### [**3413ICT Network Security**](file:///D:\Profiles\user\My%20Documents\Teaching\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop – 8A**

|  |
| --- |
| **Review Questions:**   1. Explain the security service(s) provided by the SSH Transport Layer Protocol. Name and briefly explain two encryption algorithms that are used by this protocol.   Authentication (SSH User authentication Protocol)  Encryption (SSH Connection Protocol)  2 encryption algorithms that are used by this protocol include: 3DES, AES, RC4, CAST128, HMAC-SHA1. All algorithms must be opened in CBC mode except RC4.   1. Describe the SSH packet format. How is a SSH packet produced from the original data?   -Packet Length  -Padding Length  -Payload  -Random Padding  -MAC  payload-----------------------------------------------[Compression]  |  |packet length|padding length| compressed payload |padding|  -------------------------------------------------------------------------------------------------------  | |  [ Encryption ] [MAC]  | CipherText | MAC|     1. What is the main functionality of the SSH Connection Protocol?   Provide a secure authenticated connection known as a tunnel. This tunnel can be used for multiple logical channels.   1. What is VPN? Explain the two types of VPN, namely, remote access VPN and site-to-site VPN.   VPN: Virtual Private Network allows private networks to be safely extended over a public WAN (such as the internet) during transportation and ensured data confidentiality. The 2 types of VPN include: remote access, and site-to-site VPN.   1. Explain the encryption and authentication techniques and protocol that are used by VPN.   IPSec,  Firewalls,  Encryption techniques:  IPSec (ESP (Encapsulated Security Payload) Headers)  Authentication techniques:  -User/System data  -AAA Servers (Authentication, Authorization, Accounting)   1. List and briefly explain two symmetric encryption schemes and two asymmetric encryption schemes that we have studied. Are these ciphers that you just explained block ciphers or stream ciphers?   Symmetric: DES(block), AES (block) Asymmetric: RSA(block), PGP (block)   1. Name five encryption modes. Are these modes usually used by block ciphers or stream ciphers?   ECB: Electronic Code Book (block cipher) CBC: Cipher block chaining (block cipher)  OFB: Output Feedback (stream cipher) CFB: Cipher Feedback (stream cipher) CTR: Counter (block cipher)  Both.   1. Explain why the ECB mode is easy to implement; however, it does not hide the data patterns well.   The encrypted message blocks are independent making data patterns recognizable. Particularly if aligned with message block, graphics, or messages that change very little.   1. Compared with the ECB, why CBC can implement better Confusion and Diffusion? (Hint: Confusion and Diffusion are part of security requirement in the theory of Shannon, which we have studied previously.)   CBC diffuses the association between cipher text and key because it uses the output of the previous block to XOR the next block that makes it very difficult to cryptanalyze.   1. The CBC mode requires using an initialization vector (IV). Does the application of IV always increase security? Explain the disadvantage of using IV.   IV must be shared with receiving party before transmission. IV might be intercepted  during transmission. IV is like a key, it can make an encryption algorithm stronger if the number has a strong random generation that does not repeat.   1. Given the following LFSR     1 1    Suppose the initial bits are given as  Answer the following questions:   1. What are the first 15 bits of the output stream? 2. Did you find any pattern repeated in the output stream? What is the period of the output stream? 3. Briefly describe the operation of two commonly used Hash algorithms and compare them.   SHA (Secure Hash Algorithm): based on the design of MD4 with key differences. Produces 160-bit hash value. Later revised to support 256, 384, and 512 bit blocks.  Whirlpool: Uses modified AES internals as compression function. Addresses concerns on use of block ciphers with performance comparable to SHA.Designed specifically for hash function use with security and efficiency of AES. Input is mapped row wise, 10 rounds, uses different S box designs and values.   1. Design a simple 64-bit Hash function, which uses only XOR operation. Clearly explain, with the aid of a diagram, the operation of the algorithm, including how it deals with an arbitrary message size.   A 64-bit hash function can be used with an XOR operation by padding excess message sizes to be multiples of 64 bits. If the message size is larger than 64 bits the 64 bits will increase increase using another 64 bit block, for example 64, 128, 192, etc.   1. Briefly describe HMAC and CMAC operations and compare the security of them.   **HMAC**: The idea of a keyed hash evolved into HMAC, designed to overcome some problems with the original proposals. It involves hashing padded versions of the key concatenated with the message, and then with another outer hash of the result prepended by another padded variant of the key. The hash function need only be used on 3 more blocks than when hashing just the original message (for the two keys + inner hash). HMAC can use any desired hash function, and has been shown to have the same security as the underlying hash function. Can choose the hash function to use based on speed/security concerns.  **CMAC**: This cipher-based MAC has been widely adopted in government and industry. Has been shown to be secure, with the following restriction. Only messages of one fixed length of mn bits are processed, where n is the cipher block size and m is a fixed positive integer. This limitation can be overcome using multiple keys, which can be derived from a single key. This refinement has been adopted by NIST as the cipher-based message authentication code (CMAC) mode of operation, for use with AES and triple DES.     1. Discuss four common approaches used to providing both confidentiality and integrity simultaneously (Authenticated Encryption).   **Hash then Encrypt**  First compute the cryptographic hash function over M as h = H(M). Then encrypt the message plus hash function: E(K, (M || h)  **Mac then Encrypt**  Use two keys. First authenticate the plaintext by computing the MAC value as T = MAC(K1, M). Then encrypt the message plus tag: E(K2, (M || T) cf SSL/TLS  **Encrypt then MAC**  Use two keys. First encrypt the message to yield the ciphertext C = E(K 2, M). Then authenticate the ciphertext with T = MAC(K1, C) to yield the pair (C, T) cf IPsec  **Encrypt and MAC**  Use two keys. Encrypt the message to yield the ciphertext C = E(K 2, M). Authenticate the plaintext with T = MAC(K1, M) to yield the pair (C, T). These operations can be performed in either order. cf SSH   1. Explain what a “Birthday paradox” is. How does that affect the security of hash functions?   The Birthday Attack exploits the birthday paradox – the chance that in a group of people two will share the same birthday – only 23 people are needed for a Pr>0.5 of this. Can generalize the problem to one wanting a matching pair from any two sets, and show need 2m/2 in each to get a matching m-bit hash.  Note that creating many message variants is relatively easy, either by rewording or just varying the amount of white-space in the message. All of which indicates that larger MACs/Hashes are needed.   1. Explain the AES structure for both encryption and decryption processes.     Encryption: A 128-bit block of input is represented as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption. After the final stage, State is copied to an output.  The key is expanded into 44/52/60 lots of 32-bit words (see later), with 4 used in each round.  The data computation then consists of an “add round key” step, then 9/11/13 rounds with all 4 steps, and a final 10th/12th/14th step of byte subs + mix cols + add round key. This can be viewed as alternating XOR key & scramble data bytes operations. All of the steps are easily reversed, and can be efficiently implemented using XOR’s & table lookups.  Decryption: AES decryption uses essentially the same algorithm, with the following changes:  The inverse of the four main operations are used  -These consists simply of using a different set of lookup tables    The round keys are used in the reverse order     1. Explain, with the help of diagrams, each of the four basic operations in AES.   - Byte Substitution: byte is separated into two 4-bit chunks. Using a lookup table each chunk is replaced by the value in the table.  - Shift Rows:1st row unchanged, 2nd row shifts 1 byte, 3rd row 2 bytes, 4th row 3 bytes  - Mix Columns: Expressed as the transformation on each column as 4 equations to compute the new bytes for that column. This computation only involves shifts, XORs & conditional XORs (for the modulo reduction).  - AES Round: bitwise XOR of the current block with a portion of the expanded key. Note this is the only step which makes use of the key and obscures the result, hence MUST be used at start and end of each round, since otherwise could undo effect of other steps. But the other steps provide confusion/diffusion/non-linearity. That us you can look at the cipher as a series of XOR with key then scramble/permute block repeated.  **Questions 19 – 20 are optional:**   1. Is it possible to construct a hash function using a block cipher?   Yes CMAC   1. Is it possible to construct a block cipher using a hash function?   NO |

**Hands-on Exercises:**

This week you need to complete the 2nd lab (available on the course website).

Please ensure that you have already completed the first lab.