

## Information Assurance: Exam 2 – Answer Key

89 points total

### Multiple Choice – 2 points each

1. Double encrypting with DES has an effective key length of 57 bits instead of the effective key length of 112 bits due to which reason?
  - a. Pigeon hole principle
  - b. Complementation property
  - c. Birthday paradox
  - d. *[ Meet in the middle attack ]*
  
2. The correct definition for HMAC is:
  - a. An algorithm to make stream ciphers self healing
  - b. *[An algorithm that combines a keyless hash function and a cryptographic key to make a keyed hash function]*
  - c. A key management algorithm that leverages the discrete logarithm problem to derive a shared secret without hiding intermediate messages
  - d. A high integrity medium access control
  
3. The correct definition for totient  $\Phi(n)$  is:
  - a. *[The number of numbers less than n with no factors in common with n]*
  - b. The number of primes less than n
  - c. The number of factors of n
  - d. The number of numbers of less than n with a factor in common with n
  
4. If you analyze a block of cipher text and the character frequency matches that of English text, this is a clue for the following:
  - a. A substitution cipher is being used.
  - b. *[A transposition cipher is being used.]*
  - c. A proposition cipher is being used.
  - d. A stream cipher is being used.

5. In an authentication system the complementation information C is:
  - a. A complement of the authentication information
  - b. Additional information that can be used to authenticate the individual
  - c. Information that is added to the authentication information that makes brute force searches more difficult
  - d. *[Information the system stores and uses to validate the authentication information]*
  
6. If you wanted to configure IPSec to provide traffic confidentiality, you would use which protocol:
  - a. *[ESP – Encapsulating Security Protocol]*
  - b. SPI – Security Parameter Index
  - c. AH – Authentication Header
  - d. SA – Security Association
  
7. Which most accurately describes the system design problems associated with address hiding or NATP?
  - a. Only one connection from inside network can access machines beyond the address translation point at a time.
  - b. The target of the communication does not know how to send the traffic back.
  - c. The change of address confuses tunneling protocols like IPSec.
  - d. *[The address translation point must understand and fixup communication streams for protocols that negotiate ports and addresses.]*
  
8. A message encrypted by a shared secret is not sufficient for a digital signature. Why not?
  - a. *[A third party judge does not have proof to differentiate between parties that know the secret.]*
  - b. The third party judge cannot be sure that another party has not stolen the shared secret.
  - c. Symmetric encryption is not sufficiently strong to guarantee that long term signatures are not broken.
  - d. The secret must be revealed to the judge to verify the signature.

## Short Answer

9. (8 points total) Consider the following list of encryption modes that can be used with symmetric algorithms like DES and AES
- CBC – Cipher Block Chaining
  - ECB – Electronic Code Book
  - OFB – Output Feedback
  - Counter
  - CFB - Cipher Feedback
- a. Which modes are appropriate for operating in as a block cipher? (2 points)

*CBC, ECB*

- b. Which modes are appropriate for operating in as a stream cipher? (2 points)

*OFB, Counter, CFB*

- c. If you had to select a mode for AES to operate in block mode, which would you choose and why? (2 points)

*CBC. By chaining recurring blocks in the stream, repeating blocks of plaintext in the stream will not result in repeating blocks of ciphertext. In addition, CBC has a self healing mode where a dropped packet will only result in errors in the following packet.*

- d. If you had to select a mode for AES to implement a stream cipher, which would you select and why? (2 points)

*Counter mode. The key stream can be precomputed reducing the time to actually perform the encryption/decryption. Also one can calculate the key stream starting at an arbitrary offset.*

*Would take other answers that justify the other modes well.*

10. (8 points total) Alice needs to pick a public and private RSA key to communicate with Bob. They will be encrypting and signing messages that are only a character long (values from 0 to 25), so the values selected do not need to be nearly as large as you would expect in a real system.

a. Alice selects  $p=7$  and  $q=13$ . What is  $n$ ? (2 points)

$$n = p * q = 91$$

b. Alice select  $e=29$  and  $d=5$ . Show that these are valid RSA encrypting and decrypting values. (2 points)

$$e * d \text{ mod } \Phi(n) = 1$$

$$29 * 5 \text{ mod } (6 - 1)(12 - 1) = 145 \text{ mod } 72 = 1$$

*And 29 is relatively prime to 91*

c. What would Alice publish as the public key? (2 points)

$$e = 29 \text{ and } n = 91$$

d. Now Bob wants to send the message “test” so it only can be read by Alice. Compute the cipher text he should send to Alice. Assume  $a = 0$ . (2 points)

$$T=19, e = 4, s = 18$$

$$c = m^e \text{ mod } n$$

$$ct = 19^{29} \text{ mod } 91 = 80$$

$$ce = 4^{29} \text{ mod } 91 = 23$$

$$cs = 18^{29} \text{ mod } 91 = 44$$

*So the messages would be 80, 23, 44, 80.*

11. (10 points total) Consider the encrypted key exchange proposed by Bellovin-Merritt that aims to protect against type 1 dictionary attacks (which uses the complementation information and functions to determine authentication information). Here is the protocol for your review. The protocol assumes Alice and Bob share a secret  $K_{ab}$ .
- Alice->Bob:  $\{e_{Alice, n_{Alice}}\}K_{ab}$ , where  $e_{Alice, n_{Alice}}$  is a randomly selected public key for a public key system.
  - Bob->Alice:  $\{\{k\}e_{Alice}\}K_{ab}$ , where  $k$  is a randomly selected secret key.
  - Alice->Bob:  $\{rand1\}k$ , where  $rand1$  is a random nonce selected by Alice.
  - Bob->Alice:  $\{rand1, rand2\}k$ , where  $rand2$  is a random nonce selected by Bob.
  - Alice->Bob:  $\{rand2\}k$

Answer the questions below about this protocol.

- Why does Alice's key ( $e_{Alice, n_{Alice}}$ ) have to be picked randomly, instead of using the same key each time? (2 points)

*If an attacker somehow found out what Alice's key was, he could use a known-plaintext attack to discover  $K_{ab}$ . It could also be used to track the uniqueness of the request rather than using a random nonce. Therefore, the unique public key enables the detection of replay attacks.*

- Why does Bob have to encrypt twice on his reply? (2 points)

*By encrypting with  $K_{ab}$ , Alice knows the response must have come from Bob. By encrypting with  $e_{Alice}$ , Alice knows that the key response matched her most recent request (and is not just a replay of some previous message).*

- c. Suppose we want to guard against a denial-of-service attack where the attacker sends nonsense data during this initial exchange (thus occupying the receiver's resources). How would you modify the protocol to allow either side to determine if this is happening and stop wasting time? (4 points)

*A DoS attack would try to make Alice and Bob run out of computation resources by performing pointless cryptographic calculations on garbage data.*

*We could prevent this by including some recognizable text in the messages (e.g. “{Alice || Bob ||  $e_{Alice}$  ||  $n_{Alice}$ } $K_{ab}$ ” for message a) so that if the decryption is unrecognizable, we could stop.*

*Or, for the last three messages, we could augment the message so rand1 or rand2 is in the clear in the message in addition to being encoded in the message. The first message is updated with a sequence number, which is sent in the clear and encrypted:  $N || \{N || e_{Alice} || n_{Alice}\}K_{ab}$ . Bob can use a sliding window replay algorithm as described for AH to detect if the request is recent enough to be new request. The second message will also contain  $N$ , so Alice can quickly determine if the packet is a response for her most recent request.*

- d. Would this open up vulnerabilities in the protocol? If so, what vulnerabilities? (2 points)

*The first solution, or for the first two messages of the second solution, the attacker has a partial known plaintext that he can recognize in a brute force attack. For messages 3 and 5 in the second solution, placing the rand in the clear and encrypted will give the attacker a pair of known plaintexts.*

12. (8 points total) Alice and Bob will use Diffie-Hellman to compute a shared secret. They select  $p=57$  and  $g=2$ . Alice picks a  $k_{\text{Alice}}$  of 11 and Bob picks a  $k_{\text{Bob}}$  of 7.
- Show the computations performed by Alice and Bob to calculate a shared secret. (4 points)

$$K_{\text{alice}} = g^{k_{\text{alice}}} \bmod p = 2^{11} \bmod 57 = 53$$

$$K_{\text{bob}} = g^{k_{\text{bob}}} \bmod p = 2^7 \bmod 57 = 14$$

$$k = K_{\text{alice}}^{k_{\text{bob}}} \bmod p = 53^7 \bmod 57 = 32$$

$$k = K_{\text{bob}}^{k_{\text{alice}}} \bmod p = 14^{11} \bmod 57 = 32$$

- What values are hidden? (2 points)

$$k_{\text{alice}}=11 \text{ and } k_{\text{bob}}=7$$

- What values can be sent over an insecure channel? (2 points)

$$p, g, K_{\text{alice}}, K_{\text{bob}}$$

13. (6 points) Alice wants to determine a trust level for Fred based on his signature. The certificate notation used in the text is augmented with H or L to indicate whether the signer has a high or a low degree of trust in their signature. Alice knows and trusts highly Harold's and Jane's opinions. Alice only knows Iago casually and so does not know how if his opinions are trustworthy. Alice does not know the other participants at all. Given the signatures below, present a strong argument from Alice's point of view that Fred's signature should be trusted.

Ellen(H),Iago(H),George(H),Fred(H)<<Fred>>  
 Ellen(H),Harold(L),George(H)<<George>>  
 Jane(L),Harold(H),Ellen(H)<<Ellen>>

*Alice trusts Harold  
 Harold signs Ellen's certificate with a high level of trust  
 Ellen sign's Fred's certificate with a high level of trust  
 Therefore, Alice can grant Fred's certificate a high level of trust.*

14. (6 points total) Consider double encryption, where  $c = E_{k'}(E_k(m))$  with keys  $k$  and  $k'$  that are each  $n$  bits long. Assume it takes one time unit to perform an encryption or a decryption. The attacker will use two known plaintext pairs to derive the keys,  $c_1 = E_{k'}(E_k(m_1))$  and  $c_2 = E_{k'}(E_k(m_2))$ .
- The attacker computes  $E_x(m_1)$  for each possible key  $x$  and stores the result in a table. How many bits will the table be? How long will it take to compute the table? (4 points)

*Time =  $2^n$  time units*

*Space =  $2^n * (n + \text{block size})$*

- The attacker then computes  $y = D_{x'}(c_0)$  for each possible key  $x'$ . He checks the table built in step a to see if  $y$  is in the table. If so,  $(x, x')$  is a candidate key pair. How should the table be organized, so that the attacker can check for the presence of  $y$  in  $O(1)$  time? (2 points)

*Should be a hash table keyed by the cipher text calculated in step 1.*

- How can the attacker confirm that  $(x, x')$  is indeed the desired key pair? (2 points)

*Compute  $E_{x'}(E_x(m_2))$  if it equals  $c_2$  you have the right keys.*

15. (4 points) List two techniques for countering online or type 2 dictionary attacks.

*Answers could include: using challenge-response or one-time passwords, using backoff or disconnection to slow the attack, disabling or jailing accounts*

16. (4 points total) IPSec can operate in tunnel mode or transport mode.
- a. List one benefit of tunnel mode. (2 points)

*Answers could include: prevents eavesdropping between routing points, protects confidentiality of traffic destination*

- b. List one benefit of transport mode. (2 points)

*Answers could include: protects confidentiality of message contents, reduced header overhead by not replacing original IP headers, knowledge that the tunnel is end-to-end.*

17. (5 points) Identify three limitations of perimeter-oriented system security architectures.

*Cannot prevent inside attacks, difficult to find all perimeter points, have to include remote connections which we may not have control over, secure-tunneled payloads cannot be analyzed*

18. (4 points) List two of the problems with WEP that causes the overall system to be broken.

*Answers could include: too-frequent reuse of keys, transmitting part of the key (IV) in the clear, no prevention of use of weak RC4 keys, using a CRC for a message digest instead of a cryptographic hash*

19. (8 points) Diane runs a business that involves advising customers how to network desktop computers, designing database management systems, and advising about security. Currently she is designing a database management system for the personnel office of a medium-sized company. Diane has described several options to the client. Because the system is going to cost more than they planned, the client has decided to opt for a less secure system. She believes the information they will be storing is extremely sensitive. It will include performance evaluations, medical records for filing insurance claims, salaries, and so forth.
- With weak security, employees working on desktop computers may be able to figure out ways to get access to this data. Hackers might gain access to the data too. Diane feels strongly that the system should be much more secure. She has tried to explain the risks, but the CEO, director of computing, and director of personnel all agree that less security will do.
- Prepare an ethical argument about whether she should or should not agree to implement the system requested by her client. Use the Reversibility Test and the Publicity Test in your argument.

*Answers will vary. The Reversibility Test should include some consideration of how Diane would view the decision if she were in charge of the company, and the Publicity Test should describe how the decision would look to the general public if they knew about it.*