For each multiple-choice question and each answer choice, write 3-5 sentences explaining why that answer choice either is, or is not, correct

Question 1- to 15 (each is 5 points):

Q1: Answer (A or B or C or D or E): B

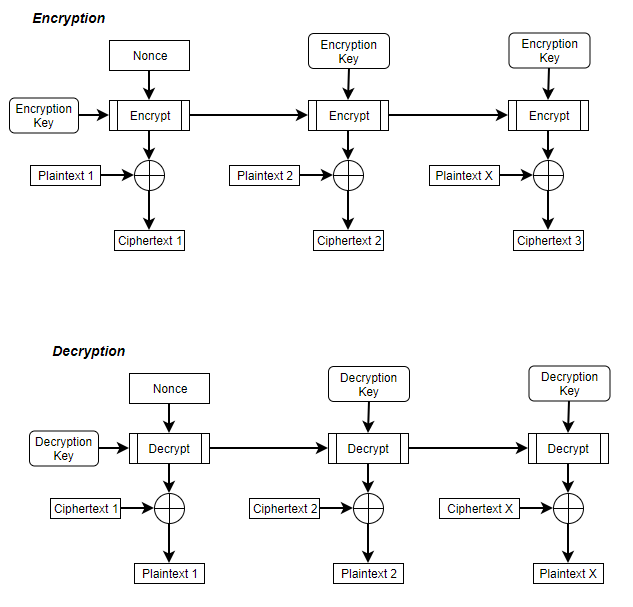
Explain Other Choices:

In cryptography, a cipher is an algorithm for performing encryption and decryption. An encrypted message in the output of a cipher, not the cipher itself. A zero is simply a binary bitwise value used to create the ciphertext output. However, a zero was also used interchangeably with the work cipher in medieval times. A code can mean a variety of things in cryptography. The code can be the ciphertext created by a cipher. Outside of the world of technical cryptography, one will often hear the term code used as a synonym for cipher.

Q2: Answer (A or B or C or D or E): B

In Q2, the diagram is to help you explain the operation. The diagrams are already in the online videos.

After drawing the diagram, you add the sentences that explain the mode itself



Output feedback mode converts block cipher concepts into a stream cipher. For encryption, OFB is initialized using a nonce (a random number used once). The first block of plaintext is XORed to produce the first unit of ciphertext which is then transmitted. The output of the encryption function is fed back to become the input for encrypting the next block. This process continues until all blocks of plaintext have been encrypted. The decryption process works the same way in reverse. Blocks of ciphertext are translated to plaintext.

Q2 Resource:

Figure 6.6, course textbook

Q3: Answer (A or B or C or D or E): B

Explain Other Choices:

The foundation of internet security is trust. Specifically, establishing mutual trust being parties exchanging information is the foundation of internet security. Cryptography encryption, decryption, authentication, public key certificates and digital signatures are techniques and algorithms designed to establish mutual trust between parties.

Q4: Answer (A or B or C or D or E): D

Explain Other Choices:

All choices are plausible definitions of general security. A more cybersecurity specific definition is security is the measures taken to protect a computer, computer systems and information from unauthorized access or attack.

Q5: Answer (A or B or C or D or E): D

Explain Other Choices:

Decryption can be parallel in counter mode, cypher block chaining mode and electronic codebook mode. Decryption in Counter Mode can be performed in parallel. There is no chaining of ciphertext blocks in counter mode. Encryption in counter mode uses a nonce to which is included in the ciphertext. This value is incremented for each block. During counter mode decryption, the initial counter value is made available, and the same sequence of counter values are used for each ciphertext block. Decryption in ECB mode operates by decrypting each block separately. As with counter mode, output from decrypting the prior block is not required to decrypt the next. While cipher block chaining encryption of blocks cannot be parallel. Decryption in CBC mode can be parallel. In CBC mode, each block is XORed with the ciphertext of the previous block. So, CBC decryption does not depend on decryption of previous blocks before decrypting the next.

Q6: Answer (A or B or C or D or E): D

Explain Other Choices:

Preimage resistance, second preimage resistance and collision resistance are all properties of a secure hash function. Preimage resistance is the one-way property. Under preimage resistance it is easy to generate a secure hash code from a message, but almost impossible to generate a message from a hash code. Second preimage resistance makes it impossible to find an alternative message with the same secure hash code. A collision resistant secure hash code protects against an attack in which one party generates a message for another party to sign. Other properties of a secure hash function are variable input size, fixed output size and efficiency.

Specifically, choice D, all of the above, was selected due to the cumulative nature of the requirements of a secure hash function. A collision resistant hash function is naturally second preimage resistant. However, a collision resistant hash function is not necessarily preimage resistant. And, a second preimage resistant hash function is not necessarily preimage resistant or collision resistant. Additionally, the properties of fixed output size and efficient calculation must be satisfied as well. Thus, all of the above is the best answer to this question.

Q6 Resources

pp. 323 – 324 in course textbook

Q7: Answer (A or B or C or D or E): A

Explain Other Choices:

A hacker best describes someone who gains illegal access to a computer system. An identity thief may or may not use computer resources to impersonate someone. An intruder doesn’t necessarily have to gain illegal access to a computer system. An intruder could be someone with computer system access to uses these privileges for illegal purposes. A cyber-terrorist doesn’t have to gain illegal access to a computer system to engage in this type of behavior.

Q8: Answer (A or B or C or D or E): D

Explain Other Choices:

E-mail privacy, software piracy, intellectual right and copyrights are all ethical issues facing the use of technology in business today. A reasonable level of e-mail privacy is expected in both the business and personal world. Personal email providers such as Google are obligated to not turn over or sell personal email details to third parties without obtaining permission from the user or being provided some sort of government order. While businesses often make it clear that emails sent from a work address are property of the company, there is also an expectation the company is not snooping on employee emails or providing a boss access to an employee’s emails. Software piracy is a common issue faced by software users. Using a “cracked” version of a pay version of software, while seemingly harmless, is essentially stealing from the software vendor. Intellectual rights and copyrights protect the original work of the authors, artists, inventors, etc. As with software piracy, using someone else’s work without obtaining permission or paying for access is theft.

Q9: Answer (A or B or C or D or E): A

Explain Other Choices:

Scalability is a desired characteristic of a PRNG. In terms of a PRNG, scalability is a property of the randomness requirement. It states any test applicable to a sequence can also be applied to subsequences extracted at random.

Backward predictability is the opposite of a desired characteristic of a PRNG. Backward unpredictability is a desired characteristic. Backward unpredictability assures it is not practical to determine the seed from the generated values. Similarly, a shared initialization vector is not a desired characteristic of a PRNG. A true random IV is preferred for a PRNG.

Q9 Resource

pp 207 – 208 in course text.

Q10: Answer (A or B or C or D or E): A

Explain:

One of the benefits of the hash function is protecting message integrity. A strong, collision resistant hash function efficiently computes a fixed-length code that is unlikely to match the hash key of a different message calculated by the same hash function. Assuming the hash function is secretly shared between the sender and receiver, a message is sent with a hash code the receiver of the hash code can run the same function a verify the hash code calculated by the receiver to the hash code provided by the sender. If the hash codes match, the message has not been altered. Private key operation and symmetric key models provide a level of confidentiality. However, these key sharing methods do directly address data integrity.

Q10 Resources

Asynchronous Videos 7.3

pp. 260, 323-324 course textbook

Q11: Answer (A or B or C or D or E): C

Explain:

Using a key with a larger number of bits an approach to strengthen a cipher. Larger encryption keys can make it more difficult to crack the key through computational and brute-force attacks. Keeping a key secret is great, and it is important for basic security. However, this does nothing to increase the strength of the cipher. Similarly, keeping a cipher’s encryption / decryption algorithms secret is a great idea to preserve the integrity of the cipher. However, the actual strength of the cipher is unchanged by secrecy.

Q12: Answer (A or B or C or D or E): C

Explain:

There are three critical aspects of block cipher design. The number of rounds, design of the function F and key scheduling. Using one or two more rounds than the minimum to achieve randomness is an ambiguous and erroneous guideline. The number of rounds should be chosen so that known crypto-analytic efforts require greater effort than a simple brute-force attack. Additionally, the sensitivity of the information being protected by the cipher should be a consideration as well. Sensitive information could dictate that even more rounds be added. The design of the function F should use non-linear functions not “both linear and non-linear functions”. Non-linear functions increase the difficulty of using crypto-analysis to crack the cipher. Good avalanche properties are a critical aspect of the design of the function F. Avalanche criterion suggests that a change in a single bit should result in a change of several bits.

Q13: Answer (A or B or C or D or E): D

Explain:

Authenticated encryption is an encryption system that simultaneously protects confidentiality and authenticity of communications.

Grain 128-A

<http://skew2011.mat.dtu.dk/proceedings/A%20New%20Version%20of%20Grain-128%20with%20Authentication.pdf>

Grain 128-A is a stream cipher which builds upon the original Grain-128 with support for authentication as well as fortification against newer known attacks.

Hummingbird 2

<https://eprint.iacr.org/2011/126.pdf>

Hummingbird2 is an authenticated encryption algorithm with a 128-bit key. Hummingbird2 is designed for resource constrained micro-devices such as RFID tags.

Keyak

<https://arxiv.org/ftp/arxiv/papers/1510/1510.02856.pdf>

<https://conorpp.com/keyak-a-candidate-for-the-authenticated-encryption-standard>

Keyak is a permutation-based authenticated encryption algorithm based on Keccak functions.

Q14: Answer (A or B or C or D or E): E

Explain:

All of the above are true in this question. In public key cryptography, each participant creates a pair of keys. One key is placed in a public register. The other key is kept private. If George sends Amber a confidential message using the public key encryption model, George encrypts the message using Amber’s public key. Amber would then decrypt the message using her private key. This assures confidentiality as long as Amber keeps her key secret.

Option A in the question states the public key encrypts only and must take plaintext. Option B states the private key is used only for decryption and must take ciphertext as input. These may be good practices, but it is not mandatory. The only requirement in public key encryption is one key is used to encrypt and the other key is used to decrypt. Option C states the cipher is not secure if the public key is kept secret and the private key is made public. The terms public key and private key are semantics. Public key encryption states only one of the two keys must be secret for the cipher to be considered secure.

Q14 Resource

pp. 257 – 259, course textbook

Q15: Answer (A or B or C or D or E): B

Explain:

The assumption for all attack scenarios below is the attacker does not know the secret key used to calculate the MAC. Message authentication code modification is altering the MAC appended to the message. If the attacker somehow alters the MAC appended to the message by the sender, the MAC calculated by the receiver will not match the altered MAC. This would indicate the MAC has been tampered with. Message modification is changing the contents of a transmission. If the attacker modifies the message, the receiver’s calculation of the MAC value will not match the MAC appended to the message by the sender. This would indicate the message has been altered. Option C has to do with source repudiation. Source repudiation is the denial of transmission of message by source. The question asks us to show how MAC “mitigates” attacks. MAC does not offer ironclad source repudiation protection. A digital signature would help accomplish this objective. This leaves us with two potential answers: A and B. B is the best choice as the intent of the MAC is message authentication.

Q15 Resources

Ch. 12, course textbook

pp. 357, 362 – 363,

<https://www.tutorialspoint.com/cryptography/message_authentication.htm>

Q16 (6 points)

In a room of twenty-three people, there is a 50% chance of two people having the same birthday. This is the classic example of the birthday paradox. This is a seemingly low number. Intuitively, one many think it would take approximately 365/2 people before there would be a 50% chance two people in the room would have the same birthday. This may be true if the question was how many people need to be in a room to assure there is a 50% chance a single person has the same birthday as someone else in the room. This ignores the exponential reality of the comparisons between all 23 people in that one room.

When extrapolated to the security of a computer system, the concept of collision resistance in cryptographic hash functions emerges. One of the requirements for a strong hash function is collision resistance. In collision resistance, it is computationally infeasible to find a scenario where two hash functions are the same. If we apply the birthday paradox to collision resistant hash functions, the level of effort required to find a collision is lower than we may expect.

The following table shows the number (k) of hash codes required to achieve a 50% probability two hash codes are the same for each bit size (m). k = 2(m-1)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 16 bit | 32 bit | 64 bit | 128 bit | 256 bit | 512 bit |
| k | 32,768 | 2,147,483,648 | 9.2233 e+18 | 1.7014 e+38 | 5.7896 e+76 | 6.7039 e+153 |

Q16 Resources

pp. 325 – 326, course textbook

<https://betterexplained.com/articles/understanding-the-birthday-paradox/>

<http://www.solipsys.co.uk/new/TheBirthdayParadox.html>

<http://gvpcse.helplena.co/pdf/Cryptography_and_Network_Security_Principles_and_Practice_5thEdition.pdf>

Q17 (7 points)

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.

|  |  |  |
| --- | --- | --- |
| Layer | Layer Name | Security Protocol |
| 5 | Application | ALPN |
| 4 | Transport | TLS |
| 3 | Network | PANA |
| 2 | Data Link | PAP |
| 1 | Physical | 802.11x |

The application layer is the top layer of the layered network model. User facing software applications interact directly with this layer. HTTP is one of the most commonly used protocols used within this layer. Application Layer Protocol Negotiation (ALPN) allows the application layer to negotiate which protocol will be used in the transport layer.

The transport layer security protocol provides communication security over the internet. It is designed to prevent eavesdropping, tampering or forgery. TLS is a robust protocol utilizing message authentication codes, record payload protection, handshake protocols, certificates, key exchanges and cryptographic computations to secure data in the transport layer. TLS utilizes HMAC and pseudorandom functions to protect message integrity. Handshake protocols used by TLS allow peers to agree on security parameters for authentication and error reporting. Parameters determined by the handshake protocol include, but are not limited to: session identifiers, peer certificates, method of compression, ciphers, signature algorithms, certificate requests, various status and state messages and a shared secret key. Cryptographic computations used are required to be specified for TLS. The cipher suite selected during the handshake protocol agreement is utilized to initiate information protection computations.

The protocol for carrying authentication for network access (PANA) exists at the network layer and allows a device to authenticate with a network. PANA allows for authentication and authorization. PANA handles authentication of the PANA client seeking authentication. The identity of the PANA client is supplied by a user of the client or the client device itself. PANA only authenticates the client device. User authentication is outside of the purview of PANA. After the client is authenticated, PANA verifies the authorization of the client to access the network.

The point-to-point protocol (PPP) is a communication protocol of the data link layer. The password authentication protocol (PAP) is used to provide a simple method to establish the identity of a peer device. After the data link is established, an id and password are sent to an authenticator until authentication is established.

The IEEE’s 802.11 standard includes a set of protocols and physical layer specifications for implementing wireless communications. 802.11 protocols provide for authentication and link security. From an authentication perspective, 802.11 provides several methods of authentication before granting access to a point on the network. These methods can range from simple open authentication to more secure methods such as WPA and cryptographic exchanges to establish a trusted authentication between workstations and network access points.

Q17 Resources

<https://www.sans.org/reading-room/whitepapers/protocols/understanding-security-osi-model-377>

<http://microchipdeveloper.com/tcpip:tcp-ip-five-layer-model>

<https://tools.ietf.org/rfc/rfc7301.txt> - ALPN

<https://tools.ietf.org/html/rfc5246#section-11> - TLS

<https://tools.ietf.org/html/rfc4058#section-5> – PANA

<https://tools.ietf.org/html/rfc4016> - PANA

<https://en.wikipedia.org/wiki/Protocol_for_Carrying_Authentication_for_Network_Access> - PANA

<https://www.ietf.org/rfc/rfc1334.txt> - PPP, PAP, CHAP

<http://www.ccs-labs.org/~dressler/teaching/netzwerksicherheit-ws0607/10_LinkLayerSecurity.pdf> – PPP, PAP, CHAP

<https://tools.ietf.org/html/rfc5418#section-3> – 802.11, CAPWAP

<https://en.wikipedia.org/wiki/IEEE_802.11#Security> – 802.11

Q18 (6 points)

A denial of service (DoS) attack interferes with the normal use or management of communication paths. This type of attack could target an individual destination or an entire network. The United States Computer Emergency Team (US-CERT) has published guidelines to help determine when a denial of service attack may be taking place: degradation of network performance, unable to reach a particular website, inability to access any website when there are no known network or hardware issues and higher than normal volumes of network traffic. This question will describe two recent denial of service attacks and potential strategies to mitigate these attacks.

On New Year’s Eve 2015, the British Broadcasting Company (BBC) and Donald Trump’s campaign website where both hit with a distributed denial of service (DDoS) attack. A distributed denial of service attack involves multiple connected devices overwhelming a target network or website with bogus traffic. During the attack on the BBC, the perpetrators of this attack (New World Hacking) claimed the DDoS attack peaked at 602Gbps. This disabled the BBC’s website for several hours. One interesting find from this attack is New World Hacking created this attack from cloud-based servers in the Amazon cloud. New World Hacking used stolen credit card information to pay for these cloud-based servers.

Over the past month of 2018, there has been a new type of DDoS attack being used to target networks and websites with incredible amounts of traffic. GitHub’s website was taken down for about 10 minutes as the result of a DDoS attack. The GitHub attack reached an estimated 1.3Tbps. Even a DDoS protection company, Arbor Networks, survived a massive DDoS attack where the traffic peaked at an incredible estimate of 1.7Tbps. These two attacks appeared to have something in common. They utilized Memcached servers to amplify traffic by a factor of 50,000. A Memcached server attempts to optimize websites which rely on external databases. Although Memcached servers should not be openly exposed on the internet, a large number are left exposed. The Memcached based attack involves faking a target IP address to the default UDP port on exposed Memcached amplifiers. This returns very large responses to the target IP address.

There are some recommended approaches to help mitigate a DoS attack. One approach is to have a backup internet service provider (ISP) available. During a DoS attack, the target of the attack could potentially lessen the impact of the attack by routing traffic through the backup ISP. This approach doesn’t prevent the attack, but it does allow the target of the attack to resume operations relatively quickly while working to stop the ongoing DoS attack against the primary ISP. After the DoS attack has been suppressed, traffic can be switched back to the primary ISP. Second, cloud based third party service parties (such as Arbor Networks) offer anti-DoS services. Having an established service contract with a company dedicated to fighting DoS attacks can help severely limit the impact of a DoS attack. As evidenced in the recent attack against Arbor Networks, they were able to survive a record DDoS attack. This demonstrates their capabilities in providing anti-DoS services to companies whose area of expertise is not combatting DoS attacks. Finally, a DoS response plan should be in place. The response plan outlines the steps to take when a DoS attack is underway. This helps produce a coordinated effort to efficiently mitigate and stop the DoS attack.

Q18 Resources

p. 39, course textbook

<http://searchsecurity.techtarget.com/definition/denial-of-service>

<https://www.csoonline.com/article/3020292/cyber-attacks-espionage/ddos-attack-on-bbc-may-have-been-biggest-in-history.html>

<https://www.csoonline.com/article/2133613/network-security/malware-cybercrime-ddos-protection-mitigation-and-defense-7-essential-tips.html>

<https://www.incapsula.com/ddos/denial-of-service.html>

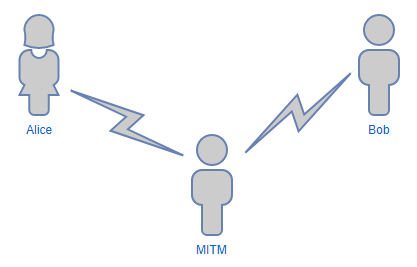
<https://www.forbes.com/sites/leemathews/2018/03/07/a-frightening-new-kind-of-ddos-attack-is-breaking-records/#49f6a20078e0>

<http://www.zdnet.com/article/new-world-record-ddos-attack-hits-1-7tbps-days-after-landmark-github-outage/>

Q19 (6 points)

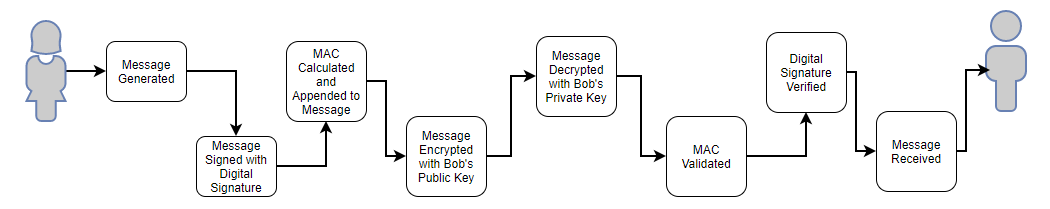
A Man-In-The-Middle (MITM) attack occurs when the intruder secretly intercepts, transmits and possibly changes the communications between a sender and receiver. The MITM could simply eavesdrop on communications and collect sensitive information. The MITM could also insert their own messages to achieve some desired outcome that is advantageous for the MITM.

Basic MITM attack



Guard Against MITM Attack

The following model should protect against a MITM attack:



Public and Private key encryption:

In the communication between Alice and Bob, Alice and Bob make public encryption keys available while keep their private keys secret. When Alice sends a message to Bob, she encrypts the message with Bob’s public key. Bob then decrypts the message with his private key. As long as the private keys are kept secret, confidentiality of the message is assured.

Message Authentication Code:

Alice and Bob share a secret MAC. Alice calculates the MAC value which is appended to the message to be encrypted with Bob’s public key. When Bob receives and decrypts the message, Bob calculates the MAC value to verify the MAC value appended to the message by Alice matches his calculated value. This assures Bob the message has not been altered.

Digital Signature:

Adding a digital signature provides a level of assurance message of the originator of the message. As opposed to Public key encryption and MAC, digital signature calculation is not shared. The digital signature is unique to the sender, can be verified by the receiver and cannot realistically be forged.

A secure communication channel robust to MITM attacks include a form of endpoint authentication to prevent the MITM attack. Public – private key certificates, MAC, digital signatures.

Q19 Resources

pp. 290 – 291, 318 – 319, 362 – 368, 395 – 398 course textbook

<http://www.ccdcoe.org/cycon/2014/proceedings/d2r2s2_delahoz.pdf>

<https://en.wikipedia.org/wiki/Man-in-the-middle_attack>