDP as well as any other protocol above IP such as ICMP, OSPF etc. * IPsec protects the entire packet presented to IP layer including higher layer headers. * Since higher layer headers are hidden which carry port number, traffic analysis is more difficult. * IPsec works from one network entity to another network entity, not from application process to application process. Hence, security can be adopted without requiring changes to individual user computers/applications. * Tough widely used to provide secure communication between network entities, IPsec can provide host-to-host security as well. * The most common use of IPsec is to provide a Virtual Private Network (VPN), either between two locations (gateway-to-gateway) or between a remote user and an enterprise network (host-to-gateway). | [Article](https://www.usenix.org/legacy/events/sec2000/full_papers/zhangipsec/zhangipsec_html/) |
| Data-link | Wireless LAN | WAP (Wi-fi Protected Access) | This protocol implements the majority of the IEEE 802.11i standard. It existed before IEEE 802.11i and uses RC4 algorithm for encryption. It has two modes of operation. In ‘Enterprise’ mode, WPA uses authentication protocol 802.1x to communicate with authentication server, and hence pre-master keys (PMK) is specific to client station. In ‘Personal’ mode, it does not use 802.1x, PMK is replaced by a pre-shared key, as used for Small Office Home Office (SOHO) wireless LAN environments | [Article](https://patents.google.com/patent/US8954069B2/en) |
| Physical | Ethernet | CSMA/CD(Carrier sense multiple access/collision detection) | CSMA/CD is a media access control method used mostly in ethernet technology for local area networking | [Article](http://rionhollenbeck.com/GradPortfolio/Papers/620-Ethernet/Ethernet.pdf) |

*Table 2*

Q18 (6 points) A Denial of Service (DoS) attack is a security event that occurs typically over the Internet. Identify and describe two

approaches/mechanisms that attackers use or have used to carry out DoS (or Distributed DoS - DDoS) attacks. For each

attack approach identify an article (peer reviewed, white paper or non-peer reviewed) that describes how the attack was

used in an actual attack. Summarize the attack in 2-3 paragraphs and identify potential approaches that could be used

or have been implemented to mitigate the attack.

A denial-of-service(DoS) attack is an attempt to prevent legitimate users of a service from using that service. when this attack comes from a single host or network node then it is simply referred to as a DoS attack. A more serious threat is posed by a DDoS, Distributed denial of service attack. DDoS attacks make computer systems inaccessible by flooding servers, networks, or even end-user systems inaccessible by flooding servers, networks, or even end-user systems with useless traffic so that legitimate users can no longer gain access to those resources. In a typical DDoS attack, a large number of compromised hosts are amassed to send useless packets.

One way, we can classify DDoS attacks in terms of the type of resource that is consumed. Broadly speaking, the resource consumed is either internal resource attack or data transmission capacity in the local network to which the target is attacked.

Example of an Internal resource attack is the SYN flood attack.

Figure 4a. shows the steps involved:

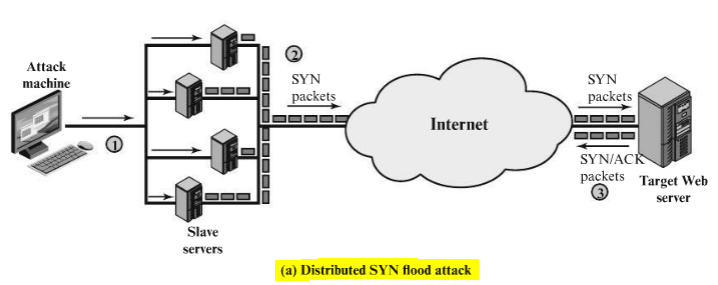
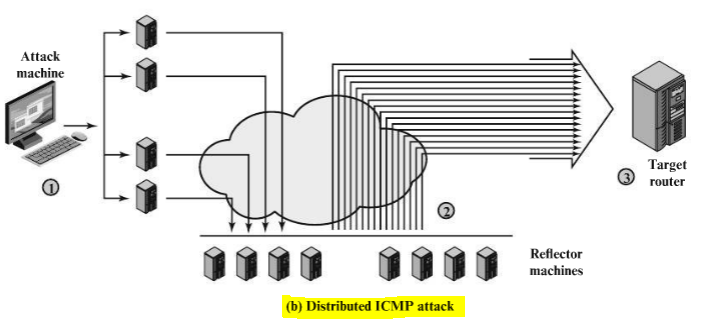
* The attacker takes control of multiple hosts over the internet, instructing them to contact the target web server.
* The slave hosts begin sending TCP/IP SYN (synchronize/initialization) packets, with erroneous return IP address information, to the target.
* Each SYN packet is a request to open a TCP connection. For each such packet, the web server responds with a SYN/ACK(synchronize/acknowledge) packet, trying to establish a TCP connection with a TCP entity at a spurious IP address. The Web server maintains a data structure for each SYN request waiting for a response back and becomes bogged down as more traffic floods in. The result is that legitimate connections are denied while the victim machine is waiting to complete bogus "half-open" connections.

The TCP state data structure is a popular internal resource target but by no means the only one.[CERT01] gives the following examples:

* An intruder may attempt to use up available data structures that are used by the OS to manage processes, such as process table entries and process control information entries. The attack can be quite simple, such as a program that forks new processes repeatedly.
* An intruder may attempt to allocate to itself large amounts of disk space by a variety of straightforward means. These include generating numerous e-mails, forcing errors that trigger audit trails, and placing files in shareable areas.

Figure 4b. illustrates an example of an attack that consumes data transmission resources. The following steps are involved:

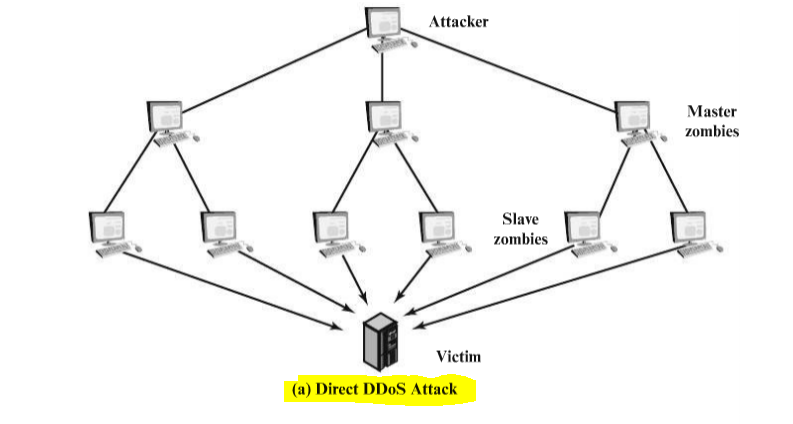
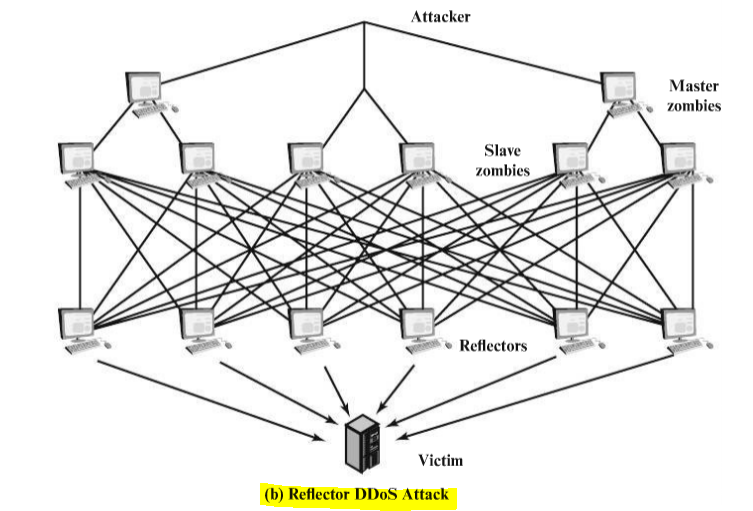
* + The attacker takes control of multiple hosts over the Internet, instructing them to send ICMP ECHO packets with the target's spoofed IP address to a group of hosts that act as reflectors, as described subsequently.
  + Nodes at the bounce site receive multiple spoofed requests and respond by sending echo reply packets to the target site.
  + The target's router is flooded with packets from the bounce site, leaving no data transmission capacity for legitimate traffic.

*Figure 4a and 4b.*

Another way to classify DDoS attacks is as either direct or reflector DDoS attacks. In a direct DDoS attack(Figure 5a), the attacker is able to implant zombie software on a number of sites distributed throughout the Internet. Often, the DDoS attack involves two levels of zombie machines: master zombies and slave zombies. The hosts of both machines have been infected with malicious code. The attacker coordinates and triggers the master zombies, which in turn coordinate and trigger the slave zombies. The use of two levels of zombies makes it more difficult to trace the attack back to its source and provides for a more resilient network of attackers.

A reflector DDoS attack adds another layer of machines (Figure 5b). In this type of attack, the slave zombies construct packets requiring a response that contain the target's IP address as the source IP address in the packet's IP header. These packets are sent to uninfected machines known as reflectors. The uninfected machines respond with packets directed at the target machine. A reflector DDoS attack can easily involve more machines and more traffic than a direct DDoS attack and hence be more damaging. Further, tracing back the attack or filtering out the attack packets is more difficult because the attack comes from widely dispersed uninfected machines.

*Figure 5a and 5b.*

**Countermeasures:** In general, there are three lines of defense against DDoS attacks[CHAN02]:

* **Attack prevention and preemption (before the attack) :** These mechanisms enable the victim to endure attack attempts without denying service to legitimate clients. Techniques include enforcing policies for resource consumption and providing backup resources available on demand. In addition, prevention mechanisms modify systems and protocols on the Internet to reduce the possibility of DDoS attacks.
* **Attack detection and filtering( during the attack) :** These mechanisms attempt to detect the attack as it begins and respond immediately. This minimizes the impact of the attack on the target. Detection involves looking for suspicious patterns of behavior. Response involves filtering out packets likely to be part of the attack.
* **Attack source traceback and identification (during and after the attack) :** This is an attempt to identify the source of the attack as a first step in preventing future attacks. However, this method typically does not yield results fast enough, if at all, to mitigate an ongoing attack.

The challenge in coping with DDoS attacks is the sheer number of ways in which they can operate. Thus, DDoS counter measures must evolve with the threat.

References:

CERT01 : CERT Coordination Center. "Denial of Service Attacks" June 2001. http://www.cert.org/tech\_tips/denial\_of\_service.html

CHAN02 : Chang, R "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A tutorial." IEEE Communications Magazine, October 2002.

HONE05 : The Honeynet Project. Knowing your Enemy: Tracking Botnets. Honeynet White Paper, March 2005. <http://honeynet.org/papers/bots>

Q19 (6 points) Describe how a man-in-the-middle attack can be defeated during the process of establishing a secure communication channel between Alice and Bob. You may use symmetric key ciphers, public key ciphers, certificates, hash algorithms, or any other security mechanism discussed in class. [Hint: describe the complete sequence of steps in as much detail as

possible. Do not skip steps. Do not skip details. Draw a communication diagram that illustrates each step.]

[References](https://wordtothewise.com/2014/09/cryptography-alice-bob/)

**Man-in-the-middle attack:** An intruder injects himself into an ongoing conversation between two computers so that she can intercept and read messages being passed back and forth. These attacks can be countered with digital signatures and manual authentication techniques.

Computer to computer communication

Hello, 10.20.213.32

Hi, 10.20.211.21

10.20.211.21 10.20.213.32

Typical communication between two computers is depicted as above.

Hello, 10.20.213.32

Hi, 10.20.211.21

10.20.211.21 10.20.213.32 10.20.213.32

(impersonator) (original)

A rouge computer, impersonator can pose as 10.20.213. 32 and start receiving the communication from 10.20.211.21. Whereas 10.20.211.21 has no idea about the rogue computer. There should be a third party that validated 10.20.213.32 is the right computer before 10.20.211.21 start communicating. That can be achieved through Secure Socket Link (SSL) over PKI infrastructure. In PKI infrastructure, we will have third party validator, it is called Certificate Authority (CA). Both 10.20.211.21 and 10.20.213.32 will subscribe to CA to receive PKI certificates. That provides public and private key combinations to both the computers.