[Lead2pass New Latest SY0-401 Dumps PDF Free Download In Lead2pass (701-725)

This Lead2pass SY0-401 braindumps still valid, I got 979/1000 today. Thanks to Lead2pass. Following questions and answers are all new published by CompTIA Official Exam Center: https://www.lead2pass.com/sy0-401.html QUESTION 701All of the following are valid cryptographic hash functions EXCEPT: A. RIPEMD.B. RC4.C. SHA-512.D. MD4.Answer: B Explanation:RC4 is not a hash function. RC4 is popular with wireless and WEP/WPA encryption. QUESTION 702Which of the following concepts is used by digital signatures to ensure integrity of the data? A. Non-repudiationB. HashingC. Transport encryptionD. Key escrow Answer: BExplanation:Most digital signature implementations also use a hash to verify that the message has not been altered, intentionally or accidently, in transit. QUESTION 703A security administrator discovers an image file that has several plain text documents hidden in the file. Which of the following security goals is met by camouflaging data inside of other files? A. IntegrityB. ConfidentialityC. SteganographyD. Availability Answer: CExplanation:Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. QUESTION 704A security analyst discovered data such as images and word documents hidden within different types of files. Which of the following cryptographic concepts describes what was discovered? A. Symmetric encryptionB. Non-repudiationC. SteganographyD. Hashing Answer: CExplanation:Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. QUESTION 705Which of the following can hide confidential or malicious data in the whitespace of other files (e.g.JPEGs)? A. HashingB. Transport encryptionC. Digital signaturesD. Steganography Answer: DExplanation:Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. QUESTION 706Which of the following must a user implement if they want to send a secret message to a coworker by embedding it within an image? A. Transport encryptionB. SteganographyC. HashingD. Digital signature Answer: BExplanation:Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. QUESTION 707Digital Signatures provide which of the following? A. ConfidentialityB. AuthorizationC. IntegrityD. AuthenticationE. Availability Answer: CExplanation:A digital signature is similar in function to a standard signature on a document. It validates the integrity of the message and the sender. QUESTION 708Matt, a security analyst, needs to select an asymmetric encryption method that allows for the same level of encryption strength with a lower key length than is typically necessary. Which of the following encryption methods offers this capability? A. TwofishB. Diffie-HellmanC. ECCD. RSA Answer: CExplanation:Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. QUESTION 709Which of the following types of cryptography should be used when minimal overhead is necessary for a mobile device? A. Block cipherB. Elliptical curve cryptographyC. Diffie-Hellman algorithmD. Stream cipher Answer: BExplanation:Regarding the performance of ECC applications on various mobile devices, ECC is the most suitable PKC (Public-key cryptography) scheme for use in a constrained environment. Note: Elliptic curve cryptography (ECC) is an

approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. Using smaller key size would be faster. QUESTION 710A security technician is attempting to access a wireless network protected with WEP. The technician does not know any information about the network. Which of the following should the technician do to gather information about the configuration of the wireless network? A. Spoof the MAC address of an observed wireless network clientB. Ping the access point to discover the SSID of the networkC. Perform a dictionary attack on the access point to enumerate the WEP keyD. Capture client to access point disassociation packets to replay on the local PC's loopback Answer: AExplanation:With ARP spoofing (also known as ARP poisoning), the MAC (Media Access Control) address of the data is faked. By faking this value, it is possible to make it look as if the data came from a network that it did not. This can be used to gain access to the network, to fool the router into sending data here that was intended for another host, or to launch a DoS attack. In all cases, the address being faked is an address of a legitimate user, and that makes it possible to get around such measures as allow/deny lists.Note: As an example, the initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack. QUESTION 711The IT department has installed new wireless access points but discovers that the signal extends far into the parking lot. Which of the following actions should be taken to correct this? A. Disable the SSID broadcastingB. Configure the access points so that MAC filtering is not usedC. Implement WEP encryption on the access points D. Lower the power for office coverage only Answer: DExplanation:On the chance that the signal is actually traveling too far, some access points include power level controls, which allow you to reduce the amount of output provided. QUESTION 712Joe, the systems administrator, is setting up a wireless network for his team's laptops only and needs to prevent other employees from accessing it. Which of the following would BEST address this? A. Disable default SSID broadcasting.B. Use WPA instead of WEP encryption.C. Lower the access point's power settings.D. Implement MAC filtering on the access point. Answer: D Explanation:If MAC filtering is turned off, any wireless client that knows the values looked for (MAC addresses) can join the network. When MAC filtering is used, the administrator compiles a list of the MAC addresses associated with users' computers and enters those addresses. When a client attempts to connect and other values have been correctly entered, an additional check of the MAC address is done. If the address appears in the list, the client is allowed to join; otherwise, it is forbidden from doing so. QUESTION 713Which of the following provides the strongest authentication security on a wireless network? A. MAC filterB. WPA2C. WEPD. Disable SSID broadcast Answer: BExplanation:The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP. QUESTION 714 Which of the following is a concern when encrypting wireless data with WEP? A. WEP displays the plain text entire key when wireless packet captures are reassembledB. WEP implements weak initialization vectors for key transmissionC. WEP uses a very weak encryption algorithmD. WEP allows for only four pre-shared keys to be configured Answer: BExplanation:The initialization vector (IV) that WEP uses for encryption is 24-bit, which is quite weak and means that IVs are reused with the same key. By examining the repeating result, it was easy for attackers to crack the WEP secret key. This is known as an IV attack. QUESTION 715Which of the following provides the HIGHEST level of confidentiality on a wireless network? A. Disabling SSID broadcastB. MAC filteringC. WPA2D. Packet switching Answer: CExplanation:The Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) authentication protocols were designed to address the core, easy-to-crack problems of WEP. QUESTION 716 While setting up a secure wireless corporate network, which of the following should Pete, an administrator, avoid implementing? A. EAP-TLSB. PEAPC. WEPD. WPA Answer: CExplanation:WEP is one of the more vulnerable security protocols. The only time to use WEP is when you must have compatibility with older devices that do not support new encryption. QUESTION 717Joe, an employee, was escorted from the company premises due to suspicion of revealing trade secrets to a competitor. Joe had already been working for two hours before leaving the premises.A security technician was asked to prepare a report of files that had changed since last night's integrity scan.Which of the following could the technician use to prepare the report? (Select TWO). A. PGPB. MD5C. ECCD. AESE. BlowfishF. HMAC Answer: BFExplanation:B: MD5 can be used to locate the data which has changed. The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2.F: A common method of verifying integrity involves adding a message authentication code (MAC) to the message.HMAC (Hash-Based Message Authentication Code) uses a hashing algorithm along with a symmetric key. QUESTION 718Users report that after downloading several applications, their systems' performance has noticeably decreased. Which of the following would be used to validate programs prior to installing them? A. Whole disk encryptionB. SSHC. TelnetD. MD5 Answer: DExplanation:MD5 can be used to locate the data which has changed.The Message Digest Algorithm (MD) creates a hash value and uses a one-way hash. The

hash value is used to help maintain integrity. There are several versions of MD; the most common are MD5, MD4, and MD2. QUESTION 719Which of the following is used to verify data integrity? A. SHAB. 3DESC. AESD. RSA Answer: A Explanation:SHA stands for "secure hash algorithm". SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols including TLS and SSL, PGP, SSH, S/MIME, and IPsec. It is used to ensure data integrity. Note:A hash value (or simply hash), also called a message digest, is a number generated from a string of text. The hash is substantially smaller than the text itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value. Hashes play a role in security systems where they're used to ensure that transmitted messages have not been tampered with. The sender generates a hash of the message, encrypts it, and sends it with the message itself. The recipient then decrypts both the message and the hash, produces another hash from the received message, and compares the two hashes. If they're the same, there is a very high probability that the message was transmitted intact. This is how hashing is used to ensure data integrity. QUESTION 720Which of the following can be implemented with multiple bit strength? A. AESB. DESC. SHA-1D. MD5E. MD4 Answer: AExplanation:AES (a symmetric algorithm) uses key sizes of 128, 192, or 256 bits. QUESTION 721To ensure compatibility with their flagship product, the security engineer is tasked to recommend an encryption cipher that will be compatible with the majority of third party software and hardware vendors. Which of the following should be recommended? A. SHAB. MD5C. BlowfishD. AES Answer: DExplanation: AES (Advanced Encryption Standard) has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES) which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. AES is used to encrypt data, not to verify data integrity. QUESTION 722Which of the following provides additional encryption strength by repeating the encryption process with additional keys? A. AESB. 3DESC. TwoFishD. Blowfish Answer: BExplanation:Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys). QUESTION 723Which of the following are restricted to 64-bit block sizes? (Select TWO). A. PGPB. DESC. AES256D. RSAE. 3DESF. AES Answer: BE Explanation:B: The Data Encryption Standard (DES) has been used since the mid-1970s. It was the primary standard used in government and industry until it was replaced by AES. It's based on a 56-bit key and has several modes that offer security and integrity. It is now considered insecure because of the small key size.E: Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys). QUESTION 724A bank has a fleet of aging payment terminals used by merchants for transactional processing. The terminals currently support single DES but require an upgrade in order to be compliant with security standards. Which of the following is likely to be the simplest upgrade to the aging terminals which will improve in-transit protection of transactional data? A. AESB. 3DESC. RC4D. WPA2 Answer: BExplanation:3DES (Triple DES) is based on DES.In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it (e.g. EMV). Microsoft OneNote, Microsoft Outlook 2007, and Microsoft System Center Configuration Manager 2012, use Triple DES to password protect user content and system data. QUESTION 725Which of the following would Matt, a security administrator, use to encrypt transmissions from an internal database to an internal server, keeping in mind that the encryption process must add as little latency to the process as possible? A. ECCB. RSAC. SHAD. 3DES Answer: DExplanation:3DES would be less secure compared to ECC, but 3DES would require less computational power. Triple-DES (3DES) is a technological upgrade of DES. 3DES is still used, even though AES is the preferred choice for government applications. 3DES is considerably harder to break than many other systems, and it's more secure than DES. It increases the key length to 168 bits (using three 56-bit DES keys). More free Lead2pass SY0-401 exam new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDLXZsWm9MWmh0a0E Please read all of theory and then use this Lead2pass SY0-401 study guide. 2017 CompTIA SY0-401 (All 1868 Q&As) exam dumps (PDF&VCE) from Lead2pass: https://www.lead2pass.com/sy0-401.html [100% Exam Pass Guaranteed]