CS 7349
Data and Network Security
Exam #1

Name: Bingying Liang
ID: 48999397

Due: Mar 4 2024

Exam 1: Directions

This document contains the questions for the exam. For your answers, create a pdf document that clearly identifies every question number and your answer to that question. Name the file containing your answers 'yourLastNameCS7349Exam1.pdf'. For example, the file for Shaibal Chakrabarty would have the name ChakrabartyCS7349Exam1.pdf. Submit your pdf file.

Answer each question fully and completely. The highlighted words are your response guide – missing them will result in points deduction. Show all of your work and state your assumptions where appropriate. The questions may have 'hints' embedded within them regarding the answer. Treat these as directions. Follow these hints as appropriate for full points.

Collaboration is expected and encouraged; however, each student must hand in their own exam. To the greatest extent possible, answers should NOT be copied but, instead, should be written in your own words. Copying answers from anywhere is plagiarism, this includes copying text directly from the textbook. Any copied answers, identical answers to other students in the course (past or present) or otherwise plagiarized answers will receive a grade of zero. More than one plagiarized answer will result in a grade of 'F' for the exam with zero points earned and the procedure for academic dishonesty will be initiated. Do not copy answers. Always use your own words. Directly under each question list all persons with whom you collaborated and list all resources used in arriving at your answer. Resources include but are not limited to the textbook used for this course, papers read on the topic, class presentations and Google search results. Note that Google is not a reference. It is a tool to find references. Don't forget to place your name in the document itself.

ALWAYS provide references, your collaborators, and submit your answers in the format, and font, of the questions, in a .pdf file. Write the question and provide the answer in the same order (numbering) as the question.

Exam 1: Questions

1. In cryptography, what is a cipher? [Hint: be sure to define each of the answers as they relate to cryptography and choose the answer that is most appropriate to what has been discussed in class.]

   (a) An encrypted message

   (b) An algorithm for performing encryption and decryption

   (c) A zero

(d) A code

Solution: (b) An algorithm for performing encryption and decryption.

Explanation: A cipher in cryptography refers to an algorithmic process, which is often used to encrypt, or decrypt, to make readable data plaintext into unreadable format ciphertext and vice versa, ensuring confidentiality of the transmitted or stored information[1].

2. 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? [Hint: explain each of the identified modes of operation and use a diagram to help explain how it operates.]

   (a) Counter Mode

   (b) Output Feedback Mode

   (c) Stream Mode

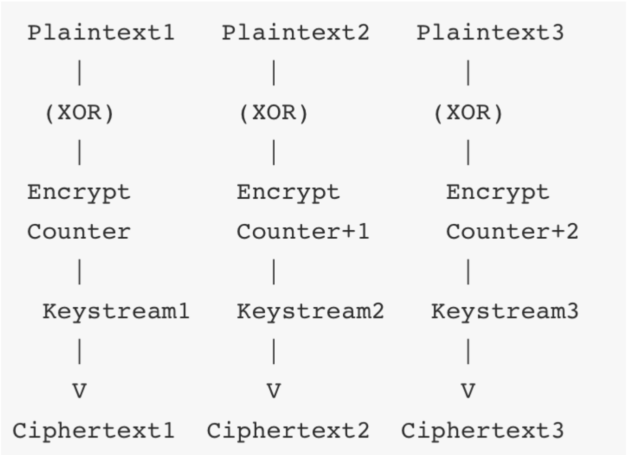
   (d) All of the above.

   (e) None of the above.

Solution: (a) Counter Mode (b) Output Feedback Mode

Explanation: There is no mode explicitly named ”Stream Mode” in standard cryptographic texts; however, the concept of using a block cipher in a way that it generates a keystream to encrypt plaintext bits or bytes at a time is characteristic of stream cipher operation. Counter Mode can turn a block cipher into a stream cipher, and Output Feedback Mode same.

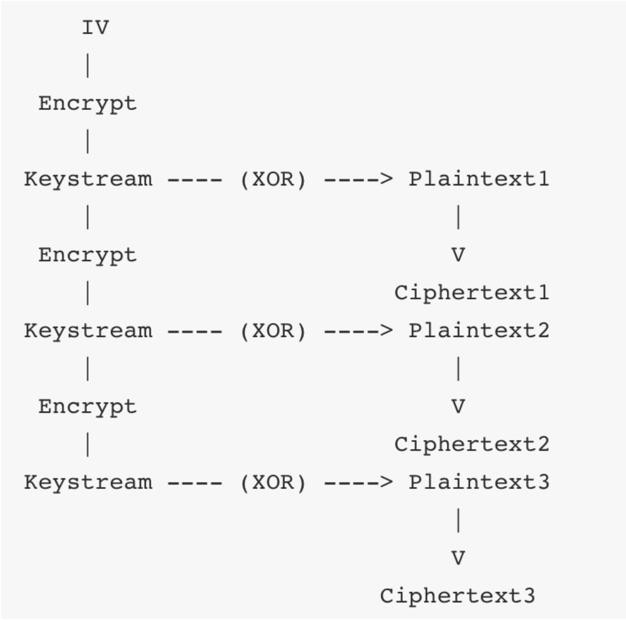
Counter Mode (CTR): it can encrypt successive values of a counter to generate a keystream. The plaintext is XORed with this keystream to produce the ciphertext. This process generates a key stream, which can then be xor with plaintext to become ciphertext. When decrypting, the same keystream generation process can be used.



```
 Plaintext1   Plaintext2   Plaintext3
     |            |            |
   (XOR)        (XOR)        (XOR)
     |            |            |
 Encrypt       Encrypt       Encrypt
 Counter       Counter+1     Counter+2
     |            |            |
  Keystream1   Keystream2   Keystream3
     |            |            |
     V            V            V
Ciphertext1  Ciphertext2  Ciphertext3
```

[1]

Output Feedback Mode (OFB): In Output Feedback Mode, an initial vector (IV) is encrypted, and the output is fed back as the input for the next encryption.



```
    IV
    |
 Encrypt
    |
Keystream ---- (XOR) ----> Plaintext1
    |                          |
 Encrypt                       V
    |                      Ciphertext1
Keystream ---- (XOR) ----> Plaintext2
    |                          |
 Encrypt                       V
    |                      Ciphertext2
Keystream ---- (XOR) ----> Plaintext3
                               |
                               V
                         Ciphertext3
```

[1]

3. 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.]

   (a) Cryptography Encryption and Decryption

   (b) Trust

   (c) Authentication

   (d) Public Key Certificates

   (e) Digital Signatures

   Solution: (a) Trust

   Explanation:

   Trust is the fundamental cornerstone upon which all aspects of Internet security are built. Without trust, none of the technical mechanisms (like encryption, authentication, certificates, or digital signatures) can effectively ensure security.

   (a) Cryptography Encryption and Decryption

   Explanation: Cryptography involves methods of secure communication that remain confidential even when potentially observed by unauthorized parties. [1]. It encompasses techniques such as encryption and decryption to safeguard information.

   Dependence on Trust: For encryption and decryption to be effective, there must be trust in the algorithms, the security of the keys, and the integrity of the parties exchanging the keys. Trust in the cryptographic system underpins its effectiveness.

   (c) Authentication

   Explanation: Authentication refers to the procedure of confirming the identity of a user, system, or entity. It ensures that an entity is who it claims to be.

   Dependence on Trust: Authentication mechanisms rely on trust in the methods used for authentication (passwords, biometrics, etc.) and the systems that manage these methods (authentication servers, databases, etc.). Trust in the entity's claim and the system's verification process is essential.

(d) Public Key Certificates

Explanation: Public key certificates are electronic documents that verify the ownership of a public key. These certificates are used in various security protocols to ensure that public keys are authentic and belong to the entity claimed.

Dependence on Trust: The effectiveness of public key certificates hinges on trust in the certificate authority (CA) that issues them. Users must trust that the CA has properly verified the identity of the certificate holder and that the CA's infrastructure is secure.

(e) Digital Signatures

Explanation: Digital signatures are a cryptographic method employed to validate the authenticity and integrity of a message, software, or digital document. It assures that the message has not been altered and confirms the identity of the signer.

Dependence on Trust: Digital signatures rely on trust in the private key's security (used to create the signature) and the public key's authenticity (used to verify the signature). Trust in the issuing authority of the signing certificate is also crucial.

4. What does it mean to be secure?

   (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 well-being, such as food, health care, and the opportunity to live well.

   (d) All of the above.

   (e) None of the above.

Solution: (d) All of the above.

Explanation:

(a) This perspective focuses on country security and war. The power of the military. It shows that security can bring peace. It plays a very important role in peace.

(b) This perspective focuses on society. It shows security in the whole society, like the economy.

(c) This perspective focuses on people's lives. It shows security is everywhere, happening in every day, like food, and water.

(d) Different perspectives of security of above. It shows that security is everywhere. For different people and different situations, the definition of security is different. But the world needs it everywhere. It suggests an inclusive understanding that recognizes the complexity of security in the modern world, where threats are diverse and interconnected, and responses must be multifaceted to ensure the safety and well-being of states and their populations.

5. 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).]

(a) Counter Mode

(b) Cypher Block Chaining Mode

(c) Electronic Codebook Mode

(d) All of the above.

(e) None of the above.

Solution: (a) Counter Mode and (c) Electronic Codebook Mode.

Explanation:

(a) Counter Mode (CTR)[1]: In Counter (CTR) mode, a unique counter for each plaintext block is encrypted and then XORed (exclusive OR) with the plaintext block to generate the ciphertext. To decrypt, the same encrypted counter is XORed with the ciphertext, yielding the original plaintext. Decryption in CTR mode can be performed in parallel because each block is decrypted independently of others, relying on the counter and key only.

(b) Cipher Block Chaining Mode (CBC)[1]: In Cipher Block Chaining (CBC) mode, each plaintext block is encrypted by first XORing it with the preceding ciphertext block, using an initialization vector for the first block. For decryption, the ciphertext is first decrypted and then XORed with the previous ciphertext block to retrieve the plaintext. Decryption in CBC mode cannot be parallelized since decrypting each block relies on the ciphertext of the block before it.

(c) Electronic Codebook Mode (ECB)[1]: ECB mode encrypts each block of plaintext independently of any other block. This implies that identical blocks of plaintext will result in identical blocks of ciphertext when encrypted. For decryption, each block is decrypted independently. Decryption in ECB mode can be performed in parallel because the decryption of each block is independent of any other block.

(d) Given the explanations above, the modes that allow for decryption to be performed in parallel are Counter Mode (CTR) and Electronic Codebook Mode (ECB).

(e) This option is incorrect based on the explanation provided.

6. 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.]

(a) The hash value is preimage resistant.

(b) The hash value is second preimage resistant.

(c) The hash values are collision resistant.

(d) All of the above.

(e) None of the above.

Solution: (d) All of the above.

Explanation:

(a) Preimage resistance signifies that it should be computationally challenging to identify any input that, when hashed, produces a specified output. This is crucial to prevent attackers from discovering the original data from its hash value.

(b) Second preimage resistance indicates that it should be computationally difficult to find any second input that results in the same hash output as a given specific input. This ensures data integrity by preventing an attacker from creating a different input that results in the same hash as the original input.

(c) Collision resistance implies that it is computationally impractical to discover two different inputs that produce the same hash output. This property is important to prevent different messages from being intentionally manipulated to produce the same hash, which could undermine systems relying on hashes for identification, integrity checks, or digital signatures.

7. 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.]

   (a) Hacker

   (b) Identity Thief

   (c) Intruder

   (d) Cyber-terrorist

   Solution: (a) Hacker.

   Explanation:

   (b) Identity Thief specifically refers to someone who steals personal information to impersonate someone else, often for financial gain.

   (c) Intruder is a broader term that could apply to unauthorized access but lacks the specificity related to computer systems implied by "hacker."

   (d) Cyber-terrorist refers to individuals or groups that use hacking to conduct terrorist activities, implying a motive of causing fear or harm for ideological, political, or similar purposes.

   Thus, "hacker" is the most fitting term to describe someone who unlawfully breaches a computer system in a broad context.

8. 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.]

   (a) e-mail privacy

   (b) Software piracy

   (c) Intellectual property rights and copyrights

   (d) All of the above

   (e) None of the above

   Solution: (d) All of the above.

   Explanation:

(a) E-mail privacy: This involves the confidentiality and integrity of e-mail communications. Ethical issues arise regarding the extent to which businesses can monitor or access employee emails, balancing the company's right to protect its interests and assets with employees' expectations of privacy. Unauthorized access or misuse of email content can lead to breaches of trust and privacy violations.

(b) Software piracy: Software piracy involves the illegal copying, distribution, or usage of software without authorization. It raises ethical issues related to the theft of intellectual property, as it deprives software creators of compensation for their work and undermines the market's fairness and integrity. Software piracy can also expose users to legal risks and security vulnerabilities.

(c) Intellectual property rights and copyrights: These are legal rights that protect the creators of original works from unauthorized use of their creations. Ethical issues stem from the need to respect and uphold these rights in the digital age, where copying and distributing content can be easily done. Violations of intellectual property rights and copyrights can lead to a loss of revenue for creators and distort the incentives for innovation and creativity.

Each of these issues involves ethical considerations regarding respect for privacy, the protection of intellectual property, and the fair use of technological resources and content in the business world.

9. 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.]

(a) Scalability

(b) Backward Predictability

(c) A Shared Initialization Vector

(d) All of the above

(e) None of the above

Solution: (a) is desired, (c) is context-dependent.

Explanation:

(a) Scalability: Yes, it's desired. It allows the PRNG to efficiently generate a large volume of numbers as needed.

(b) Backward Predictability: No, it's not desired. A PRNG should not allow someone to predict previous numbers from its output, as this compromises security.

(c) A Shared Initialization Vector: Conditionally desired. While sharing an IV is necessary in some cryptographic protocols to synchronize the PRNG between systems, it must be managed securely to avoid compromising the PRNG's outputs.

Based on these points, the correct answer is not straightforward from the given options, as (a) is desired, (b) is not, and (c) is context-dependent. Thus, none of the provided options (d) or (e) perfectly fits without additional context or clarification.

10. 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.]

(a) Hash function

(b) Private key operation

(c) Symmetric key operation

(d) All of the above

(e) None of the above

Solution: (d) All of the above.

Explanation:

(a) Hash function: A hash function takes a message and generates a fixed-size byte sequence, known as the message digest or hash, uniquely representing the original message. If the message changes during transmission, its hash will also change, revealing any alterations. Hash functions are key in ensuring message integrity, particularly when used alongside digital signatures or HMACs (Hash-based Message Authentication Codes).

(b) Private Key Operation: In digital signatures, a sender uses a private key to sign a message. The receiver verifies this signature with the corresponding public key. If the message is altered after signing, verification fails, ensuring message integrity. Private key operations mainly provide authentication, non-repudiation, and integrity protection.

(c) Symmetric Key Operation: Symmetric key algorithms use the same key for encryption and decryption. While their primary use is for confidentiality, they can also provide integrity protection when used in modes that include integrity checks, such as Authenticated Encryption with Associated Data (AEAD) modes (e.g., AES-GCM). In such cases, the symmetric key operation ensures that any alteration of the encrypted message or its associated data will be detected upon decryption.

(d) Each of the options can be used to provide integrity protection, albeit in different ways: Hash functions directly provide integrity checking; Private key operations (as part of digital signatures) ensure integrity along with authentication; Symmetric key operations can provide integrity through specific encryption modes designed to detect alterations.

11. 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. Hint Hint: 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.]

(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

Solution: (c) Use a Key with a Larger Number of Bits.

Explanation:

(a) Shared Secret Key: Sharing a secret key is a fundamental part of symmetric cryptography. However, simply sharing a secret key does not inherently increase the strength of the cipher itself; the security of the encryption is more about how the key is used and managed rather than the act of sharing it.

(b) Keep Algorithm Details Secret: This approach, known as ”security through obscurity,” is generally not recommended in cryptography. The strength of a cipher should not rely on the secrecy of its algorithm. Kerckhoffs's principle states that a cryptographic system should remain secure even when all details about the system, with the exception of the key, are publicly known.

(c) Use a Key with a Larger Number of Bits: Increasing the key size directly increases the cipher's strength by making it more resistant to brute-force attacks. The larger the key size, the more possible key combinations there are, exponentially increasing the difficulty for an attacker to guess the correct key.

12. 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.]

    (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

    Solution: (d) All of the above.

    Explanation:

    (a) Use both linear and non-linear functions: This is indeed a basic design principle of block ciphers. Incorporating both types of functions guarantees that the connection between plaintext and ciphertext is intricate and challenging to reverse without possessing the key, thereby enhancing the security of the encryption process. Non-linear functions help to prevent linear attacks, while linear functions can ensure efficient diffusion throughout the block.

    (b) Use one or two more rounds than the minimum to achieve randomness: Adding extra rounds beyond the minimum required for achieving what might be considered sufficient mixing (or randomness) of the plaintext into the ciphertext helps in increasing the security margin. This principle acts as a safeguard against unforeseen vulnerabilities and ensures that the cipher remains robust against exhaustive key search and cryptanalytic attacks as methods improve over time.

    (c) Have good avalanche properties: The avalanche effect refers to a crucial characteristic of cryptographic algorithms, wherein a minor alteration in the input, whether in the plaintext or the key, results in a substantial transformation in the output, or the ciphertext. This attribute guarantees that the ciphertext is profoundly responsive to changes in the plaintext and key, enhancing the cipher's security by complicating attackers' attempts to infer any valuable information without precise knowledge of the initial input.

13. 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

Solution: (d) All of the above.

Explanation:

(a) Grain 128-A: Grain 128-A is primarily known as a stream cipher, designed for use in constrained environments such as RFID tags and sensors. While it emphasizes low power consumption and efficient implementation, it is not specifically classified as an AE or AEAD cipher in its standard form. Grain 128-A is part of the eSTREAM portfolio[2].

(b) Hummingbird 2: Hummingbird-2 is an ultra-lightweight cryptographic algorithm tailored for use in devices with limited resources. It combines encryption and MAC functionalities, indicating a step towards authenticated encryption. However, it's not widely recognized as a standard AEAD scheme but rather as a cipher suitable for specific applications requiring both encryption and integrity in constrained environments[3].

(c) Keyak: Keyak is included in the CAESAR competition, which focuses on Authenticated Encryption: Security, Applicability, and Robustness, as an AEAD scheme. It is designed to provide both encryption and authentication efficiently and is suitable for a wide range of applications. Keyak is explicitly designed as an AEAD cipher, supporting the secure encryption of data along with the authentication of associated data[4].

14. 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

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

Explanation: This statement correctly captures the essence of public key cryptography, wherein the public key encrypts data, and its corresponding private key decrypts the data. This mechanism allows data to be encrypted by anyone using the public key, yet ensures that only the private key holder can decrypt it, thereby safeguarding confidentiality.

15. 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

(b) Message modification

(c) Source repudiation

(d) All of the above

(e) None of the above

Solution: (b) Message modification, by ensuring that any changes to the message during transmission are detected, making it a direct application of MACs to protect message integrity.

Explanation:

(a) Message authentication code modification: If a MAC itself is modified during transmission, the integrity check at the receiver's end will fail when the MAC is compared with the recalculated MAC of the received message content. This discrepancy indicates tampering, thus mitigating the attack by alerting the receiver to the alteration. However, the MAC's primary role is not to protect its own integrity but the integrity of the message it accompanies. The mitigation comes from the fact that a valid MAC cannot be generated without knowing the secret key used to create it.

(b) Message modification: A MAC effectively mitigates message modification attacks. If a message is modified during transmission, the Message Authentication Code (MAC) calculated by the receiver with the shared secret key won't align with the MAC that was sent along with the message. This discrepancy alerts the receiver that the message has been tampered with. Thus, a MAC ensures the integrity of the message by enabling the detection of unauthorized changes.

(c) Source repudiation: Source repudiation refers to the sender denying that they sent a message. MACs help counter this issue by authenticating the message's origin, under the assumption that the MAC is created using a secret key shared exclusively between the sender and the receiver. However, non-repudiation (preventing denial of authorship) is more strongly associated with digital signatures, which use public key cryptography. While a MAC can imply the message came from someone who had access to the secret key, it does not by itself provide non-repudiation in the way that a digital signature can, because the shared key is known by both parties, not just the sender.

(d) All of the above: Based on the explanations, MACs can mitigate message modification attacks by ensuring the integrity and authenticity of a message. However, for source repudiation, while MACs provide some level of assurance regarding the message's source, they do not offer full non-repudiation capabilities. Therefore, the statement that all the listed attacks can be mitigated by a MAC might be misleading without the nuance that MACs do not fully address non-repudiation.

16. 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. Calculate the table values yourself.]

Solution: The birthday paradox describes the surprising likelihood in statistics that among a group of randomly selected individuals, there will be at least two who share the same birthday much earlier than one might guess. Notably, it takes only 23 individuals for the probability of a shared birthday to reach 50%. This concept holds importance in the fields of cryptography and security, particularly in relation to the collision resistance of hash functions, where it illustrates the unexpected frequency of collisions between different inputs producing the same output.

The birthday paradox reveals that in cryptography, finding two unique inputs that result in the same hash output (a collision) is easier than expected, emphasizing the importance of collision-resistant hash functions. For example, if a hash function produces a 64-bit hash, one might think that one would need to try about 2^{64} different inputs to find a collision. But, birthday paradox, a collision will likely be found after trying only about $2^{(\frac{64}{2})} = 2^{32}$ inputs. This adversely affects the security of systems that rely on cryptographic hashes for digital signatures or blockchain technology, which undermines the credibility and reliability of cryptographic guarantees.

Suppose, the probability of finding a collision is 50% for hash functions of various bit sizes. The formula to estimate this number, based on the birthday problem, is approximately

$$\sqrt{2nln(0.5)}, \text{ where } n = 2^{\text{bit size}}$$

For $n = 16, 32, 64, 128, 256, 512$:

Bit Size (n)	Approx. Trials for 50% Collision
16	256
32	65,536
64	4,294,967,296
128	1.84×10^{19}
256	3.40×10^{38}
512	1.16×10^{77}

For instance, for a 64-bit hash, the intuitive expectation might be that one would need to try half of the total hash space 2^{63} to find a collision. However, the birthday paradox shows that only about 4 billion trials are needed to have a 50% chance of finding a collision, highlighting its impact on the security of systems using cryptographic hash functions. As the bit size increases, the number of trials needed grows exponentially, yet it's still significantly less than half the total hash space, underlining the importance of using hash functions with sufficiently large output sizes in cryptographic applications to mitigate collision attacks.

17. 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.]

Solution: In computer networks, security protocols are implemented across different layers of the network architecture to ensure secure communication. The five-layer network model includes the Physical, Data Link, Network, Transport, and Application layers[9]. The overview of a security protocol for each layer is in the following table[5]:

Layer	Security Protocol	Reference
Physical	IEEE 802.11i (WPA2)	RFC 7212
Data Link	MACsec (IEEE 802.1AE)	IEEE 802.1AE-2006
Network	IPsec	RFC 4301
Transport	TLS	RFC 8446
Application	HTTPS (over TLS)	RFC 2818

TLS (Transport Layer Security)

TLS 1.3, which is detailed in RFC 8446, marks a significant update from its predecessor, TLS 1.2, with a strong emphasis on improving both security and performance. One of the key enhancements is the optimization of the handshake process, which now necessitates fewer exchanges between the client and server, thus accelerating the time it takes to establish a connection. This version introduces a requirement for forward secrecy, ensuring that even if future security breaches occur, past communications remain protected. This is achieved through the use of ephemeral key exchange mechanisms, such as Diffie-Hellman, which are designed to safeguard sessions against subsequent compromises.

Furthermore, TLS 1.3 discards several cryptographic methods that were deemed outdated and susceptible to vulnerabilities in earlier versions. Specifically, it moves away from RSA key transport and CBC mode ciphers, opting instead for AEAD (Authenticated Encryption with Associated Data) ciphers. AEAD ciphers are favored for their ability to provide both encryption and integrity verification in a single framework. These modifications collectively enhance the security and efficiency of TLS 1.3, making it a robust protocol for securing transport layer communications[8].

18. 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.

    Solution: Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are designed to render a network service inaccessible to its legitimate users by flooding the service with unnecessary requests. Below are two prevalent strategies employed in these types of attacks:

    (a) SYN Flood Attack A SYN Flood attack takes advantage of the TCP handshake mechanism by inundating a target's port with a deluge of TCP/SYN packets, frequently using a falsified source IP address, aiming to swamp the target with connection attempts. In trying to finalize the handshake, the server allocates resources for each incoming request, leading to the exhaustion of all available resources and subsequently blocking access to genuine users.

    Example: David Moore, Geoffrey M. Voelker, and Stefan Savage, which appeared in the Transactions on Computer Systems[6]. This research provides insights into the nature and impact of DoS attacks, including SYN Floods, by analyzing three weeks of network traffic directed towards the University of California, San Diego (UCSD) network.

    Mitigation Approaches: To mitigate SYN Flood attacks, techniques such as SYN cookies can be employed, which eliminate the need for the server to allocate resources in the initial phase of the TCP handshake without a successful completion. Additionally, setting up rate limiting for incoming connection requests and using intrusion detection systems to identify and block malicious traffic are effective strategies.

    (b) Amplification Attack Amplification attacks involve the attacker sending small query requests to a reflector (typically servers with large amounts of bandwidth) with the source IP spoofed to that of the victim. The server then sends a large reply to the victim's IP address. When multiple reflectors are used, this can generate a significant amount of traffic directed towards the victim, resulting in a DDoS.

    Example: A notorious example of an amplification attack is the DNS amplification attack against the Dyn DNS service in October 2016, which caused major internet platforms and services to be unavailable. This event examines the mechanics of the attack and its impact on internet infrastructure[7].

Mitigation Approaches: Mitigating amplification attacks involves preventing the spoofing of IP addresses through ingress filtering (BCP 38), reducing the number of publicly accessible amplification reflectors, and implementing rate limiting on response sizes for services that can be exploited as reflectors. Additionally, deploying DDoS protection services that can absorb and filter out attack traffic before it reaches the target can be effective.

19. 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.]

    Solution: To combat a Man-in-the-Middle (MitM) attack during the setup of a secure communication channel between Alice and Bob, a combination of cryptographic methods and protocols is employed. These measures are designed to verify the authenticity and maintain the integrity of their exchange. Key steps typically include:

    (a) In Public Key Infrastructure and Certificates, Alice and Bob each acquire digital certificates from a trusted Certificate Authority. These digital certificates include the public key of the holder and are digitally signed by the CA, certifying their authenticity.

    (b) Secure Channel Establishment:

    i. Step 1: Alice and Bob exchange their digital certificates.

    ii. Step 2: Upon receiving the certificate, both Alice and Bob verify the signature on the certificate using the CA's public key, which they already trust. This step ensures that the public key they received truly belongs to the other party and not to an attacker.

    iii. Step 3: After verifying the certificates, Alice and Bob extract the public key of the other party from the certificate.

    (c) Key Exchange:

    i. Alice creates a symmetric session key for their communication, encrypts this key with Bob's public key, and then sends it to Bob.

    ii. Bob receives the encrypted session key and decrypts it using his private key, enabling both Alice and Bob to share a secret symmetric key.

    (d) Secure Communication:

    i. All subsequent communications are encrypted using the symmetric session key. This ensures confidentiality.

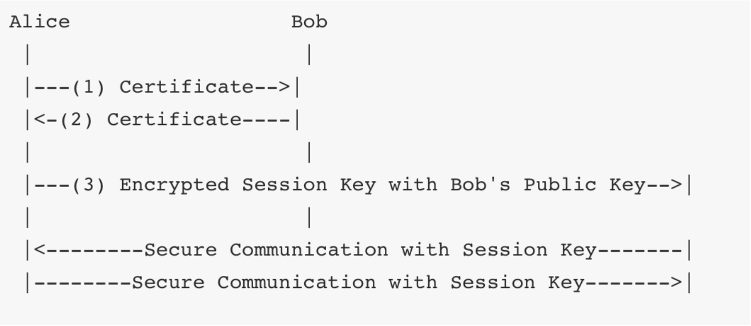
    ii. Each message is hashed, and then the hash is encrypted (forming a digital signature) using the sender's private key. The receiver can then decrypt the hash using the sender's public key and compare it to the hash of the message they received, thereby verifying both its integrity and authenticity.

    (e) Mitigation of MitM:

    i. By verifying the digital certificates against a trusted CA, Alice and Bob can be assured of each other's identities, defeating impersonation attempts by a MitM attacker.

    ii. Employing asymmetric encryption to exchange the symmetric session key guarantees that only the intended recipient can decrypt and retrieve the session key.

iii. The symmetric key ensures a secure and efficient communication channel, while the use of hashes and digital signatures ensures integrity and non-repudiation.



```
Alice                  Bob
 |                      |
 |---(1) Certificate-->|
 |<-(2) Certificate----|
 |                      |
 |---(3) Encrypted Session Key with Bob's Public Key-->|
 |                      |
 |<--------Secure Communication with Session Key-------|
 |--------Secure Communication with Session Key------->|
```

(1) & (2) means exchange of digital certificates; (3) means Alice sends the encrypted session key to Bob.

References

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 0008 ed. Pearson, 2020.

[2] M. Hell et al., ‘Grain-128AEADv2 - A lightweight AEAD stream cipher’.

[3] D. Engels, M.-J. O. Saarinen, P. Schweitzer, and E. M. Smith, ‘The Hummingbird-2 Lightweight Authenticated Encryption Algorithm’. 2011. Accessed: Mar. 01, 2024. [Online]. Available: https://eprint.iacr.org/2011/126

[4] F. Denis, F. E. R. Scotoni, and S. Lucas, ‘The AEGIS family of authenticated encryption algorithms’, Internet Engineering Task Force, Internet Draft draft-denis-aegis-aead-02. Accessed: Mar. 01, 2024. [Online]. Available: https://datatracker.ietf.org/doc/draft-denis-aegis-aead-02

[5] E. Rescorla, ‘The Transport Layer Security (TLS) Protocol Version 1.3’, Internet Engineering Task Force, Request for Comments RFC 8446, Aug. 2018. doi: 10.17487/RFC8446.

[6] D. Moore, G. M. Voelker, and S. Savage, ‘Inferring Internet Denial-of-Service Activity’.

[7] Y. Cao, Y. Gao, R. Tan, Q. Han, and Z. Liu, ‘Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives’, IEEE Access, vol. 6, pp. 66641–66648, 2018, doi: 10.1109/ACCESS.2018.2877710.

[8] ‘A Detailed Look at RFC 8446 (a.k.a. TLS 1.3)’, The Cloudflare Blog. Accessed: Mar. 01, 2024. [Online]. Available: https://blog.cloudflare.com/rfc-8446-aka-tls-1-3

[9] A. S. Tanenbaum, N. Feamster, and D. Wetherall, Computer networks, Sixth edition, Global edition. Harlow, United Kingdom: Pearson, 2021.