Your Name: Nicole Wittlin

Q1: **Answer B.**

*A cryptographic system or cipher is a scheme or algorithm used for encryption, per our online videos and the Stallings textbook. The cipher is what converts the “plaintext” original message to a coded message, or “ciphertext.” Dr. Engels noted in the videos that there are more than 160 ciphers now available, but that is probably an underestimate. However, most ciphers have been or can be easily broken.*

Explain Other Choices:

*Each of the other answers is related to the cipher, but none are the actual cipher itself as defined above. Choice A. An encrypted message is the output of the cipher, also known as the ciphertext. Choice C. A zero could be part of the ciphertext, if for example, the cipher converts the plaintext into binary 1 and 0 values or another scheme where letters are replaced by numbers. Lastly, Choice D. A code could be used to describe a cipher, particularly by people not familiar with cryptography. As the Stallings text notes (p. 28): “Cryptanalysis is what the layperson calls ‘breaking the code.’” Thus, a cipher could be a code, but I think the strongest answer is B.*

Q2: **Answer D.**

*All three modes of operation create a keystream to be XORed with the plaintext for encryption as explained below. Note, all the encryption and decryption functions below utilize a key, even if not noted in the drawings.*

|  |  |
| --- | --- |
| **Counter Mode (CTR)** | |
| In CTR mode, each block of plaintext is XORed with the Initialization Vector, or encrypted counter; the counter incremented for each subsequent block (i.e. IV + 1). The encryption of blocks can take place in parallel because each process stands alone. Because the input of each process is different, the key stream changes each time. | |
| Encryption | Decryption |
|  |  |

|  |  |
| --- | --- |
| **Output Feedback Mode (OFB)** | |
| In OFB (similar to CFB), the output of the encryption is fed back as the input of the encryption for the next block. The plaintext has no impact on the key stream or value of the ciphertext; however, the ciphertext is created from the XOR of encrypted Initialization Vector (IV) and plaintext. This mode operates on full blocks and is similar in structure to a typical stream cipher. | |
| Encryption | Decryption |
|  |  |

|  |  |
| --- | --- |
| **Stream Mode** | |
| In stream mode, the encryption takes place when the key stream is XORed with the plaintext in order to generate the ciphertext. The three modes that make it possible to convert a block cipher to a stream cipher are: CFB, OFB, and CTR. | |
| Encryption | Decryption |
|  |  |

*Reference: Unit 4 online videos, Chapter 6 of the Stallings text, and class discussion.*

Q3: **Answer B.**

*Trust is the foundation of all security on the Internet, as stated in both Week 1 videos by Dr. Engels and in our week 1 lecture with Dr. Meky (see slide 31). As part of an organization’s security goals and objectives, it must take into account the hardware, software, networks, data, people, and policies that compose the organization when implementing technical mechanisms to create and achieve a trusted cyberspace environment. Five key aspects include: data confidentiality, data integrity, availability, authenticity, and accountability.*

Explain Other Choices:

*Each of the other answers plays a role in good cyber security, depending on the goals and objectives desired.*

*Choice A. Cryptography Encryption and Decryption helps with both data confidentiality and data integrity, depending on the systems used. Choice C. Authentication is related to the key aspects noted above – authenticity – and proves the identity of the claimed user is valid or that the claimed source of data is valid. Authentication and Choice E. Digital Signatures help achieve authenticity. Digital Signatures also support accountability by demonstrating proof of data origin and proof of data delivery. Lastly, Choice D. Public Key Certificates are a part of asymmetric encryption and indicate that the subscriber identified in the certificate has sole control and access to the corresponding private key (Stallings, Chapter 9, pg. 255). The use of a Certification Authority binds together a private key and a public key of a confirmed specific user.*

Q4: **Answer D.**

*I believe that all of these can be considered part of security. As Dr. Engels noted in the week 1 videos, security as defined by Merriam Webster, can be any of the following: freedom from risk or danger; safety; freedom from doubt, anxiety, or fear; confidence; or something that gives or assures safety. To me, Choices A through C all relate to the points above.*

Explain Other Choices:

*However, these do not necessarily capture the definition of “cyber security,” which Merriam Webster defines as measures taken to protect a computer or computer system from unauthorized access or attack.*

Q5: **Answer D.**

*All three modes of operation allow for decryption in parallel as described below. Note: all of the encryption/decryption functions utilize a key, even if not noted in the drawings below.*

|  |  |
| --- | --- |
| **Counter Mode (CTR)** | |
| In CTR mode, each block of plaintext is XORed with encrypted counter; the counter incremented for each subsequent block (i.e. IV + 1). The encryption of blocks can take place in parallel because each process stands alone. The decryption process uses the same Initialization Vector (IV) and the encryption algorithm; the output is XORed with the ciphertext to create the plaintext. | |
| Encryption | Decryption |
|  |  |

|  |  |
| --- | --- |
| **Cipher Block Chaining Mode (CBC)** | |
| In CBC mode, the input to the encryption requires an Initialization Vector XORed with the plaintext in round 1; subsequent encryption processes use the encrypted output XORed with the next block of plaintext. For decryption, each process requires the ciphertext and the key, so the processes can be done in parallel. The decryption of the dependencies happens after the decryption function, as illustrated in the drawing on the right. | |
| Encryption | Decryption |
|  |  |

|  |  |
| --- | --- |
| **Electronic Code Book (ECB)** | |
| In ECB, each block of plaintext is encoded independently using the same key; thus, the decryption of the ciphertext would follow a similar process using the same key and decryption algorithm. This is the simplest mode of operation and is best used for small amount of data. | |
| Encryption | Decryption |
|  |  |

*Reference: Unit 4 online videos, Chapter 6 of the Stallings text, and class discussion.*

Q6: **Answer D.**

*There are 7 requirements for a cryptographic hash function, as defined on pg. 323 of the Stallings textbook: variable input size, fixed output size, efficiency, Preimage resistant, Second Preimage resistant, Collision resistant, and Pseudorandomness. The first three are necessary for the practical application of a hash function. When number 4 and 5 – Preimage resistant and Second Preimage resistant – are met, the hash function is considered a “weak hash function.” For a hash function to be considered strong, the sixth requirement must also be met: Collision resistant. Therefore, for a hash to be secure, the answer is D. All the above. (Note, requirement 7 – pseudorandomness – is has not been listed as a true requirement but is implied.*

Explain Other Choices:

*Definitions of note, from pg. 323-324 in Stallings text:*

* *Preimage resistant – a one-way property that allows for the generation of a code for a given message, but it is virtually impossible to generate a message from the given code.*
* *Second preimage resistant – guarantees that it is impossible to find an alternative message with the same hash value as a given message.*
* *Collision resistant – it is computationally infeasible to find any pair (x, y) such that the hash function output of x is equal to the hash function output of y.*

Q7: **Answer A.**

*I believe the best answer describing someone that gains illegal access to a computer system is a hacker. While the other choices may involve hackers, at the most basic level, a hacker is trying to access a system for some gain (personal, financial, predatory, etc.). The activity of hacking is solely online and does not have an offline equivalent, which is important when considering the other choices.*

Explain Other Choices:

*Choice B. Identity Thief and Choice C. Intruder both existed before Internet technology became a prevalent part of our lives. Identity theft now most notably involves stealing a person’s identity online; however, it is not solely an online crime. Therefore, this is not necessarily the best description for someone who gains illegal access to a computer system. Likewise, an intruder is someone that “enters a building, grounds, etc., without permission” (from the Collins English Dictionary:* [*https://www.thefreedictionary.com/intruder*](https://www.thefreedictionary.com/intruder)*). An intruder can infiltrate online computer systems, but in my opinion, the more common interpretation is in the offline space. Additionally, two researchers, Asmaa Shaker Ashoor and Prof. Sharad Gore, attempted to differentiate between hackers and intruders in the paper “What is the difference between Hackers and Intruders.” (citation:* [*https://www.ijser.org/researchpaper/What\_is\_the\_difference\_between\_Hackers\_and\_Intruders.pdf*](https://www.ijser.org/researchpaper/What_is_the_difference_between_Hackers_and_Intruders.pdf)*). My interpretation of their writing leads me to conclude that an intruder is more opportunistic, taking advantage of found vulnerabilities, where a hacker has true malicious intent. Finally, Choice D. Cyber-terrorist/cyberterrorism is defined, on Wikipedia, as “the use of the Internet to conduct violent acts that result in, or threaten, loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation” (citation:* [*https://en.wikipedia.org/wiki/Cyberterrorism*](https://en.wikipedia.org/wiki/Cyberterrorism)*). While hackers may be involved in cyberterrorism, the stated goals of political or ideological gains go far beyond someone that gains unauthorized access to a computer system.*

Q8: **Answer D.**

*I believe that all three choices present some ethical issues for businesses’ use of technology today. Choice A. Email privacy could apply to both internal and external scenarios. Internally, a company needs to decide how much oversight and monitoring of employee email is necessary. ACM Code of Ethics guideline 1.6 is respect privacy, so computing professionals need to establish policies and protocols that balance the needs and expectations of the company with an employee’s ability to be comfortable using email for various types of communication, particularly those sensitive in nature. Externally, a company needs to be certain that email communications are secure, especially if they have confidential or client information. Choice B. Software piracy and Choice C. Intellectual property rights and copyright present similar ethical issues, in that both scenarios violate the ACM Code of Ethics standards 1.5 to “respect the work required to produce new ideas, inventions, creative works, and computing artifacts” and 2.6 to “access computing and communication resources only when authorized or compelled by the public good.” It would be both unethical and a bad business practice to allow employees to use software that has not been properly acquired or purchased, as it is cheating another company. Similarly, businesses need to be knowledgeable about IP and copyright to also make sure proper credit is given (along with payment if necessary) to the correct parties.*

Explain Other Choices:

*Process of elimination rules out Choice E. None of the above.*

Q9: **Answer A.**

*The requirements of a pseudorandom number generator (PRNG) are: randomness, unpredictability, and the characteristics of the seed. Related to randomness, there are 3 characteristics of importance, as noted on pg. 207 of the Stallings text: uniformity,* ***scalability****, and consistency. Choice A. Scalability is defined as a test of randomness applied to a PRNG sequence – and the sequence is random – then any extracted subsequence from the PRNG would also be random. This is the best answer of the choices available.*

Explain Other Choices:

*Choice B. Backward Predictability is not the correct answer because within the unpredictability requirements for PRNGs, the characteristics are forward unpredictability (not a choice) and backward* ***UN****predictability (also not a choice). Choice C. A Shared Initialization Vector is not the correct choice because, while an initialization vector could used as a seed, it should not be shared. The seed that serves as input to the PRNG must be secure. Process of elimination removes Choices D and E.*

Q10: **Answer A.**

*The key phrase of this question is “which of the following is primarily used to provide integrity protection for a message.” Each of these can provide some integrity protection for message communication, but Choice A. Hash function is the option that is* ***primarily*** *used to do this. A hash function, whose main objective is data integrity, produces a fixed-length output from a message and creates a “hash” that is unique to the specific message. In practice, Alice will use a hash function to compute a hash value for a message and transmit both the hash and message to Bob. He will use the same hash function to create the hash value and then compare the two hashes. If they match, Bob can be confident that the message and the hash value were not altered in transit. However, it is important to keep the hash function secret and secure between Alice and Bob.*

Explain:

*The remaining two choices provide some integrity depending on the situation in which each is used. Choice B. Private key operation, also known as Public Key Encryption where one key – the private key – is secret to one person and the public key known by all, has some message integrity built in, depending on the order in which the private and public keys are used to encrypt the message. For authentication, Alice would need to use her private key to encrypt the message, and Bob would use her public key to decrypt. For Choice C. Symmetric key operation, the encryption using a shared private key between the sender and receiver provides some measure of authentication. In symmetric encryption, no other party has access to the key, so the receiver can be assured that the message only came from the sender with the key. However, a caveat to note here is that the assumption is that the decrypted plaintext is intelligible. If it is a binary file or digitized image or X-ray, message integrity is more difficult to prove. (This is also true for Public Key Encryption.) Process of elimination removes Choice D. All of the above and Choice E. None of the above.*

Q11: **Answer C.**

*Of the choices, C. Using a Key with Larger Number of Bits is the best option to increase the strength of a specific cipher. The longer the key, the stronger the encryption mechanism. The stronger the encryption mechanism, the longer it would take a brute-force attack to break the cipher (if at all depending on the algorithm). This has been discussed in class and in the online videos.*

Explain:

*Of the remaining answers, Choice A. Shared Secret Key is critical for private (symmetric) key encryption, and maintaining the secrecy of that shared key is what preserves the integrity of the encryption/decryption process. However, having a shared secret key alone does not necessarily strengthen the cipher. Similarly, Choice B. Keep Algorithm Details Secret does not necessarily strengthen the cipher either. As Dr. Engels noted in the Unit 3 videos, there are upwards of 160 ciphers, and most have been broken. While keeping the algorithm secret might delay breaking, it also limits the peer review and community testing process that could ultimately help strengthen a cipher. Similarly, the Stallings text on pg. 70 notes “although we would like to make our algorithm as difficult as possible to cryptanalyze, there is great benefit in making the algorithm easy to analyze. That is, if the algorithm can be concisely and clearly explained, it is easier to analyze that algorithm for cryptanalytic vulnerabilities and therefore develop a high level of assurance as to its strength.” Process of elimination removes Choice D. All of the above and Choice E. None of the above as correct answers.*

Q12: **Answer C.**

*In Unit 3 videos, Dr. Engels discussed the basic design principles of a block cipher: the number of rounds, the function F, and the key schedule algorithm. Related to the design of function F, he noted that the more non-linear an equation is, the harder the cryptanalysis will be. He also noted that the function should have good avalanche properties, where a small change in either the plaintext or key will result in a significant change in ciphertext. Thus, I selected C. Have good avalanche properties.*

Explain:

*In considering the answer options, I did not select Choice A. because linear functions were included and that would make the block cipher design less resistant to cryptanalysis. Also, as noted above, the number of rounds is important the design of a block cipher; however, Choice B. Use one or two more rounds than the minimum is not robust enough. On pg. 79 of the Stalling text, it says: “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.” To me, one or two more rounds may not be enough, so I did not select that choice. Finally, having ruled out Choices A and B, neither Choice D. All of the above or Choice E. None of the above made sense.*

Q13: **Answer D.**

*Each of the following is an authenticated encryption (AE) cipher, also known as an authenticated encryption with associated data (AEAD) cipher.*

*Grain 128-A*

*Grain 128-A is stream cipher that improved upon its predecessor Grain 128. Grain ciphers are notable for the small hardware footprint used (or stated another way, the throughput can be increased at the expense of additional hardware). The new version has two main parts: “pre-output function” and “MAC,” per Wikipedia. It also can work with or without authentication and uses different non-linear function to protect against known attacks. See article below for additional details and diagrams.*

<https://en.wikipedia.org/wiki/Grain_128a>

Ågren, M., Hell, M., Johansson, T., & Meier, W. (2011). Grain-128a: a new version of Grain-128 with optional authentication. International Journal of Wireless and Mobile Computing, 5(1), 48-59. Accessed via: <https://portal.research.lu.se/ws/files/3454246/2296485.pdf>

*Hummingbird 2*

*As noted in the article cited below, the Hummingbird-2 cipher is “an encryption algorithm with a 128-bit secret key and a 64-bit initialization vector. Hummingbird-2 optionally produces an authentication tag for each message processed.” Designed for use in RFID tags, wireless sensors, smart meters, and industrial controllers, it “can be implemented with very small hardware or software footprint.” Additionally, it displays properties of both traditional stream ciphers and block ciphers.*

Engels, D., Saarinen, M., Schweitzer, P., and Smith, E. “The Hummingbird-2 Lightweight Authenticated Encryption Algorithm.” Accessed via: <https://eprint.iacr.org/2011/126.pdf> (2011)

*Keyak*

*Per Team Keccak, Keyak is “an authentication encryption scheme based on Keccak-p. It takes as input a ‘secret and unique value’ (SUV), then some associated data (or metadata) that are authenticated but not encrypted and finally some plaintext.” The result is ciphertext and a tag, which authenticates both the metadata and plaintext. It also “supports the concept of session,” meaning messages can continue to be exchanged without needing to input the key or a new nonce.*

<https://keccak.team/keyak.html>

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

Q14: **Answer C.**

*The foundation of asymmetric encryption is the use of two keys, a public key and a private key, and the integrity of the process is based on keeping the private key secret. If the keys were switched, it would render the cipher insecure, especially when considering public key infrastructure (PKI) set up through a certificate authority. As noted in the Wikipedia article, “the security of the certification hierarchy must be considered when deploying public key systems. Some certificate authority … vouches for the identities assigned to specific private keys by producing a digital certificate … when a private key … is compromised, or accidently disclosed, then a ‘man-in-the-middle attack’ is possible, making any subordinate certificate wholly insecure.” In sum, it is best to not mix up or swap the keys, because it will make process vulnerable.*

Explain:

*I did not select Choice A. or B. relating to the use of public and private keys solely because each answer was limited by the word “only,” in my opinion. Generally, yes, a public key can be used to encrypt a message and does take plaintext as input; similarly, a private key can be used for decryption. However, variations on the encryption and decryption processes, notably when adding additional layers of authentication and signature may utilize the keys in different orders than the public key only encrypting and the private key only decrypting. Without the restriction of “only” in Choice A or B, I would have selected D. All of the above.*

*Reference: Stallings text pg. 359, class discussion, and* <https://en.wikipedia.org/wiki/Public-key_cryptography>

Q15: **Answer D.**

*The best answer is Choice D. All of the above; message authentication – either through the use of a message authentication code or a digital signature – can mitigate the types attacks noted.*

Explain:

*A secure message authentication code uses a secret key to generate a block of data that is appended to the message. This additional data is a “cryptographic checksum” or “Message Authentication Code (MAC).” Both the sender and the receiver share the secret key used to generate the code, and upon receipt, the receiver uses the key and message to generate the MAC. If the two are identical, the recipient can be confident that the neither the message nor the MAC has been altered in transit. Thus, mitigating against choice A. Message authentication code modification is achieved through the use of the MAC and the comparison process. Similarly, the use of the MAC can identify Choice B. Message modification, or if changes to the content of message have occurred (insertion, deletion, transposition, or modification) because the MAC is generated from the original message. Additional levels of confidentiality and authentication can be achieved depending on the order in which plaintext and MAC are encrypted and added to the original message. Lastly, Choice C. Source repudiation (a situation where the source denies that a message has been transmitted) can be mitigated through the use of a digital signature, “which is an authentication technique that also includes measures to counter repudiation by the source” (pg. 357 in Stallings text). While a digital signature is not specifically a MAC (because the sender and recipient share the same key), I opted to include the digital signature choice in this answer because it is part of the suite of techniques used for message authentication.*

Q16 (6 points)

*As Daniel Miessler clearly explains in the article referenced below, the Birthday Paradox states: to achieve a 50% chance that someone in a given group shares* ***your birthday****, there would need to be 253 people in the group. However, if the goal is to find* ***any two people*** *in the group with the same birthday, only 23 people are needed to achieve the 50% chance (or greater). The premise of the paradox depends on desired pairs.*

|  |  |  |
| --- | --- | --- |
| Number of bits | Possible Combinations | Attempts until 50% probability of Collision |
| 16 | 216 | 2(16/2) = 28 |
| 32 | 232 | 2(32/2) = 216 |
| 64 | 264 | 2(64/2) = 232 |
| 128 | 2128 | 2(128/2) = 264 |
| 256 | 2256 | 2(256/2) = 2128 |
| 512 | 2512 | 2(512/2) = 2256 |

*Mr. Miessler goes on to explain how this relates to information security and how the birthday paradox makes a brute force attack on a one-way hash easier. He states the birthday paradox “applies to finding collision in hashing algorithms because it’s* ***much*** *harder to find something that collides with a* given *hash than it is to find any two inputs that hash to the same value.” The Stallings text (pg. 325) goes into further detail about how an attack of this nature would happen and the mathematics behind it. First, a sender prepares a message, appends a hash code, and encrypts the package with the private key. Then, an attacker generates 2m/2 variations of the message and stores them with the hash generated for each. It has been mathematically derived that, for an m-bit hash value, data blocks with the same hash value can be found within √2m (square root of 2m) = 2m/2 attempts. Therefore, for each of the bit lengths given, the table below summarizes how many attempts would be needed until a 50% likelihood for a collision attack.*

[*https://danielmiessler.com/study/birthday\_attack/*](https://danielmiessler.com/study/birthday_attack/)

Q17

*In the TCP/IP Model (the 5-layer model), the layers are defined as follows. Additionally, each layer has defined protocols. In general, layers 1 – 3 focus on delivering and transporting data; layers 4 – 5 focus on application services. As discussed in live session 2 with Dr. Meky, definition of each layer and protocols include:*

|  |  |  |
| --- | --- | --- |
| *Layer* | *Layer Definition* | *Protocol Examples* |
| *Application Layer (5)* | *Provides network service to applications (i.e. email or file transfer); establishes agreement on procedures for error recovery and data integrity between systems.* | *SMTP, FTP, telnet*  *HTTP, DNS*  *https://fcit.usf.edu/network/chap2/chap2.htm* |
| *Transport Layer (4)* | *Establishes communication services between end systems; initiates, maintains, and terminates circuits between end systems; define error detection, recovery, and flow between end systems.* | *TCP and UDP*  *SPX https://fcit.usf.edu/network/chap2/chap2.htm* |
| *Network Layer (3)* | *Provides connectivity, path selection, addressing, routing between end systems.* | *IGRP (Internet Gateway Routing Protocol), RIP (Routing Information Protocol), BGP (Border Gateway Protocol), OSPF (Open Shortest Path First)*  *IP, IPX*  *https://fcit.usf.edu/network/chap2/chap2.htm* |
| *Data-Link Layer (2)* | *Data transfer across media; defines frame structures, delivery order, and access; defines network topology, physical system address, and methods to access transmission medium.* | *Link access protocols, Address Resolution protocols, Bonding protocols, Ethernet, IEEE 802/IEEE 802.11, Wi-Fi*  [*https://en.wikipedia.org/wiki/Category:Link\_protocols*](https://en.wikipedia.org/wiki/Category:Link_protocols)  *Utopia/Unrestricted Simplex Protocol, Simplex Stop-and-Wait Protocol, Simplex Protocol for Noisy Channel, One Bit Sliding Window Protocol, Pipelining*  [*https://web.cs.wpi.edu/~cs4514/b98/week3-dllprot/week3-dllprot.html*](https://web.cs.wpi.edu/~cs4514/b98/week3-dllprot/week3-dllprot.html) |
| *Physical Layer (1)* | *Defines electrical and mechanical specifications for physical link (cable) and end systems (routers, servers, workstations); defines voltage levels for bits, data rate, and timing of voltage change; defines maximum transmission distance and data rate.* | *Ethernet*  *https://fcit.usf.edu/network/chap2/chap2.htm* |

Q18

*The website Secure List has a comprehensive and detailed overview of the Denial of Service (DoS) Attacks from quarter 4 of 2018, summarizing statistics and trends from the Kaspersky Lab reports. (*<https://securelist.com/ddos-attacks-in-q4-2018/89565/>)

*One DDoS attack was executed by the Chalubo botnet (*[*https://www.zdnet.com/article/this-botnet-snares-your-smart-devices-to-perform-ddos-attacks/*](https://www.zdnet.com/article/this-botnet-snares-your-smart-devices-to-perform-ddos-attacks/)*). It targets devices and servers that are poorly-secured to carry out the distributed denial of service (DDoS) attacks. The bot uses code from both Xor.DDoS and Mirai (which took down Internet across Europe and the US three years ago) and is known to impact Linux systems as well as Internet of Things products.*

*Another attack noted by Secure List is FragmentSmack, which is an attack mechanism rather than a botnet. FragmentSmack was a DDoS vulnerability first discovered to impact Linux systems and has now been confirmed to affect Windows and nearly 90 Cisco products (*[*http://ddosattacks.net/fragmentsmack-how-is-this-denial-of-service-exploited/*](http://ddosattacks.net/fragmentsmack-how-is-this-denial-of-service-exploited/)*). The attack disables servers with a stream of fragmented IP packets that activate the vulnerability noted above. The system under attack uses its computational power to gather these packets back into one, which makes it unable to handle other requests.*

*Other interesting statistics and trends from Q4 of 2018 include, as cited on Secure List and drawn from the Kaspersky report:*

* *13% less DDoS activity than the previous year*
* *Most common type of attack is UDP flooding, by a large margin over other methods*
* *In Q4, the longest attack monitored was 329 hours (14 days)*

Q19

*If Alice and Bob want to set up a secure communication channel, they must be wary of a man-in-the-middle attack with Public Key or Asymmetric Encryption. This type of attack can occur if Darth, their adversary, intercepts a message in transit between Alice and Bob and uses two sets of his own Private and Public Keys to disrupt the communications. Darth can respond to Alice using one set of his keys, and now Darth and Alice share a key. Darth transmits a communication on to Bob using the other set of (Darth’s keys), and now Darth and Bob share a key. Alice and Bob think they share a secret key, but in actuality, Darth is now in the middle intercepting and resending messages.*

Bob

Alice

Darth

*I would suggest Alice and Bob consider two alternative options to set up their secure communication channel. First, they could use symmetric encryption, where they both share ONE, identical private key. In this set up, only they can use that key to encrypt and decrypt messages. However, it would be paramount that they DO NOT share that key with anyone else. If that secrecy is maintained, they can communicate with confidentiality and authentication ensured as part of the process. This would work well if they were exchanging simple messages. If the communications were more complex, other encryption/decryption methods should be considered.*

Alice

D

E

Bob

Decrypt w/ Private, Shared Key

Encrypt w/ Private, Shared Key

*Alternatively, if they still wanted to consider public key or asymmetric encryption, they should take advantage of the sequencing the encryption/decryption processes with the private and public keys to achieve confidentiality, authentication, and signature confirmation. These three elements will help guard against a man-in-the-middle attack because Alice and Bob will be able to confirm the origin of the message and that the contents of the message have not been altered.*

E

Alice

Bob

D

E

D

Decrypt w/ Alice Public Key

Encrypt w/ Bob Public Key

Decrypt w/ Bob Private Key

Encrypt w/ Alice Private Key

*Reference: Stallings text, pg. 291 and pg. 359*

*OTHER NOTES:*

*Most information to complete this exam was drawn from the MSDS 7349 Data and Network Security videos by Dr. Engels, as well as the course textbook and discussions in class by Dr. Meky. Our project group – composed of Steven Hayden, Eric McCandless, Olga Tanyuk, and Nicole Wittlin – met to review exam questions. Other resources are noted throughout the exam write up where necessary.*

Stallings, William. (2014). *Cryptography and Network Security: Principles and Practice. 6th Edition.* Boston: Pearson.