

Information Assurance: Midterm 2 – Answer Key

Multiple Choice – 2 points each

1. Which of the following cryptographic algorithms is self healing?
 - a. AES in Electronic Code Book (ECB) mode
 - b. *DES in Cipher Feedback (CFB) mode***
 - c. Vigenere Cipher
 - d. AES in Counter mode

2. What hard problem is the security of the Diffie-Hellman public key algorithm based on?
 - a. Factoring large primes
 - b. *Computing discrete logarithms***
 - c. Traveling salesman optimization
 - d. Bin packing

3. The Enigma cipher is an example of which of the following types of ciphers?
 - a. *Substitution cipher***
 - b. Transposition cipher
 - c. Proposition cipher
 - d. Product cipher

4. Which of the following encryption algorithms is an example of a Feistel network?
 - a. AES
 - b. *DES***
 - c. RSA
 - d. Enigma

5. Which of the following statements must be true for a RSA system? Where **e** is the public exponent, **d** is the private exponent, and **n** is the modulus.
 - a. **e** must be relatively prime to **d**
 - b. **n** and **d** must be kept private
 - c. $ed \bmod n = 1$
 - d. *ed mod $\Phi(n) = 1$***

6. Which of the following is **not** traditionally an information source for proving an entity's identity?
 - a. Something you know
 - b. Something you have
 - c. *Something you like***
 - d. Something you are

Net ID:

7. Which of the following is **not** an operation performed by a standard firewall?
 - a. *Deduce that incoming traffic on a random port is using the HTTP protocol and automatically apply HTTP analyzer.*
 - b. Filter packets based on header data.
 - c. Verify that packets are well formed for specific protocols and no known protocol attacks are being launched.
 - d. Analyze packet stream and dynamically open access for protocol related streams.

Short answer

8. (3 points each, 6 points total) Cryptographic hashes can be either keyed (require secret information to generate and verify) or keyless (require no secret information to generate and verify).
- Describe a scenario where a keyed cryptographic hash is appropriate.

The cryptographic hash is used for a message authentication code (MAC) for a message file where the MAC is stored with the message. The MAC must be keyed otherwise, an attacker with access to the message could also compute a new MAC that matches the altered message.

- Describe a scenario where a keyless cryptographic hash is appropriate.

The cryptographic hash is used for a MAC that is stored apart from the message. For example when downloading a file from a mirror site, you can compute the same MAC on the downloaded file and compare it to the MAC stored on the main software site. The attacker would have to either find a file with the same MAC to replace on the mirror site, or he would have to replace both the file on the mirror site and the MAC on the main site.

Having a keyed hash would be problematic in this case, because we want anyone to be able to verify the hash. If the hash were keyed, the key would have to be made available to anyone downloading from the mirror site which means our attacker would have access to the key in any case.

9. (3 points each, 9 points total) You are given a piece of data. You need to provide confidentiality and integrity for the data. Storage is limited so you also need to compress the data. You are given RSA for encryption and signing and LZW for compression.
- Should you encrypt first or compress? Or does the order not matter? Why?

Compress then encrypt. A good encryption should randomize the data. Compression algorithms rely on patterns in the data. Compressing on randomized data will result in little space savings.

- Should you sign first or compress? Or does the order not matter? Why?

It does not matter. Perhaps you should sign first, so you have some understanding of what you are signing, so you are not tricked in signing arbitrary data that could be used by an attacker.

- c. Should you sign first or encrypt? Or does the order not matter? Why?

You should sign before encrypting. If you encrypt first, you are vulnerable to the attack described in the text, where the target of encryption changes his public key to make it look like we have signed something else.

10. (9 points total) A phoneme is a unit of sound which can be represented by a sequence of two or three characters. By using phonemes as the unit of password creation, you can create random but pronounceable passwords. According to the textbook there are 440 possible phonemes. Assume that an attacker can make 20,000 guesses per second. You are told that randomly chosen passwords must be secure with a probability of at least 75% at the end of a month.

- a. (4 points) Given a selection of 96 printable characters and assuming that all passwords are the same length, how long must randomly generated passwords be to meet the 75% unbroken requirement?

$$\begin{aligned} 1/4 &\geq (\text{Number guesses} * \text{Time}) / \text{Number total Passwords} \\ 1/4 &\geq (20,000 * 30 * 24 * 60 * 60) / (96^n) \\ 96^n &\geq (20000 * 30 * 24 * 60 * 60 * 4) = 2.0736 \times 10^{11} \end{aligned}$$

$$96^6 = 7.82 * 10^{11}$$

$$96^5 = 8.15 * 10^9$$

$$n = 6$$

- b. (4 points) Given a selection of 440 phonemes and assuming that all passwords are the same length, how long must the random passwords be to meet the 75% unbroken requirement? Give the length in terms of phonemes.

$$440^n \geq 2.073 \times 10^{11}$$

$$440^5 = 1.65 * 10^{13}$$

$$440^4 = 3.75 * 10^{10}$$

$$n = 5$$

- c. (1 point) Assume the average phoneme is 2.5 characters long. How long is the phoneme based password in terms of characters?

$$n = 12.5$$

Net ID:

11. (10 points total) A basic key management protocol using public key certificates only requires a single message

Alice \rightarrow Bob $\{k\}_{e_{\text{Bob}}}$

This protocol has several points for Eve to attack. Identify two weaknesses and propose extensions to the protocol to fix these weaknesses. For your analysis assume that Alice and Bob have access to trustworthy certificate servers.

First is the problem of identity. Bob cannot be sure that Alice really sent the message. Eve could create this message and make it appear that it came from Alice. This can be solved by inserting a signature of the key from Alice.

$\{k \{k\}_{d_{\text{Alice}}}\}_{e_{\text{Bob}}}$

The second is a problem of replay. Eve could save aside the message. Later if she breaks the session key, she could replay this message to convince Bob to return to the old key. This could be solved a number of ways:

- *insert a session ID and keep track of which session you are working on.*
- *Insert a time stamp and drop “stale” packets.*

Net ID:

12. (10 points total) Alice and Bob use Diffie-Hellman to compute a shared secret. They select $p=67$ and $g=13$. Alice picks a k_{Alice} of 11 and Bob picks a k_{Bob} of 7.

a. (4 points) Show the computations for K_{Alice} and K_{Bob} .

$$K_{\text{Alice}} = g^{k_{\text{Alice}}} \bmod p = 13^{11} \bmod 67 = 38$$

$$K_{\text{Bob}} = g^{k_{\text{Bob}}} \bmod p = 13^7 \bmod 67 = 2$$

b. (4 points) Show how Alice and Bob use K_{Alice} and K_{Bob} to compute the shared secret

$$k = K_{\text{Alice}}^{k_{\text{Bob}}} \bmod p = K_{\text{Bob}}^{k_{\text{Alice}}} \bmod p = 38^7 \bmod 67 = 2^{11} \bmod 67 = 38$$

c. (2 points) Which values of p , g , k_{Alice} , k_{Bob} , K_{Alice} , and K_{Bob} can be made public without affecting the security of the key exchange?

p , g , K_{Alice} , and K_{Bob} can be made public

k_{Alice} and k_{Bob} must be kept secret.

Net ID:

13. (4 points each, 8 points total) Eve wants to replace Alice's public key certificate with her own to pose as Alice to Bob. Assume that neither Alice nor Bob has cached a copy of the other's certificate at the start of this attack.
- a. Consider X.509 strict hierarchy of Certificate Authorities. What aspects of the system would Eve need to thwart to present her certificate as Alice's?

Presumably Alice already has a X.509 certificate signed by an entity in the certificate hierarchy. Eve could try to convince the original signer to sign her new certificate. To do so, she would need to convince the signer that he is working with Alice.

Alternatively, Eve could have another entity sign the certificate and place her version of Alice's certificate elsewhere in the hierarchy. For example, if Bob knows that Alice attends UIUC and works for WidgetsRUs, he may look for Alice's certificate as alice@uiuc.edu or alice@widgetsrus.com. If Alice's true certificate is at UIUC, Eve could register as alice@widgetsrus.com.

In either case, Eve would have to convince some official entity that she is really Alice. Or she could break into Bob's machine and convince his PKI software to use a CA she controls. Or she could break into the CA and steal its private key to make a signature of the fake certificate herself.

- b. Consider a GPG web of trust. How would Eve have to carry out her attack in this system?

Eve would have to understand how Bob determines the goodness of a certificate. Then she would have to get enough of Bob's friends and acquaintances to sign her version of Alice's certificate. So Eve would have to convince more people, but likely each individual will be more easily convinced (e.g. Through a email or a phone call) to sign the certificate.

Net ID:

14. (3 points) The personal firewall that comes with Windows XP allows you to prohibit incoming connections. However, it does not enable you to block connections initiating from your computer. Give an example of an attack that could be blocked with filtering of outbound connections.

If the computer is infected via an installed program or opened email attachment, the infected program may try to call home for instructions or reach out to infect other computers. If you know what protocols and addresses your computer should be communicating with, you could block all other outgoing connections which would contain such a malware program.

15. (4 points) Consider a corporate network that uses IPSec VPN's to connect people working from outside the office (e.g. at home or at a coffee shop). With IPSec, you can configure the tunnel so the traffic from the VPN are labeled with corporate addresses. Thus the corporation's network security infrastructure could treat the home worker's traffic just like traffic that originated on site. Give two reasons why the designer of the corporate network security might want to apply additional checks to traffic from home offices.

- 1) *People other than the employee may be using the computer from home. For example, the employee's children may download a cool new program which infects the computer causing many interesting packets to be spewed into the heart of the corporate network.*
- 2) *Even if the employee is the only user of the home computer, he may have configured his computer to access both the local network and the VPN network so he can access the home printer in addition to corporate email. The employee's children have downloaded the cool infecting program on another home computer. The infecting program attacks the home office computer through the local network connection. If it succeeds, then the home office computer can again be a launch point into the corporate network.*